

CEM Product Support

SAMBA for AIX installation & guidelines



Frank Conrad
CREO EMEA
Waterloo Office Park
Drève Richelle 161
Building E-F
1410 Waterloo

Phone +32 2 352 2723
Fax +32 2 352 2592
E-mail frank.conrad@creo.com

1. Inter connectivity between different Operating Systems 4
1.1 AppleShare, AppleTalk, and PC-Mac-LAN 4
1.2 TCP/IP NFS: 5
1.3 FTP (file Transfer Protocol) 6
1.4 RPC 6
1.5 SAMBA (SMB) 6
1.6 SMB networking overview 6
2 Server installation 8
2.1 Automatic installation and configuration 8
2.2 Installation verification 8
2.1 Using SWAT 9
2.2 The SAMBA swat Interface 9
3 Known Limitations: 16
3.1 Extensions 16
3.2 Unsupported characters 16
3.3 Usernames. 16
3.4 Other limitations 17
4 Joining an existing domain 18
4.1 Adding a Samba server to an NT 4.0 domain 18
4.2 Adding a Samba server to an Active Directory domain 19
4.2.1 Create an AIX Samba server account to domain 20
4.2.2 Configure the AIX Samba server 20
5 Samba Windows Client set-up 22
5.1 Locating the Samba server from Windows 9x 24
5.2 Using the Network Neighborhood program 25
5.3 Using the Find Computer option 25
5.4 Accessing resources from Windows 9x clients 26
5.4.1 Accessing files 26
5.4.2 GUI interface 26
5.4.3 Mapping network drive 27
5.4.4 Command line interface 27
5.4.5 Accessing Printer shares 27
5.4.6 GUI interface 28
5.5 Accessing Samba from Windows NT clients 29
5.5.1 Configuring Windows NT 29
5.5.2 Locating the Samba server 32
5.5.3 Locating the server through the Network Neighbourhood 32
5.5.4 Locating the server with the Find: Computer option 32
5.5.5 Locating the server from the command line 33
5.6 Accessing resources from Windows NT 33
5.7 Accessing files 34
5.7.1 Using the GUI interface 34
5.7.2 Command line interface 34
5.8 Accessing the Samba printers 35
5.8.1 GUI interface 35
5.8.2 Command line interface 36
5.9 Access the Samba server from Windows 2000 36
5.9.1 Configuring Windows 2000 36
5.9.2 Locating the Samba server 38
5.9.3 Locating the server from the command line 39
5.10 Accessing Files 40
5.10.1 Using the GUI interface 40
5.10.2 Using the command line interface 40
5.11 Accessing printers 41

5.11.1 Using the GUI interface 41
5.11.2 Command line interface 42
6 Appendix A. Troubleshooting 43
6.1 Protocol levels 43
6.2 Generic TCP/IP utilities 43
6.3 Troubleshooting utilities on Windows NT 44
6.4 TCP/IP configuration 44
6.5 NetBIOS over TCP/IP troubleshooting 45
6.5.1 tracert 45
6.5.2 nbtstat 45
6.5.3 browstat 46
6.6 Troubleshooting utilities on AIX 47
6.6.1 TCP/IP configuration checking 47
6.6.2 tcpdump 48
6.7 Common problems 50
6.7.1 NetBIOS name resolution 50
6.7.2 Browsing 50
6.7.3 Authentication 51
6.7.4 Netlogon 51

1. Inter connectivity between different Operating Systems

Inter-connectivity needs to cross the border of different communication protocols.
Many flavours of protocols are in use, but there is no real Standard, except the way to use them is standardised.
Everybody can talk to another user if it's the same operating system he is connecting to. But not to a different one without using any kind client application to emulate another network protocol.
It seems that Windows is the most sensitive to changes of default behaviour in case of network client software from non Windows source.

The most common protocols are :

1.1 AppleShare, AppleTalk, and PC-Mac-LAN

AppleShare, AppleTalk, and PC-Mac-LAN are used for the communication in between Macintoshes, PC's, and UNIX systems.
All of them are based on the AppleTalk Protocol which today runs over TCP/IP.
In previous times a very painful use because of the stupidity of the protocol itself and its slow performance.
That kind of protocol is taking care of what we call 'resource' (rsrc).
It's keeping the information about creator, file-type,……
That means two files are located on an AppleShare volume, the file itself and the resource file.
If a Macintosh/PC is connecting to such volume, it reads this information to handle the file on its own desktop. Macintosh cannot handle two files at a time (file and rsrc)
The rsrc file is updated all the time changes are made to that file.
This happens inside the rsrc directory which is somehow a mirror of the real file but much smaller in size.
All the time a file arrives, is modified, deleted, or moved the desktop information gets updated automatically (at least in theory)
In case of inconsistency the information in between the file-system and the desktop information may differ.
That's what we call 'desktop corruption'.
Rebuild desktop will usually fix that problem by comparing file-system information and desktop information (rsrc directory).
Files stored on such kind of volumes don't need an extension attached to the file, to know which file-type is used.
Another important point is the length of a filename displayed on a Macintosh using AppleShare.
The limit is 31 characters, if its more its still visible on a UNIX/Windows system, but not on a Mac Accept on OSX (OS10).
Today we are smiling about such kind of limitation but in the past the rule on Windows concerning filenames was '8 +3' and only capital letters, Apple started with 31characters.

All customers are used to create any name for files and folders, but the border is set on delimiters.
Such kind of letters and signs are used for the operating system.
An example might be '/' or '\' used by the operating system to define a path 'from' 'to'.
Its simply reserved to connect information by path (C:\\[Windows], /backup/nsr[Unix])
If we are breaking such rule there will be problems in functionality.

1.2 TCP/IP NFS:

The most common communication protocol.
It was designed to be the internet protocol defined by the US army to communicate in times of war with their own protocol.
Today almost everybody is using it to establish communication.
NFS runs on top of TCP/IP for the use of mounting and exporting file-systems.
A remote file-system is identified by its IP-address and its hostname.
It requires a network set-up where one can reach the other by IP, Router, Gateway and DNS.
But this is based on TCP/IP, underlying NFS.
NFS needs to have an export, access rights, and both need to know about each other (/etc/hosts).
There are simple rules to reach each other, one is what we call address range, and the other one is called subnet.
The subnet is masking the IP network into ranges of Class A, B, and C.
A class is covering the first 8 bit of the mask: 255.0.0.0
B class is covering the first 16 bit of the mask: 255.255.0.0
C class is covering the first 24 bit of the mask: 255.255.255.0

But this is much more complex as looks like:
A class starts with: 1.0.0.0> up to 255.0.0.0 (means 256 x 1= 256 nodes on the same network)
But its much more: 1.255.255.254
Or : 1.1.1.0
Or: 1.2.1.0
Or: 1.1.2.0
Or: 0.0.1.0

And so on.

Additional to that the mask can be used to make more difference:
192.9.100.1
255.255.0.0

192.9.101.1
255.255.0.0

192.9.102.1
255.255.0.0

192.9.103.1
255.255.0.0

As we can see the subnet mask is cutting all to the same network (16bit)

Lets assume two machines are in different networks but need to talk to each other.

1. 192.9.100.1
   255.255.255.0
   192.9.101.1
   255.255.255.0
2 192.9.101.2
   255.255.255.0

Lets say 192.9.101.1 will act as default gateway, the definition will be DG 192.9.101.1 on that machine which is using the address 192.9.100.1.

1.3 FTP (file Transfer Protocol)

Most common use is to move files through the internet from an ftp server to the final location.
But you can connect to a local machine as well by using for example: ftp://10.3.1.47/.
After authentication you have access to all folders and file.
Transfer is fast.

1.4 RPC

Used for the send function on Brisque/server.
No NFS is used for that activity.

1.5 SAMBA (SMB)

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

Samba implements the SMB/CIFS protocols that enable clients and servers to exchange messages and data. Samba enables UNIX systems to act as file and print servers for PC client systems. Although Samba is primarily used to provide Windows-like file and print services under UNIX, it also includes UNIX SMB client utilities.
Windows 95/98, Windows NT, Windows 2000, and OS/2 Warp clients do not need any extra software to access a Samba server. These operating systems all support NetBIOS over TCP/IP (NBT), which is all that is needed to access a Samba server.
Samba provides the following features:

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

1.6 SMB networking overview

Before installing Samba, it is important to have an understanding of Windows networking concepts. Windows-style SMB file and print services differ from UNIX file and print services in many ways.
In 1984, IBM and Sytec co-authored a simple API called Network Basic Input/Output System (NetBIOS). This was extended in 1985 and named NetBIOS Extended User Interface (NetBEUI). NetBEUI was limited to small LANs since it is a non-routable protocol.
To add network routing support, NetBIOS was later hosted on top of IPX, DECNet, and TCP/IP. As TCP/IP gained popularity, NetBIOS over TCP/IP (NBT) has become the most common implementation. Samba only implements NetBIOS over TCP/IP.

