AIX Fast Connect Version 3.2 Guide

SC23-4875-04

AIX Fast Connect Version 3.2 Guide

SC23-4875-04

Note
Before using this information and the product it supports, read the information in Appendix E, “Notices,” on page 95.

Fifth Edition (July 2006)

This edition applies to AIX Fast Connect Version 3.1 and to all subsequent releases of this product until otherwise indicated in new editions.

A reader’s comment form is provided at the back of this publication. If the form has been removed, address comments to Information Development, Department 04XA-905-6C006, 11501 Burnet Road, Austin, Texas 78758-3493. To send comments electronically, use this commercial Internet address: aix6kpub@austin.ibm.com. Any information that you supply may be used without incurring any obligation to you.

Contents

About This Book

This book provides network and system administrators, system engineers, programmers, and other information system professionals with the detailed configuration and installation information necessary to network AIX® Fast Connect servers with PC clients running Microsoft® Windows® and OS/2® operating systems.

Highlighting

The following highlighting conventions are used in this book:

Bold	Identifies commands, subroutines, keywords, files, structures, directories, and other items whose names are predefined by the system. Also identifies graphical objects such as buttons, labels, and icons that the user selects.
Italics	Identifies parameters whose actual names or values are to be supplied by the user.
`Monospace`	Identifies examples of specific data values, examples of text similar to what you might see displayed, examples of portions of program code similar to what you might write as a programmer, messages from the system, or information you should actually type.

Case-Sensitivity in AIX

Everything in the AIX 5L operating system is case-sensitive, which means that it distinguishes between uppercase and lowercase letters. For example, you can use the **ls** command to list files. If you type `LS`, the system responds that the command is ″not found.″ Likewise, **FILEA**, **FiLea**, and **filea** are three distinct file names, even if they reside in the same directory. To avoid causing undesirable actions to be performed, always ensure that you use the correct case.

Case-sensitive file names on AIX can also cause problems for personal computer clients running Windows operating systems because these operating systems normally treat file names as caseless. AIX file names that differ only in case would be perceived as the same file name from a PC client.

ISO 9000

ISO 9000 registered quality systems were used in the development and manufacturing of this product.

Chapter 1. AIX Fast Connect Overview

AIX Fast Connect is server software that allows AIX servers and workstations to share files and printers with personal computer clients running Windows XP, Windows 2003, Windows 2000, Windows NT®, or Windows 98 operating systems.

Because AIX Fast Connect uses industry-standard Microsoft networking protocols, PC clients can access AIX files and printers using Microsoft networking client software. PC users can use remote AIX file systems directly from their machines like local file systems, and access AIX print queues like local printers. AIX Fast Connect provides these services by implementing the Server Message Block (SMB) networking protocol to run on NetBIOS over TCP/IP (RFC-1001/1002). For clients that support it, AIX Fast Connect will run SMB on TCP/IP (without NETBIOS) using port 445. For more information about these concepts, see Chapter 2, “Windows Networking Concepts,” on page 7.

Features

Important features of AIX Fast Connect include:

- AIX-application standard and advanced features, including:
  - Tight integration with AIX, using AIX features such as threads, kernel I/O, file systems, and security
  - Maintenance and administration using SMIT, the command line, or Web-based System Manager
  - Streamlined configuration
  - Trace and log capabilities
  - SendFile API support
  - DCE/DFS integration
  - Support for JFS-Access Control Lists
  - HACMP™ support, using server name aliases
  - Support for long AIX user names (AIX 5.3 and later)
- Advanced SMB/NetBIOS features, including:
  - SMB-based file and print services
  - Passthrough authentication to Windows NT
  - Resource Browsing Protocol (Network Neighborhood)
  - Network Logon support, including roaming user profiles
  - Windows Internet Naming Service (WINS_ client and proxy, and NetBIOS Name Server (NBNS-server)
  - Opportunistic locking (oplock)
  - B-node support
  - Guest Logon support
  - Share-Level Security support
  - Messaging from server to client
  - Mapping of AIX long file names to DOS 8.3 file names
  - Unicode representation of share, user, file, and directory names
  - Mapping of PC-client user names to AIX user names
  - Multiplexed SMB-sessions (for Windows Terminal Server support)
  - Active Directory support (the **cifsLdap** command)
  - Kerberos-based Authentication
  - NetBIOS-less connections
  - SMB signing

– Directory change notification
– Level II Oplocks
– NTFS access control lists (NT ACL mapping)
– NT ACL inheritance (based on JFS2 ACL inheritance in AIX 5.3 and later)
– NT status codes
– LDAP-based authentication
– CIFS distributed File System (MSDFS) support
– Dynamic user creation

Hardware and Software Requirements

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

Server Hardware Requirements

AIX Fast Connect runs on any machine that supports AIX 5.1 or later, except for diskless or dataless machines. This server machine must have the following:

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

Server Software Requirements

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

- AIX 5.1 or later
- The size of the **/var** file system should be large enough to temporarily store the largest file that can be printed by the print service

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 Fast Connect, all client PCs must have one of the following operating systems:

- Windows XP
- Windows 2003
- Windows 2000 (with Service Pack 1 or later)
- Windows NT 4.0 (with Service Pack 3 or later)
- Windows 98

To use the Web-based System Manager, a web browser with forms support is required.

Known Incompatibilities 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 following NetBIOS-based server software is not compatible with AIX Fast Connect. Before you install AIX Fast Connect, uninstall the following products:

Fileset	Description
SAMBA.*	Samba server
netbios.*	NetBIOS/ix for AIX

Fileset	Description
connect.*	AIX Connections
TAS.*	TotalNet Advanced Server for AIX
ASU.*	Advanced Server for UNIX

Note: AIX Fast Connect does not support IPX/SPX, NetBEUI, or Netware protocols.

Packaging and Installation Requirements

This section describes the AIX Fast Connect packaging images and installation requirements.

Packaging

AIX Fast Connect packaging includes the following images:

Image	Description
cifs.base	Server Utilities
cifs.client	Client Utilities
cifs.msg.*	Server Messages (by language)
cifs.websm	Web-based System Manager Utilities

and one of the following

cifs.advanced-demo	Demo Version
cifs.advanced	Advanced Server
cifs.basic	Server

Note: The **cifs.basic** and **cifs.advanced** installation files, are mutually exclusive. Standard distributions of AIX Fast Connect contain only one of these images.

The packaging images listed above contain the following file sets:

Image	Fileset	File set Description
	cifs.base.smit	SMIT support
	cifs.base.cmd	Commands
	cifs.base.ldap	Active Directory Support
cifs.client	**cifs.client.rte**	Client support
cifs.websm	**cifs.websm.apps**	Web-based System Manager support
cifs.msg.*	**cifs.msg.***	Server messages (by language)
cifs.advanced-demo	**cifs.advanced-demo.rte**	Demo Version files
cifs.advanced	**cifs.advanced.rte**	Advanced server files
cifs.basic	**cifs.basic.rte**	Server files (for Windows clients only)

Installation

Installation of AIX Fast Connect creates the following files on the server:

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
cifsLdap	binary	**/usr/sbin**	Command line utility for Active Directory support
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**)
cifsSnap	script	**/usr/sbin**	Script to aid in collecting system information for support personnel.
cifsUserProc	binary	**/usr/sbin**	Client-session daemon (one process per PC-client session)
cifsConfig	text	**/etc/cifs**	Server configuration file
cifsPasswd	text	**/etc/cifs**	User-database file
README.html	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**	Run-time message catalogs (by language)

Notes:

1. If **cifs.advanced** or **cifs.advanced-demo** is installed, then the **cifsServer** file is created as a soft link to **cifsServerAdv** or **cifsServerAdvDemo**, as appropriate.
2. The **cifsTrace** file does not appear on the system until tracing is enabled using the **net trace** subcommand. For details, see “net trace Subcommand” on page 67.
3. If **cifs.*** or *_all_latest* is chosen during the installation process, some of the filesets will fail to install and will report `FAILED` as the result of the installation. Note the following:
   - The **cifs.base.ldap** file set is optional and will not install if the **ldap.client.rte** file set is not installed.

Configuration of Network Interfaces

Every time that 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 configures itself as an SMB/NetBIOS file server with the following default parameters:

Parameter	Initial Value
servername	*hostname* (TCP/IP hostname)
comment	"Fast Connect server on *hostname*"
domainname	WORKGROUP
encrypt_passwords	0 (Plain text passwords)
guestlogonsupport	0 (disabled)
networklogon	0 (disabled)
share_level_security	0 (disabled)

In addition, the **HOME** file share is predefined, and it maps to **$HOME**, the AIX Fast Connect user's home directory on AIX.

Other server parameters are set initially at the default values.

Chapter 2. Windows Networking Concepts

The following definitions explain some common Windows networking terms:

B-Node
(Broadcast node)
Type of NetBIOS end node that supports NetBIOS service and contains applications. B-nodes communicate using a mix of UDP datagrams and TCP connections. B-nodes can freely interoperate with one another within a broadcast area; normally a single LAN segment. Other standard end nodes are point-to-point nodes (*P-nodes*) and mixed-mode nodes (*M-nodes*).

Browsing
Viewing the resources available on a network. The *browse list* on a Windows network is the list of other hosts and domains available on a network. Windows maintains the browse list to present other hosts offering network services through a point-and-click user interface rather than asking users to remember the names of remote hosts and services. Windows clients use the browse list to construct the view of the network shown in the Network Neighborhood (renamed *My Network Places* in Windows XP and Windows 2000) and Windows Explorer. The browse list is also accessible from the command line using the `NET VIEW` command.

Windows NT domains maintain the browse list on a computer called the Master Browser. Whenever a computer offers a network service for the first time, it broadcasts a server announcement packet. The Master Browser receives this packet and adds the computer's name to its browse list. In response, the Master Browser transmits a list of backup browsers to the new computer.

Each domain or workgroup contains at least one backup browser. A copy of the browse list is maintained on the backup browser to eliminate the need to rebuild the browse list if the Master Browser goes down. For more information about NT domains and network browsing, see the related Microsoft **technet** site on the World Wide Web.

CIFS Common Internet File System protocol. CIFS provides an open cross-platform mechanism for client systems to request file services from server systems over a network. It is based on the SMB protocol widely used by PCs and workstations running a wide variety of operating systems.

NetBIOS
NetBIOS, or Network Basic Input/Output System, is a vendor-independent network interface originally designed for IBM® PC computer systems running PC-DOS or MS-DOS. NetBIOS is a software interface, not an actual networking protocol. It specifies the services that should be available without putting any restrictions on the protocol used to implement those services.

No officially defined NetBIOS standard exists. The original version, as described by IBM in 1984 in the *IBM PC Network Technical Reference Manual*, is treated as the de facto standard. Since its introduction, the following versions of NetBIOS have emerged, each using its own transport protocol: NetBEUI, NetBIOS over IPX, and NetBIOS over TCP/IP.

AIX Fast Connect supports NetBIOS over TCP/IP.

NetBIOS Interface to Application Programs
On PCs, NetBIOS includes both a set of services and an exact program interface to those services. The following types of NetBIOS services exist:

Name Service
NetBIOS resources are referenced by name. Lower-level addresses are not available to NetBIOS applications. An application representing a resource registers one or more names that it wants to use.

The name space is flat and not hierarchically organized. It uses 15 alphanumeric characters, plus a 16th ″subcode″ byte. Names cannot start with an asterisk (*).

Registration implies bidding for use of a name. The bid may be for exclusive (unique) or shared (group) ownership. Each application contends with other applications in real time. No two applications on the NetBIOS network can use the same unique name until the originating application requests that its name be deleted or the host is powered off or reset.

Name Service provides the **Add Name**, **Add Group Name**, and **Delete Name** primitive operations.

Session Service

A *session* is a full-duplex, sequenced, and reliable message exchange conducted between a pair of NetBIOS applications. Data is organized into messages.

Multiple sessions can exist between any two applications. Both applications participating in the session have access to the name of the remote application. No specification is given for resolving session requests to a group name into a data connection. A service is provided for the detection of a session failure by an application.

The Session Service provides the **Call**, **Listen**, **Hang Up**, **Send**, **Receive**, and **Session Status** primitive operations.

Datagram Service

The Datagram Service is an unreliable, nonsequenced, and connectionless communication between two NetBIOS applications. It is analogous to UDP service under TCP/IP.

Datagrams are sent under cover of a name properly registered to the sender. Datagrams can be sent to a specific name or be explicitly broadcast.

Datagrams sent to an exclusive name are received, if at all, by the holder of that name. Datagrams sent to a group name are multicast to all holders of that name. The sending application cannot distinguish between group and unique names and thus must act as if all nonbroadcast datagrams are multicast.

As with the Session Service, the receiver of the datagram is provided with the sending and receiving names.

The Datagram Service provides the **Send Datagram**, **Send Broadcast Datagram**, **Receive Datagram**, and **Receive Broadcast Datagram** primitive operations.

NetBIOS Name Resolution

Mapping a NetBIOS name to its corresponding IP address. The techniques commonly used for name resolution are the Windows Internet Name Service (WINS), the **LMHOSTS** file, and the domain name system (DNS). For information about DNS, see “NetBIOS Name Resolution” on page 20. The other techniques are defined as follows:

WINS/NBNS

When a new service is made available on the network, such as when a Windows machine boots or when AIX Fast Connect is started, the service must be registered with a WINS server before it can be available to clients located on other subnets. The WINS server records the name of the host, the NT domain the host is part of, and the IP address of the host. Whenever a machine attempts to resolve a host name, it first checks with the WINS server. If the host is not registered there, it attempts to find the host using a broadcast. If the host is still not found, the system returns the message`A computer or sharename could not be found`. AIX Fast Connect registers itself with any WINS server.

WINS also includes a method for replicating its database of host names with other WINS servers to create a backup WINS server that can host queries if the primary WINS server is unavailable. It also allows large networks that are encumbered by slow links to distribute WINS servers closer to clients and provide faster name resolution. (WINS is a proprietary Microsoft protocol.)

AIX Fast Connect can be configured to act as an NBNS (NetBIOS Name Service) server, providing most WINS functionality. AIX Fast Connect can also be configured to act as a WINS proxy to other WINS or NBNS servers. For details, see “NetBIOS Name Service (NBNS)” on page 16.

LMHOSTS
LMHOSTS (LanManager Hosts) is analogous to the UNIX® **/etc/hosts** file. The **LMHOSTS** file allows specific NetBIOS server names to be mapped to IP addresses. It also provides a syntax for defining the domain in which a NetBIOS server resides, as well as loading an **LMHOSTS** file from a shared directory on a server.

Broadcast
NetBIOS names may be resolved using broadcast on the local subnet. It is analogous to address resolution protocol (ARP) in TCP/IP. The requesting machine broadcasts a NetBIOS Name Query. If the requested host receives the broadcast, it replies with its IP address. Because broadcasts are not forwarded, only hosts on local subnets may be resolved in this manner.

NetBIOS over TCP/IP
NetBIOS over TCP/IP was first proposed in RFCs 1001 and 1002. These RFCs describe an implementation of NetBIOS using Transmission Control Protocol (TCP) for connection-oriented session services and User Datagram Protocol (UDP) for datagram services.

This design has some significant advantages over NetBEUI and NetBIOS over IPX, as follows:

- NetBIOS uses the existing TCP/IP protocols, so it can be routed across the global Internet and any other wide area networks.
- Software implementing the NetBIOS interface can be built using existing TCP/IP implementation without requiring any new network drivers. Because most operating systems already support TCP/IP, most are capable of supporting NetBIOS with minimal additional effort.

NetBIOS Scope
Population of computers across which a registered NetBIOS name is known. NetBIOS broadcast and multicast datagram operations must reach the entire extent of the NetBIOS scope.

net Command
The **net** command and its subcommands can be used to configure and administer the AIX Fast Connect Server from the command line. Alternatively, the Web-based System Manager and SMIT offer menu-driven interfaces for the same tasks. For detailed information, see “net Command” on page 61.

Passthrough Authentication
Mechanism employed by the AIX Fast Connect server to validate user credentials with a domain controller and, if validated, to grant the user access to a resource on the AIX Fast Connect server.

SMB Server Message Block protocol used to run on NetBIOS to implement Windows file sharing and print services.

With this protocol, clients exchange messages (called *server message blocks*) with a server to access resources on that server. Every SMB message has a common format, consisting of a fixed-sized header followed by a variable-sized parameter and data component.

SMB messages are of the following types:

- Session control messages start, authenticate, and terminate sessions.
- File and printer messages control file and printer access, respectively.
- Message commands allow an application to send or receive messages to or from another host.

When an SMB client negotiates a connection with an SMB server, the two parties determine a common protocol to use for communication. This capability allows protocol extensions but can make SMB quite complex.

Shares

Resources exported to the network by the AIX Fast Connect server. AIX Fast Connect supports AIX file shares and printer shares.

Workgroups

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

Chapter 3. Configuration and Administration

This chapter discusses basic configuration and operation of AIX Fast Connect.

Note: Unless otherwise noted, all references to the **net** command in this section refer to the AIX Fast Connect command (**/usr/sbin/net**) not the `NET` command used on DOS and Windows. (Examples of the `NET` command use on PC clients are shown in the next section, Chapter 4, "Configuring Client PCs," on page 19.)

You can use the Web-based System Manager, SMIT, the **net** command, or a combination of these methods to configure and administer the AIX Fast Connect server for your site.

As indicated in "Packaging and Installation Requirements" on page 3, AIX Fast Connect preconfigures itself to provide basic access to AIX user home directories (as defined in **/etc/passwd**) using plain–text network passwords. When started, the AIX Fast Connect server responds to SMB/NetBIOS requests on all operational TCP/IP interfaces.

Configurable Parameters

AIX Fast Connect is designed for ease of administration, but provides a set of customizable parameters to support various configurations. Several of these parameters are dynamically configurable and do not require the server to be stopped and restarted for the changes to become effective.

These parameters are found in the **/etc/cifs/cifsConfig** file and can be configured by using the **net config** command with the following syntax:

```
net config /parameter_name:parameter_value
```

The complete list of these configurable parameters is shown in Appendix B, "Configurable Parameters for the net Command," on page 79 or by typing: `net config help` on the command line.

Note: Use the Web-based System Manager or SMIT for most changes to the AIX Fast Connect configuration parameters, both to avoid spelling mistakes and because some of these parameters must be changed simultaneously. However, examples of the **`net config`** command are shown below, for AIX Fast Connect system administrators who prefer this method.

- To show the current configuration (an abbreviated list), type:

  ```
  net config
  ```

  This command shows some of the most important parameters, including *servername*, *domainname*, and *primary_wins_ipaddr*.
- To show a single parameter (for example, *servername* parameter), type:

  ```
  net config /parm:servername
  ```
- To change a parameter (for example, changing the *domainname*, the *autodisconnect* timeout, and the server *comment*), type:

  ```
  net config /domainname:testdomain
  net config /autodisconnect:60
  net config /comment:"String parameter containing Spaces"
  ```

Configuration of File Shares and Print Shares (Exports)

AIX Fast Connect can configure and export file shares and print shares. File shares are exported AIX directories. Print shares are exported AIX print queues. Every time that 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 **$HOME**, the AIX home directory (from the **/etc/passwd** file) of any PC-client user that connects to AIX Fast Connect. (Additionally, the file shares `IBMLAN$` and `ADMIN$` may be created by default, to support the

Network Logon feature of AIX Fast Connect.) More file shares or print shares can be added by the system administrator using Web-based System Manager, SMIT, or the **net** command.

Note: The default shares `HOME`, `IBMLAN$`, and `ADMIN$` cannot be changed or deleted.

Each file share or print share represents an object that AIX Fast Connect is exporting to the Windows network, accessed by its *netname*. Below are some common tasks related to file shares and print shares:

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

  ```
  net share
  ```

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

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

- To add a new printer share (for example, to export the **psColor1** AIX print queue as network name `PSCOLOR1`), type:

  ```
  net share /add /type:p /netname:PSCOLOR1 /printq:psColor1 /desc:"Print share test"
  ```

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

- To delete a share (for example, share `NETTEMP` listed above), type:

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

Note: If files seem to be missing in the directory when viewed from a PC client, AIX Fast Connect uses the AIX file permission bits to encode DOS file attributes (ReadOnly, Archive, System, Hidden). For more information, see “Support for DOS File Attributes” on page 44. Also, you can review “Mapping Long AIX File Names to 8.3 DOS File Names” on page 43.

Changing a file share or print Share (including the share description) causes that share definition to be deleted and then re-added with its new values. This change affects all PC clients that are connected to that share when it is redefined. These PC clients may experience `Network error` or `Shared not found` error messages until they remap the share manually or reboot the PC.

Hidden shares (not displayed by the Network Neighborhood or by NET VIEW) may be defined by adding a $ (dollar sign) at the end of the share name when creating the share.

If the AIX Fast Connect server has too much data to report, ″NET VIEW \\servername″ (on PC clients) can report an empty list.

User Administration

Access to AIX Fast Connect shares is managed internally by AIX user-security mechanisms. For example, if an AIX user has write access to a particular AIX subdirectory that is being exported by AIX Fast Connect, any PC client connecting to AIX Fast Connect (as that AIX user) would then have write access to that same subdirectory. (There are cases when an external PC client accesses AIX Fast Connect with a client user name that is different from the server user name being used for access checking; for example, guest mode, share-level security, and user name mapping.)

User accounts can be configured on the server using Web-based System Manager, SMIT, or the **net** command. Each defined AIX Fast Connect user must also be a defined AIX user. AIX Fast Connect supports user-level authentication using several mechanisms described in the following section. Resource access is permitted based on the authenticated AIX user credentials.

Note: Every AIX user name used for AIX Fast Connect authentication *must* have an AIX home directory specified. Otherwise, that user cannot access the AIX Fast Connect server.

Overview of User-Authentication Mechanisms

AIX Fast Connect supports several different types of user-authentication for access to the AIX Fast Connect server. Which authentication method you choose depends on your existing network environment and your network policies. These authentication methods are discussed briefly in this section. For more information, see Chapter 5, “Advanced Configuration Features,” on page 27.

AIX-based User Authentication (using plain text network passwords)

When the AIX Fast Connect server is configured for plain text passwords (and *not* for NT-Passthrough authentication), incoming SMB user name/password logins are sent to standard AIX system services for user authentication, which includes integrated DCE login, if specified for that AIX user.

To enable Plain Text passwords for AIX Fast Connect, type the following:

```
net config /encrypt_passwords:0
```

Note: SMB networking does not support mixed case for plain text passwords. In plain text mode, every AIX user accessing AIX Fast Connect must have AIX passwords that are in all uppercase or all lowercase.

CIFS Password Encryption Protocols

When the AIX Fast Connect server is configured for encrypted passwords (and *not* for NT-Passthrough authentication), incoming SMB user name/encrypted_password logins are validated by AIX Fast Connect against the **/etc/cifs/cifsPasswd** file, which is a database of AIX Fast Connect users (and their encrypted passwords). The **/etc/cifs/cifsPasswd** file is initialized and maintained by the **net user** command (see “Configuring Encrypted Passwords” on page 14).

To enforce encrypted passwords for AIX Fast Connect, type the following:

```
net config /encrypt_passwords:2
```

NT- Passthrough Authentication

When the AIX Fast Connect server is configured for NT-Passthrough Authentication, then the `encrypt_passwords` parameter is ignored, and incoming PC client login requests are routed through the network to an external Windows NT server for user authentication. (Normally, the PC-client uses encrypted passwords to authenticate with the external Windows NT server.) This method is often used when an NT server is already being used as a Network Logon server for the Windows network.

To enable AIX Fast Connect to authenticate to an external NT server (located at TCP/IP address *IPaddress*), type:

```
net config /passthrough_authentication_server:IPaddress
```

You can also designate a backup server for NT authentication with the following command:

```
net config /backup_passthrough_authentication_server:IPaddress2
```

Network Logon to AIX Fast Connect

AIX Fast Connect itself can be configured to act as a Network Logon server. (Windows NT, Windows 2000, and Windows XP clients require the IBM Primary Logon Client to use this feature.) For more information, see “Network Logon to AIX Fast Connect” on page 29 and Chapter 6, “Configuring Network Logon,” on page 51.

DCE/DFS Support

AIX Fast Connect can be configured for DCE/DFS support using plain text or encrypted passwords. In this mode, Fast Connect uses DCE-authentication mechanisms to validate PC clients for DFS™ access.

For more details, see “DCE/DFS Support” on page 30.

Kerberos-based Authentication
AIX Fast Connect supports the Kerberos 5-based authentication feature of Windows XP and Windows 2000 clients. To use this feature, the Windows XP and Windows 2000 clients must be configured for this mode.

Guest Logon
AIX Fast Connect can support guest-mode logon when configured for either plain-text or encrypted passwords. If AIX Fast Connect is enabled for guest-mode logins, an incoming PC client user name (which AIX Fast Connect must recognize as *not* a standard AIX Fast Connect user) is granted guest-mode access rights based on the AIX Fast Connect user name specified as the guest user (*guestname* parameter).

For more details, see "Guest Logon" on page 32.

Share-Level Security
When the AIX Fast Connect server is configured for share-level security, passwords are associated with individual file and print shares, not with PC client user names. In this mode, AIX Fast Connect provides access rights to PC clients based on a share-mode user name specified as the *share_level_security_username* parameter, similar to the guest-logon access mode.

For more details, see Chapter 5, "Advanced Configuration Features," on page 27.

Client-to-Server Username Mappings
As an extension of the **net user** command, AIX Fast Connect can map PC client user names (or *sets* of PC client user names) to AIX user names, for user-mode authentication and file access.

For more details, see "User-Name Mappings" on page 34.

LDAP User Authentication
AIX Fast Connect can be configured to authenticate to remote AIX LDAP servers, Windows Active Directory servers, or NDS servers, using industry-standard LDAP protocols. For more details, see "LDAP support for User Authentication" on page 31.

Configuring Encrypted Passwords

When the AIX Fast Connect server is configured for encrypted passwords, AIX Fast Connect attempts to authenticate all incoming SMB username/encrypted_password logins against the AIX Fast Connect **/etc/cifs/cifsPasswd** file, which is a database of AIX Fast Connect users (and their encrypted passwords). This file is initialized and maintained by the **net user** command.

Note: When AIX Fast Connect is configured to use encrypted passwords, only AIX Fast Connect usernames configured to use encrypted passwords by **net user** are able to log in to AIX Fast Connect. These passwords are distinct from (and may differ from) the standard AIX passwords in the **/etc/security** file. When an AIX user changes their password (using **/usr/bin/passwd**), the AIX Fast Connect password for that user does not automatically change. Nevertheless, you may want to use encrypted passwords on your network to enhance network security or to simplify configuration of recent Windows clients (who assume encrypted passwords, by default).

- To enforce Encrypted Passwords for AIX Fast Connect, type:
  ```
  net config /encrypt_passwords:2
  ```
- To list all users configured in the **/etc/cifs/cifsPasswd** file, type:
  ```
  net user
  ```
- To configure a new user for encrypted passwords, type:
  ```
  net user username password /add
  ```
  or:
  ```
  net user username -p /add
  ```
  The **-p** flag prompts for a no-echo password.
- To change a user's encrypted password, and also update that user's AIX password, type:

net user *username password* /changeaixpwd:yes

-or-

net user *username* -p /changaixpwd:yes

- To delete a user from the encrypted-passwords database, type:

  net user *username* /delete

- For security reasons, the default **/etc/cifs/cifsPasswd** file maps the client user name *root* to the server user name *nobody*. If you want to allow the user name *root* to map to itself (as a server user name), delete the default mapping by typing:

  net user /delete root

  The user name *root* can then be added as a Fast Connect user with its own encrypted password.

Basic Server Administration

You can use Web-based System Manager, SMIT, or the **net** command to manage AIX Fast Connect server operations. The following sections show basic server operations, using the AIX Fast Connect **net** command, and highlight the fast paths for SMIT at the end of the section.

Starting and Stopping the AIX Fast Connect Server

Follow these steps to start or stop the AIX Fast Connect Server:

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

  /etc/rc.cifs start

- To stop the server, (and unload the server daemon), type:

  /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 /usr/sbin/cifsServer on the command line. This enables the **net** command to function, 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 existing connections), type:

  net pause

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

  net resume

Showing Server Status Information

AIX Fast Connect provides several mechanisms for displaying current server status, including general status, configuration information, statistical information, and user-session information.

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

  net status

- To show general configuration information, type:

  net config

- To show statistical information (for example, packets delivered), type:

  net statistics

  Note: You can reset the statistics counts by typing net statistics /reset on the command line.

- To query the status of logged-in user sessions, type:

  net session

Web-based System Manager, SMIT Fast Paths, and net Commands

You can use the Web-based System Manager PC Services container to administer AIX Fast Connect, or you can use the SMIT fast paths and **net** commands shown in the following table.

Table 1. SMIT Fast Paths and commands or files to use when performing common AIX Fast Connect tasks.

Task	SMIT fast path	Command or file
Starting the Server	**smit smbadminstart**	**net start**
Stopping the Server	**smit smbadminstop**	**net stop**
Pausing the Server		**net pause**
Resuming the Server		**net resume**
Changing Parameters	**smit smbcfghatt**	**net config**
Changing Resources	**smit smbcfgresi**	**net config**
Adding Users	**smit smbcfgusradd**	**net user**
Changing Users	**smit smbchgusrlis**	**net user**
Changing a User Password	**smit smbusrpwd**	**net user**
Deleting a User	**smit smbrmusrlis**	**net user**
Configuring nbns	**smit smbwcfgn**	
Listing All Shares	**smit smbsrvlisall**	**net share**
Listing All File Shares	**smit smbsrvfilist**	**net share**
Adding a File Share	**smit smbsrvfiladd**	**net share**
Changing a File Share	**smit smbsrvfilchg**	**net share**
Deleting a File Share	**smit smbsrvfilrm**	**net share**
Adding Printer Share	**smit smbsrvprtadd**	**net share**
Changing Printer Share	**smit smbsrvprchg**	**net share**
Deleting Printer Share	**smit smbsrvprtrm**	**net share**
Showing Server Status	**smit smbadminstatu**	**net status**
Showing the Configuration	**smit smbcfg**	**net config**
Showing Statistics	**smit smbadminstats**	**net statistics**
Showing Share	**smit smbsrvlisall**	**net share**
Getting Help	(**smit** help-panels)	**net help**

NetBIOS Name Service (NBNS)

NetBIOS Name Service (NBNS) for AIX Fast Connect provides name-resolution services. It also supports some functions of Windows Internet Name Service (WINS), such as registration of multihomed name and Internet group name.

- To activate NBNS, type:

  ```
  net config /nbns:1
  ```

- To turn off NBNS, type:

  ```
  net config /nbns:0
  ```

Note: The *nbns* parameter is static, not dynamic. The AIX Fast Connect server must be shut down and restarted to enable NBNS service.

Table 2. SMIT Fast Paths and commands or files to use when performing common administrative NBNS tasks.

Task	SMIT fast path	Command or File
List all names in the NetBIOS Name Table		**net nblistnames**
Add a static NetBIOS Name	**smit smbwcfgadd**	**net nbaddname /name:***NBname* **/ipaddress:***IPaddress* [**/sub:***XX*] *or* **net nbaddgroup** *or* **net nbaddmulti**
Delete a NetBIOS name in Name Table	**smit smbwcfgdel**	**net nbdelname /name:***NBname* [**/sub:***XX*]
Delete by Name and Address	**smit smbwcfdadd**	**net nbdeladdr /name:***NBname* **/ipaddress:***IPaddress*
Back up the NBNS Name Table to a File	**smit smbwcfgbak**	**net nbbackup** [**/file:***filename*]
Restore the NBNS Name Table from Backup	**smit smbwcfgres**	**net nbrestore** [**/file:***filename*]

Notes:

1. The value of *IPaddress* can be any number in IP address range.
2. The subcode value *XX* is any two-digit hexadecimal number in the range *00-FF*.

Chapter 4. Configuring Client PCs

Use the information in this chapter to connect a PC client to the AIX Fast Connect server.

TCP/IP Configuration

To access the AIX Fast Connect server, each client PC must be configured for NetBIOS over TCP/IP (RFC1001/1002), or must support direct hosting of SMB over TCP/IP (see Microsoft Knowledge Base article 204279). Also, each client PC needs to have Client for Microsoft Networks installed. This can be accomplished for the various clients as shown in the following sections.

Windows 98 Clients

To configure Windows 98 clients to access the AIX Fast Connect server, follow these steps:

1. From the Start button, select **Settings -> Control Panel -> Network**.
2. On the *Configuration* tabbed panel (initially shown), verify that the following entries exist:
   - An entry for your networking-card (hardware driver)
   - TCP/IP (protocol)
   - Client for Microsoft Networks (client)

   If any entry is missing, add it from your Windows installation media.
3. Click the TCP/IP entry and select Properties.
   The TCP/IP Properties dialog box has several tabbed panels. Verify the following:

   IP Address panel
   Configure as needed. (For initial testing, you might want to disable DHCP and manually specify unique IP addresses for each PC.)

   Bindings panel
   Select **Client for Microsoft Networks**.

   Additionally, you might want to enable WINS support, DNS support, or gateway support for each client. If so, configure each as needed.
4. Test the client TCP/IP configuration by pinging (by IP address) from the PC client DOS prompt to the AIX Fast Connect server, and in reverse.

Windows NT Clients

To configure Windows NT clients to access the AIX Fast Connect server, follow these steps:

Note: You must be logged in as an Administrator.

1. From the Start button, select **Settings -> Control Panel -> Network**.
2. On the ***Adapters*** tabbed panel, verify that you have a correctly configured entry for your networking card (hardware driver).
3. On the ***Services*** tabbed panel, verify that there are entries for the following services:
   - Computer Browser
   - NetBIOS Interface
   - Workstation

   If any entry is missing, add it from your Windows NT CD.
4. On the ***Protocols*** panel, add TCP/IP (if missing), then select **Properties**.
   The TCP/IP Properties dialog box has several tabbed panels. Verify the following:

IP Address panel

Configure as needed. (For initial testing, you might want to disable DHCP and manually specify unique IP addresses for each PC.)

You might also want to configure DNS, WINS Address, and Routing.

5. Test the client TCP/IP configuration by pinging (by IP address) from the PC client DOS prompt to the AIX Fast Connect server and in reverse.

Windows XP, Windows 2003, and Windows 2000 Clients

To configure Windows 2000/XP/2003 clients to access the AIX Fast Connect server, follow these steps:

Note: You must be logged in as an Administrator.

1. From the Control Panel, open **Network and Dialup Connections** (Windows 2000) or **Network Connections** (Windows XP/2003).
2. Right-click on the Local Area Connection icon of the network adapter to be configured. Select **Properties**.
3. On the ***General*** tabbed panel, verify that there are checked entries for the following components:
   - Your networking card entry (Windows 2000)
   - Client for Microsoft Networks
   - Internet Protocol (TCP/IP)

   If any entry is missing, add it from your Windows CD.
4. Select the TCP/IP entry, then select **Properties**. Configure as needed.
   (For initial testing, you may want to disable DHCP and manually specify unique IP addresses for each PC.)
5. Test the client TCP/IP configuration by pinging (by IP address) from the PC client DOS prompt to the AIX Fast Connect server and in reverse.

NetBIOS Name Resolution

In addition to being able to **ping** the AIX Fast Connect server over TCP/IP, each client PC also must be able to resolve the NetBIOS name of the AIX Fast Connect server (the AIX Fast Connect *servername*) to an IP address. This can be done using UDP-Broadcast, **LMHOSTS** files, DNS, or WINS.

UDP-Broadcast (B-node)

The simplest NetBIOS name resolution (both in terms of setup and functionality) is UDP-Broadcast (B-node name resolution). No additional setup is required on the PC client as long as the client is on the same physical network segment (such as Ethernet or Token Ring) as the AIX Fast Connect server. The PC client broadcasts a UDP NetBIOS query to the local network, to which the AIX Fast Connect server responds.

Note: This mechanism does not work across TCP/IP routers, or gateways. Larger networks typically use DNS or WINS.

LMHOSTS files

Windows PCs can provide local **LMHOSTS** files for resolving NetBIOS names. Similar to **/etc/hosts** on AIX, each PC can have an **LMHOSTS** file to statically resolve NetBIOS names to IP addresses. (This mechanism might be unsuitable for DHCP environments or networks with many client PCs, because every **LMHOSTS** file must change whenever the AIX Fast Connect servers' IP addresses change.)

The following is an example of editing an **LMHOSTS** file on Windows 98 from the DOS prompt:

```
C:\>  cd \windows
C:\>  edit lmhosts     (LMHOSTS.SAM is included with Windows as an example.)
```

On a Windows NT, Windows 2000, Windows XP, or Windows 2003 machine, do the following:

```
C:\> cd \winnt\system32\drivers\etc
C:\> edit lmhosts
```

After editing the **LMHOSTS** file, run the Windows PC command **nbtstat -R**.

DNS If your network is running the domain name service (DNS) for TCP/IP and your AIX Fast Connect *servername* is registered in the DNS, each client PC can be configured to use DNS for NetBIOS name resolution. (This must be enabled under TCP/IP Properties for Windows NT.)

During installation, the AIX Fast Connect *servername* defaults to match the AIX *hostname*.

WINS Your Windows network might use Windows Internet Naming Service (WINS) for NetBIOS name resolution. Similar to DNS for TCP/IP, WINS allows NetBIOS service names to be resolved to IP addresses across multiple LAN segments. When this is the case, each Client PC is configured to use the WINS server under TCP/IP Properties.

Additionally, use the SMIT fast path **smit smbcfghatt** to set the WINS Address entry and Backup WINS Server for the AIX Fast Connect server. The AIX Fast Connect server uses these IP addresses to automatically register its NetBIOS server name with the WINS servers.

You can configure one or more AIX Fast Connect servers to act as NBNS/WINS servers. For more information, see “NetBIOS Name Service (NBNS)” on page 16.

At this point, if you have LMHOSTS, DNS, or WINS correctly configured, you can **ping** from the client PC by using the NetBIOS server name.

Workgroups, Domains, and User Accounts

AIX Fast Connect supports several different types of user authentication/access mechanisms. (See “User Administration” on page 12 and “Basic Server Administration” on page 15.) Each client PC should be configured to match the AIX Fast Connect user-access method you have chosen for your network.

For ease of use, client PCs should be in the same Windows domain as the AIX Fast Connect server (the reverse is also true). Windows NT, Windows 2000, and Windows XP all use `WORKGROUP` as a default workgroup name, and AIX Fast Connect server also initializes itself to use `WORKGROUP`. If your network uses NT domain login authentication, you can configure the AIX Fast Connect server to verify AIX Fast Connect access using the NT domain authentication servers.

Whether you use Workgroups or NT domains, access to AIX Fast Connect is managed by user security. You must set up AIX user accounts for each Windows user who is accessing AIX Fast Connect. It is easiest to use if the user accounts (and passwords) on AIX match the Windows or NT domain user accounts (and passwords).

- On the AIX Fast Connect server, use the SMIT fast path:

  ```
  smit smbcfghatt
  ```

  Within the SMIT panel, do the following:
  - To use Workgroups, type the workgroup name in the Domain Name field.
  - To use NT domain validation, type the IP addresses for the NT domain authentication server(s) in the **Passthrough Authentication Server** and **Backup Passthrough Authentication Server** fields.
- On PC clients running Windows 98, do the following:
  1. Select **Start button -> Settings -> Control Panel -> Network**.
  2. On the ***Identification*** panel, type the computer name for that PC.
  3. Configure the domain:
     - To use workgroups, type the workgroup name in the **Workgroup** field.
     - To use NT domain validation,
       a. On the ***Configuration*** tabbed panel, select **Client for Microsoft Networks**, and click **Properties**.

b. Check the NT domain checkbox, and type the NT domain name. (To join an NT domain, you must have Domain Administrator privileges.)

- On PC clients running Windows NT, make sure you are logged in as Administrator. Then:
  1. Select **Start button -> Settings -> Control Panel -> Network**.
  2. On the ***Identification*** panel, select **Change...** .
  3. Type the Computer Name for that PC.
  4. Type the appropriate workgroup or domain name. (To join an NT domain, you must have Domain Administrator privileges.)
- On PC clients running Windows 2000, make sure you are logged in as Administrator. Then:
  1. Select **Start button -> Settings -> Control Panel -> System**.
  2. On the ***Network Identification*** panel, select **Properties**.
  3. Type the Computer Name for that PC.
  4. Type the appropriate workgroup or domain name. (To join an NT domain, you must have Domain Administrator privileges.)
- On PC clients running Windows XP or Windows 2003, make sure you are logged in as Administrator. Then follow these steps:
  1. From the Control Panel, choose **System**.
  2. On the ***Computer Name*** panel, select **Change**.
  3. Type the computer name for that PC.
  4. Type the appropriate workgroup or domain name. (To join an NT domain, you must have Domain Administrator privileges).

Enabling Windows Clients for Plain Text Passwords

For security reasons, Microsoft has disabled support for nonencrypted (plain text) network passwords in all supported versions of Windows. If you want to use plain text passwords on your network, these clients must be upgraded with the following Registry patches.

Note: Microsoft has recommended the current System Registry be saved as a backup before any manual changes are made to it. For details, see Microsoft's **technet** web site.

- To enable plain text passwords on Windows 98, complete the following:
  1. Use your favorite text editor to create the following text file, named **W98plain.reg**, as a local file on the Windows 98 machine:

```
REGEDIT4

; Registry file to allow plaintext passwords on Windows 98

[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VNETSUP]
"EnablePlainTextPassword"=dword:00000001
```

  2. Using Windows Explorer, double-click the **W98plain.reg** file name in the directory where you saved it. This action will update the Windows Registry for that client to allow plain text passwords.
  3. Shut down and restart the Windows 98 machine. (Shut down and restart is required for this patch to take effect.)
- To enable plain text passwords on Windows NT 4.0, log in as Administrator. Then:
  1. Use **EDIT** or the NOTEPAD accessory to create the following text file, named **NT4plain.reg**, as a local file on the Windows NT machine:

```
REGEDIT4

; Registry file to allow plaintext passwords on Windows NT 4.0

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Rdr\Parameters]
EnablePlainTextPassword=dword:00000001
```

2. Using Windows NT Explorer, double-click the **NT4plain.reg** file name in the directory where you saved it. This action will update the Windows Registry for that client to allow plain text passwords.
3. Shut down and restart the Windows NT machine. (Shut down and restart is required for this patch to take effect.)

Note: Even with the previous patch installed, all Windows NT 4.0 clients still require users to type their password every time the user first connects to the AIX Fast Connect server (by browsing, mapping drives, and so on). After the user is successfully connected, additional browsing or drive-mapping operations proceed successfully. The initial `Password Invalid` message occurs because Windows NT 4.0 attempts to use encrypted passwords rather than plain text passwords, while connecting to AIX Fast Connect server.

- To enable plain text passwords on Windows 2000, Windows XP, and Windows 2003, log in as Administrator. Then:
  1. From the Control Panel, open **Administrative Tools**, then open **Local Security Policy**.
  2. On the Tree view, select **Local_Policies -> Security_Options**.
  3. On the Policy list (right-hand panel), enable the entry **Send unencrypted password to connect to third-party SMB servers**.
  4. Shut down and restart the Windows machine

Browsing the Network

AIX Fast Connect supports browser operations such as NET VIEW and Network Neighborhood (renamed *My Network Places* on Windows XP and Windows 2000). These operations show the user a list of file shares and printer shares exported by each server.

Network Neighborhood can also be used to map drives. To do this, right-click on a file share name, then select **Map Network Drive** from the menu.

Note: Network browsing has the following limitations:

- To see the AIX Fast Connect server in Network Neighborhood, a client PC needs to be able to see the Master Browser for the workgroup or domain for which that AIX Fast Connect server is configured.