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

NetBIOS name resolution varies depending on the type of node and configuration of the client. In its most basic form, NetBIOS clients announce their existence and any services provided across the local network. Other NetBIOS clients cache this information to produce a map of the available network services, thus creating the browse list.
Microsoft's NetBIOS name server is called the Windows Internet Name Service (WINS). Samba can function as a NetBIOS name server but cannot replicate data with Microsoft WINS servers.
The SMB protocol defines two models of security. In the original model, share level security, the client need only provide a password to access a share. A username is not required in share level security. Once a client has access to a share, he or she can access any files contained within that share. The more recent model, user level security, requires the client to provide a username and password to access a share. Additionally, user level security can protect individual files within a share.
A Domain is a collection of computers whose security information is centrally managed by a Domain Controller. There can only be one Primary Domain Controller in any given Domain, although there may be multiple Backup Domain Controllers. In a Workgroup, each client maintains their own security information. Generally, a workgroup is restricted to a single subnet. Since Version 2.0, Samba can function as a Primary Domain Controller.
Recently, Microsoft has enhanced and renamed the SMB protocol to the Common Internet File System (CIFS). The CIFS 1.0 protocol specification has been submitted to the Internet Engineering Task Force (IETF).

2 Server installation

2.1 Automatic installation and configuration

Samba server installation is performed as following:

Insert the Creo Samba CD into the CD drive .

015-00654A SAMBA CONNECTIVITY TO BRISQUE SERVE

651-00173A SAMBA CONNECTIVITY TO BRISQUE SERVE

From the terminal type:
smit install_latest
Select the CD as the installation source ,then select **ALL** for the installed software.
The Samba software will be automatically installed and configured.

2.2 Installation verification

In this section, we discuss how to verify that the installation was successful.
Basically there is no need to change any configuration file to start using Samba.

- Verify that the 'smb.conf' file has the correct hostname, necessary to start SWAT
- Verify that the file '/etc/services' has a line like 'swat 901/tcp'.
- Verify that the /etc/inetd.conf has to include the smbd, nmbd, and SWAT entries.

After the installation, the following directory structure exists:
• *//usr/local/bin* - Samba binaries
• *//usr/local/lib* - smb.conf configuration file and Samba directory structure
• *//usr/local/man* - Samba man pages
• *//var/samba* - Logs and miscellaneous files

The following scripts can be useful for the Samba debugging (starts/stops samba daemons):
/scitex/version/scripts/startsmb
/scitex/version/scripts/stopsmb

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

/usr/local/bin/smbclient -L yourhostname (use root/ripro as username/login)

If this command shows a list of the resources configured in smb.conf, you have a properly-running Samba server. You should now be able to access the shared resources from your clients.
To enable and start SWAT (the Web-based Samba administration interface) perform the following steps:

Verify the following entries in **/etc/inetd.conf :**

The following three lines are for the Samba SMB Server (freeware)
netbios-ssn stream tcp nowait root /usr/local/samba/bin/smbd smbd

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

1. Type refresh -s inetd

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

http://yourhostname:901

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

2.3 Using SWAT

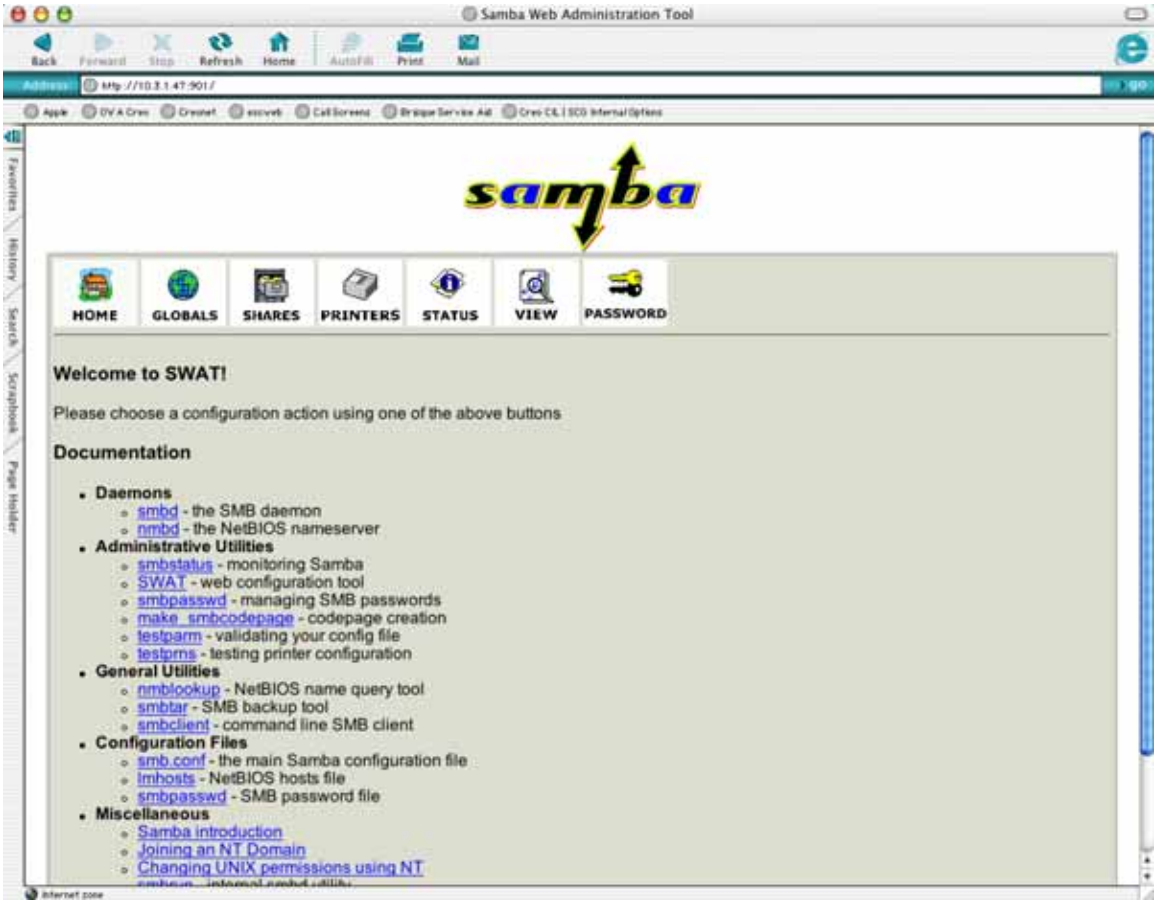
Note: We recommend to use SWAT with a great care ! Normally the engineer will not need to use SWAT,since the configuration is fully automatic.
We expect the only SWAT usage in case where more then standard shares have to be added.
DOD NOT CHANGE ANY FOLDERS SECURITY !!!!

The Samba Web Administration Tool (SWAT) is a common way to set up and maintain the smb.conf configuration file. It presents a nice, simple graphical interface using your favourite Web browser. All of the pages have a similar look and feel; so, it is very easy to learn to use SWAT. SWAT itself is a small Web server and CGI scripting application designed to run from inetd, which provides access to the smb.conf configuration file.
Authorized users can configure the smb.conf file via a Web interface. SWAT also has links to help for each option on every page.

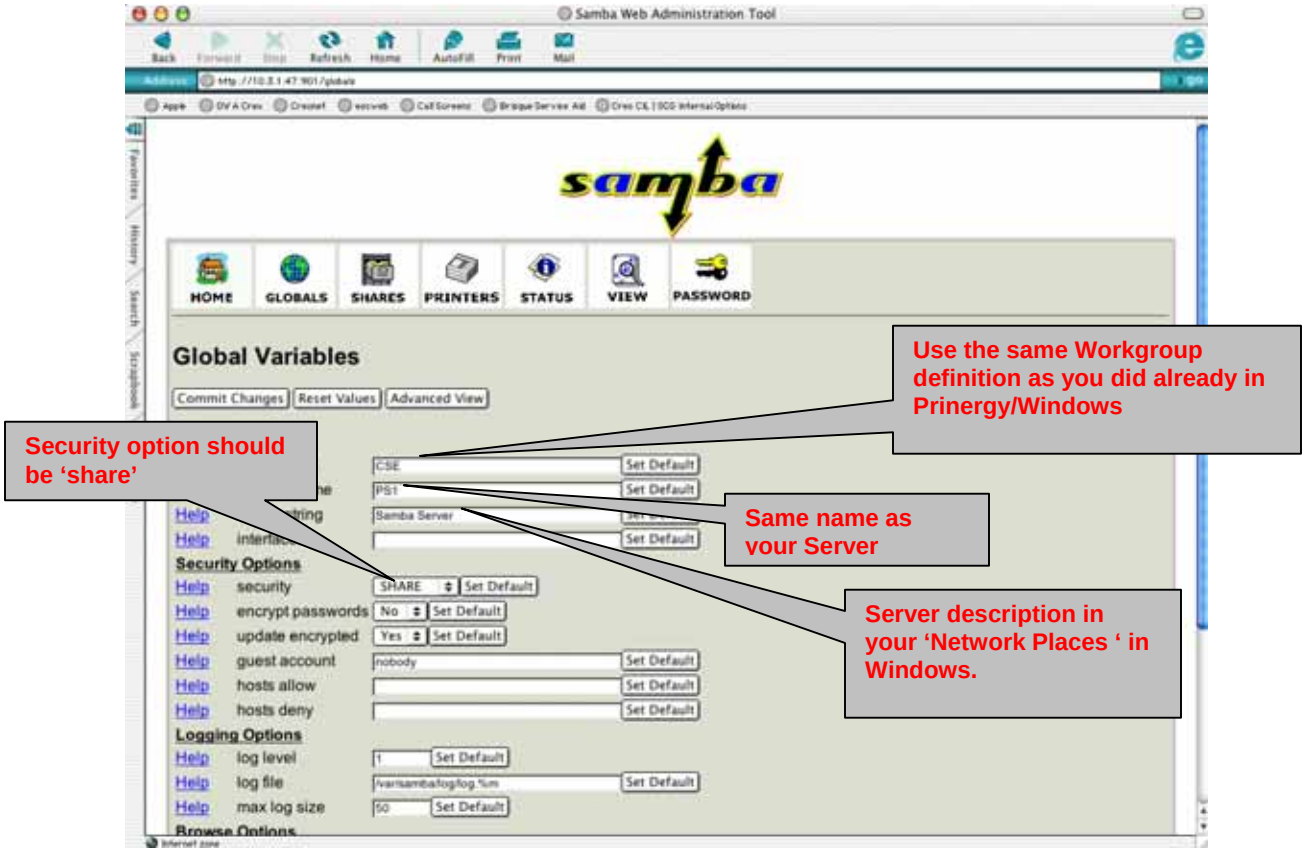
If you set up and configured everything without errors, you are ready to use SWAT.
To start SWAT, point your favourite Web browser to the Internet address of your Samba server on port 901. You will be asked to authenticate; so, enter a username and the password of a user defined on your server. You can access SWAT with any AIX user, but you can only make changes when logged in as the root user.
Remember, when you are logging on to SWAT from a remote machine, you are sending passwords in plain text. This can be a security issue; so, it is recommended that you do SWAT administration locally on the server.
If you make any changes to the smb.conf file, the Samba server will reread the file and pick up the changes every 60 seconds. If you cannot wait that long, you can send a HUP signal to the smbd and nmbd daemons to force them to honour the changes. The SWAT opening page is shown in the attached screen grabs.
where you will see that there are seven categories available: Home, Globals, Shares, Printers, Status, View, and Passwords.