  Network browsing generally works best if the client PC and the AIX Fast Connect server are in the same workgroup/domain.
- The browse list database that is maintained by the Master Browser is not always up-to-date. The list can show AIX Fast Connect server names for servers that are currently down, off, physically disconnected, or otherwise unreachable. The Master Browser does not delete a server from the browse list until that server name's refresh timeout has expired, which can take several days. However, if a user tries to access that server name (by browsing share names, mapping drives, and so on), a disconnected AIX Fast Connect server is detected as unavailable.

Mapping Drives

Normally, PC clients must define drive mappings to use the AIX Fast Connect exported file shares. These drive mappings can be done from Windows or from the DOS command prompt.

You can use the following mechanisms to define or undefine mappings between PC drive letters and AIX Fast Connect file shares. For the following examples, assume that the NetBIOS server name is `cifs01`, and that file share `apps` is defined.

From DOS:

```
DOS> net help                    (help info for DOS)
DOS> net use H: \\cifs01\home    (pre-defined AIX Fast Connect share)
DOS> net use F: \\cifs01\apps
DOS> copy F:\oldfile H:\newfile  (uses the mapped drives)
DOS> net use F: /delete          (delete the drive-mapping)
```

From Windows:

1. In the Map Network Drive dialog box:
   - Select **Windows Explorer -> Tools -> Map Network Drive**.

     -or-
   - Right-click on Network Neighborhood and select **Map Network Drive**.
2. Select the drive from the Drive: drop-down list, then:
   - Enter the path: (for example, `\\cifs01\apps`).

     -or-
   - Use the Shared Directories (browse tree) panel to select the network share.

Using AIX Fast Connect Printers

For printing, DOS and Windows mappings are somewhat different. For the following examples, assume that AIX Fast Connect server `cifs01` has print shares `netprint1` and `pscolor` defined.

For DOS applications, the following simple device-mappings can be used:

```
DOS> net use LPT1: \\cifs01\netprint1
DOS> net use LPT2: \\cifs01\pscolor
```

To test these DOS printer-mappings, use the following:

```
DOS> COPY text_file LPT1:
DOS> COPY Postscript_file LPT2:
```

Note: During print-spooling, neither DOS nor AIX Fast Connect auto-convert Postscript to text, or in reverse. However, this auto-detection/auto-convert feature can be enabled using AIX print-spooling options.

For Windows applications, install a Windows printer driver and map it to the network printer, as follows:

1. Select **Start -> Settings -> Printers -> Add Printer**.
2. Select **Network Printer**.
3. Enter the AIX Fast Connect print share name (for example, `\\cifs01\netprint1`) or use the browse list to select the print share.
4. Select the correct Windows printer driver for that network printer (for example, IBM 4039 Laser Printer PS), which is installed from your Windows installation disks.

Test Windows printer-driver functionality by printing a test file from any Windows application (for example, Notepad), or by using the Print Test Page feature as follows:

1. Select **Start -> Settings -> Printers**.
2. Select the printer driver (for example, `pscolor`).
3. From the Menu Bar, select **File -> Properties**.
4. From the tabbed panel labeled General, select **Print Test Page**.

Note: For windows 98 and NT clients, AIX Fast Connect supports displaying the full name of the document being printed (in the client's print status window). For other clients, a generated name will be displayed.

Support for Windows Terminal Server

AIX Fast Connect is compatible with the Windows Terminal Server program. This program allows multiple PC clients running Windows Terminal Client software to log in to the Windows Terminal Server and establish a remote console session. Any network drive (or network printer) mapping made within that console session is forwarded by Windows Terminal Server to other NetBIOS servers, as required.

Windows Terminal Server (and other similar terminal-server programs) must accommodate multiple net mappings by multiple user names coming from multiple client PCs. Windows Terminal Server (and other terminal servers) can multiplex these requests to AIX Fast Connect using the following mechanisms:

- Multiple TCP/IP sessions (from a single Windows Terminal Server PC) to AIX Fast Connect
- Multiple SMB sessions multiplexed into a single TCP/IP session

To enable Windows Terminal Server support, set **multiuserlogin=1**.

If either Network Logon support or NT-passthrough authentication is enabled, Windows Terminal Server is not supported.

For specific information about setup and use of Windows Terminal Server and Windows Terminal Client, see your Windows Terminal Server documentation.

Support for Windows Active Directory Server

AIX Fast Connect can use the AIX LDAP client (**ldap.client.rte**) to access a Windows Active Directory Server. The **cifsLdap** command allows AIX Fast Connect to register and unregister its file share names and print share names into the Windows Active Directory. For more information, see the “cifsLdap command” on page 76.

Configuring LAN Manager authentication level

By default, AIX Fast Connect supports the LM (LAN Manager) authentication only. AIX Fast Connect can be configured to support NTLM (NT LAN Manager) authentication instead by enabling the **lm_encryption_level** parameter (For details, see Appendix B, “Configurable Parameters for the net Command,” on page 79). Most Windows clients will support either LM or NTLM authentication methods by default.

Windows 2003 clients must be specifically configured to support LM authentication.

1. From the Control Panel, open **Administrative Tools**, then open **Local Security Policy**.
2. On the tree view, select **Local Policies** -> **Security Options**.
3. On the Policy list (right-hand panel), set the **LAN Manager authentication** level to **Send LM & NTLM responses**.
4. Shut down and restart the Windows machine

Chapter 5. Advanced Configuration Features

This chapter discusses various AIX Fast Connect authentication methods and advanced AIX Fast Connect features used for customized configurations. For basic administrative procedures, see Chapter 3, "Configuration and Administration," on page 11.

Note: Several of the features described in this chapter cannot be used simultaneously.

Many choices for the features described in this chapter depend on the type of authentication method selected. Each type has its advantages and disadvantages. Which authentication method or methods you choose depends on your environment, your administration policy, and the ease of administration and use. The following methods for user authentication are described in detail in this section:

AIX Fast Connect supports the following advanced features:

Several performance considerations for AIX Fast Connect are also discussed in "Performance Considerations" on page 48.

AIX-Based User Authentication (Plain-Text Passwords)

AIX-based authentication uses AIX user definitions and passwords. All AIX authentication grammars are supported, including DCE and LDAP. Following session setup, a AIX Fast Connect session obtains the authenticated AIX user's credentials (UID, GID, and secondary groups).

The following requirements apply:

- Clients must be able to negotiate plain-text passwords. This might require updating registry entries on all Windows clients. (See "Enabling Windows Clients for Plain Text Passwords" on page 22.)
- AIX Fast Connect must be enabled for plain-text passwords. To do this, type:

  ```
  net config /encrypt_passwords:0
  ```

Plain-text passwords have the following advantages:

- Low administrative overhead because they use existing AIX user information.
- AIX tools for managing users can be used.

Plain-text passwords have the following disadvantages:

- Windows registry update might be required, on a per-client basis.
- Windows might require user ID and passwords to be retyped, on a per-SMB-login basis.
- Clear-text passwords are sent over the network.

Notes:

1. SMB networking does not support mixed case for plain-text passwords. Every AIX user accessing AIX Fast Connect must have AIX passwords that are in all uppercase or all lowercase.
2. Case insensitive user name matching is not supported when plain-text passwords are being used. For example: if `uSeR1` is defined as an AIX user and the client tries to map as `USER1`, authentication will fail.
3. When AIX Fast Connect is configured for plain-text passwords, AIX authentication rules are followed.

CIFS Password Encryption Protocols

The CIFS password encryption protocol method uses AIX Fast Connect user definitions and encrypted passwords for user authentication. Each user must be defined under the same user name as an AIX user. AIX Fast Connect encrypts passwords and saves them in its user database (**/etc/cifs/cifsPasswd**) for use during session setup. (See "Configuring Encrypted Passwords" on page 14.) Following session setup, a AIX Fast Connect session obtains the authenticated user's credentials (UID, GID and secondary groups).

CIFS password encryption protocol method has the following requirements:

- Users must be defined to AIX Fast Connect using Web-based System Manager, SMIT, or the **net user** command.

  (User passwords need not match on both systems.)
- AIX Fast Connect must be enabled for encrypted passwords. To do this, type:

  ```
  net config /encrypt_passwords:2
  ```
- Changing AIX Fast Connect passwords requires root authority.

This method has the following advantages:

- No additional log in, beyond logging into the Windows workstation, is required.
- Clear-text passwords are not sent over the network, which provides additional security.

This method has the following disadvantages:

- Additional administrative tasks are needed for AIX Fast Connect users.
- Root authority is needed to update passwords in AIX.

NT Passthrough Authentication

This authentication method uses AIX user definitions and NT-based server user authentication. In this mode, each AIX Fast Connect user must also be defined as an AIX user. Passthrough authentication is enabled using Web-based System Manager, SMIT, or the **net** command by specifying an IP address for the NT Passthrough Authentication Server.

To configure this mode using the **net** command, type:

```
net config /passthrough_authentication_server:IPaddress
```

You can also designate a backup server for NT authentication by typing:

```
net config /backup_passthrough_authentication_server:IPaddress2
```

During session setup, AIX Fast Connect forwards the session setup request to the NT-based server. If the NT-based server authenticates the user, AIX Fast Connect grants access. Following session setup, an AIX Fast Connect session obtains the authenticated user's credentials (UID, GID and secondary groups).

Passthrough authentication has the following requirements:

- User must be defined on the passthrough authentication server.
- AIX Fast Connect must be enabled for passthrough authentication.
- The NT user name must match the AIX user name, although passwords can be different.

This method has the following advantages:

- No additional login, other than logging into the Windows workstation is required.
- Clear-text passwords are not sent over the network, which provides additional security.
- Less administrative overhead is needed because this method uses NT user definition.

This method has the following disadvantage:

- An NT authentication server, which must be a secure system, is required.

Notes:

1. If passthrough authentication or backup passthrough authentication servers cannot be reached, only local authentication will be in effect (based on the value of the **encrypt_passwords** parameter). If the passthrough or backup passthrough authentication servers are reached, but authentication fails because of an incorrect name or password, then no local authentication will be attempted.
2. When passthrough authentication is enabled, guest logon support cannot work. These options are mutually exclusive. Disable guest logon by typing:

   ```
   net config /guestlogon:0
   ```
3. When passthrough authentication is enabled, AIX Fast Connect's network logon feature cannot work. These options are mutually exclusive. (Frequently, the external NT authentication server is also acting as a Network Logon server, or even a Primary Domain Controller for NT domains.)
   Disable AIX Fast Connect's network logon feature by typing:

   ```
   net config /networklogon:0
   ```
4. An additional AIX Fast Connect server can be used as the passthrough authentication server, instead of using a Windows NT-based server.

Network Logon to AIX Fast Connect

AIX Fast Connect can be configured to act as a Network Logon server. In this mode, Windows-based PCs are configured for network logon, rather than local logon, which provides the following benefits:

Network Password
PC users can log in to any network workstation using their network password, without having separate Local-Logon passwords per workstation.

Startup Scripts
During network login, startup scripts can be executed from the Network Logon server, based on user name and workstation name.

Roaming Profile
After network login, each PC user's desktop environment is automatically initialized to the correct network settings, regardless of which workstation that user is using.

Home Directories
After network login, each PC user's home directory is available, regardless of which workstation that user is using.

The following restrictions apply to AIX Fast Connect's network logon feature:

- Windows 98 clients can use either:
  - Microsoft Client for Microsoft Networks

    or
  - IBM Client for IBM Networks
- Windows NT, Windows 2000, and Windows XP clients must use the IBM Primary Logon Client.
- NT passthrough authentication must be disabled.

AIX Fast Connect's Network Logon feature is enabled (or disabled) using the *networklogon* parameter. For more information, see Chapter 6, "Configuring Network Logon," on page 51.

DCE/DFS Support

AIX Fast Connect can be configured to provide access to DFS for Windows clients. Each AIX Fast Connect user name is used as a DCE principal name. Mixed-case user names or passwords are only supported when encrypted passwords are used.

DCE support is controlled through the **dce_auth** configuration option, which can be set to 0 or 1. A value of 1 indicates that DCE authentication option is enabled. When **dce_auth=1**, all incoming PC client logins are sent to DCE for authentication. All PC-client user names and passwords must also be valid DCE user names and passwords (UID, GID, and groupset are defined by the DCE authentication). If DCE authentication is enabled and if AIX Fast Connect is configured to use encrypted passwords, each AIX Fast Connect user must be configured by entering the DCE password for that user by using the **net user** Subcommand (see "net user Subcommand" on page 67). In addition, multiple AIX Fast Connect servers in a DCE environment can be configured to share one common user database (for encrypted passwords) using the DCE-Registry User Database feature.

When **dce_auth=0**, AIX Fast Connect can still provide some access to DFS files under the following conditions:

- If AIX-based authentication is being used (plain-text passwords), all AIX accounts configured for Integrated Login to DCE are allowed DCE-authenticated access to DFS when connecting to AIX Fast Connect.
- In all other cases, AIX Fast Connect users are allowed non-authenticated access to DFS, using the any_other ACL.

Notes:

1. When DCE integration is enabled and the user's AIX UID is different from DCE UID, the user might not have the same access rights as an AIX login shell.
2. DCE/DFS authentication (**dce_auth=1**) is mutually exclusive with NT Passthrough authentication.

3. DCE/DFS authentication (**dce_auth=1**) is mutually exclusive with the guest logon feature.

LDAP support for User Authentication

AIX Fast Connect supports LDAP bind mechanisms for user authentication. This allows AIX Fast Connect to authenticate to remote AIX LDAP servers, Windows Active Directory servers, or NDS servers, using industry-standard LDAP protocols.

The following AIX Fast Connect configuration options are used for this feature:

ldap_auth
enables or disables the LDAP authentication feature

ldap_server_name
server name of LDAP authentication server

ldap_admin_user
user name with administrative access to LDAP directory

ldap_userDN
Distinguished Name context where user names are searched

To setup and use the LDAP authentication feature, follow these steps:

1. Configure AIX Fast Connect for plaintext passwords by typing the following command:
   ```
   net config /encrypt_passwords:0
   ```
   This is a requirement for using the LDAP authentication feature.
2. Setup a special LDAP user account (on the LDAP server) that has full-search capabilities on the LDAP database (for example, **fcadmin**) This LDAP account will be used by AIX Fast Connect to search the LDAP user-database for usernames.
3. Setup this LDAP admin account as an AIX Fast Connect user by following these steps:
   a. Create the LDAP admin account as an AIX user. Every LDAP user to be used by AIX Fast Connect must also exist as a local AIX user.
   b. Register the LDAP admin account password to AIX Fast Connect using the **net user** command. For example:
      ```
      net user /add fcadmin adm_pwd /comment:"This is the LDAP admin account"
      ```
4. Configure the LDAP authentication options for AIX Fast Connect by typing the following commands:
   a. `net config /ldap_admin_user:`*`fcadmin`*
   b. `net config /ldap_server_name:`*`ldapServerName`*
   c. `net config /ldap_userDN:`*`userDN`*
5. Enable the LDAP authentication feature by typing the following command:
   ```
   net config /ldap_auth:1
   ```
6. Re-start the AIX Fast Connect server to use the new settings:
   a. `/etc/rc.cifs stop`
   b. `/etc/rc.cifs start`

   If errors occur when starting AIX Fast Connect, check the Fast Connect log file, **/var/cifs/cifsLog**.)

Notes:

1. The **ldap_auth** feature requires plaintext passwords (`encrypt_passwords=0`), and is not compatible with any of the other remote authentication mechanisms supported by AIX Fast Connect (NT-Passthrough, DCE-authentication, DCE user-registry, and Kerberos-authentication). These other authentication methods must be disabled to use LDAP authentication. (The default for all of these authentication methods is `disabled`, unless any of the them has been previously enabled.)

2. When the **ldap_auth** feature is being used, every AIX Fast Connect user must also exist as a local AIX user.
3. Guest logon is not supported with LDAP authentication. When LDAP authentication is used, the **guestlogonsupport** parameter should be disabled.

Kerberos-based Authentication

AIX Fast Connect supports the Kerberose5 authentication feature of Windows XP and Windows 2000 clients (Windows XP and Windows 2000 clients must be configured for this mode). The AIX Fast Connect configuration option, **krb5_auth**, is used to enable this feature, and **krb5_service_name** is used to configure AIX Fast Connect for the external Kerberos Domain-Controller (KDC).

When this feature is enabled, other AIX Fast Connect clients can use other authentication methods, such as plain-text passwords or encrypted passwords, to connect to the AIX Fast Connect server and access its file shares and print shares.

Notes:

1. NT passthrough authentication is not supported if **krb5_auth** is enabled.
2. Kerberos-based authentication is only supported for Windows XP and Windows 2000 clients configured for that functionality.
3. If **krb5_auth** is enabled, AIX Fast Connect must be configured for either plain-text passwords or encrypted passwords in order to support non-Kerberos clients, such as Windows 98 and Windows NT. These clients cannot be authenticated by NT-passthrough or DCE/DFS authentication if the Kerberos feature is enabled.

Use the following instructions to configure an AIX Fast Connect server for Kerberos-based authentication of Windows XP or Windows 2000 clients. These instructions assume that the Windows XP or Windows 2000 clients have been successfully configured for Kerberos-based authentication to a working Kerberos Domain Controller.

1. If the AIX Fast Connect server is running on an AIX server that has already been successfully configured as a Kerberos client machine, run the following commands:

   ```
   net config /krb5_service_name:krb5svc
   net config /krb5_auth:
   ```

   where *krb5svc* is a Kerberos Service in the following form: HOST@server1.austin.ibm.com.
2. Restart AIX Fast Connect with the new configuration by running the following commands:

   ```
   /etc/rc.cifs stop
   /etc/rc.cifs start
   ```

For a more detailed example, see Appendix C, “Kerberos setup example,” on page 91.

Guest Logon

AIX Fast Connect can support guest-mode logins when configured for either plain text or encrypted passwords. To enable guest-mode logins, the following parameters must be configured:

```
net config /guestlogonsupport:1          (enables guest logons)
```

and

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

When guest logon support is enabled (**guestlogonsupport=1**), and the **guestname** field is set, non-AIX users can connect to the AIX Fast Connect Server. The credentials for guest clients is set to those of the *guestname* attribute.

The name specified by the **guestname** attribute must be an AIX user. Optionally, the **guestname** user can also be defined as an AIX Fast Connect user.

- If **guestname** is defined as an AIX Fast Connect user, then guest users will be authenticated using the name and password specified for the AIX Fast Connect user (matching guestname).
- If **guestname** is not defined as an AIX Fast Connect user, then guest users will be authenticated using **guestname**, and a null password. For successful authentication, this will require that the AIX user (matching **guestname**) have a null password. This guest account can access all of the file system directories exported by AIX Fast Connect (as file shares). Therefore, to simplify access control, this guest account should probably be in its own unique AIX group.

Guest access is only given to user names that are *not* defined AIX Fast Connect users with passwords that are *not* null.

Incoming login requests are authenticated as follows:

- If the incoming user name is recognized as a valid user, the password is checked. If the password is correct, standard user-mode access is granted; otherwise, the login attempt fails.
- If the incoming user name is *not* recognized as a valid user, the password is checked. If the password is not null, guest-mode access is granted; otherwise, the login attempt fails.

To disable guest logon support, type:

```
net config /guestlogonsupport:0
```

Notes:

1. When guest logon support and encrypted passwords are both enabled, it is not required that the **guestname** user be added to the AIX Fast Connect user database (**/etc/cifs/cifsPasswd**). However, the AIX password for **guestname** must be null if a matching AIX Fast Connect user is not added.
2. Users cannot authenticate as a guest user when logging in to their client workstation with a network logon (using the network logon server feature). However, users can still map to AIX Fast Connect as guest users after successfully logging into their client systems. This limitation only applies when using the **guestlogonsupport** and **networklogon** features simultaneously. It prevents the creation of additional users on the client systems in certain cases, and prevents users from mistakenly logging on to their client system as a guest user.
3. To use guest logon support with DCE authentication, the name chosen for **guestname** must be a valid DCE user. Also, the **guestname** user must be added as an AIX Fast Connect user with a non-null password that matches the DCE password.
4. Guest logon is not supported with LDAP authentication. When LDAP authentication is used, the **guestlogonsupport** parameter should be disabled.

Share-Level Security

When the AIX Fast Connect server is configured for share-level security, passwords are associated with individual file shares and print shares, not with PC client user names. In this mode, AIX Fast Connect provides access rights to PC clients based on a share-mode user name specified as the *share_level_security_username* parameter, similar to the guest logon access mode.

Note: When share-level security is enabled, all user-level authentication mechanisms are disabled.

To enable share-level security, type:

```
net config /share_level_security:1                (enable share-level security)
net config /share_level_security_username:AIXuser  (configure share user)
```

In share-level security mode, AIX Fast Connect supports both ReadWrite passwords and ReadOnly passwords. When a PC client tries to connect to a share, the following can occur:

- If that client provides the ReadWrite password for a share (or if that share's ReadWrite password is null or undefined), that client is granted ReadWrite access to the share.
- If that client fails to get ReadWrite access, but provides the ReadOnly password for a share (or if that share's ReadOnly password is null or undefined), that client is granted ReadOnly access to the share.

Note: These access modes are also affected by the access credentials of the *share_level_security_username* for that share, and by the **mode** share option, both of which can effectively change ReadWrite access to ReadOnly access.

- To create a NETTEMP share with a ReadWrite password of `write-is-okay`, type:

  ```
  net share /add /netname:NETTEMP /path:/tmp /rw_password:"write-is-okay"
  ```

- To create a USERS share with both ReadWrite and ReadOnly passwords, type:

  ```
  net share /add /netname:USERS /path:/home /rw_password:writeme /ro_password:readme
  ```

  Note: Specifying a ReadOnly password without specifying a ReadWrite password normally allows all clients to get ReadWrite access (if the ReadWrite password is null).