2.4 The SAMBA swat Interface

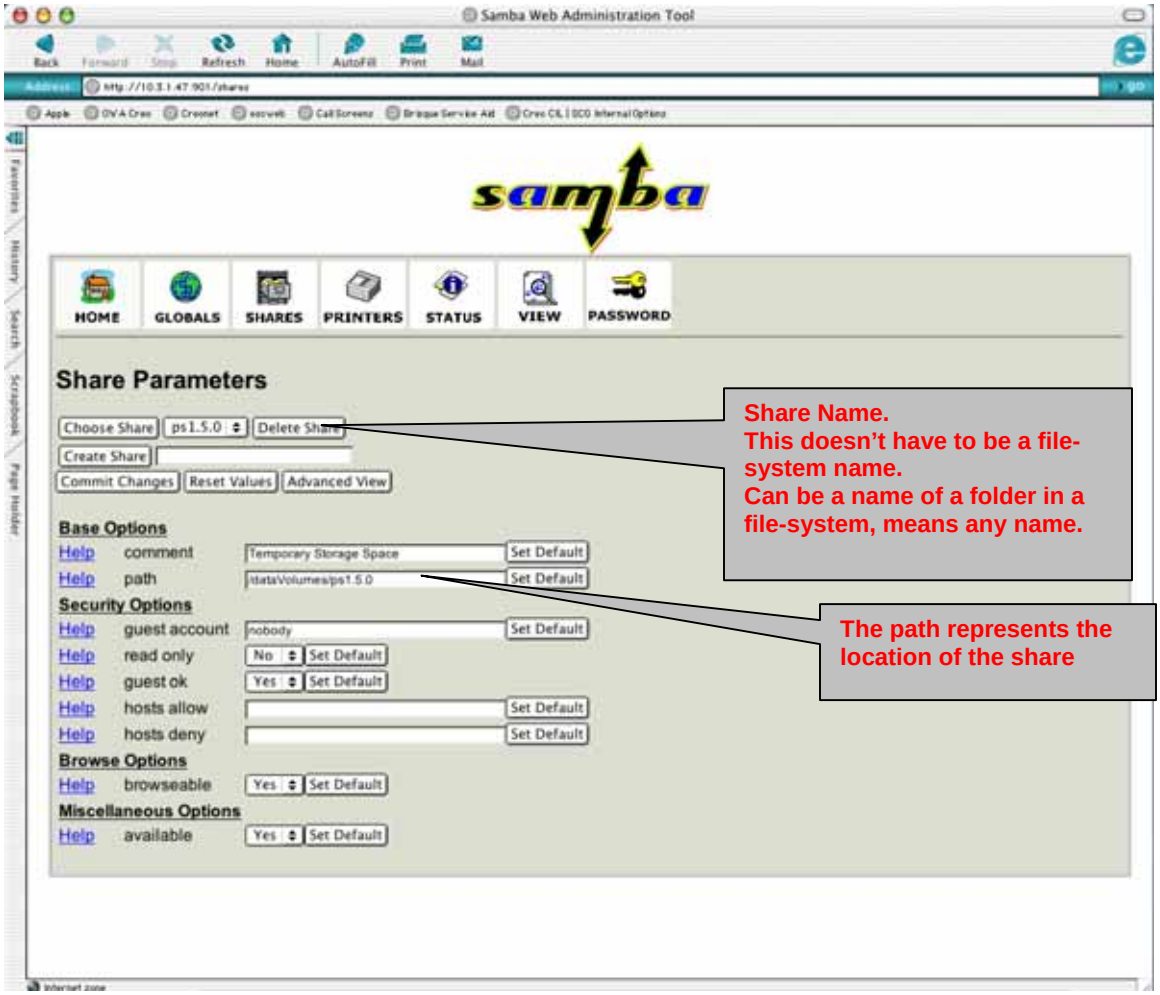
The swat is the Browser GUI of SAMBA to ease the configuration
To logon you open a browser window and type:
http://<ip address>:901.
Alternatively the host name could be used if the client address is in the host file of the server.



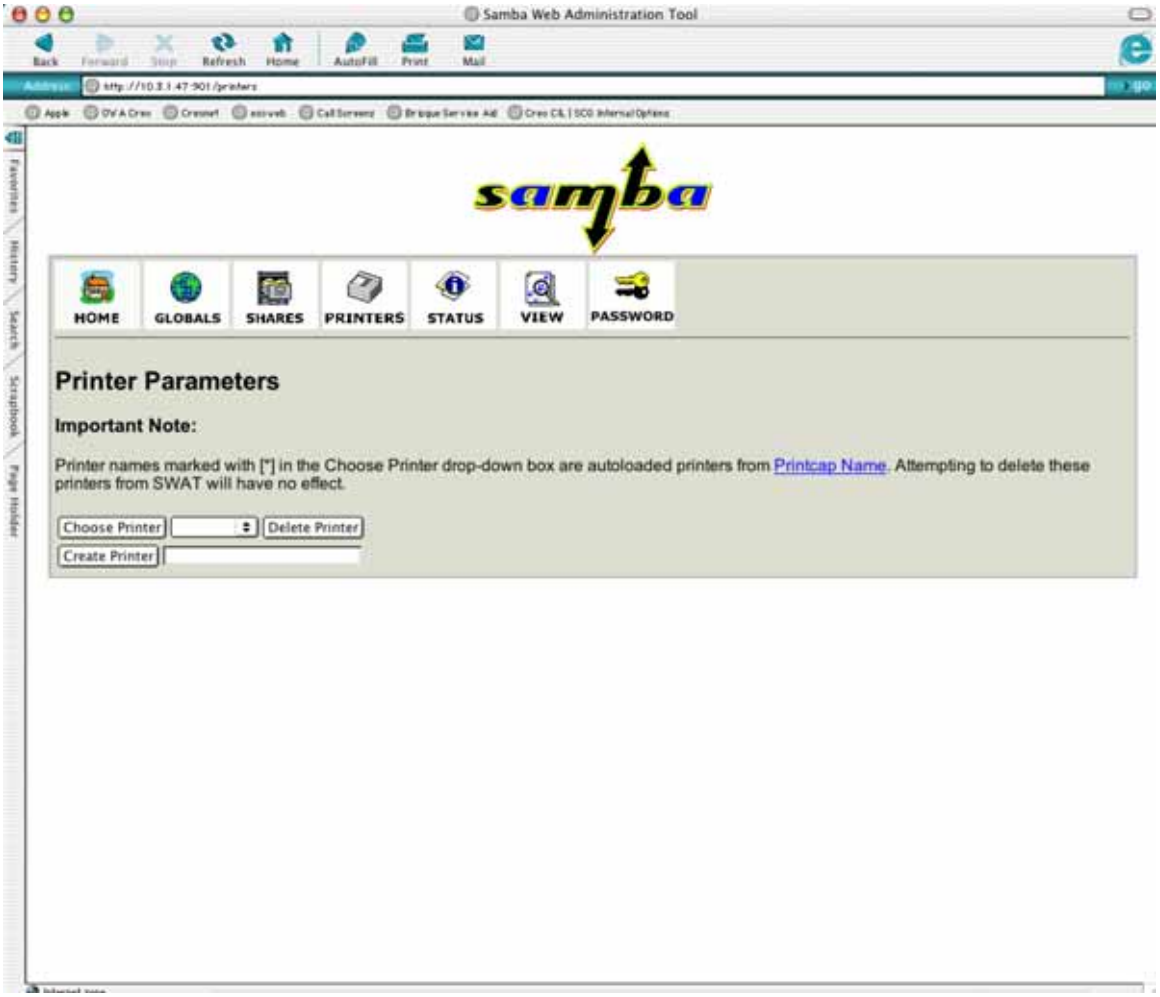
Home is linking to the documentation part of SAMBA (/usr/local/samba/man)



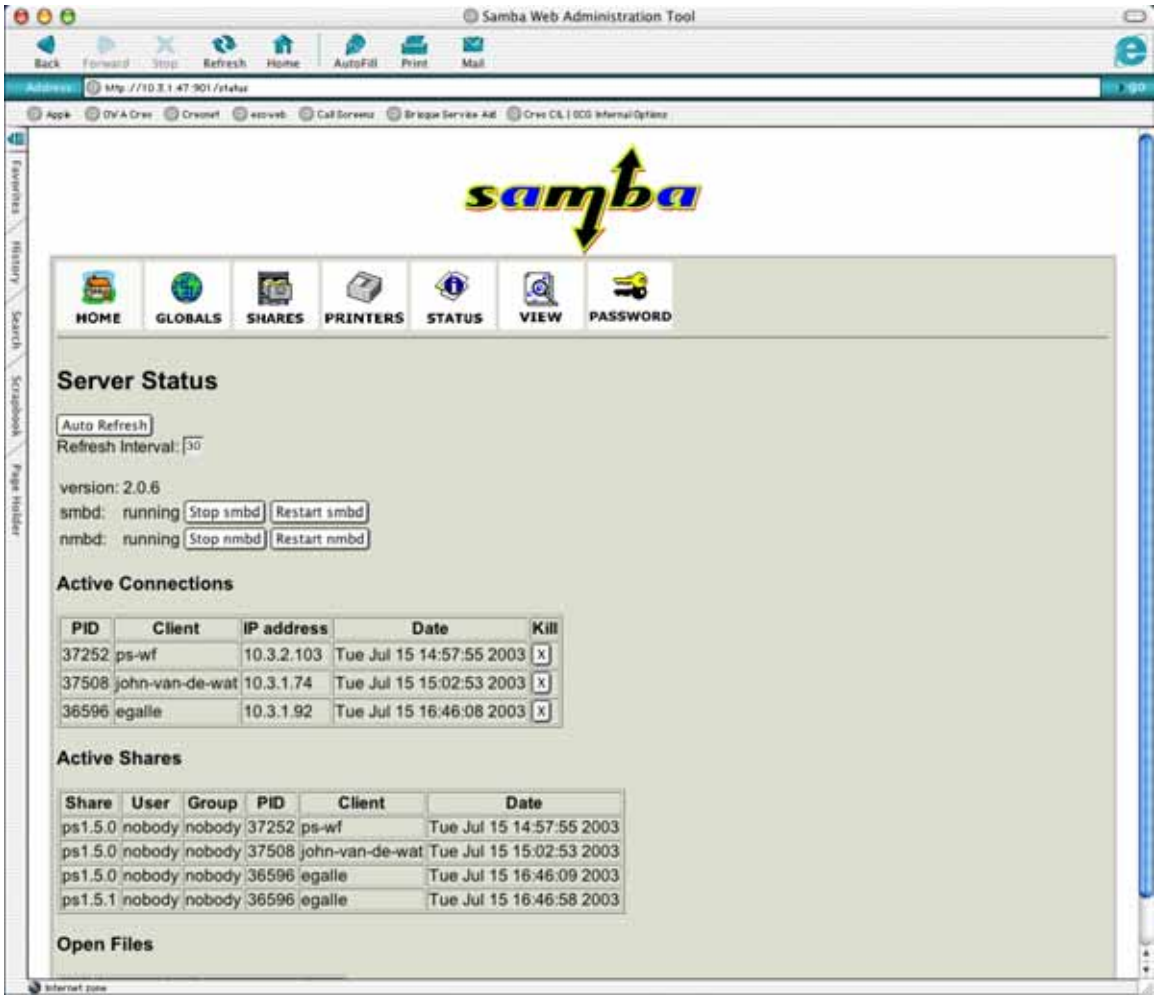
Global variables to set-up the base parameters for the SAMBA Server.
After doing all changes press the 'commit changes' button.
Guest Account MUST BE "macuser" !!!



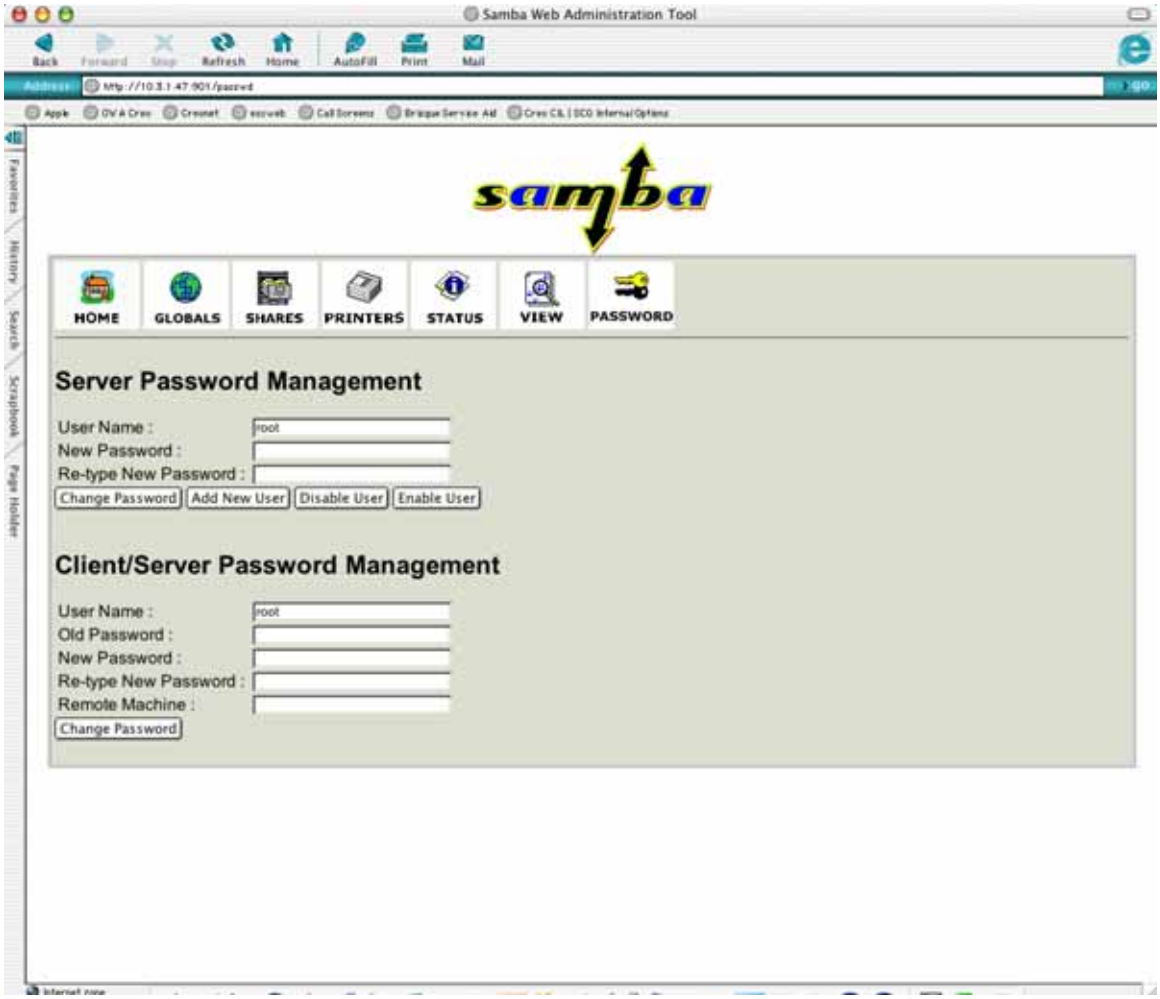
Dialog window for share set-up.
All additional options are set in Globals already.
Create share first.
Then choose share to open the dialog.
Guest Account MUST BE "macuser" !!!



Printer set-up to print via Unix.



Server Status gives information about clients connected and Server shares.
To disconnect a client click the kill button.
Stop and restart are also options in that menu.



Password set-up file.

3 Known Limitations:

3.1 Extensions

Windows cannot handle files with no extension, but this is not SAMBA related, its just because Windows is not able to handle resources. Lets say, resources doesn't exist on Windows, its always
one file including all information about preview, creator,…….
Anyway, there are no problems to use files, open them, modify them by accessing the SAMBA server.
SAMBA is fast, reliable, easy to install and configure.

3.2 Unsupported characters

The following characters are not supported by Windows:
\ / : * ? " < > |
Windows will not even allow to use those characters.

3.3 Usernames.

Invalid characters for usernames:
Invalid characters
AIX
: Colon
/ Forward slash
\ Back slash
= Equal sign
, Comma
? Question mark
" Double quote
Pound sign

Windows
; Semi-colon
/ Forward slash
\ Back slash
= Equals sign
, Comma
? Question mark
[Left square bracket
] Right square bracket
| Vertical bar
+ Plus sign
* Asterix
< Less than sign
> Greater than sign

3.4 Other limitations

AIX
Must not start with a - (dash),
+ (plus sign), @ (at sign), or
~ (tilde)
Windows
Must include more than only
periods (.) and spaces
AIX usernames are case-sensitive and limited to no more than eight characters in length. They can include double-byte characters. AIX passwords are case-sensitive and can be arbitrarily long, although, **only the first eight characters are considered distinct, with extra characters ignored during the logon process.**
The various Windows clients each have their differing limitations on username and password syntax. Most Windows systems allow usernames of up to 20 characters, although, Windows 98 allows up to 128 characters.
Windows usernames are not case-sensitive. Older Windows clients only allow short, case-independent passwords and often uppercase them during authentication. More recent Windows clients use case-sensitive passwords of up to 14 characters in length.
The best cure for these incompatibilities is forward planning when designing your user account policies, but Samba also offers some mechanisms to map between the AIX and Windows standards.