- To disable share-level security (to use other user-authentication mechanisms), type:

  ```
  net config /share_level_security:0
  ```

- If Windows Terminal services is used with Share-Level Security, (**multiuserlogin=1** and **share_level_security=1**), only the *first* user that connects to a share will prompt for the share's password — all successive users that connect to that share will not be prompted for a password (and no password will be sent to the server, even if specified). This is a problem with Windows Terminal Services. See Microsoft KnowledgeBase article Q260853 for more information.

User-Name Mappings

This feature allows AIX Fast Connect to map PC client user names (or *sets* of PC client user names) to server (AIX) user names, for purposes of user-mode authentication and file access. All user-authentication mechanisms are supported, although the behavior is different depending on the authentication method used.

- With plain-text passwords, encrypted passwords, DCE, or LDAP authentication methods, AIX Fast Connect will resolve any client-to-server user name mappings prior to authentication. Authentication will then be done based on the server user name (*aixname*).
- When enabled with NT passthrough or Kerberos authentication methods, AIX Fast Connect will first authenticate the client user name (as received from the PC client). Upon successful authentication of the client user name, AIX Fast Connect will resolve any client-to-server user name mappings, and grant access to the share as the server user name (*aixname*).
- All authentication methods will function normally for users which do not have a mapping.

The feature is controlled by the *usernamemapping* parameter, and mappings are configured by the **net user /map** command.

- To enable the user-name mappings feature type:

  ```
  net config /usernamemapping:1
  ```

- To define a mapping from ***longclientname*** to ***aixname***, type:

  ```
  net user /map longclientname aixname
  ```

- To define a ***second*** mapping to that same AIX user, type:

  ```
  net user /map secondclientname aixname
  ```

- To delete a mapping, use the *client* user name similar to the following:

  ```
  net user /delete longclientname
  ```

- To disable this feature, type:

  ```
  net config /usernamemapping:0
  ```

Notes:

1. PC client user names are restricted to 20 characters.
2. When user-name mapping is enabled, the user name `root` is mapped to the user name `nobody` by default. This mapping can be changed.
3. After mapping a client user name *XXXX* to an AIX server user name, that client user name cannot be defined as a *server* user name (with its own unique encrypted password) until that user-name mapping is deleted by **net user/delete**.
4. When user-name mapping is enabled, the user name `root` is mapped to the user name `nobody` by default. This mapping can be changed. To allow the user name *root* to map to itself (as a server user name), this default mapping must be deleted with the **net user/delete root** command (See "net user Subcommand" on page 67).

User-name mappings Example

Following is an example for mapping multiple PC client user names to a single server (*aixname*) using the NT passthrough authentication method.

Environment:

- A Windows NT Server (in this scenario, `NT_server`) is configured as the passthrough authentication server for AIX Fast Connect (in this scenario, `FC_server`).
- Users `John Doe` and `Jane Doe` are defined as users on `NT_server`, and on Windows client PCs.
- User `doe` is defined as an AIX user.

The network administrator wants to give `John Doe` and `Jane Doe` the same access to the AIX Fast Connect shares, and is unable to create users `John Doe` and `Jane Doe` on AIX. The solution is to map these user names to the existing AIX user `doe` as follows:

1. `net user /map "John Doe" doe`
2. `net user /map "Jane Doe" doe`

Now when `John Doe` or `Jane Doe` maps a drive to the AIX Fast Connect server, the following sequence occurs:

1. `FC_server` receives request from the client PC to map drive as `John Doe` (along with their password).
2. `FC_server` forwards the credentials to `NT_server` for authentication.
3. `NT_server` replies to `FC_server` with authentication results.
4. On successful authentication, `FC_server` checks for existing user name mappings, and finds that `John Doe` is mapped to `doe`. Access is granted to the AIX Fast Connect share as AIX user `doe`.

Dynamic User Creation

This feature allows the CIFS server to automatically create and map local users and groups for authenticated Windows users and groups. This allows Windows users to seamlessly access CIFS file shares on the AIX Fast Connect server without having a File Access User account. Dynamic user creation is disabled by default.

Note: Passthrough authentication must be enabled to use this feature. The passthrough authentication server must be a Windows Domain Controller or Active Directory server.

If dynamic user creation is enabled, when an authenticated Windows user attempts to access a CIFS share, the CIFS server will create a UNIX user and appropriate groups, mapping them to the Windows users and groups (if a mapping does not already exist). The group information is obtained from the passthrough authentication server, and is synchronized at each successful login. Users are created with a

name of **usr***name* where *name* is a unique identifier (such as UID) created for that user. Groups are created with a name of **grp***name*, where *name* is a unique identifier (such as GID) created for that group. The user and group prefixes are configurable.

Dynamic user creation is most useful in an environment where Windows users do not share files with UNIX users, or in a purely Windows-based network. The following scenarios should be considered for any environments where UNIX and Windows users may both log in.

- If a UNIX user account with the same name as the Windows user already exists on the CIFS server, then the Windows user will be mapped to the existing UNIX user (rather than creating a name of **usr***name*). In this case, the groups information for the UNIX user will be modified whenever synchronization with the passthrough authentication server occurs.
- If a Windows user (for example, foo) has successfully logged into the CIFS server and is mapped to the CIFS user **usr***name*, it is possible that a UNIX user named foo could be manually added at a later time. This could cause some confusion as the Windows user foo would be mapped to **usr***name*, not foo.

To enable dynamic user creation, type:

```
net config /dynuser:1
```

To disable dynamic user creation, type:

```
net config /dynuser:0
```

To change the user prefix, type:

```
net config /dynuser_prefix: username
```

To change the group prefix, type:

```
net config /dyngroup_prefix: username
```

SMB Signing

SMB signing provides mutual authentication and message authentication capabilities for the AIX Fast Connect server. During session setup, mutual authentication requires the client prove its identity to the AIX Fast Connect server and the server to prove its identity to the client. Message authentication requires that even after the initial authentication, each message (or SMB packet) is also validated through a digital signature.

By default, SMB signing is disabled on the AIX Fast Connect server. When disabled, no digital signing takes place. Clients that require SMB signing will fail to connect. To disable SMB signing, type:

```
net config /smbsigning:0
```

Enabling SMB signing on AIX Fast Connect will utilize SMB signing with any client that is enabled for SMB signing. Clients that are not enabled for SMB signing will continue to connect without any digital signing. To enable SMB signing, type:

```
net config /smbsigning:1
```

Requiring SMB signing on AIX Fast Connect will force SMB signing with all clients. If the clients are not enabled for SMB signing, they will not be able to connect to the AIX Fast Connect server. To require SMB signing, type:

```
net config /smbsigning:2
```

Client Configuration for SMB Signing

By default, most Microsoft Windows clients will be enabled to support SMB signing (when the server agrees). For recent versions of Windows, SMB signing can be configured in the security options (in Local Security Settings). See Microsoft Knowledge Base article 230545 to enable SMB signing in Windows 98, and article 161372 to enable SMB signing in Windows NT.

Notes:

1. Using SMB signing will incur a performance penalty, as each message (SMB) needs to be verified. Although it doesn't consume any more network bandwidth, it does use more CPU cycles on the client and server side.
2. SMB signing is supported only with local authentication using encrypted passwords.

CIFS Distributed File System (MSDFS) support

AIX Fast Connect supports CIFS Distributed File System (MSDFS) functionality for Windows clients. The AIX Fast Connect configuration option, **msdfs**, is used to enable this feature, and option **msdfs_ordering** can be used to further enhance this feature.

MSDFS allows multiple CIFS file-servers to be seamlessly integrated into one logical namespace, which results in the following:

- A single drive-mapping can be used to access multiple file-servers, possibly dispersed across the entire network.
- Multiple file-servers can be mapped to the same name, thus providing redundancy and locality of data-access.
- This complexity of logical and physical topology appears as a single directory-tree (drive-mapping), with sub-directories that may actually be located on remote servers.

MSDFS is organized as a topology of MSDFS *root* file-shares, which can contain MSDFS *links* to other local or remote file-shares. These MSDFS links appear as sub-directories, and so that transparent re-direction to the remote file-shares occurs, as long as the user is properly authenticated at the remote servers. (Windows client software manages the MSDFS re-direct and remote-server authentication.)

With the MSDFS feature enabled, AIX Fast Connect will treat all its file-shares as MSDFS root shares, except for the built-in file-shares. These are needed as non-MSDFS file-shares, as explained below.

MSDFS links contain one (or more) references to other file-shares, to which the link refers. AIX Fast Connect implements MSDFS-links as AIX soft-links, using a special syntax. For example, to create a MSDFS-link **link1** for AIX Fast Connect that points to remote file-share **\\server1\share1**, type the following command:

```
ln -s msdfs:server1\\share1 link1
```

This will create a soft-link `link1 -> msdfs:server1\share1`, which is the correct syntax that AIX Fast Connect.

A single MSDFS-link can point to multiple references, by separating them with commas. For example, the following command will create multiple references:

```
ln -s msdfs:server1\\share1,server2\\share2,server3\\share3 link3
```

This will create a MSDFS-link `link3` that contains three MSDFS-referrals: `server1\share1`, `server2\share2`, and `server3\share3`.

Note: A PC-client accessing this MSDFS-link would receive all three referral-references, and would then be able to choose whichever referrals it wanted to access. (The AIX Fast Connect MSDFS-server will always send all referrals specified in the MSDFS-link, but if the **msdfs_ordering=1** option is used, the order will be rotated on every query. This can potentially reduce bottlenecks on the network, by distributing the data-access workload across multiple file-servers. However, PC-clients will still tend to use file-servers that they are already connected to.

The syntax Fast Connect uses for MSDFS-links provides the following benefits:

- MSDFS-links can be placed anywhere within an AIX Fast Connect MSDFS file-share, which may help to provide flexibility of design.
- SAMBA-server uses this same syntax for MSDFS-links, thus allowing easy transitions to and from SAMBA-server installations.

To enable the MSDFS feature for Fast Connect, type:

```
net config /msdfs:1
```

To disable the MSDFS feature for AIX Fast Connect, type:

```
net config /msdfs:0
```

To allow the MSDFS multi-referrals to be rotated, to potentially balance the workload, type:

```
net config /msdfs_ordering:1
```

To keep MSDFS multi-referrals constant (original order only), type:

```
net config /msdfs_ordering:0
```

Notes:

1. Re-direction to a remote file-server is only successful if the current user credentials are recognized by the remote server. MSDFS operates optimally if the PC-user's login user name and password are recognized as valid on all file servers being accessed; otherwise, authentication errors will occur, and the user may not be given the opportunity to re-authenticate with different user-credentials.

   One possible workaround to this issue is to pre-map a file-share to each file server that needs special user credentials (other than the logged-in user name and password). In this case, the MSDFS redirect proceeds smoothly because the PC-client already has an established session with the target file-server.
2. MSDFS is not supported on Windows 98.

Changing Passwords Remotely

AIX Fast Connect supports two methods for users to change their AIX Fast Connect encrypted passwords and, optionally, their AIX password from remote locations. These methods are described below.

cifsPasswd Command

The **/usr/bin/cifsPasswd** command is provided with AIX Fast Connect to allow users to change their own encrypted password without having root authority. To use this command, a telnet or other AIX-login session is required.

For details, see "cifsPasswd Command" on page 75.

Web-based System Manager

CIFS passwords can be changed using Web-based System Manager.

Remote Password Change

If AIX Fast Connect is being used as a Network Logon Server, the Remote Change Password feature can be used. This feature allows Windows 98 clients to change their AIX Fast Connect passwords from a remote location using the Passwords applet in the Control Panel application. The Windows 98 clients must be configured for network logon to the AIX Fast Connect server using either the Microsoft Client for Microsoft Networks or the IBM Network Client for IBM Networks (if the IBM Network Client for IBM Networks is being used, AIX Fast Connect must be configured to use plain-text passwords).

Remote password change is not supported from clients running Windows NT-based operating systems. In addition, remote password change is ignored if network logon is disabled. For more information about network logon, see “Network Logon to AIX Fast Connect” on page 29. Remote password change does not work with NT-passthrough authentication.

If User-name mapping is being used, only server user names can use remote password change.

Follow these procedures to enable or disable remote password change:

- To enable remote password change, type the following:
  ```
  net config /remote_password_change:1
  ```
- To disable remote password change, type the following:
  ```
  net config /remote_password_change:0
  ```

sync_aix_password Option

If remote password change is enabled, the **sync_aix_password** option can also be enabled. When the **sync_aix_password** is enabled, every successful remote password change will also change the AIX password for that user name. This functionality is useful in environments where the Windows 98 users frequently log in to the AIX server using tools such as telnet and FTP. The **sync_aix_support** feature is ignored if network logon is disabled.

Follow these procedures to enable or disable **sync_aix_password**:

- To **enable sync_aix_password**, type the following:
  ```
  net config /sync_aix_password:1
  ```
- To **disable sync_aix_password**, type the following:
  ```
  net config /sync_aix_password:0
  ```

AIX Fast Connect User Management and File Access

AIX Fast Connect provides several additional features for file access and user management, which are described in the following sections.

User-Session Management Using the net session Command

AIX Fast Connect supports the **net session** command, for displaying and managing logged-in user sessions.

- To display all connected user sessions, type:
  ```
  net session
  ```
- To display all share resources currently mapped by a specific session, type:
  ```
  net session /user:username /workstation:IPaddress /shareinfo
  ```
- To display all open files for a specific session, type:
  ```
  net session /user:username /workstation:IPaddress /fileinfo
  ```
- To abort a user’s session, type:
  ```
  net session /user:username /workstation:IPaddress /close
  ```
- To close a user’s share-mapping, type:
  ```
  net session /user:username /workstation:IPaddress /close /netname:sharename
  ```
- To close a user’s file, type:
  ```
  net session /user:username /workstation:IPaddress /close /file:filename
  ```

Note: The `workstation` parameter also works with NetBIOS names.

Establishing Resource Limits

AIX Fast Connect provides several parameters to specify limits on resource use:

maxusers	Maximum number of user sessions (logins), at any given time
maxconnections	Maximum number of connections to a single share-resource
maxopens	Maximum number of open files allowed
maxsearches	Maximum number of open file searches
autodisconnect	Autodisconnect time for idle sessions (in minutes)

For more details, see “net Command” on page 61 or Appendix B, “Configurable Parameters for the net Command,” on page 79.

Disk Quotas

AIX Fast Connect supports disk quotas (user limits on disk space) when the **bos.sysmgt.quota** file is installed and configured. No additional configuration of AIX Fast Connect is necessary.

Auditing File Access

The **audit** system command can be used to log all file operations from AIX Fast Connect clients. To display this file activity by Real User Name rather than by Login ID, use the following command:

```
auditpr -h e,r,R,t,c
```

No additional configuration of AIX Fast Connect is necessary.

Changing the umask

AIX Fast Connect provides a *umask* global parameter to control permission bits on all files created by all AIX Fast Connect users. The *umask* parameter is specified as an octal number (with a leading zero), and defaults to 022.

To change the umask to 002, type:

```
net config /umask:002
```

Specifying Per-Share Options

Several advanced features of AIX Fast Connect are available as per-share options. These options are encoded as bit fields within the `sh_options` parameter of each share definition. These options must be defined when the share is created with the **net share /add** command.

Per-share options currently allowed by **net share /add** are as follows:

Parameter	Values	Default	Description
sh_oplockfiles	(0,1)	1	Enables opportunistic locks (oplocks and level II oplocks) on this share, if **oplockfiles=1**
sh_searchcache	(0,1)	0	Enables search caching on this share, if **cache_searches=1**
sh_sendfile	(0,1)	0	Enables SendFile API on this share, if **send_file_api=1**
mode	(0,1)	0	Allows ReadWrite access to this share. (1 indicates ReadOnly mode.)

Example: To create a ReadOnly share that has SendFile enabled, type:

```
net share /add /netname:ROSHARE /path:/usr/etc /mode:0 /sh_sendfile:1
```

Support for AIX JFS Access Control Lists

AIX Access Control Lists (ACLs) allows extended control of files and directories of the AIX Journaled File System (JFS). AIX Fast Connect exploits this features by honoring AIX ACLs.

AIX Fast Connect extends this support by implementing ACL inheritance for AIX Fast Connect file shares. This feature can be used to implement default ACLs for created file objects. When ACL inheritance is enabled, the *umask* parameter is not effective.

ACL inheritance is enabled by setting the **acl_inheritance** option to 1. This option can be viewed and changed using the **net config** command. After it is enabled, it applies to *all* the AIX Fast Connect file shares.

ACLs are inherited from the ACL defined on the base directory of the share. For example, if you have a share named TEMP mapped to the AIX directory `/tmp` (assuming a valid ACL is defined for this directory and `acl_inheritance=1`), all files created in this share now inherit the ACLs defined for `/tmp`.

- To enable ACL inheritance for all AIX Fast Connect file shares, type:
  ```
  net config /acl_inheritance:1
  ```
- To disable ACL inheritance for all AIX Fast Connect file shares, type:
  ```
  net config /acl_inheritance:0
  ```
- To view the current setting of the acl_inheritance option, type:
  ```
  net config /parm:acl_inheritance
  ```

Note:

- When the **acl_inheritance** option is enabled, you may also want to enable the **accesscheckinglevel** option to ensure file attributes are properly reported. However, enabling the **accesscheckinglevel** option does slow down performance of the AIX Fast Connect server.
- When the **acl_inheritance** option is enabled and the **Dos_Attribute_Mapping** option is also enabled, any execute permissions resulting from the extended ACLs do not control execute permissions on those files, but are used to encode the DOS file attributes instead. The **Dos_Attribute_Mapping** option is enabled by default.

NT ACL Support (ACL mapping)

AIX Fast Connect supports NT-style ACLs (as displayed in the security tab of the file properties in Windows Explorer).

This support has the following requirements:

- Passthrough authentication must be enabled for AIX Fast Connect. For details, see “NT Passthrough Authentication” on page 29. The passthrough authentication server must be either a Windows domain controller, or a Windows Active Directory server.
- Dynamic User Creation must be enabled. To enable dynamic user creation, type:
  ```
  net config /dynuser:1
  ```
- ACL Mapping must be enabled. To enable support for ACL mapping, type:
  ```
  net config /acl_mapping:1
  ```

  ACL Mapping (acl_mapping) is mutually exclusive with ACL inheritance (acl_inheritance) and DOS file attribute mapping (dosattrmapping). These features should be disabled when ACL Mapping is enabled.

Notes:

1. When adding group or user names (through the Windows security tab), a password dialog box may appear to confirm credentials. The credentials should be filled in as follows:

User name: *ComputerName**User*
Password: *User's Password*

where *ComputerName* is the name of the local workstation (which can be obtained using ″net config workstation″ from DOS), and *User* is the name used to map to the AIX Fast Connect share (may or may not be the same as the logged-in user).

2. Currently, browsing AIX Fast Connect users and groups through the security tab on client PCs will display the **user** icon to the left of both users and groups.
3. AIX Fast Connect support for NT ACLs (basic and advanced) functions only with Windows 2000, XP, and 2003 clients. Windows NT 4.0 clients are not supported.

Support for basic NT ACLs

The CIFS server supports basic NT Access Control Lists (ACLs) by mapping them to the underlying JFS file system's own ACLs.

NT ACLs will be mapped to the JFS base permissions for owner and group when setting permissions for the owner or group of that file. When setting permissions for other users and groups (not owner or group of that file), NT ACLs will be mapped to the JFS ACLs. Due to differences between JFS ACLs and NT ACLs, certain permissions may not be honored in the same way. The **deny** setting is mapped as an absence of permissions. The following table shows the mapping of NTFS permissions to JFS permissions:

Permission	Permit	Deny
Full control	+r +w +x	-r -w -x
Modify	ignored	ignored
Read and execute	+r +x	-r -x
Read	+r	-r
Write	+w	-w
Special permissions	ignored	ignored

Note: Delete, Change Permissions, and Take Ownership permissions are ignored.

Support for Advanced NT ACLs

On AIX 5.3 and above, with the JFS2 filesystem, AIX Fast Connect supports NT advanced ACLs. This support allows AIX Fast Connect to utilize the additional ACLs that are displayed when advanced button is selected from the security tab (of file properties in Windows Explorer). The option to inherit permissions from the parent is also supported with this feature.

With earlier versions of AIX (or on non-JFS2 file systems), support of NT ACLs is limited to the basic ACLs displayed in the security tab of the file properties (through Windows Explorer).

Notes:

1. We do not support the ″Take Ownership″ permission.
2. If files are moved from a JFS2 to non-JFS2 filesystem, the advanced ACLs will be converted to basic ACLs. Conversion will be done by the ACL engine on AIX and not by AIX Fast Connect. Also, any ACL Inheritance information will be lost.

Sending Messages to Clients

When necessary, the AIX Fast Connect administrator can use the **cifsClient** command to send messages to individual workstations, or to all user sessions connected to AIX Fast Connect.

- To send a message to all users connected to AIX Fast Connect, type:

  ```
  cifsClient send -a -m "message"
  ```

- To send a message to a specific computer, type:

```
cifsClient send -c computer -m "message"
```

- To send a message to a specific connected user, type:

```
cifsClient send -u username -m "message"
```

- To send a message to a NetBIOS domain, type:

```
cifsClient send -d domainname -m "message"
```

Notes:

1. A file may be sent as the message using the **-f** *filename* option, or the message can be read from standard input.
2. The *domainname* is optional. The default domain is the AIX Fast Connect server's domain.
3. The target computer must be enabled to receive messages, using messaging software. On Windows NT clients, the messaging service is started by default. To start the messaging service on Windows 98, run the following command:

   ```
   WIN95> winpopup
   ```

4. When share-level security is enabled (**share_level_security=1**), the user-specified messaging command **cifsClient send -u username** is not supported.

Mapping Long AIX File Names to 8.3 DOS File Names

Older PC client operating systems do not support long file names. This restriction is also true for many older (16-bit) applications running under Windows 98, and Windows NT. This restriction requires mapping long names of AIX files to DOS file name format. (The DOS format is also called *8.3* format because file names are limited to a maximum of eight characters followed by a period and a three-character extension.)