4 Joining an existing domain

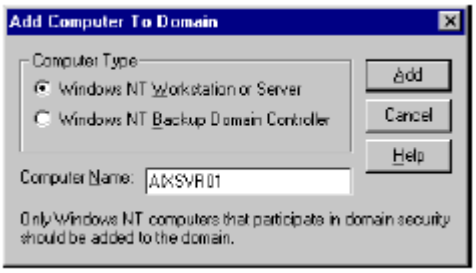
Since Version 1.9.18, Samba has included the ability to authenticate users against a remote password server, whether this is another Samba server or a Windows NT server. This was called server-level security and was configured by way of the security=server parameter in smb.conf. Server-level security has some limitations: It only returns a simple success/failure on password authentication and must maintain a connection with the password server for the duration of the client connection.
Samba Version 2.0.0 introduced domain-level security, which allows the Samba server to act as a member server in an existing domain. This is configured via the security=domain parameter in smb.conf. Domain-level security has several advantages over server-level security: Authentication returns the full set of user attributes (not just success/failure), and there is participation in domain trust relationships and reduced load on the password server (no unnecessary connection).
When a client attempts to access the server, Samba contacts the remote password server with the user's username and password. If the password is accepted by the remote password server, Samba grants the client access to the resources it requested.

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

4.1 Adding a Samba server to an NT 4.0 domain

In order for a Samba server to join an NT 4.0 domain, you must first add the NetBIOS name of the Samba server to the Domain using the Server Manager for Domains tool (srvmgr.exe). This creates the machine account in the Primary Domain Controller's (PDC) System Administration Manager (SAM). You will need Domain Administrator privileges to accomplish this. Perform the following steps:
1. On a Windows client; Run the Server Manager for Domains tool, svrmgr.exe, and from the menu, select **Computer -> Add to Domain**.

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



Add Computer To Domain - Server Manager for Domains

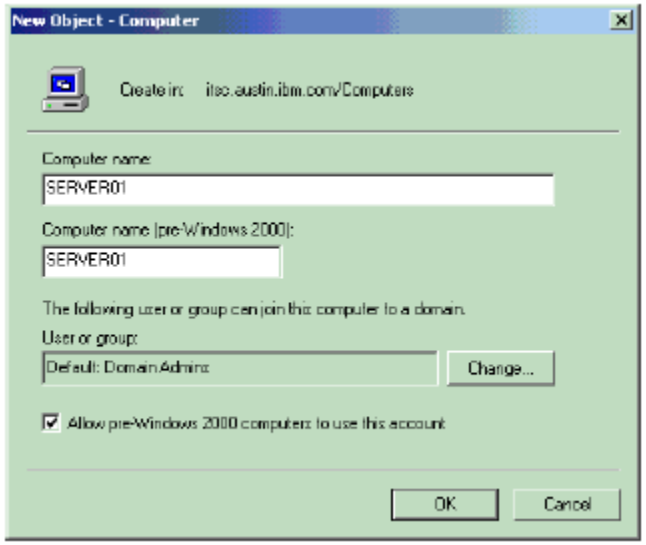
Your Samba server should now appear in the browse list for this domain.

4.2 Adding a Samba server to an Active Directory domain

Windows 2000 supports a mixed-mode domain model, which is, supposedly, 100 percent backwards-compatible with the pre-Windows 2000 domain model. This allows us to use a very similar process when joining the Active Directory domain as a member server.
Just as with an NT 4.0 domain, you must add the NetBIOS name of the Samba server to the Active Directory before configuring Samba. This creates the machine account in the Active Directory database. You will need Domain Administrator privileges to accomplish this.
The following description can be found on the Web site, http://web.mit.edu/pismere/directory-services/migration-4to5.html:
Windows NT supports a mixed environment of Windows NT 5.0 Active Directory domain controllers and Windows NT 4.0 domain controllers. Customers can migrate at their own pace, based on business needs. Down-level clients will think they are accessing Windows NT 4.0 domain controllers. Windows NT Workstation and Windows® 95 clients that do not have the Active Directory access software will be able to log on to Active Directory domain controllers by using Windows NT LAN Manager (NTLM) challenge/response authentication.
1. On a Windows 2000 client, either manually run the Server Manager for Domains tool (svrmgr.exe), or, from the Start menu, select **Start -> Programs -> Administrative Tools -> Active Directory Users and Computers**.

2. From within the Active Directory Users and Computers tool, click the right-hand button in the Computers folder, and select **New -> Computer**.

3. Next, enter the NetBIOS name of the Samba server you wish to add. Select the **Allow pre-Windows 2000 computers to use this account** option as shown.



Adding Samba to an Active Directory domain - Users and Computers

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

4.2.1 Create an AIX Samba server account to domain

Assume you have a Samba 2.0.x server with a NetBIOS name of SERVER01 and are joining an NT domain called DOMAIN01, which has a PDC with a NetBIOS name of DOMPDC and two backup domain controllers with the NetBIOS names, DOMBDC1 and DOMBDC2.
1. In order to join the domain, first, stop all Samba daemons and run the following command:

smbpasswd -j DOMAIN01 -r DOMPDC

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

smbpasswd: Joined domain DOM.

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

The filename looks like this:

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

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

DOMAIN01.SERVER01.mac

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

4.2.2 Configure the AIX Samba server

Before restarting the Samba daemons, you must edit your smb.conf file to tell Samba it should now use domain-level security. Perform the following steps:
1. Alter the security parameter in the [global] section of your smb.conf to read:

security = domain

2. Next, change the workgroup parameter to read:

workgroup = DOMAIN01

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

encrypt passwords = Yes

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

password server = DOMPDC DOMBDC1 DOMBDC2

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

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

5. Finally, restart your Samba daemons and try to connect to your Samba server using a valid Domain username and password.
Remember, even with domain-level security, you still need an AIX account on the Samba server, although you do not need the ability to log in to AIX. If you have any difficulty, examine Samba's log files while attempting to connect.

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

5 Samba Windows Client set-up

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

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

Windows 9x Windows 9x was not designed to have multiple users; so, we need to customize it in order to have at least one different profile for each user. Click **Start -> Settings -> Control Panel** and double-click the **Passwords** icon. The Passwords Properties dialog box appears as shown in Figure 1.



Figure 1. User profiles

Select the **User profiles** tab, and then click the lower of the two radio buttons. Now, click the **Change Passwords** tab. You should see the tab as shown in Figure 2 on page 3.

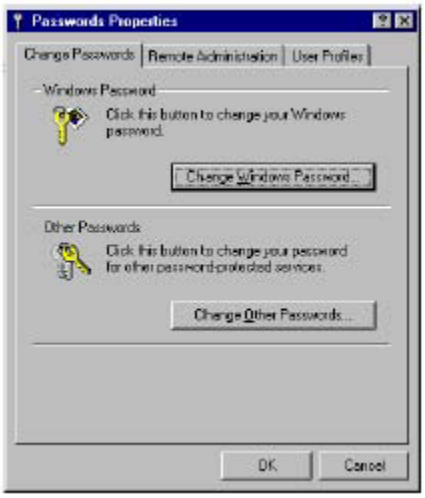


Figure 2. Change Windows passwords

In this tab, you can change the password that you are going to use with the Samba server. If this tab does not appear, you need to reboot Windows, and, when it starts, log on with a user name and password. Return to the Control Panel and select the **Network** icon. You should now see the Network dialog box shown in Figure 3 on page 4.

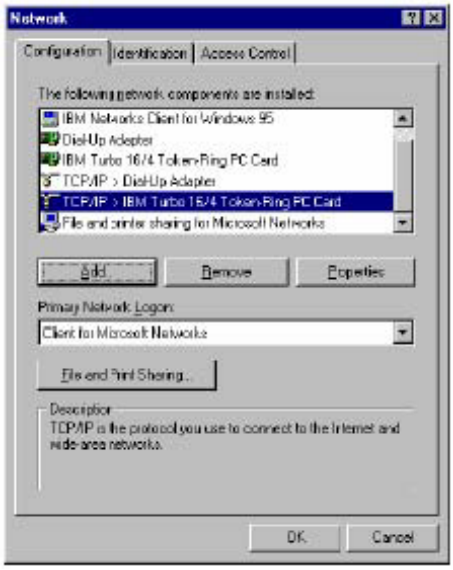


Figure 3. Network dialog box

Choose the TCP/IP protocol with the adapter with which that you want to access the Samba server, and click **Properties**. Select the **WINS Configuration** tab, and you should now see the dialog box shown in Figure 4 on page 5.

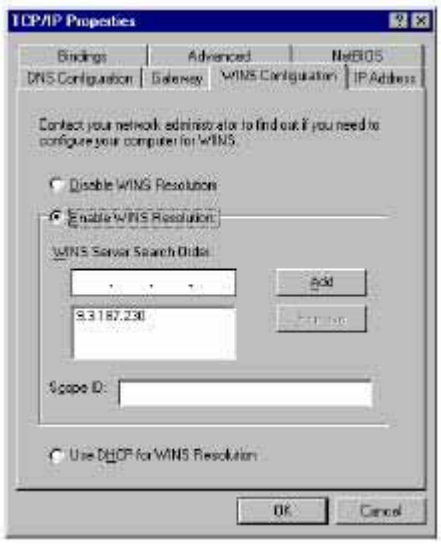


Figure 4. WINS configuration

Click the **Enable WINS Resolutions** radio button. Now, you have to enter the IP Address of the WINS server. Click **Add** and then **OK**. You should see the Network dialog box again; so, select the **Identification** tab. You should see a dialog box similar to Figure 4 on page 5.

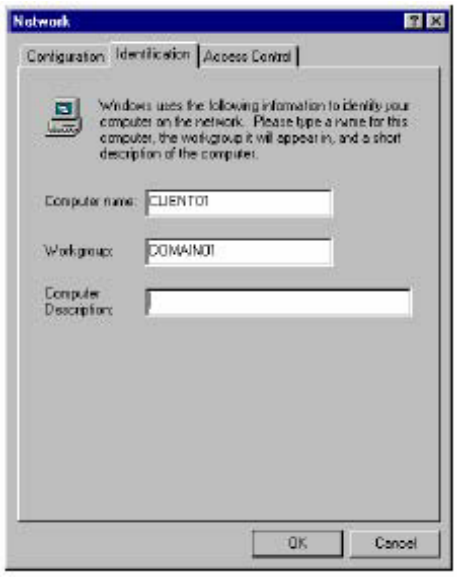


Figure 5. Windows 95/98 Identification

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

Accessing the Samba server

You must have a valid Windows logon to get access to the Samba server. See Figure 6 on page 7 for information on how to select the primary network logon to be a valid logon session.



Figure 6. Select Primary Network logon

5.1 Locating the Samba server from Windows 9x

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

- Using the Network Neighbourhood option
- Using the Find Computer option
- Using the command line We will use the following parameters in this chapter:
- Domain name: LV200
- Samba servers: lva200a, lva200b
- NetBIOS name server (NBNS): lva200a

5.2 Using the Network Neighborhood program

The Network Neighbourhood option comes standard with all Windows versions. This option is added to the station desktop after the network configuration is done. Perform the following steps to locate the Samba server through the Network Neighbourhood program:
1. Double-click on the **Network Neighbourhood** icon.
2. Double-click on the **Entire Network** icon.

3. Double-click on the **Microsoft Windows Network** icon.
4. Select the correct domain name (LVA200) and double-click.
5. You will see the server name (lva200a) and other machines of the same domain as shown in Figure 7.



Figure 7. LVA200 domain

5.3 Using the Find Computer option

Another way to locate the Samba server is by using the Find Computer option. To find the Samba server (lva200b) using this option, perform the following steps:
1. Select the find **Computer** option from the **Find** menu located in the **Start Menu** of Windows 9x (**Start -> Find -> Computer**).
2. Enter the NetBIOS name of the Samba server to locate as shown in Figure 8.



Figure 8. Find Computer

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

Using the command line To locate the Samba server from the command line interface, use the NET VIEW command in the command line window. The NET VIEW command displays a list of computers in the specified domain or shared resources available on the specified computer.
To find the Samba server (lva200a) using this option, perform the following steps:
1. Open an MS-DOS command line interface by selecting **Start -> Programs -> Command Prompt**.
2. Enter the following command to locate the Samba server (lva200a), and you will see a list of shared resources on this server:

net view \\<server name>

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

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

Samba Server

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

Or enter:
net view /DOMAIN:<domain name>

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

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

-------------------------------------------------------------------------------
\\AUSRH306
\\LVA200A               43P Samba
\\LVA200B               SAMBA Server
\\LVA200PDC
\\LVA200X2
\\LVA200X3
The command completed successfully.
C:\>
```

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

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

5.4 Accessing resources from Windows 9x clients

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

5.4.1 **Accessing files**

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

5.4.2 GUI interface

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

Using a UNC name

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

1. After having located the Samba server, double-click on the server, and select the shared folder where your files reside. See Figure 9 on page 10.



Figure 9. Shares resources on Samba server

Or

2. Select the **Run** option from Start menu and enter the following command using this syntax:
\\<Server Name>\<Shared Resource>\[Path]

Where:

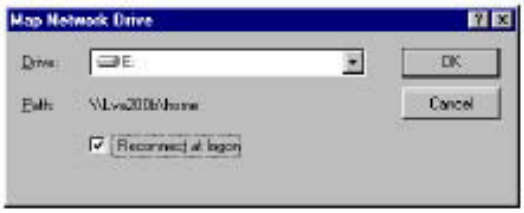
- <Server Name> is the NetBIOS name of the Samba server.
- <Shared Resource> is the shared name.
- [Path] is the path where the files reside. See Figure 10.



5.4.3 Mapping network drive

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

1. Locate the server and share name where the files reside.
2. Select the shared resource and select the **Map Network Drive** option from the File menu or by right-clicking on it.
3. Select an available drive letter to which to link the UNC name and check the Reconnect at Logon option to make this map available every time the machine is restarted. See Figure 10.



5.4.4 Command line interface

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

```
C:\>net use d: \\lva203a\home
The command completed successfully.