Simply truncating a long name to a shorter name is not the solution, because multiple files could get mapped to the same name whenever the first eight characters are same. AIX Fast Connect maps AIX file names (AFN) to DOS File Names (DFN), ensuring file-name uniqueness. It maps AFNs to DFNs using the Microsoft Windows NT method for mapping names (that is, name conflicts are handled by using a delimiting character in the short name, followed by a unique numeric to make the name unique).

For example, consider two files in the root directory of an exported SMB share:**LongFileName1.txt** and **LongFileName2.txt**. Assume a 16-bit application mounts this share and searches the directory. The resulting file names are as follows:

```
LONGFI~1.TXT for LongFileName1.txt
LONGFI~2.TXT for LongFileName2.txt
```

AIX Fast Connect generates a mapped name whenever the AFN must be passed back to a DOS client. DFNs generated by AIX Fast Connect are not remembered across server restarts. File-name mappings remain consistent until the AIX Fast Connect server is restarted.

AIX Fast Connect can be configured to turn off the mapping. When the mapping is turned off, no mapping is attempted. When disabled, any mapping of long names must be done by the PC client software.

- To enable file-name mapping (default), type:

```
net config /dosfilenamemapping:1
```

- To disable file-name mapping, type:

```
net config /dosfilenamemapping:0
```

Notes:

1. AFN-to-DFN mapping might not map correctly if the server restarts. Given the previous example, assume a user opens **LONGFI~1.TXT**, edits it, and saves the changes. Then the server shuts down. Someone then removes**LongFileName1.txt** from the server file system. After the server is up and running, the user on the client again edits **LONGFI~1.TXT**. This time, however, the same file maps to

LongFileName2.txt, not the previously deleted file name, and the client edits the wrong file. To prevent this situation, after the network drive is reconnected following server restart, new file lists must be obtained before accessing any mapped names.

2. If your site does not need this feature, disable the **dosfilenamemapping** option to reduce memory and CPU usage and thereby improve performance.
3. It is recommended to have the **dosfilenamemapping** option enabled if 16-bit applications or DOS is being used. Leaving the **dosfilenamemapping** option disabled in these environments can lead to unpredictable results and is neither recommended nor supported.

Support for DOS File Attributes

AIX Fast Connect provides optional support for the ReadOnly, Archive, System, and Hidden file attribute bits of DOS files. These bits are encoded by AIX Fast Connect into the AIX file-permission bits of the AIX file system.

- The ReadOnly attribute is encoded by turning off the AIX User/Group/Other Write bits. (**chmod a-w** *filename*)
- The Archive attribute is encoded by turning on the AIX *User* Execute bit. (**chmod u+x** *filename*)
- The System attribute is encoded by turning on the AIX *Group* Execute bit. (**chmod g+x** *filename*)
- The Hidden attribute is encoded by turning on the AIX *Other* Execute bit. (**chmod o+x** *filename*)
- For directories, AIX Fast Connect does not support the Archive, System, or Hidden attributes — only the ReadOnly attribute is supported. (AIX directories use the Execute bits to allow change directory permission, so AIX Fast Connect does not use these bits on exported directories.)

AIX Fast Connect automatically handles these bits in the AIX file system; the examples listed above simply show how AIX Fast Connect interprets these AIX-permission bits, when reporting DOS file attributes to a PC client. If you have AIX Fast Connect configured to support DOS file attributes (the default), you might need to manually turn *off* the Execute bits in your AIX directories that are being exported as AIX Fast Connect file shares.

- To clear the Execute bits on files (in an entire ***dirname*** tree), so that these files are not listed as System or Hidden, type:

  ```
  find dirname -type f -exec chmod a-x "{}" ";" -print
  ```

- To disable support for Archive, System, and Hidden bits, type:

  ```
  net config /dosattrmapping:0
  ```

Specifying NetBIOS Aliases for HACMP support

AIX Fast Connect supports server-name aliases, which allows a AIX Fast Connect server to respond to multiple NetBIOS server names. This feature is helpful in HACMP mutual takeover. Server aliases can be configured using the **net name** command, as follows:

- To show the primary AIX Fast Connect server name, type:

  ```
  net config /parm:servername
  ```

- To list ***alias*** server names, type:

  ```
  net name /list
  ```

- To add an alias server name (for example, *sname2*), type:

  ```
  net name /add sname2
  ```

- To delete an alias servername (for example, *sname2*), type:

  ```
  net name /delete sname2
  ```

Server aliases normally use NetBIOS subcodes 0x00 and 0x20, but other subcodes can be specified, for example:

```
net name /add test3 /sub:03
net name /delete sname2 /sub:2f
```

Notes:

1. Whenever adding or deleting an alias name without specifying a subcode, or if subcode 0x00 or 0x20 is specified, the alias name is added or deleted with subcodes 0x00 and 0x20.
2. The **net name /list** command uses angle brackets (″<″,″>″) to show subcodes other than 0x00 and 0x20.
3. To register alias name(s) to WINS or NBNS (including the local NBNS), the IP address of the WINS or NBNS server needs to be specified in the *primary_wins_ipaddr* or *secondary_wins_ipaddr* parameters.
4. When adding an alias name:
   - If someone on the same subnet is currently holding the name, adding fails.
   - If no one on the same subnet is holding the name, but it exists in name table of the NBNS, the name cannot be registered to the NBNS, but is still added to the local name table.

Browse Master Support

AIX Fast Connect supports Browse Master functionality. This feature, when enabled, allows AIX Fast Connect to act as a data repository for network browse information for support of Network Neighborhood, My Network Places, and NET VIEW.

- **Enable Browse Master support** by typing:

  ```
  net config /browsemaster:1
  ```

- **Disable Browse Master support** by typing:

  ```
  net config /browsemaster:0
  ```

Notes:

1. Whenever Network Logon support is enabled, Browse Master support is automatically enabled regardless of the **browsemaster** setting. Browse Master support is needed for support of Network Logon. If AIX Fast Connect cannot successfully register as Browse Master, the Network Logon feature is automatically disabled.
2. AIX Fast Connect maintains browse information only for its own local subnets (based on IP interface definitions).
3. AIX Fast Connect maintains browse information only for its own local domain/workgroup (based on the **domainname** option.

DBCS and Unicode Considerations

Following are some DBCS and Unicode considerations:

- Share names and share descriptions must be in ASCII.
- The **LC_MESSAGES=C&lft** environment variable does not support multibyte characters. If AIX Fast Connect is running in a multibyte environment and the **LC_MESSAGES** environment variable 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. When **/etc/rc.cifs start** is used to start the AIX Fast Connect server, the **LC_MESSAGES** environment variable is automatically set to match the **LANG** environment variable.
- Prior to AIX Fast Connect version 3.1.0.1 (and 2.1.1.51), there were several Japanese characters that were not supported because of differences in Unicode mapping between Microsoft ms932 and IBM cp943. These are as follows:

Table 3. Different SJIS codes, MS codes, and IBM codes that resolve to the same character.

SJIS code	MS code	IBM code	Character name
815C	2015	2014	EM DASH
8160	FF5E	301C	WAVE DASH
8161	2225	2016	DOUBLE VERTICAL LINE
817C	FF0D	2212	MINUS SIGN

Table 3. Different SJIS codes, MS codes, and IBM codes that resolve to the same character. (continued)

SJIS code	MS code	IBM code	Character name
FA55	FFE4	00A6	FULL WIDTH BROKEN BAR

These characters (and any other Unicode conversions needed) are supported by the AIX Fast Connect **double_byte_char** configuration parameter . To configure AIX Fast Connect to support Japanese characters, run the following command:

```
net config /double_byte_char:"0x20152014 0xFF5E301C 0x22252016 0xFF0D2212 0xFFE400A6"
```

- Each grouping in the parameter string specifies a single character conversion between MS and IBM.
- These hexadecimal numbers may be separated by spaces or tabs only.
- Any invalid token invalidates the entire string. An error message will be recorded in the **/var/cifs/cifsLog** file and the Unicode mapping feature is disabled.

- The AIX language locale is which AIX Fast Connect was started is significant. File names created in one language locale may not be recognizable or usable from a different language locale.
- If AIX Fast Connect is started in a non-Unicode (DBCS) language locale, the following source Unicode characters are not fully supported on AIX Fast Connect. These source Unicode values have no corresponding DBCS equivalents.

  System conversion routines effectively remap these source Unicode values to their target Unicode values, which do each have their own DBCS equivalents.

Table 4. The Target Unicode, Target JIS, and TARGET SJIS that each Source Unicode maps to.

Source Unicode	Target Unicode	Target JIS	Target SJIS
555E	5516	3022	88A0
7130	7114	316B	898B
9DD7	9D0E	322A	89A8
5699	565B	337A	8A9A
4FE0	4FA0	3622	8BA0
8EC0	8EAF	366D	8BEB
7E6B	7E4B	3752	8C71
9E7C	9E78	3834	8CB2
9EB4	9EB9	396D	8D8D
5C62	5C61	3C48	8EC6
7E61	7E4D	3D2B	8F4A
8523	848B	3E55	8FD3
91AC	91A4	3E5F	8FDD
6414	63BB	415F	917E
7626	75E9	4169	9189
6451	63B4	444F	92CD
5861	586B	4536	9355
985A	985B	453F	935E
79B1	7977	4578	9398
7006	6D9C	4642	93C0
56CA	56A2	4739	9458
6F51	6E8C	482E	94AC
91B1	9197	4830	94AE

Table 4. The Target Unicode, Target JIS, and TARGET SJIS that each Source Unicode maps to. (continued)

Source Unicode	Target Unicode	Target JIS	Target SJIS
9830	982C	4B4B	966A
9EB5	9EBA	4C4D	96CB
840A	83B1	4D69	9789
881F	874B	4F39	9858
6522	6505	5A39	9DB7
00A6	FFE4	9336	FA55

If AIX Fast Connect is started in a Unicode–based language locale, all of these source values are supported without any remappings being performed.

Using ATM Interfaces

- Using the **at#** (Classical IP) interfaces

  These interfaces do not support TCP/IP broadcast IP addresses. Therefore, several inconsistencies related to NetBIOS protocols that use broadcast messages may result. When using any **at#**, filterbroadcast must be enabled.
- Using the **atmle** (LAN_emulation) drivers

  These drivers emulate standard Ethernet interfaces and support the TCP/IP broadcast messages used by NetBIOS. However, the default ATM–Lane installation supports only 32 simultaneous sessions over one ATM line. This is not sufficient for most AIX Fast Connect environments. Whenever a new TCP/IP session is requested, one of the oldest previous sessions gets disconnected, which can lead to thrashing sessions. This situation is solved by increasing the ATM arp cache parameter to 1000 in the SMIT panel for ATM.

Limiting memory usage with the maxthreads parameter

The AIX Fast Connect **cifsServer** process, like all 32 bit processes, is limited to 4 gigabytes of memory. Of this, 2 gigabytes are available for the heap. Each **cifsServer** thread will consume approximately 1/2 Mb of memory (heap), so the number of client connections could eventually consume all available heap space for **cifsServer**. Two different methods of thread utilization for **cifsServer** are offered in order to allow more flexibility in tuning AIX Fast Connect.

Dedicated thread per connection

By default, the main AIX Fast Connect process (**cifsServer**) uses one dedicated thread per client connection. This design may offer improved performance, but can consume large amounts of memory in environments with thousands of users. This default behavior is optimal for most environments, and is enabled when either of the following is true:

- The value of the **maxusers** parameter is 0 (unlimited)
- The value of the **maxusers** parameter is less than or equal to the **maxthreads** (2048 by default)

Dedicated thread per request

By tuning the **maxthreads** and **maxusers** parameters, the behavior of the **cifsServer** parameter can be modified to use one thread per incoming request (rather than a dedicated thread per connection). This way, you can limit the number of threads (thus limiting memory usage), but still allow thousands of client connections. In this case, the **maxthreads** parameter will limit the number of simultaneous requests that can be processed. This may result in slightly slower performance overall, and may cause some delays when the current number of simultaneous requests is greater than the value of **maxthreads**. This behavior may be useful for managing memory usage in environments with thousands of users, and is enabled when the value of the **maxusers** parameter is greater than the value of the **maxthreads** parameter.

Opportunistic Locking

This feature enables some clients to perform read-ahead and write-behind caching through the use of opportunistic locks (oplocks). AIX Fast Connect supports oplocks and level II oplocks, which can be enabled and disabled with the **oplockfiles** parameter (see **oplockfiles**, in Appendix B, "Configurable Parameters for the net Command," on page 79). Further explanation of opportunistic locking can be found in Microsoft Knowledge Base Article 129202.

Opportunistic locking has the following advantages:

- In environments where files are not frequently opened by more than one user at a time, users may benefit from read-ahead and write-behind caching (when granted an oplock).
- In environments where files may be opened by multiple users but are not frequently written to, users may benefit from read-ahead caching (when granted a level II oplock).

Opportunistic locking has the following disadvantages:

- In environments where files are frequently accessed by more than one user at a time, the overhead involved with oplocks could outweigh any benefits from caching.
- If the shared files are being accessed outside of AIX Fast Connect (such as NFS or AIX applications), then oplocks may not be properly honored. This can be corrected by enabling the **oplock_unix_lock** (see **oplock_unix_lock** in Appendix B, "Configurable Parameters for the net Command," on page 79). If frequent access of the files outside of AIX Fast Connect is expected, the benefits of oplocks may not be seen, and the **oplockfiles** parameter should be disabled.

Notes:

1. Users cannot explicitly request an oplock. Requesting of oplocks is handled automatically by the redirector on the client PC.
2. Oplocks can be enabled and disabled on a per share basis. See "Specifying Per-Share Options" on page 40.
3. In some cases, client PCs may not respond to the AIX Fast Connect server's request to release an oplock. If this happens, the AIX Fast Connect server will wait for a given amount of time (specified by the **oplocktimeout** parameter) before allowing other clients to access the file.

Performance Considerations

This section discusses several issues affecting AIX Fast Connect performance.

Large Directories

Directory enumerations are frequent network operations on Windows clients. Whenever Network Neighborhood (or Windows Explorer) opens a network directory, that entire directory is enumerated over the network, for display in a Explorer window. Windows Explorer usually waits to display the contents of the window until the entire network directory has been listed. 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.

Try to prevent your AIX Fast Connect users from having to access large directories to get to the network files they need. One possible solution is to define smaller-sized AIX directories to be exported by AIX Fast Connect. These directories can contain links to files in the large directories.

If large directories are needed but rarely change (for example, CD-ROM), you might find the search caching features useful.

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 file name is performed. (For example, simply opening a document in Microsoft Word can cause multiple directory searches for that file name.)

The AIX Fast Connect search-caching feature 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 can enhance performance.

Search caching is implemented in AIX Fast Connect by taking snapshots of directories and their modification times, as follows:

1. When AIX Fast Connect needs to perform a directory search, AIX Fast Connect first checks its search cache (if enabled).
2. If a search-cache entry is found, it is first validated. If that directory's current modification time is different from the cached time, the feature determines that the cache entry is not valid.
3. Whenever the search-cache table is full, older entries are deleted to make space for new entries.

Search caching is configured on AIX Fast Connect by the following parameters:

Parameter	Default	Description
cache_searches	0 (disabled)	Globally disable the search-caching feature. (Set to 1 to enable.)
sh_searchcache	0 (disabled)	Disable search caching on a per-share basis. (Set to 1 to enable.)

Note: To enable search caching on any file shares, the *cache_searches* parameter must be enabled (set to 1), and the *sh_searchcache* parameter must be enabled for every file share for which search caching is desired.

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 the following:

Parameter	Default	Description
send_file_api	1 (enabled)	Flag to enable/disable the SendFile API to be used by AIX Fast Connect. Default is enable. To disable SendFile, set to 0.
send_file_cache_size	0 (disabled)	Maximum Read-Request size that is cached by the SendFile API.
send_file_size	4096	Minimum Read-Request size, before SendFile API is used.
sh_sendfile	0 (disabled)	Flag to enable/disable per-share option. Default is disable. To enable SendFile for that file share, set to 1.

Notes:

1. To enable SendFile API on any file shares, the *send_file_api* parameter must be enabled, and the *sh_sendfile* parameter must be enabled for every file share for which the SendFile API is desired.
2. For systemwide SendFile configuration parameters, see the **no** command.

Memory-Mapped Files

AIX Fast Connect can be configured to use AIX memory-mapped files during CIFS read and write operations. This feature is enabled with the **mmapfiles** configuration option. By default, it is disabled.

- To enable the Memory-Mapped files feature, run the following:

  ```
  net config /mmapfiles:1
  ```

- To disable the Memory-Mapped files feature, run the following:

  ```
  net config /mmapfiles:0
  ```

Chapter 6. Configuring Network Logon

AIX Fast Connect can be configured to support Network Logon. Network Logon support allows centralizing the user accounts, startup scripts, home directories, and configuration policy of Windows systems participating in a workgroup to a single AIX system running the AIX Fast Connect server. This support does not allow an AIX Fast Connect server to act as a Windows NT Domain Controller. However, with the IBM Networks Client software, both Windows NT-based and Windows 98 clients can be configured to perform network logon to an AIX server using the Network Logon feature of AIX Fast Connect.

AIX Fast Connect Network Logon feature supports Windows 98, Windows NT, Windows 2000, and Windows XP clients. Network Logon support has not been added to AIX Fast Connect for Windows 2003 clients. Windows 98 clients are supported using the standard Microsoft Client for Microsoft Networks or the IBM Client for IBM Networks. Windows NT-based clients require the IBM Networks Primary Logon Client for NT.

IBM Network Client can be downloaded from the following IBM Internet sites:

- **http://service.boulder.ibm.com/asd-bin/doc/en_us/winntcl2/f-feat.htm** for the Windows NT-based logon client. (Use the Primary Logon Client rather than the Coordinated Logon Client.)
- **http://service.boulder.ibm.com/asd-bin/doc/en_us/win95cl/f-feat.htm** for Windows 98 clients.

Configuration Options

The following AIX Fast Connect configuration options are available for Network Logon feature customization.

Option	Default Value	Description
`networklogon`	`0`	This option is used to enable or disable the Network Logon feature of AIX Fast Connect — 1 indicates enabled, and 0 indicates disabled.
`startup_script`	`startup.bat`	This option specifies the file name of the startup script (in the NETLOGON share) used by the Microsoft Client for Windows 98 during network logon. Two metatags in this string allow customization of the startup script file name during client logon — `%U` is expanded to the client's user name, and `%N` is expanded to the client's computer name. (IBM Networks clients always search for filename **profile.bat**, in **\dcdb\users*username*** directory in the IBMLAN$ file-share.)
`profiles_path`	`/home`	This string option specifies the AIX pathname for the PROFILES share, which the Network Logon feature uses to store user profiles and home directories.
`netlogon_path`	`/var/cifs/netlogon`	This string option specifies the UNIX path to the top of the NETLOGON and IBMLAN$ shares. These shares are used to store the startup scripts. This is also where the Windows client searches for the configuration policy files at domain network logon time (for example: **\\Server\netlogon\config.pol**).

Enabling the Network Logon Feature

To enable domain network logon support, set the **networklogon** option to 1. This option can be enabled (or disabled) using Web-based System Manager, SMIT, or the **net** command. To enable the Network Logon feature, type:

```
net config /networklogon:1
```

Then restart the server. The AIX Fast Connect server then acts as a domain logon server for your workgroup.

Setting Up Startup Scripts

Startup scripts are DOS batch files that are executed automatically when client users log on to the domain through a domain logon server. Typically, these scripts are defined as user-specific. By default, AIX Fast Connect installs a sample startup script (**/var/cifs/netlogon/startup.bat**), which can be customized as needed as a global startup script.

For Windows 98 clients using the Microsoft Networks client, the default installation of AIX Fast Connect configures **/var/cifs/netlogon/startup.bat** as a global startup script for all these clients. The *startup_script* parameter can be modified for these clients to support per-user or per-workstation scripts:

- Setting *startup_script* to **%N.bat** specifies that each login from *workstation* look for a startup script *workstation*.BAT, (in **/var/cifs/netlogon**, the NETLOGON share), regardless of the login user.
- Setting *startup_script* to **%U.bat** specifies that every login from *username* looks for a startup script *username*.BAT, (in **/var/cifs/netlogon**, the NETLOGON share), regardless of the PC workstation used.
- Setting *startup_script* to **dcdb\users\%U\profile.bat** provides compatibility with workstations configured for the IBM Networks client software, so every login goes to that user's profile directory and executes the **profile.bat** startup script, regardless of which client software is configured.

For Windows 98 or Windows NT clients using the IBM Networks client, the IBM Networks client *always* uses **dcdb\users*username*\profile.bat** (in share IBMLAN$) as its startup script. By default, AIX Fast Connect sets **/var/cifs/netlogon/dcdb/users** as a link to the **/home** directory (which is also the default for *profiles_path*). This allows the user-specific **profile.bat** files to reside in those users' profile directories, which are also AIX-user home directories, by default.

To set up a global startup script for all users using the IBM Networks client (and provide compatibility with Microsoft clients), do the following:

1. Edit the **/var/cifs/netlogon/startup.bat** global startup script.
2. Create file links from **profile.bat** in every users' profile directory to the **/var/cifs/netlogon/startup.bat** file.

Setting Up Home Directories (Profile Directories)

Home directories, or *profile directories*, are used to store a Windows user's profile (**USER.DAT** and **USER.MAN**). Additionally, any application-specific settings and data are also stored in the Windows user's home directory. When the AIX Fast Connect server is configured as a domain network logon server, these home directories can reside on the AIX server.

AIX Fast Connect uses the *profiles_path* option to indicate where these profile directories are located. AIX Fast Connect expects the directory specified by *profiles_path* to contain a subdirectory for each AIX Fast Connect user. By default, AIX Fast Connect configures *profiles_path* to be **/home**, where most AIX user directories are kept.

If you want to change *profiles_path*, you must create subdirectories for each AIX Fast Connect user, with ownership and read/write permissions per user.

Windows Configuration Policy Files

When the AIX Fast Connect server is configured to support domain network logons, Windows 98 and Windows NT configuration policy files can be placed in the directory specified by the *netlogon_path* option. If **CONFIG.POL** or **NTCONFIG.POL** exist in the NETLOGON share at logon time, the Windows client uses this policy file. By default, the location for these files is **/var/cifs/netlogon**.

Configuring Windows 98 Clients for Network Logon

If IBM Network Client is being used, Follow the steps described in the IBM Network Client software readme file.

If Microsoft Network Client is being used, select **Client for Microsoft Networks** as the default logon, and then change the Properties of this client software to log on to NT domains, using the AIX Fast Connect *domainname* as the NT-logon domain.

Configuring Network Logon for NT clients from Remote Subnets

The following are required to configure network logon from remote subnets:

- You must use encrypted passwords.
- The AIX Fast Connect logon server must have a domain name that is different from the NT domain controller's domain (if present), because the AIX Fast Connect logon server provides the logon services.
- If the client is not in the same subnet as the AIX Fast Connect logon server, you need either an LMHOSTS or an NBNS entry that maps AIX Fast Connect's *domainname*<00> to the AIX Fast Connect logon server. You also need the entry *domainname*<1C>, which is automatically registered to the NBNS by the AIX Fast Connect NetLogon server. (The AIX Fast Connect NBNS server allows you to add *domainname*<00> as an Internet group name.)
- For browsing to work correctly, you need at least one master browser (NT workstation, for example) to be in the same workgroup as the AIX Fast Connect server domain name, on each network segment.

The location of the LMHOSTS file varies depending on the system configuration. It can be found on the client by typing **dir /s lmhosts** from the Windows base directory. If this file does not exist on the system, the LMHOSTS.SAM default file can be copied to LMHOSTS and then modified.

An example of the LMHOSTS file follows:

```
192.1.2.3  fcserver    #PRE     #DOM:fcdomain  #AIX Fast Connect domain
192.1.2.3  "fcdomain       \0x00"  #PRE # 15 Bytes for the name, and
192.1.2.3  "fcdomain       \0x1C"  #PRE # the last byte is a hex subcode
```

These entries map the AIX Fast Connect name and domain to the server's IP address. The `#PRE` operative indicates that this is to be preloaded, and the `#DOM` operative indicates the domain this server maps to. The other text, following the '#' character is simply a comment statement. For more details on this file, see the comment section of the LMHOSTS file.

After changing the LMHOSTS file, the PC client must be restarted, or run the **nbtstat -R** command to refresh the local name table.

AIX Fast Connect NetLogon Limitations

The following restrictions apply to the AIX Fast Connect implementation of Network Logon:

- The AIX Fast Connect logon server must be configured in the same IP subnet as the NT clients running the IBM Network client, or else follow the steps described above.
- AIX Fast Connect must be configured to use encrypted passwords to provide logon services to NT clients.

- If the **multiuserlogin** option is enabled, Network Logon is not supported. These two options are mutually exclusive.
- If the **profiles_path** feature is set to a directory on DFS, the root user cannot automatically create subdirectories for each user when saving user profiles. To work around this problem, each user who wants to save a profile on DFS must manually create a directory named *profiles_path*/*username*/Profiles.
- Network Logon from Windows XP and Windows 2000 clients is supported using the IBM Primary Logon Client for Windows XP and Windows 2000. The IBM Network Client must be installed on the Windows NT, Windows 2000, or Windows XP workstation after all service packs have been applied. To install a service pack after the IBM Network Client has been installed, you must first uninstall the IBM Network Client. After installing the service packs, the IBM Network Client must be reinstalled.
- If Network Logon is enabled, Browse Master support is also enabled regardless of the **browsemaster** setting. Browse Master support is needed for support of Network Logon. If AIX Fast Connect cannot register as Browse Master, the Network Logon feature is automatically disabled. For more information on Browse Master, see “Browse Master Support” on page 45.
- The Network Logon feature supports Remote Password Change functionality for Windows 98 clients. For details, see “Changing Passwords Remotely” on page 38.
- Users cannot authenticate as guest users when logging in to their client workstations (using the Network Logon Server feature). However, users can still map to AIX Fast Connect as guest users once successfully logged into their client systems.

Chapter 7. Problem Determination and Limitations

This chapter contains information on solving AIX Fast Connect problems. The following topics are dicussed in this chapter:

Traces

To isolate problems, the AIX Fast Connect server can create AIX trace files. When a trace facility is active, information about selected events is recorded in the trace file. To obtain trace files, you must have the **trace** command installed on your machine. The **trace** command is in the **bos.sysmgt.trace** package.

The following trace hooks are used by the AIX Fast Connect server:

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 command line.

Using the SMIT interface, complete the following:

1. On the command line, type the **smit trcstart** fast path.
2. Select the CIFS hooks for ADDITIONAL event IDs to trace field, then exit SMIT. This action creates a trace file named **trcfile** in the **/var/adm/ras** directory (default).
3. Re-create the problem.
4. On the command line, type **smit trcstop**.
5. Exit SMIT.
6. On the command line, type **smit trcrpt** and select the output format.

Using the command line, complete the following:

1. On the command line, type the following:

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

   This action creates a trace file named **cifs.trace** in the **/tmp** directory.
2. Re-create the problem.
3. Type:

   ```
   trcstop
   ```
4. Type:

   ```
   trcrpt -t /etc/trcfmt /tmp/cifs.trace
   ```

   The **trcrpt** command formats the trace file into readable text and writes a report to standard output.

Logs

The AIX Fast Connect server writes information and error messages to a file in the **/var/cifs** directory named **cifsLog**.

Solutions to Common Problems

Following are some examples of common problems experienced while using AIX Fast Connect, along with some possible solutions.

Table 5. Actions to be taken when errors occur or when error messages are given.

Error or error message	Action to be taken

`access is denied`
`password is invalid`
`password is not correct`
`not authorized to login`
	• Enter the correct password.
	• Check logon user ID and its password on clients that should have an account on the AIX server. Log clients off and on with correct user ID and password.
	• For clients with Window NT with Service Pack 3 installed, the NET VIEW command returns `access is denied`. See "Enabling Windows Clients for Plain Text Passwords" on page 22 for more information.
	• For Windows 2003 clients, ensure that the client is configured for LM authentication (see "Configuring LAN Manager authentication level" on page 25.)
	
	Note: AIX Fast Connect does not support mixed-case passwords when **encrypt_passwords=0**.

`System error 53 has occurred.`
`The network path was`
`not found.`
	• Check the NetBIOS name of the AIX Fast Connect server.
	• Check server status.
	• See the "Connection Checking Procedure" on page 58.

`System error 51 has`
`occurred. The remote`
`computer is not`
`available.`
	When you get this error message on the client PC, check server status. It might be paused.

Connection Error when using a Passthrough Server	• Be sure the *passthrough_authentication_server* parameter is set to the IP Address (rather than the host name) by typing **net config /parm:passthrough_authentication_server**. • Test the network connection by pinging this machine. See "Connection Checking Procedure" on page 58. • Check that the *networklogon* or *guestlogonsupport* option is not being used. These options are mutually exclusive with passthrough authentication.
Cannot view Network Neighborhood from Entire Network on Windows clients	Each Windows Workgroup must have a master browser present for network browsing to work properly. By default, any Windows NT or Windows 98 client is set up to act as a master browser. The *domainname* parameter on the AIX Fast Connect Server determines which workgroup this AIX Fast Connect server is a member of.
Windows Primary Domain Controller reports that it cannot be started when AIX Fast Connect is running:	If the *networklogon* parameter is set to 1, the AIX Fast Connect server acts as the Logon Server for Windows 98 or Windows NT clients. Set this parameter to `0` if you do not want this behavior.

Client reports
`Account is not authorized to logon`
`from this station`
	Occurs when AIX Fast Connect is configured for plain-text passwords but the client has not been configured to support plain-text passwords. See "Enabling Windows Clients for Plain Text Passwords" on page 22.

Table 5. Actions to be taken when errors occur or when error messages are given. (continued)

Error or error message	Action to be taken
Server reports `Net:connect: A remote host refused an attempted connection`, `Can't start server: Operation could not be performed`, or similar message.	• Usually means the server cannot be started. Ensure the server has not started by running the `ps -ef | grep /usr/sbin/cifs` command. • Check for other services using the NetBIOS port or port 445 (`netstat -an | grep -e 139 -e 445`). • If services are found, this problem was caused by the current installation of an application using the NetBIOS ports (such as AIX Connections, SAMBA). The intruding application must be removed so the port can be made available to AIX Fast Connect. • Additionally, check to be sure you have sufficient disk space available in the **/var** file system by using the **df /var** command, and that sufficient paging space is available and active by using the **lsps -a** command.
Guest user cannot logon, Client reports `Unknown user or password` or similar error.	• Ensure *guestlogonsupport* is set to 1. • Ensure *guestname* is set to a valid AIX user. • Ensure that either the *guestname*'s AIX password is null, or that an AIX Fast Connect user is defined for *guestname* • Additionally, check that the **passthrough_authentication_server** option is not being used.
Client reports `The credentials supplied conflict with existing credentials` or similar error.	Client must log out and log on again with the user ID granting the desired access on the server. This usually happens when one client attempts to access the same server as two different users.
Client reports that it cannot create a file on the server.	• In most cases this is an AIX permissions problem. Check the AIX share path to ensure permissions are set correctly. (Also, if **acl_inheritance** is enabled, examine the AIX ACLs using the **acledit** command or a similar command. • If permissions are not the problem, check that the file system where the share exists has enough space by using the **df [share path]** command. • The administrator might want to log on to the AIX machine as the user who is having problems and attempt to create a file in the path that is causing problems.
Printing from client results in garbled printout	Some AIX back-end printer drivers add controls to the file that is being printed. Windows clients always send print jobs in a format that needs no controls. If your AIX printer driver adds controls, set the **-o -dp** printer share options when you create the printer share.
100% CPU usage occurs when starting AIX Fast Connect	Enable filterbroadcast, which will prevent AIX Fast Connect from potentially detecting broadcast messages from itself. See the **filterbroadcast** parameter in Appendix B, "Configurable Parameters for the net Command," on page 79.

Technical Service Information

If you need to contact technical support, the following information can help support personnel diagnose your problem.

- Your machine type
- Output from **oslevel** command - Operating System Level
- Output from **netstat -an** command - Network Information
- Output from **lsps -a** command - Paging Space Information

- Amount of memory on the machine
- **/etc/cifs/cifsConfig** - Server Configuration File
- **/var/cifs/cifsLog** - Server Error Log
- Output from **lslpp -l** command - Software Installed
- Full output from **errpt** and **errpt -a** commands - System Errors
- Output from **ps aux** and **ps -efl** commands - Process Listing
- Output from trace

The above information (other than trace output), can be automatically collected using the **/usr/sbin/cifsSnap** command. This command will collect information from the system that will be useful in diagnosing general problems related to AIX Fast Connect. This command requires root authority. It can be run as follows:

```
cifsSnap target_directory
```

where *target_directory* is the location where you want the results saved. This command will consolidate the information into a single tar.Z file

Additionally, it might be helpful to have full core enabled, especially in the event that the AIX Fast Connect server crashes. To enable a full core, use the **chdev -l sys0 -a fullcore='true'** command and ensure you have sufficient space in your root (**/**) file system.

Connection Checking Procedure

Follow these steps to complete the connection checking procedure:

1. Test the connection by **ping**ing the AIX Fast Connect server by IP address. If timeout occurs, check the following:
   - Cable for physical connection
   - Status of the AIX machine
   - TCP/IP configuration on clients and on the AIX server
2. Test the connection by **ping**ing the AIX Fast Connect server with its NetBIOS name. If it fails, see "NetBIOS Name Resolution" on page 20 for more information.
3. Check the server status on the AIX machine using **net config**, **net status**, and **net statistics** commands.

Usage Limitations

The following limitations apply to AIX Fast Connect:

- The maximum file size is limited by the underlying file system.
- All AIX user names that access AIX Fast Connect must have an AIX home directory specified. Otherwise, access is not granted to that user name.
- Users of other clients that do not support Unicode must ensure client and server locales match.
- AIX Fast Connect does not allow multiple printer share names for a single AIX print queue name. If you try to create a printer share for an AIX print queue that is already being mapped to another printer share, the system displays the message `Operation could not be performed.`
- Some AIX back-end printer drivers add controls to the file that is being printed. Windows clients always send print jobs in a format that needs no controls. Therefore, if your AIX printer driver adds controls, set the **-o -dp** printer share options when you create the printer share.
- Network Logon support is mutually exclusive to NT Passthrough Authentication. Network Logon is supported for Windows NT-based clients only through IBM Networks Primary Logon Client (http://service.boulder.ibm.com/asd-bin/doc/en_us/winntcl2/f-feat.htm).
- Share names and comments can only be in ASCII.

- The **LC_MESSAGES=C@lft** environment variable does not support multibyte characters. If AIX Fast Connect is running in a multibyte environment and the **LC_MESSAGES** environment variable 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.
- Windows XP limitations:
  - Switch user functionality under Windows XP requires the parameter **multiuserlogin** to be enabled. Use of Switch user without **multiuserlogin** can cause unexpected results.
  - With **multiuserlogin** enabled, several attempts may be required to successfully map a drive to the Fast Connect server from Windows XP.
- Opening a .bmp file from an AIX Fast Connect share via Adobe Image Ready 2.0 may fail. This is a current limitation of AIX Fast Connect.
- Using Microsoft Backup to restore files to an AIX Fast Connect share may produce errors and 0 byte files when performed as a user not belonging to the Administrators or Backup Operators group. This is a current limitation of AIX Fast Connect.

Appendix A. Command Descriptions

This appendix contains descriptions of the following commands:

net Command

Purpose

Configures and controls Fast Connect servers.

Syntax

net [**help** | **start** | **stop** | **pause** | **resume** | **config** | **status** | **statistics** | **trace** | **user** | **share** | **name** | **session** | **(NBNS subcommands)**]

Description

The **net** command configures and controls Fast Connect servers.

Subcommands

help	Displays help on the subcommand.
start	Starts the server.
stop	Stops the server.
pause	Stops the server temporarily.
resume	Resumes the paused server.
config	Lists and changes configuration parameters for the server.
status	Gives status of the server.
statistics	Gives statistics on server resources.
trace	Turns the server tracing on and off.
user	Lists, adds, deletes, and modifies user accounts on the server.
share	Lists, adds or deletes file and printer shares on the server.
name	Lists, adds, or deletes server name aliases.
session	Administer user sessions on the server.
nblistnames	Lists the NBNS name table.
nbbackup	Writes the NBNS name table to a file.
nbrestore	Restores the NBNS name table from a file.
nbaddname	Adds a NetBIOS unique name to the NBNS name table.
nbaddgroup	Adds a NetBIOS group name to the NBNS name table.
nbaddmulti	Adds a NetBIOS multihomed name to the NBNS name table.
nbdelname	Deletes a name from the NBNS name table.
nbaddingrp	Adds a NetBIOS internet group name to the NBNS name table.
nbdeladdr	Deletes an IP address in the NBNS name table of an NetBIOS internet group name.
nbstatus	Gives status of NetBIOS Name Server.

net help Subcommand

Syntax

net help *subcommand*

or

net *subcommand* **help**

Description

Provides help information about the *subcommand*s.

net start Subcommand

Purpose

Starts the server

Syntax

net start [**/load**]

Description

The **start** subcommand starts and initializes the server using parameters from the configuration file. It can start the server only if the server process is already loaded but the server is in stopped (not running) state.

> **Note:** Normally, instead of **net start /load**, use **/etc/rc.cifs start** to load and start the server, so that extra performance parameters are configured for AIX Fast Connect.

Flags

/load Loads the server process if it is not already loaded.

Return Codes

0 The server (%s) is already running.

0 The server (%s) has started successfully.

1 Syntax error was detected: Unknown keyword or command option (%s).

2 The server (%s) could not be started because its process was not running.

3 The request is not valid for the current state of the server (%s).

4 Operation could not be performed.

net stop Subcommand

Purpose

Stops and unloads the server process.

Syntax

net stop [**/unload**]

Description

The **net stop** subcommand stops and unloads the server. It can stop the server only if it is running or paused. After it is stopped, the server can be restarted using **/etc/rc.cifs start**.

Flags

/unload

Unloads the server process.

Return Codes

0 The server (%s) has stopped successfully.

0 The server (%s) has stopped and its process unloaded successfully.

1 Syntax error detected: Unknown keyword or command option (%s).

2 The request is not valid for the current state of the server (%s).

3 Error in unloading the server process on the server (%s).

4 Operation could not be performed.

5 Either **cifsUserProc** is not running or it could not be terminated.

net pause Subcommand

Purpose

Pauses the server

Syntax

net pause

Description

The **net pause** subcommand pauses the server. It can pause the server only if it is running. After it is paused, the server does not accept any new connections but continues serving the existing ones. It can be resumed with the **net resume** subcommand.

Return Codes

0 The server (%s) has paused successfully.

1 Syntax error detected: Unknown keyword or command option (%s).

2 The request is not valid for the current state of server

3 Operation could not be performed.

net resume Subcommand

Purpose

Resumes the server.

Syntax

net resume

Description

The **net resume** subcommand resumes the server. It can resume the server only if it is paused. After it is resumed, it starts accepting new connections.

Return Codes

0 The server (%s) has resumed successfully.

1 Syntax error detected: Unknown keyword or command option (%s).

2 The request is not valid for the current state of server

3 Operation could not be performed.

net config Subcommand

Purpose

Lists and changes the configuration parameters of the server.

Syntax1

net config

Syntax2

net config /component

Syntax3

net config /component:*cname* **/***parameter***:***value*

Syntax4

net config [**/listparm**] [**/component:***cname*] **/parm:***parameter*

Description

The **net config** subcommand lists and changes the configuration parameters of the server. For example:

Syntax1

Lists the configuration parameters.

Syntax2

Lists all the components or groups of configuration parameters for the server.

Syntax3

Adds or changes the given *parameter* for the given component *cname*.

Syntax4

Lists the entry for the given *parameter* for the given component *cname* from the configuration file.

Note: Only the root user can change configuration parameters.

Flags

/listparm

Lists the given parameter for the given component.

/component:*cname*

Specifies the component in the configuration file whose parameter needs to be added or changed. The default component is **smbserver**, the AIX Fast Connect server.

The *parameter* can be one of the following:

/maxconnections:*number*

Maximum number of connections to server resources. 0 specifies unlimited number.

/maxusers:*number*

Maximum number of users (sessions) that are permitted. 0 specifies unlimited number.

/autodisconnect:*number*

Timeout (in minutes) for inactive, unused sessions.

/maxopens:*number*

Maximum number of open files on the server. 0 specifies unlimited number.

/maxsearches:*number*

Maximum number of open searches on the server. 0 specifies unlimited number.

/servername:*s_name*

The name of the server.

/domainname:*d_name*

The name of the domain that the server belongs to.

/guestname:*g_name*

Logon name as guest on the server.

/passthrough_authentication_server:*pas_name*

The name of the passthrough authentication server.

/backup_passthrough_authentication_server:*bpas_name*
The name of the backup passthrough authentication server.

/primary_wins_ipaddr:*pwins_addr*
Specifies the dotted IP address of the primary WINS server.

/secondary_wins_ipaddr:*swin_ipaddr*
Specifies the dotted IP address of the secondary WINS server.

/wins_proxy:0|1
Specifies whether the server must act as WINS PROXY. Valid values are 0 for no and 1 for yes, with 0 as the default value.

/send_file_api:0|1
Specifies whether the **send_file** API is to be used. Valid values are 0 for off and 1 for on, with 1 as the default value.

/send_file_size:*sf_size*
If the **send_file_api** is 1 and the requested SMB read size is greater than the value of this parameter, **send_file** API will be used in the SMB operation. The value ranges between 1 and 4194304, with 4096 as the default value.

/send_file_cache_size:*sfc_size*
If the **send_file_api** is 1 and the requested SMB read size is less than the value of this parameter, the **send_file** API will cache the file. The value ranges between 0 and 4194304 with 0 as the default value, which means that the **send_file** API will not cache the file.

/umask:*u_mask*
umask. It is an octal value and ranges between 0 and 0777, with 022 as the default value.

/guestlogonsupport: 0|1
Specifies whether guest access is allowed. Valid values are 0 for no and 1 for yes, with 0 as the default value.

/dosattrmapping:0|1
If set to 1, Archive, System, and Hidden attributes will be mapped to user, group, and other execute bits, respectively. Otherwise, these attributes are not supported.

/dosfilenamemapping:0|1
If set to 1, long file names will be mapped to 8.3 format. Otherwise, long file names will be truncated.

/dosfilenamemapchar:*m_char*
The character used to map long file names to 8.3 format. Valid values are'~' and '^' with '~' being the default.

Return Codes

0 Command completed successfully.

1 Syntax error: Unknown keyword or command option (%s).

2 Command could not be executed. Invalid parameter value (%s).

3 Operation could not be performed.

Output for syntax1 command **net config**

```
Server Name                                 ........
Server Description                          ........
Server Software version                     ........
Domain Name                                 ........
Primary WINS IP Address                     ........
Secondary WINS IP Address                   ........
Passthrough Authentication Server           ........
Backup Passthrough Authentication Server    ........
Guest logon ID                              ........
```

Assuming that the smbserver has shares `FILE0` and `PRINT1` defined, and also has the following entries:

```
servername = fcserver
comment = Fast Connect server
```

Output for syntax2 command **net config /component**

```
smbserver
en
FILE0
PRINT1
```

Output for syntax4 command **net config /parm:servername**

```
fcserver
```

Output for syntax4 command **net config /parm:comment**

```
Fast Connect server
```

net status Subcommand

Purpose

Displays status of the server.

Syntax

net status

Description

The **status** subcommand displays status of the server, as either running, paused, or stopped.

Return Codes

0 Server (%s) is running.

1 Syntax error: Unknown keyword or command option (%s).

2 Server (%s) is not running.

3 Server (%s) has been paused.

4 Operation could not be performed

net statistics Subcommand

Purpose

Displays the statistics on server resource usage.

Syntax

net statistics [**/reset**]

Description

Lists the statistics on server resources since it was started, or it resets the statistics.