C:\>
```

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

5.4.5 Accessing Printer shares

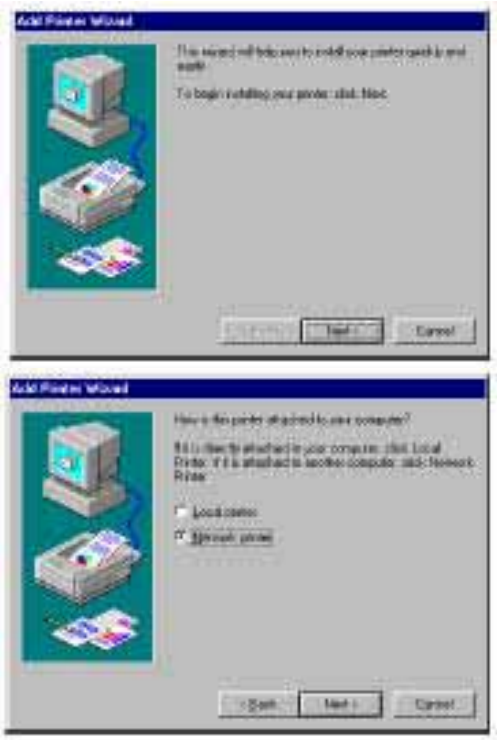
To access printers located in the Samba server acting as a print server, it is required to add this printer and install the appropriate printer driver.
There are two ways of configuring a network printer in Windows 9x:

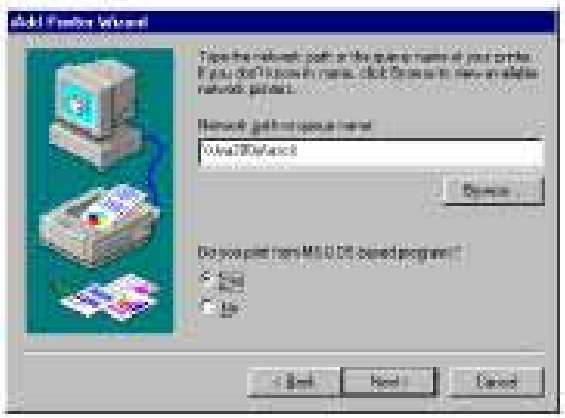
- Using the GUI interface.
- Using the command line interface.

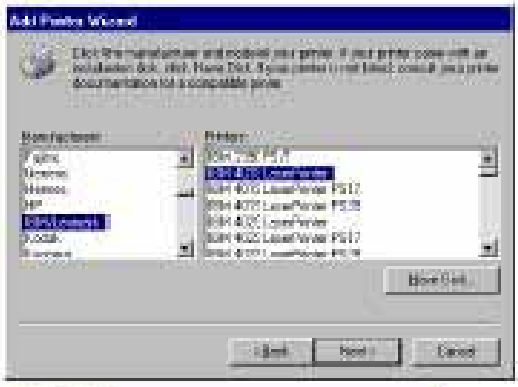
5.4.6 GUI interface

Perform the following steps to configure a network printer located in the Samba server:
1. Select the **Printers** administration folder from Start menu or My Computer icon: **Start -> Settings -> Printers** or **My Computer -> Printers**.
2. Double-click on the **Add Printer** icon to create a new printer. The **Add** Printer Wizard will appear as shown in Figure 11 on page 13.
3. Press the **Next** button and select the type of connection with the printer. In this case, it is a **Network printer** as shown in Figure 12.
4. Press the **Next** button and enter the network path where this printer is located (UNC). Select the **Yes** or **No** radio button option if you want to use this printer from MS-DOS based programs. See Figure 13 on page 14.
5. Press the **Next** button and select the printer driver that will be used with this printer. You may have to provide the CDROM containing this driver during this step. See Figure 14.
6. Press **Next** and enter the printer name for your client. See Figure 15 on page 15.
7. Press the **Finish** button. The printer is now ready to be used from any Windows program.

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









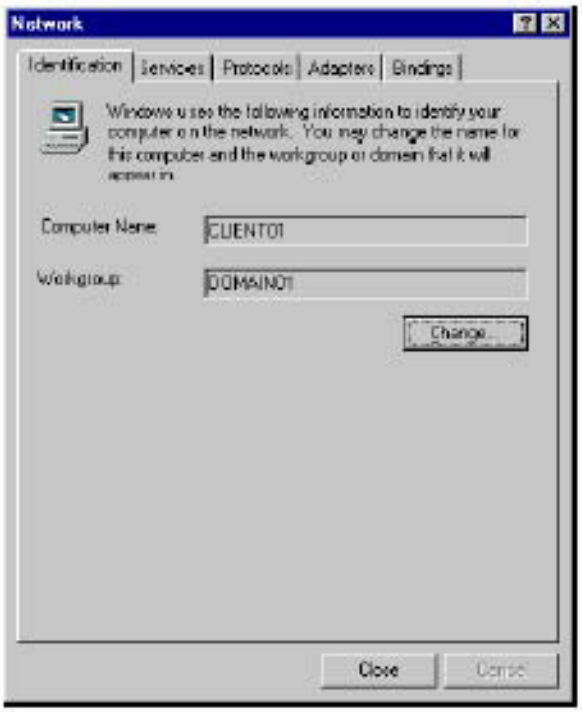
net use LPT1: \\lva200a\ascii
You will then have to follow the steps described in “GUI interface” to associate a driver and a name to this printer.

5.5 Accessing Samba from Windows NT clients

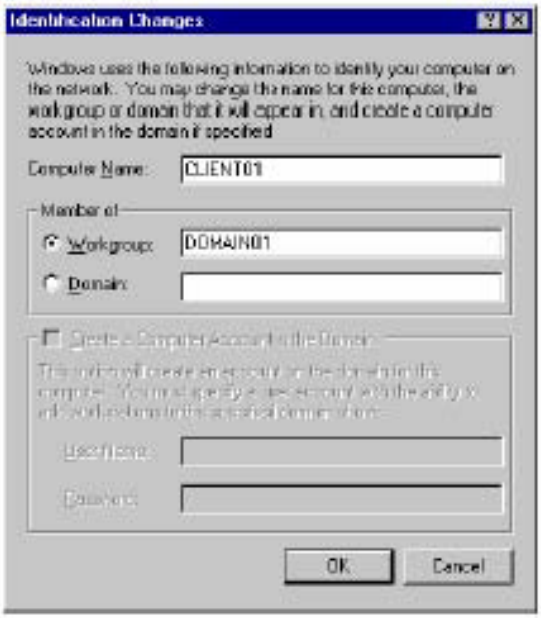
This section will describe how to access shared resources, such as files and printers, from Samba server using Windows NT client.

5.5.1 Configuring Windows NT

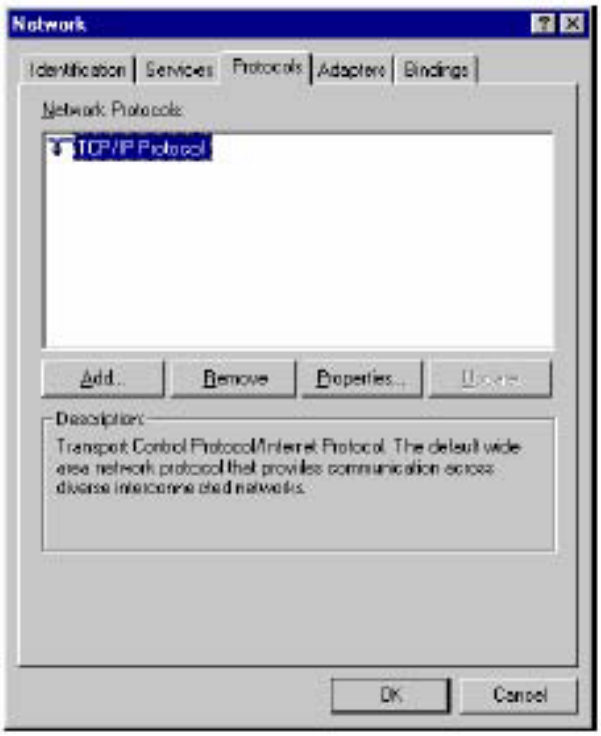
Before you start to configure Windows NT, make sure that you have installed the Workstation service and the TCP/IP protocol. Make sure that you are logged on as Administrator or at least with a user that is included in the local Administrators group. Click on **Start -> Settings -> Control Panel** and double-click on the **Network** icon. The Network dialog box should appear as shown in Figure 15 on page 16.



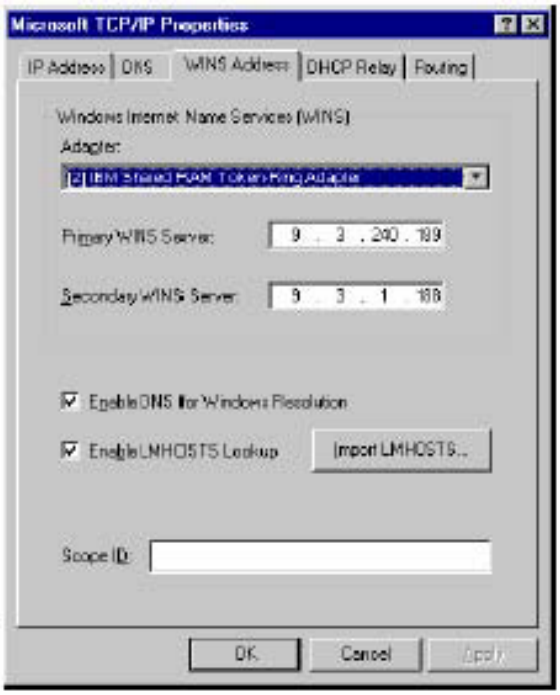
While on the Identification tab, click the **Change** button, and you will see the dialog box shown in Figure 16 on page 17.



You should first enter your Computer Name. You will see that you will not be able to change the Workgroup at this moment in time; so, you have to click **OK**, and then click the **Change** button again to return to the Identification Changes dialog box. Now, you should click the **Workgroup** radio button and enter your Workgroup name. Put the same workgroup name that you have set up in your Samba server. You can use the same Computer Name that you enter in your TCP/IP configuration. Click **OK** when finished. You should now be back in the Network dialog box. If you have set up your Samba server to provide WINS service, you can configure the WINS Address. Click the **Protocols** tab on the Network dialog box, and you should see a dialog box similar to the one shown in Figure 17 on page 18.



Select **TCP/IP Protocol** and click **Properties**. You should see the TCP/IP dialog box. Select the **WINS Address** tab, and you will see the dialog box shown in Figure 18 on page 19.



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

5.5.2 Locating the Samba server

There are three ways to locate a Samba server from Windows clients:
• Through the Network Neighbourhood icon
• Through the Find Computer option
• Through the Command Line

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

5.5.3 Locating the server through the Network Neighbourhood

Perform the following steps:
1. Double-click on the **Network Neighbourhood** icon.
2. Double-click on the **Entire Network** icon.

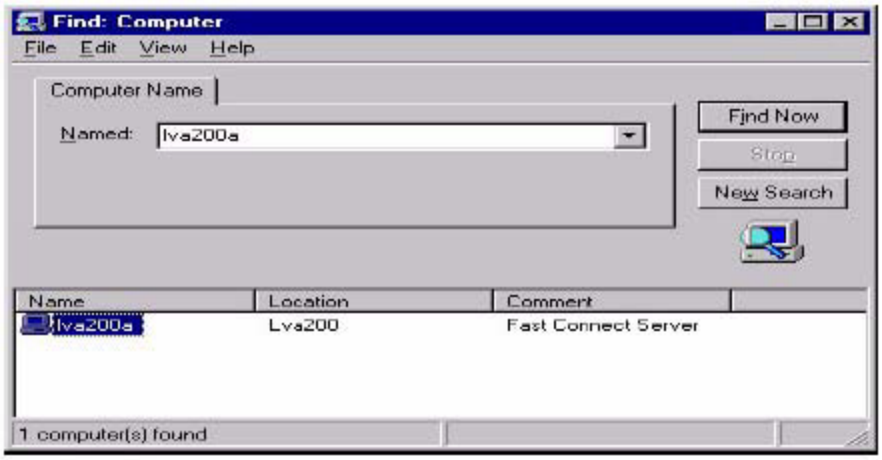
3. Double-click on the **Microsoft Windows Network** icon.
4. Double-click on the domain of your Samba server (see Figure 19)

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



5.5.4 Locating the server with the Find: Computer option

You can use the Find: Computer option to find the Samba server on the network. Perform the following steps:
1. Select **Start -> Find -> computer**.
2. Type the computer name (see Figure 20 on page 21)
3. Click on **Find Now**.



5.5.5 **Locating the server from the command line**

You can locate the Samba server with the net view command. The net view command displays a list of computers in the specified domain or shared resources available on the specified computer.
1. Select **Start -> Programs -> MS-DOS Command Prompt**.
2. At the command prompt, type: net view \\<server name> (server name is the name of the Samba server whose resources you want to view), or type net view /DOMAIN:<domain name> (domain name is the name of the domain of your Samba server).

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

Samba Server

Share name   Type         Used as  Comment

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


C:\>
```

If you use the net view command without command-line parameters, you see a list of computers with computer names in the left column and remarks in the right column.
If you use the net view command with a NetBIOS computer name (Windows server), you will see a list of available resources on that computer.

Note

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

5.6 Accessing resources from Windows NT

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

5.7 Accessing files

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

5.7.1 Using the GUI interface

When you want to access the network share from your Windows NT client, you must create a mapping to this share. You can use the Network Neighbourhood icon or the Find Computer panel to do this. In this example, we use the Find Computer option. You can follow these steps to map a network drive to a Samba shared resource:

1. Click **Start -> Find -> Computer**.
2. Enter the Computer Name and click on **Find Now** (see Figure 21 on page 23).
3. Double-click on the computer name (in this example, the computer name is lva200a)
4. You will see the shared resources of lva200a server in a new window (see Figure 22 on page 23).
5. Click on the shared resource (for example, TEST) and select **File -> Map Network Drive..** or right-click on the shared resource and select **Map Network Drive..**.
6. Select the desired drive (for example **D**:)
7. Click **OK** (see Figure 23).