Flags

/reset Resets all statistic fields for the server.

Return Codes

0 Command completed successfully.

1 Syntax error: Unknown keyword or command option (%s).

2 Operation could not be performed.

Output

```
Server statistics for server (%s) since %s time
   Sessions started              .....
   Sessions timed out            .....
   Sessions dropped              .....
   Password Errors               .....
   Permission Errors             .....
   Bytes sent low                .....
   Bytes sent high               .....
   Bytes received low            .....
   Bytes received high           .....
   Request buffer failures       .....
   Big buffer failures           .....
   Print jobs queued             .....
```

net trace Subcommand

Purpose

Turns tracing on or off for the server.

Syntax1

net trace /on

Syntax2

net trace /off

Description

Turns tracing on or off for the server. The user does not have to start or stop the server.

Flags

/on Turns tracing on.

/off Turns tracing off.

Return Codes

0 Command completed successfully.

1 Syntax error: Unknown keyword or command option (%s).

2 Operation could not be performed.

net user Subcommand

Purpose

To list, add, delete, and modify AIX Fast Connect user accounts to support password encryption and client-to-server user-name mappings.

Syntax1

net user [*username* [{*password*|**-p**} [**/changeaixpwd:**{**yes**|**no**}]] [**/active:**{**yes**|**no**}] [**/comment:***text*] [**/serverUserName:***srvUserName*]] [/**longname**]

Syntax2

net user /add *username* {*password*|**-p**} [**/changeaixpwd:**{**yes**|**no**}] [**/active:**{**yes**|**no**}] [**/comment:***text*]

Syntax3

net user /delete *username*

Syntax4

net user /map *clientUserName srvUserName*

Syntax5

net user /showmapping:*username* [/**longname**]

Description

Syntax1 lists or modifies AIX Fast Connect user accounts.
Syntax2 adds a user on the server.
Syntax3 deletes the given user from the server.
Syntax4 maps a client user name to a server user name.
Syntax5 lists all the mappings related to the specified user name.

Parameters

username
The user name of the account to list, add, delete, or modify, either a client user name or a server user name.

clientUserName
The name of the user account on the client machine. The maximum length is 20 characters.

srvUserName
The maximum length is derived from the sysconf LOGIN_NAME_MAX value.

password
The password to be assigned or changed for the account. All client usernames that map to this server account will be affected.

-p Produces a prompt for the password. The password is not displayed when it is typed at the password prompt.

Flags

/add Adds a AIX Fast Connect user account to support encrypted passwords.

/delete
Deletes the given AIX Fast Connect user-name mapping or encrypted password support.

/changeaixpwd:{yes|no}
Change the system password of the user name to match the AIX Fast Connect user password. Requires root access.

/active:{yes|no}
Activates or deactivates the account. If the account is not active, the user cannot access the AIX Fast Connect server. The default is **yes**.

/comment:*text*
Provides a descriptive comment about the user's account. Enclose the text in quotation marks.

/serverUserName:*srvUserName*
The *username* specified is remapped to *srvUserName*.

/map Creates a user-name mapping from *clientUserName* to *srvUserName*.

/showmapping:*username*
Shows all the client-name mappings for the given user name.

/longname
Displays complete user names. Without this flag, long names may be displayed as truncated.

Note: This subcommand manages a user database file (**/etc/cifs/cifsPasswd**) specific to AIX Fast Connect, which is used only for user-name mapping and encrypted passwords. These two features operate independently, and are enabled/disabled by the **usernamemapping** and **encrypt_passwords** configuration parameters.

net share Subcommand

Purpose
To list, add and delete file shares or printer shares on the server.

Syntax1
net share [**/netname:***share_name*] [**/infolevel:***N*]

Syntax2
net share /add /netname:*share_name* [**/type:**{**file**|**f**}] **/path:***path_name* [**/desc:***share_desc*]
[**/ro_password:***password1*] [**/rw_password:***password2*]
[**/mode:***x*] [**/sh_oplockfiles:***x*] [**/sh_searchcache:***x*] [**/sh_sendfile:***x*]

Syntax3
net share /add /netname:*share_name* **/type:**{**printer**|**p**} **/printq:***qname* [**/print_options:***ostr*]
[**/desc:***share_desc*]

Syntax4
net share /delete /netname:*share_name*

Syntax5
net share /change /netname:*share_name* [**/ro_password:***password1*]
[**/rw_password:***password2*]

Description
Syntax1 lists one or more shares.
Syntax2 adds a file share to the server.
Syntax3 adds a printer share.
Syntax4 deletes a share from the server.
Syntax5 changes password(s) of a file share.

Note: To change a share, you must first delete it and then add it again, except for file-share passwords.

Flags

/add Adds a share to the server.

/delete
Deletes a share from the server.

/change
Changes properties of a file share.

/infolevel:*N*
Specifies the level of information desired. Default level is 1. Valid values are 0, 1, 2 and 99.

/type:*type*
Specifies the share type. Valid values are **file** (or **f**) and **printer** (or **p**). Default value is **file**.

/netname:*share_name*
Network name of the share. Without this option, all shares will be listed.

/path:*path_name*
Absolute AIX path name being exported by that **file** share.

/printq:*qname*
AIX print queue being exported by that **printer** share.

/print_options:*ostr*
String specifying printer options.

/desc:*desc*
Brief description of the share.

/ro_password:*password1*
Share-level security password for ReadOnly access. (Default is null.)

/rw_password:*password1*
Share-level security password for ReadWrite access. (Default is null.)

/mode:*x*
File-share access mode — 0:ReadOnly, 1:ReadWrite. (Default is 1.)

/sh_oplockfiles:*x*
Allows opportunistic locks to be used — 0:Disabled, 1:Enabled. (Default is 0.)

/sh_searchcache:*x*
Allows search-caching to be used — 0:Disabled, 1:Enabled. (Default is 0.)

/sh_sendfile:*x*
Allows SendFile API to be used — 0:Disabled, 1:Enabled. (Default is 0.)

Return Codes

0 Command completed successfully.

1 Syntax error: Unknown keyword or command option (%s).

2 Operation could not be performed.

3 Command could not be executed. Invalid value (%s) of parameter.

4 Syntax Error: The share path or queue name must be specified.

5 Error adding the share - share name already exists.

6 Error deleting the share - share name not found.

7 The configuration file could not be updated to reflect the current change.

Output for info level 0 :

```
netname1
netname2
...
netnameN
```

Output for info level 1 :

```
Share Name    Share Type    Path Name/Queue Name   Share Description
----------    ----------    --------------------   -----------------

netname1      File          /home/name/xxx         File Description
netname2      Printer       lpq1                   Printer Description
......        ......        ....                   ..........
netnameN      Printer       lpq2                   Printer Description
```

Output for info level 99 :

```
netname:%s:type:%s:path:%s:printq:%s:print_options:%s:desc:%s::
```

net name Subcommand

Purpose

To list, add, and delete AIX Fast Connect server aliases (alternate NetBIOS names).

Syntax1

net name [**/list**]

Syntax2

net name /add *aliasname* [**/sub:***value*]

Syntax3

net name /delete *aliasname* [**/sub:***value*]

Description

Syntax1 lists all server aliases (NetBIOS names).
Syntax2 adds a server alias (NetBIOS name).
Syntax3 deletes a server alias (NetBIOS name).

Flags

/list Lists all server aliases (NetBIOS names).

/add:*aliasname*
Adds a server alias (NetBIOS name).

/delete:*aliasname*
Deletes a server alias (NetBIOS name).

/sub:*value*
Allows any NetBIOS subcode, (hexadecimal 00 to FF), to be specified. Default is 00.

net session Subcommand

Purpose

To list and control user sessions connected to AIX Fast Connect.

Syntax1

net session [/longname]

Syntax2

net session /user:*Username* **/workstation:**{*IPaddress*|*NetBIOSname*} [**/fileinfo** | **/shareinfo**]

Syntax3

net session /user:*Username* **/workstation:**{*IPaddress*|*NetBIOSname*} **/close**
[**/file:***filename* | **/netname:***sharename*]

Description

Syntax1 lists connected user sessions.
Syntax2 lists files or resources in use by a connected user session.
Syntax3 closes a user session, or files or resources in use by a user session.

Flags

/user:*Username*
User name of the session.

/workstation:{*IPaddress* | *NetBIOSname***}**
NetBIOS computer name or IP address of the session.

/fileinfo
Lists statistics of files currently open by the session (default).

/shareinfo
Lists statistics of share resources currently used by the session.

/close Closes specified user session, file, or resource.

/file:*filename*
Full AIX path name of file to be closed.

/netname:*sharename*
Share name resource to be closed.

Return Codes

0 Command completed successfully.

8 ERROR: Invalid Workstation Name '%s'.

231 ERROR: Missing user name or workstation name.

231 Syntax Error: Unknown command action keyword (%s).

Output for Syntax1:

```
User       Workstation    Open Files    Connection   Idle
                                        Time(days:hrs:mins:secs)
--------------------------------------------------------------------------------
user1      station1       10            10:23:45:33  00:00:55:21
user2      station2       0             00:03:45:33  00:00:20:21
 ...
userN      stationN       20            30:12:45:33  00:01:55:21
```

Output for Syntax2, fileinfo:

```
Open mode  Locks File name(s)
---------------------------------------------
r          0     /home/user3/test1.txt
w          3     /tmp/output.tmp
```

Output for Syntax2, shareinfo:

```
Share name    Connected  Path/Queue name
-----------------------------------------------
HOME          1          $HOME
NETTEMP       1          /tmp
```

NBNS Subcommands

The following subcommands are used to administer the NetBIOS Name Server (NBNS) feature of AIX Fast Connect.

net nblistnames Subcommand

Purpose
To list the NetBIOS name table.

Syntax
net nblistnames

Description

Lists all names in the NetBIOS name table.

net nbaddname Subcommand

Purpose

To add a NetBIOS unique name to the NBNS name table.

Syntax

net nbaddname /name:*name* **/ipaddress:***ipaddress* [**/sub:***value*]

Description

Adds a NetBIOS unique name and its IP address to the NBNS name table.

Flags

/name:*name*
NetBIOS unique name to be added to the NBNS name table.

/ipaddress:*ipaddress*
IP-address (dotted decimal format) of the added NetBIOS unique name.

/sub:*value*
The NetBIOS subcode *value* is a hex number from 00-ff. The default is 00.

net nbaddgroup Subcommand

Purpose

To add a NetBIOS group name to the NBNS name table.

Syntax

net nbaddgroup /name:*name* **/ipaddress:***ipaddress* [**/sub:***value*]

Description

Adds a NetBIOS group name and its IP address to the NBNS name table.

Flags

/name:*name*
NetBIOS group name to be added to the NBNS name table.

/ipaddress:*ipaddress*
IP-address (dotted decimal format) of the added NetBIOS group name.

/sub:*value*
The NetBIOS subcode *value* is a hex number from 00-ff. The default is 00.

net nbaddmulti Subcommand

Purpose

To add a NetBIOS multihomed name to the NBNS name table.

Syntax

net nbaddmulti /name:*name* **/ipaddress:***ipaddress* [**/sub:***value*]

Description

Adds a NetBIOS multihomed name and its IP address to the NBNS name table.
If the name already exists in the name table and the name is a multihomed name, *ipaddress* is added to its list of IP addresses.

Flags

/name:*name*
NetBIOS multihomed name to be added to the NBNS name table.

/ipaddress:*ipaddress*
IP-address (dotted decimal format) of the NetBIOS multihomed name.

/sub:*value*
The NetBIOS subcode *value* is a hex number from 00-ff. The default is 00.

net nbdelname Subcommand

Purpose
To delete a NetBIOS name from the NBNS name table.

Syntax
net nbdelname /name:*name* [**/sub:***value*]

Description
Deletes any type of permanent name from the NBNS name table.

Flags

/name:*name*
NetBIOS name to be deleted from the NBNS name table.

/sub:*value*
The NetBIOS subcode *value* is a hex number from 00-ff. The default is 00.

net nbaddingrp Subcommand

Purpose
To add a NetBIOS internet group name to the NBNS name table.

Syntax
net nbaddingrp /name:*name* **/ipaddress:***ipaddress*

Description
Adds a NetBIOS internet group name and its IP address to the NBNS name table.
If the name already exists in the name table and the name is a internet group name, *ipaddress* is added to its list of IP addresses. A limit of 25 IP addresses is allowed per internet group.

Flags

/name:*name*
NetBIOS internet group name to be added to the NBNS name table.

/ipaddress:*ipaddress*
IP-address (dotted decimal format) of the NetBIOS internet group name.

net nbdeladdr Subcommand

Purpose
To delete an IP address from a NetBIOS internet group name in the NBNS name table.

Syntax
net nbdeladdr /name:*name* **/ipaddress:***ipaddress*

Description
Deletes an IP address of an NetBIOS internet group name from the NBNS name table. If there is more than one IP address associated with the internet group name, only that IP address is deleted from its list. Otherwise, the internet group name is also deleted.

Flags

/name:*name*
NetBIOS internet group name.

/ipaddress:*ipaddress*
IP address (dotted decimal format) to be deleted.

net nbbackup Subcommand

Purpose
To back up the NetBIOS name table to a file.

Syntax
net nbbackup /file:*filename*

Description
Copies all of the entries that are in the NetBIOS name table to a file. Do not edit this file — it should be used only as input to the **net nbrestore** command.

Flags

/file:*filename*
The name of the file that the NetBIOS name table is written to.

net nbrestore Subcommand

Purpose
To restore the NetBIOS name table from a file.

Syntax
net nbrestore /file:*filename*

Description
Copies all of the entries that are in the file into the NetBIOS name table to a file. Do not edit this file — it should be the output file from the **net nbbackup** command.

Flags

/file:*filename*
The name of the file that the NetBIOS name table is restored from.

net nbstatus Subcommand

Purpose
To check the status of the NetBIOS Name Server.

Syntax
net nbstatus

Description
Prints the status of the NetBIOS Name Server (NBNS).

cifsPasswd Command

Purpose

Allows users to change their passwords from remote locations without having root authority.

Syntax

cifsPasswd [username] [/changeaixpwd]

Description

This command allows users to change their encrypted passwords without having root authority. To execute this command, a telnet or other AIX-login session is required.

Note:

- The **cifsPasswd** command does not work with NT-passthrough authentication
- The **cifsPasswd** command cannot be used to change DCE passwords.

Flags

username	AIX user name needing a changed AIX Fast Connect password. If unspecified, the current user name is used.
/changeaixpwd	If this flag is specified, the AIX password for that user will be changed also.

cifsLdap command

Purpose

Allows AIX Fast Connect to register and unregister its file share and print share names.

Syntax

cifsLdap –h *host* **–u** *adminDN* { **–a** *treeDN* | **–r** *treeDN* | **–f** *filename* }

Description

The **cifsLdap** command allows AIX Fast Connect to register and unregister its file share and print share names into the Windows active directory.

Flags

-h *host*	Host name of the Windows 2000 Directory Server (ADS)
-u *adminDN*	Distinguished Name (DN) of ADS administrator account used for binding to the directory. In addition to using a Distiguished Name, the administrator account can also be specified using the format: *DomainName**UserName*.
-a *treeDN*	Adds all the current AIX Fast Connect shares to *treeDN* in the active directory
–r *treeDN*	Removes all the current AIX Fast Connect shares for *treeDN* in the active directory
–f *filename*	Sends *filename* to the Active Directory Server, where *filename* is an LDF-format data file containing LDAP commands for the Active Directory Server

In all cases, the user is prompted for the *bindDN* password associated with the *adminDN* account supplied on the command line, which must have the proper administrative access for the Active Directory Server given as –h *host*.

cifsClient send Command

Purpose

Allows sending of messages to other computers and users.

Syntax

cifsClient send { **-a** | **-c** *Computer* | **-d** [*Domain*] | **-u** *User*} [**-m** *"Message"* | **-f** *Filename*]

Description

The **cifsClient send** command allows sending of messages to other computers and users. The target computer must be receiving messages.

Flags

-a	Send message to all users connected to AIX Fast Connect.
-c *Computer*	Sends messages to a specified *Computer* name connected to AIX Fast Connect.
-d [*Domain*]	Sends messages to a NetBIOS domain/workgroup name. If the *Domain* is not specified, the message is sent to the domain of the Fast Connect server.
-f *File*	Specifies the *File* containing the message text. **Note:** If **-m** or **-f** is not specified, the message is read from the standard input.
-m *Message*	Specifies *Message* text. **Note:** If **-m** or **-f** is not specified, the message is read from the standard input.
-u *User*	Sends messages to a specified *User* connected to AIX Fast Connect.

Appendix B. Configurable Parameters for the net Command

AIX Fast Connect is designed for ease of administration, but it provides a set of customizable parameters to support various configurations. Several of these parameters are dynamically configurable and do not require the server to be stopped and restarted for the changes to become effective.

These parameters are found in the **/etc/cifs/cifsConfig** file, and can be configured by using the **net** command with the following syntax:

```
net config /parameter_name:parameter_value
```

For usage help, type: `net config help`.

These parameters are described as follows:

Parameter	Description	Type	(default,min,max)	Static (S) or Dynamic (D)
accesscheckinglevel	Used to specify how directory searches are checked. If this option is enabled, access checking is done within the context of each user's **cifsUserProc** process. If this option is disabled, access checking is done by the **cifsServer** process, based upon each file's AIXpermission bits. **Note:** Enabling this option may be necessary for some AIX Fast Connect environments where AIX root user does not have access to all files, such as JFS-ACLs support or SMB-to-NFS gateway support. However, enabling this option degrades the performance of the AIX Fast Connect server.	int	(0, 0, 1)	D
acl_inheritance	Enables or disables the inheritance of AIX ACLs from the base path of a file share. Details about this feature can be found in "AIX Fast Connect User Management and File Access" on page 39.	int	(0, 0, 1)	S
acl_mapping	Enables basic NTFS ACL support by mapping NTFS ACLs to JFS ACLs	int	0, 0, 1	S
alias_names	List of servername aliases. Use **net name** to list or update this parameter. Maximum length of each alias is 15 characters. See "Specifying NetBIOS Aliases for HACMP support" on page 44.	String	(Null, n/a, n/a)	D
autodisconnect	Timeout (in minutes) to disconnect inactive sessions. Value 0 indicates sessions will not timeout.	int	(120, 0, 65535)	D
backup_passthrough_ authentication_server	IP address of the backup authentication server	String	(Null, n/a, n/a)	S

Parameter	Description	Type	(default,min,max)	Static (S) or Dynamic (D)
browsinginterval	Sets the frequency (in seconds) that the AIX Fast Connect server will announce itself to the Master Browser on its local network.	int	(60, 30, 900)	D
browsemaster	Enables the Browse Master feature, which allows AIX Fast Connect to act as a ″Browse Master″ for its domain/workgroup (specified by the domainname option). This option is automatically enabled (internally), whenever the Network Logon feature is enabled.	int	(0, 0, 1)	S
cache_searches	Global enable/disable of the Search-caching feature. See “Search Caching” on page 49.	int	(0, 0, 1)	S
casepreserve	When set to 1, AIX Fast Connect preserves mixed-case file names when creating new files or directories for PC clients. When set to 0, AIX Fast Connect converts all file names to lowercase when creating files and directories.	int	(1, 0, 1)	S
casesensitive	When set to 1, AIX Fast Connect file name searches are case-sensitive. When set to 0 (the default), AIX Fast Connect file name searches are not case-sensitive. Normally, this parameter should be set to the default because DOS and Windows use case-insensitive filename searches on their local file systems by default.	int	(0, 0, 1)	S
cifs_registry	Enables the DCE User-Registry feature of AIX Fast Connect . This feature allows multiple AIX Fast Connect servers to share a common, centralized User Database stored in the DCE-Registry (rather than multiple, separate Fast Connect user-databases kept in **/etc/cifs/cifsPasswd**). For details on using the DCE Registry Database, see Appendix D, “DCE Registry User Database,” on page 93.	int	(0, 0, 1)	S
comment	Server description (for network browsing); maximum of 49 characters.	String	n/a	S

Parameter	Description	Type	(default,min,max)	Static (S) or Dynamic (D)
dce_admin_keytab	Specifies the file name of the DCE keytab file needed for the DCE-Registry User Database feature. This keytab file must contain at least one entry, for the DCE account specified by the dce_admin_user parameter.	String	(Null, n/a, n/a)	S
dce_admin_user	Specifies the DCE user name of the DCE admin user needed for the DCE-Registry User Database feature. This DCE user must have read/write access to the DCE-Registry records for AIX Fast Connect users. Each AIX Fast Connect server has a keytab file to use this DCE account, as specified by the **dce_admin_keytab** parameter.			
dce_auth	Setting to enable AIX Fast Connect's support features for DCE and DFS. When enabled (set to 1), AIX Fast Connect uses DCE-authentication for all PC client logins and file accesses. Requires AIX Fast Connect is installed *after* **dce.client.***. For details, see "DCE/DFS Support" on page 30.	int	(0, 0, 1)	S
domainname	Server domain (maximum of 15 characters).	String	(WORKGROUP, n/a, n/a)	S
dosattrmapping	DOS attribute mapping. If set to 1, the Archive, System, and Hidden attributes are mapped to User, Group, and Other execute bits. Otherwise, these attributes are not supported. This is only valid for files.	int	(1, 0, 1)	D
dosfilenamemapchar	The character used to map long file names to 8.3 DOS filename format. Valid values are tilde (~) and caret (^). Tilde (~) is the default.	char	~	S
dosfilenamemapping	DOS file-name mapping, If set to 1, long file names are mapped to 8.3 format. Otherwise, no file-name mapping is attempted. See "Mapping Long AIX File Names to 8.3 DOS File Names" on page 43.	int	(1, 0, 1)	S

Parameter	Description	Type	(default,min,max)	Static (S) or Dynamic (D)
double_byte_char	This string option allows Unicode character conversions to be specified (primarily to support known differences between Microsoft ms932 Unicode mappings, and IBM cp943 Unicode mappings, for Japanese characters.) This string is specified as a series of single-character conversions, separated by spaces. Each character conversion must be specified as an 8-digit hexadecimal number, preceded by `0x`, with the MS-code listed first (hi-order bits), followed by the IBM-code. Up to 16 character conversions can be specified. For more information, see “DBCS and Unicode Considerations” on page 45.	String	(null, n/a, n/a)	S
dyngroup_prefix	Prefix for groups created with dynamic user mapping feature	String	grp, n/a, n/a	S
dynuser	Automatically creates local users and groups for authenticated Windows users	int	0, 0, 1	S
dynuser_prefix	Prefix for users created with dynamic user mapping feature	String	usr, n/a, n/a	S
encrypt_passwords	Encrypted passwords. If set to 0, plain text passwords are used. A value of 1 will negotiate with the client. A value of 2 forces encrypted passwords.	int	(1, 0, 2)	S
force_fileattr_change	If enabled, users can change the permissions of a file or folder if they have write permissions on the parent directory, or if they are the owner of the file or folder. When disabled, users can only change the permissions of files or folders for which they are the owner.	int	(0, 0, 1)	S

Parameter	Description	Type	(default,min,max)	Static (S) or Dynamic (D)
filterbroadcast	Enables the AIX Fast Connect server to detect its own NetBIOS broadcast packets across different IP interfaces. Normally, for performance reasons, incoming broadcast packets are compared only with the IP address of the receiving IP interface. This feature allows incoming broadcast packets to be compared to all local IP interfaces, in case the packet was originally broadcast on one of the other interfaces. This feature is generally only needed for HACMP (multiple interfaces on a single physical LAN), or for AIX servers using ATM interfaces. Enable this feature if **net start** reports errors such as `cannot start server`, and **/var/cifs/cifsLog** contains entries such as NetBIOS name conflict.	int	(0, 0, 1)	S
guestlogonsupport	Guest Logon. A value of 1 will enable a guest user to access the server without an AIX Fast Connect password. This user will be connected with credentials defined by the user specified in the `guestname` parameter. A value of 0 disables this feature.	int	(0, 0, 1)	S
guestname	Guest Name (maximum 8 characters). This parameter specifies the user name that guest users will be connected as. The AIX Fast Connect password for this user should be null.	String	(null, n/a, n/a)	D
home_share_enable	Used to disable the HOME share that AIX Fast Connect generates, which gets mapped to an AIX Fast Connect user's home directory on AIX. (If dce_auth=1, that DCE user's DCE home directory is used instead.) This option is enabled by default.	int	(1, 0, 1)	S
krb5_auth	Enables the Kerberos-based Authentication feature of AIX Fast Connect. The **krb5_service_name** parameter must also be specified for this feature to work correctly. For more information, see "Kerberos-based Authentication" on page 32.	int	(0, 0, 1)	D

Parameter	Description	Type	(default,min,max)	Static (S) or Dynamic (D)
krb5_service_name	Specifies the Service Name of the Kerberos Domain Controller (KDC) to which AIX Fast Connect authenticates Kerberos users, if the Kerberos-based Authentication feature is enabled.	int	(null, n/a, n/a)	S
ldap_admin_user	LDAP administrative username used by AIX Fast Connect to query and update the LDAP user database, when LDAP authentication is enabled.	string	(null, n/a, n/a)	S
ldap_auth	If set to 1, AIX Fast Connect will authenticate users using the LDAP security mechanism. Default is 0 (disabled).	int	(0, 0, 1)	S
ldap_server_name	LDAP server that is used by AIX Fast Connect to authenticate users for LDAP authentication.	string	(null, n/a, n/a)	S
ldap_userDN	Distinguished Name (DN) that is used by Fast Connect to specify where usernames are located in the LDAP directory, during LDAP authentication.	string	(null, n/a, n/a)	S
lm_encryption_level	Parameter to configure use of LM password encryption, Windows NTLM encryption, or both. The default is 0, meaning LM encryption only. If set to 1, only Windows NTLM encryption is used. When set to 2, both LM and NTLM encryptions are supported.	int	(0, 0, 2)	S
maxconnections[2]	Maximum number of open connections allowed to a single resource (fileshare) on the server. (0 implies no limit.)	int	(0, 0, 1000)	D
maxmultiusersessions	Maximum number of user sessions allowed from a single client workstation.	int	(100, 16, 10240)	S
maxthreads	Maximum number of simultaneous requests that can be processed. Only effective when the value of the **maxusers** parameter is greater than **maxthreads**.	int	(2048, 50, 31744)	
S				
maxopens[2]	Maximum number of open files on the server.	int	(0, 0, 1000)	S
maxsearches[2]	Maximum number of open searches on the server.	int	(0, 0, 1000)	S

Parameter	Description	Type	(default,min,max)	Static (S) or Dynamic (D)
maxsesssearches	Maximum number of open searches per session. For performance reasons, this number should be kept as small as practicable for your installation.	int	(5, 2, 1000)	S
maxshares	Limits the number of file shares and print shares that can be defined. For performance reasons, keep this number as small as practicable for your site.	int	(16, 1, 4096)	S
maxsmbbufsize	Sets the maximum packet size allowed by the AIX Fast Connect server for SMB protocol packets. (Each PC client may negotiate a smaller packet size, if desired.)	int	(65535, 4096, 131071)	S
maxusers[2]	Maximum number of user sessions (logins) permitted.	int	(0, 0, 1000)	D
mmapfiles	When this performance option is enabled, AIX Fast Connect uses memory-mapped file-access (internally) during CIFS read and write operations, allowing more efficient data-transfers.	int	(0, 0, 1)	S
msdfs	If enabled, the AIX Fast Connect server supports CIFS Distributed File System (MSDFS) services. Default is 0 (disabled).	int	(0, 0, 1)	S
msdfs_ordering	Determines how AIX Fast Connect server responds to MSDFS queries, when the MSDFS feature is enabled.	int	(0, 0, 1)	S
multiuserlogin	Enables or disables support for multiple user sessions from a single workstation. This option is needed to support Windows Terminal Server, and similar products. This option is mutually exclusive with the Network Logon feature. This option is also mutually exclusive with NT-Passthrough authentication.	int	(0, 0, 1)	S
nbddservice	If enabled, AIX Fast Connect server supports NetBIOS DataGram service. Default is 0 (disabled).	int	(0, 0, 1)	S
nbns	If set to 1, server acts as a NetBIOS name server.	int	(1, 0, 1)	S
netlogon_path	The AIX pathname for the NETLOGON and IBMLAN$ shares (maximum 1023 characters), to store user startup scripts and policy files.	String	(/var/cifs/netlogon, n/a, n/a)	S

Parameter	Description	Type	(default,min,max)	Static (S) or Dynamic (D)
networklogon	Network Logon. This option is used to enable or disable the Network Logon feature of AIX Fast Connect.	int	(0, 0, 1)	S
oplock_unix_lock	Enables or disables AIX file-locking to be used for opportunistic locks. Enable this option if oplocks are enabled, and AIX applications need to share files with PC-clients. oplock_unix_lock and level II oplocks are mutually exclusive. If oplock_unix_lock is enabled, then level II oplocks will be internally disabled. See also **oplock_unix_lock_timeout** and **oplockfiles**.	int	(0, 0, 1)	S
oplock_unix_lock_timeout	Timeout in seconds, for `oplock_unix_lock`. (Time allowed to obtain AIX file lock.)	int	(0, 0, 1)	S
oplockfiles	Global parameter to define whether opportunistic locking (oplocks and level II oplocks) is enabled (yes) or disabled (no). Opportunistic locking is a performance feature, allowing clients to lock entire files in non-exclusive mode. Controlled by **oplocktimeout**. See also **sh_options**, **oplock_unix_lock**.	Y/N	(yes, no, yes)	S
oplocktimeout	Timeout in seconds for opportunistic locking.	int	(35, 35, 640)	S
passthrough_authentication_ server	IP address of the passthrough authentication server	String	(Null, n/a, n/a)	S
primary_wins_ipaddr	IP address of the NBNS (WINS) server. When started, the AIX Fast Connect server will register its NetBIOS name(s) with this NBNS server. See also `wins_proxy`.	String	(Null, n/a, n/a)	S
profiles_path	The AIX path name for the `PROFILES` share (maximum 1023 characters), which the Network Logon feature uses to store user profiles and home directories.	String	(home, n/a, n/a)	S

Parameter	Description	Type	(default,min,max)	Static (S) or Dynamic (D)
profiles_path_type	Determines how user profiles are accessed when the Network Logon feature is enabled. • 0: User profiles are accessed locally at each workstation. (″Loopback″ mode.) User ″Desktop″ data is not saved on the the AIX Fast Connect server and is not transmitted over the network during Network Logon. • 1: User profiles are retrieved from the AIX Fast Connect PROFILES share. • 2: User profiles are accessed from the **profiles_path** directory, which specifies a UNC path to AIX Fast Connect or some other SMB server on the network.	int	(1, 0, 2)	S
readonlydir	Allows AIX Fast Connect directories to be created as read-only. However, with this parameter set, copying a read-only directory to AIX Fast Connect (from a CD-ROM, for example) will fail—the AIX Fast Connect directory will be created as read-only and will not allow additional files to be copied into it. When this option is disabled (default), any request from a client to set a directory to read-only will be ignored.	int	(0, 0, 1)	D
remote_password_change	If the Network Logon feature is enabled, this option can be used to enable Windows 98 clients to remotely change their AIX Fast Connect passwords for Network Logon. (Remote Password-Change is not currently available on AIX Fast Connect for Windows NT, Windows 2000, or Windows XP clients.) In addition, **sync_aix_password** can be used to simultaneously change the AIX password for an AIX Fast Connect user. For more details, see “Changing Passwords Remotely” on page 38.	int	(0, 0, 1)	S
secondary_wins_ipaddr	IP address of secondary WINS address.	String	n/a	S
send_file_api	Boolean value to enable an enhanced system call to improve the performance in sending files over the network.	int	(1, 0, 1)	S

Parameter	Description	Type	(default,min,max)	Static (S) or Dynamic (D)
send_file_cache_size	Cache SendFile Option. If the send_file_api is 1 and the requested SMB read size is less than the value of this parameter, the send_file API caches the file. The default value is zero, which means send_file API will not cache the file.	int	(0, 0, 4194304)	S
send_file_size	Cache SendFile maximum size. If the send_file_api is 1 and the requested SMB read size is greater than the value of this parameter, send_file API is used in the SMB operation.	int	(4096, 1, 4194304)	s
servername	NetBIOS name of the AIX Fast Connect server (maximum 15 characters).	String	(TCP/IP hostname, n/a, n/a)	S
sh_options	Data field (per share) to allow per-share options to be defined. This field should only be accessed with the **net share** command. See "Specifying Per-Share Options" on page 40.	int	n/a	S
share_level_security	Option to enable or disable share-level security (instead of user-level security). When enabled, `share_level_security_username` must also be specified. See "Share-Level Security" on page 33.	int	(0, 0, 1)	S
share_level_security_username	AIX user name used for file-access credentials when `share_level_security` is enabled (maximum 8 characters). Similar to `guestname`, but used for share-level security mode.	String	(Null, n/a, n/a)	S
startup_script	The file name of the startup script used when **`networklogon=1`** (maximum 256 characters). Two metatags in this string allow customization of the startup script file name during client logon — %U is expanded to the client's user name, and %N is expanded to the client's computer name.	String	(startup.bat, n/a, n/a)	S
sync_aix_password	Allows the Remote Password-Change feature to change an AIX Fast Connect user's AIX password whenever changing the Network Logon password for that user. This keeps these two passwords synchronized with each other. For more details, see "Changing Passwords Remotely" on page 38.	int	(0, 0, 1)	S

Parameter	Description	Type	(default,min,max)	Static (S) or Dynamic (D)
tcp_keepalive	Allows AIX Fast Connect to generate TCP/IP keepalive messages to detect disconnected PC client sessions, and to keep Windows XP and Windows 2000 clients from disconnecting an active session containing mapped drives. (Windows XP and Windows 2000 clients will generally disconnect idle sessions after 1 hour.)	int	(1, 0, 1)	S
umask	Default permissions mask for files created from client machines. It is an octal number, and should always be prefixed with a zero.	octal	(022, 0, 0777)	D
usernamemapping	Option to enable/disable the User Name Mapping feature, configured by **net user /map**.	int	(0, 0, 1)	S
wins_proxy	Proxy Option. A value of 1 enables the forwarding of NetBIOS name resolution requests to a WINS server specified by the *primary_wins_ipaddr* parameter.	int	(0, 0, 1)	S

Notes:

1. Any changes to static parameters require a Shutdown and Restart of the AIX Fast Connect server before they take effect. Dynamic change take effect immediately if the **net** command, SMIT, or Web-based System Manager are used to configure them.
2. Any configuration parameter value not specified, or out of range, in the **/etc/cifs/cifsConfig** file, will be set to the default value for that configuration parameter.

Appendix C. Kerberos setup example

The following example is given to show the basic setup of an AIX Kerberos Server and a Windows2000 Kerberos-client, for use of the Kerberos-authentication feature of AIX Fast Connect.

For additional information on Kerberos server and client configuration, please refer to your Kerberos documentation.

__ Step 1. Perform the following steps on the AIX server machine. This machine will be used as the Kerberos server, and also as the Fast Connect server.

__ a. Install the following filesets:

- **krb5.client**
- **krb5.server**
- **krb5.msg.en_US**
- **krb5.toolkit**

__ b. Run the Kerberos configuration script as follows:

```
/usr/krb5/sbin/config.krb5 -S -r CIFSKDC -s myserver.austin.ibm.com -d austin.ibm.com
```

where

- **-r** is the Kerberos realm, in uppercase (example: CIFSKDC)
- **-s** is the server name, and is also the name of the KDC (example: myserver.austin.ibm.com)
- **-d** is the domain (example: austin.ibm.com)

__ c. In file **/etc/krb5/krb5.conf**, remove all instances to `des3-cbc-sha1`

__ d. In file **/var/krb5/krb5kdc/kdc.conf**, remove both instances to `des3-cbc-sha1:normal`

__ e. Refresh the daemons by typing the following commands:

1) `stop.krb5`
2) `start.krb5`

__ f. Create a Kerberos principal for the Windows2000 client machine. (This client machine will use Kerberos to connect to Fast Connect.) Create the Kerberos principal (example: host/win2k.austin.ibm.com) by entering the following commands:

1) Run /usr/krb5/bin/kinit admin/admin
2) Run /usr/krb5/sbin/kadmin

   (When prompted, enter the ″admin″ password that was used while configuring the kerberos server.) This will start a nested ″kadmin″ shell, used for the following commands:

3) kadmin: ank -pw w2khopwd -requires_preauth host/win2k.cifskdc

   where

   - host - is the word ″host″,
   - win2k - simple machine name of the Windows2000 client
   - cifskdc - lowercase realm name (where realm = CIFSKDC)
   - w2hopwd - is the Windows2000 client host password.

4) kadmin: list_principals should now display ″host/win2k.cifskdc@CIFSKDC″

__ g. Create a local host service name that will be used by AIX Fast Connect.

1) kadmin: ank -pw ktpass HOST/myserver
2) kadmin: ank -pw ktpass HOST/myserver.austin.ibm.com
3) kadmin: ank -pw ktpass HOST/www.xxx.yyy.zzz

   where

- myserver is the AIX Kerberos-server's hostname.
- www.xxx.yyy.zzz is the TCP/IP address of that server machine.
- ktpass is a ″host″ password for that AIX server machine.

__ h. Add the hostname to the keytab file.

```
kadmin: ktadd HOST/myserver.austin.ibm.com
```

__ i. Create a Windows2000 user name (example: user1/pass1) who will log into the KDC

```
kadmin: ank -pw pass1 -requires_preauth user1
```

__ Step 2. On the Windows2000 client:

__ a. Install sup.zip (a file containing Windows2000 Kerberos-support tools)

__ b. Add a new Windows2000 local-user, to be used for Kerberos: (example: Define username: krb5_user1 with password: pass1)

__ c. Run the following commands from the directory where sup.zip was installed

1) `ksetup /setdomain CIFSKDC`

   where CIFSKDC is the Kerberos realm

2) `ksetup /addkdc CIFSKDC myserver.austin.ibm.com`

   where CIFSKDC is the Kerberos realm and myserver.austin.ibm.com is the AIX Kerberos-server's hostname.

3) `ksetup /setmatchpassword w2khopwd`

   where w2khopwd is the password that was set previously while doing Kerberos-server setup on AIX.

4) ksetup /mapuser user1@CIFSKDC krb5_user1

   The KDC principal user1 is now mapped to local Windows2000 user krb5_user1

__ d. Login to KDC realm using kdc principal and password. (example: realm CIFSKDC, username user1/pass1)

__ Step 3. On the AIX machine:

__ a. Configure Fast Connect to use Kerberos authentication. From AIX, type:

1) `net config /krb5_auth:1`

   (to enable the Kerberos feature)

2) `net config /krb5_service_name:HOST@myserver.austin.ibm.com`

   (where myserver is the local hostname.)

__ b. Re-start the Fast Connect server, using Kerberos authentication:

1) `/etc/rc.cifs stop` (stops and unloads the Fast Connect server)
2) `/usr/krb5/bin/kinit -k HOST/myserver.austin.ibm.com` (initializes Kerberos, prior to starting the FastConnect server)
3) `/etc/rc.cifs start` (loads and starts the Fast Connect server)

Appendix D. DCE Registry User Database

AIX Fast Connect user information (including encrypted passwords) can be kept in the DCE Registry, a centralized user database that multiple AIX Fast Connect servers can access. This database uses the Extended Registry Attribute Field to maintain encrypted passwords and user descriptions for each user.

Enable the AIX Fast Connect **cifs_registry** option to use this functionality on each server. The server need not be enabled for DCE/DFS authentication.

The **dce_admin_user** and **dce_admin_keytab** configuration parameters are needed for this functionality. In addition, the DCE keytab file, which allows each AIX Fast Connect server to access and update the DCE Registry User Database, is needed.

To configure and use the DCE Registry User Database, follow these steps:

1. Install the AIX Fast Connect filesets on each server.
2. Create the Extended Registry Attribute schema needed for this feature (needed only once for the entire DCE cell, not once per server) by following these steps:
   a. dce_login as cell_admin and run the following:
      ```
      /usr/sbin/cifsRgysetup.dcecp
      ```
   b. Use acl_edit to modify the ACLs of the new Extended Registry Attributes schema so that **/.:/sec/xattrschema** is fully protected from access by unauthenticated **other_obj** or **any_other** objects. Change these ACLs from `r-----` to `------`.
3. Set up a DCE keytab file on each AIX Fast Connect server. This file contains the DCE user name and password of the dce_admin_user account that has authority to read and write data to the Extended Registry Attribute fields of every DCE user that is also an AIX Fast Connect user. For information on setting up a DCE keytab file, see “DCE/DFS Support” on page 30.
4. Configure the dce_admin_user and dce_admin_keytab parameters on each AIX Fast Connect server by running the following:
   ```
   net config /dce_admin_user:dceAdminUser
   net config /dce_admin_keytab:keytabFilename
   ```
5. Enable the **cifs_registry** feature on each AIX Fast Connect server by running the following:
   ```
   net config /cifs_registry:1
   ```
6. Restart each AIX Fast Connect server:
   ```
   /etc/rc.cifs stop
   /etc/rc.cifs start
   ```

   If any errors occur when restarting, check the **/var/cifs/cifsLog** file.
7. Add AIX Fast Connect users to the database by running:
   ```
   net user /add username password /comment:"userdescription"
   ```

   or

   ```
   net user /add username  /comment:"userdescription"
   ```

With **cifs_registry** enabled, the **net user** subcommand keeps its previous syntax with the following exceptions:

- All **net user** queries and updates are now directed to the DCE Registry version of the user database instead of the **/etc/cifs/cifsPasswd** file.
- The **net user** subcommand requires a *username* parameter to be specified when **cifs_registry** is enabled. The **List All Users** functionality is not supported in this mode.

Note the following:

- The **cifs_registry** feature is only effective when NT-passthrough authentication is disabled and encrypted passwords are enabled.
- The UserNameMapping feature is not supported when **cifs_registry** is enabled.
- When the **cifs_registry** feature is enabled, every AIX Fast Connect user name must also exist as a DCE user name. Each user name must also be recognized as a valid **uid** by the **id** command on every AIX Fast Connect server. This can be accomplished by running the DCE daemon **dceunixd**.
- User data that may be available in the local AIX Fast Connect user database (**/etc/cifs/cifsPasswd**) is not automatically transferred to or from the DCE Registry User Database. These databases can get out-of-sync and will generally contain different data. When **cifs_registry** is enabled, only the DCE Registry User Database is used and each local database will be ignored.
- When **cifs_registry** is enabled, the **List All Users** functionality of the **net user** subcommand is not supported.
- To prevent unauthorized access to DCE user information, the ACLs for the DCE Registry schema, **/.:/sec/xattrschema** must be modified from `r-----` to `------` for the **other_obj** and **any_other** objects.
- When the **cifs_registry** feature is enabled, mixed case users on the server are not supported.

Appendix E. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described 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:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION ″AS IS″ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

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. LRAS/Bldg. 003
11400 Burnet Road
Austin, TX 78758-3498
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX
DFS
HACMP
IBM
OS/2
AIX 5L

Microsoft, Windows 98, Windows NT, Windows 2000, Windows 2003, and Windows XP are trademarks of the Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be the trademarks or service marks of others.

Index

N

P

R

S

T

U

W

Readers' Comments — We'd Like to Hear from You

AIX Fast Connect
Version 3.2 Guide

Publication No. SC23-4875-04

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Name

Address

Company or Organization

Phone No.

Readers' Comments — We'd Like to Hear from You
SC23-4875-04

IBM

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Information Development
Department 04XA-905-6C006
11501 Burnet Road
Austin, TX 78758-3493

Fold and Tape | **Please do not staple** | Fold and Tape

Cut or Fold
Along Line

Printed in U.S.A.

SC23-4875-04