5.7.2 Command line interface

Windows NT will need to define a drive mapping to access the shared resources exported by Samba. These drive mappings can be done from the DOS command prompt.
You have to use the NET USE command to define mappings between PC drive letters and a Samba shared resource:

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

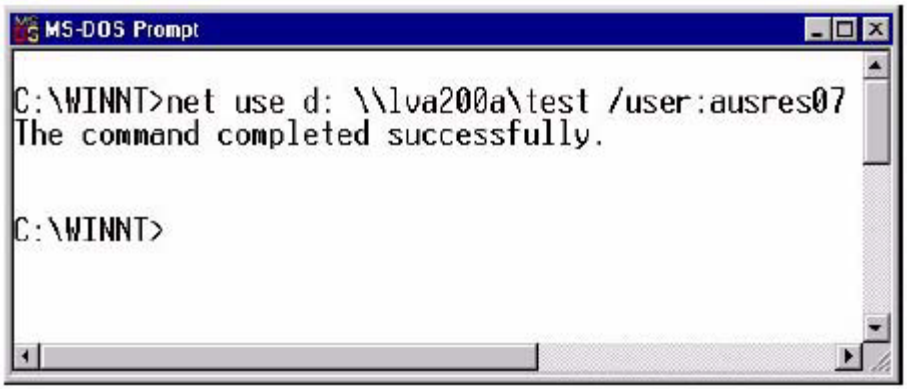


Figure 24. Map network drive from MS-DOS DOS> net help (help info for net command) DOS> net use D: /delete (delete the drive mapping) If you use the NET USE command without command-line parameters, you see the status of network connections, the local name of connections (the mapped drive letters), and the remote name of connections (the server location).

5.8 Accessing the Samba printers

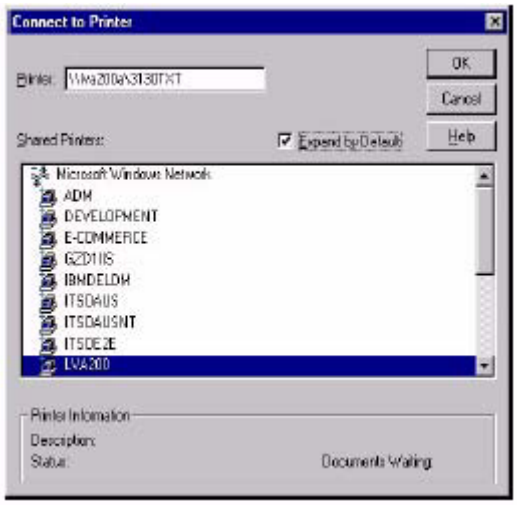
If you want to access a Samba server printer from Windows NT, you will need to install the appropriate printer driver and map the print resource to a network printer.
You have two ways to configure a network printer on Windows NT:

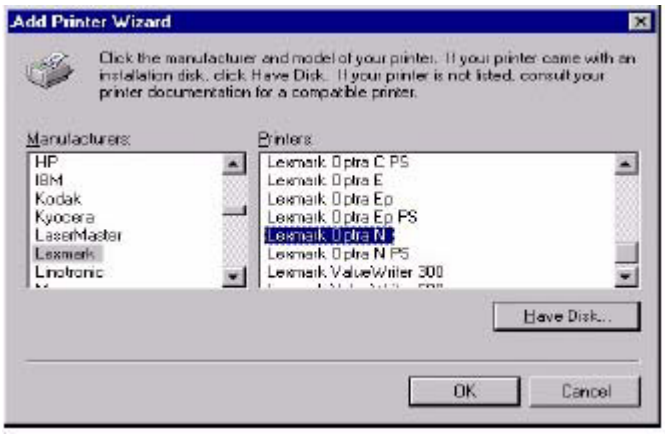
- From the GUI interface
- From the command line interface

5.8.1 GUI interface

you can follow this procedure to configure a network printer from the GUI interface:
1. Select **Start -> Settings -> Printers -> Add Printer**.
2. Select **Network printer server**.

3. Select the network printer from a list or enter its path directly (for example, :\\lva200a\3130TXT as shown in Figure 25).
4. Select the proper Windows printer driver from the list (for example, select **Lexmark Optra N**) and install it from the Windows installation media (see Figure 26 on page 26).

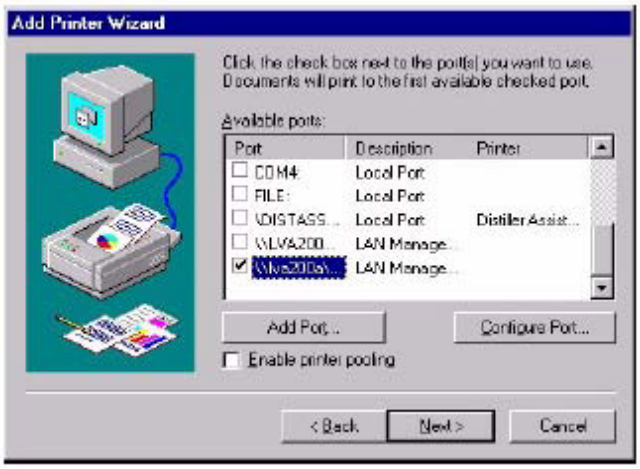




5.8.2 Command line interface

For DOS applications, you can map the network printer to local printer devices (for example LPT1). You can use the following simple device mapping on Windows NT client:
DOS> net use LPT1: \\lva200a\3130TXT
If you want to print from a Windows application, a Windows printer driver must be installed and mapped to the network printer. You must perform the following steps:
1. Select **Start -> Settings -> Printers -> Add Printer**.
2. Select **My Computer**.

3. Click the check box next to the port you want to use (see Figure 27 on page 27).
4. Select the proper Windows driver from the list (for example, select **Lexmark Optra N**) and install it from the Windows installation media.



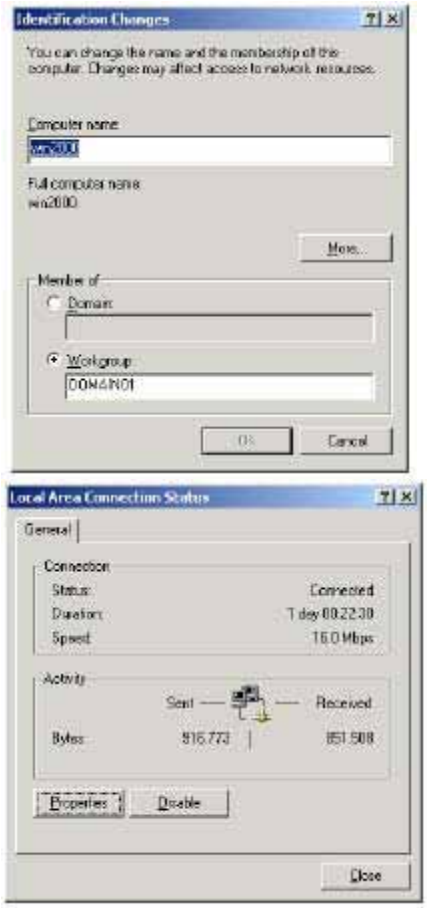
5.9 Access the Samba server from Windows 2000

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

5.9.1 Configuring Windows 2000

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

1. Click on **Start -> Settings -> Control Panel** and double-click the **System** icon. The System Properties dialog box should appear.
2. Select the **Network Identification** tab, and click the **Properties** button. You should see a dialog box as shown in Figure 28 on page 29.
3. Enter your computer name. Next, you have to click the radio button for **Workgroup** and enter the workgroup name. The workgroup name should match with the one that you set up in your Samba server.
4. Click **OK** to complete this process. Your computer will ask you to reboot. You do not need to reboot now. You can reboot when you finish the set-up.
5. Returning to the Control Panel, double-click **Network and Dial-up Connections**, and then double-click the **Local Area Connection** icon. You should see the dialog box shown in Figure 29 on page 29.
6. Click the **Properties** button, and then select **Internet Protocol (TCP/IP)** and click **Properties**. You should see the Internet Protocol (TCP/IP) Properties box dialog box as shown in Figure 30 on page 31h.
7. Click the **Advanced** button. You should see the Advanced TCP/IP Settings dialog box. Then, select the **WINS** tab. The screen, shown in Figure 31 on page 32, appears.
8. Click **Add**, and enter the IP address of your WINS server. If you have set up your Samba server to provide WINS service, you can enter the IP address of your Samba server in this field.
9. Now, click **OK** in the Advanced TCP/IP settings dialog box, click **OK** in the Internet Protocol (TCP/IP) Properties dialog box, click **OK** in the Local Area Connection Properties, and click **Close** in the Local Area Connection Status dialog box. You will need to reboot in order for the changes to take effect.



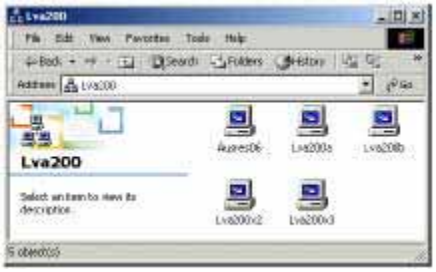


5.9.2 Locating the Samba server

There are three ways to locate a Samba server from Windows 2000 clients:
• The My Network Places icon
• The Find Computer option
• The command line

In this chapter, we use the domain name, LVA200, and the NetBIOS server name, lva200a.
Locating the server with the My Network Places icon
To locate the server with the My Network Places icon, complete the following steps:
1. Click the **My Network Places** icon.
2. Click the **Entire Network** icon.
3. Click the **Entire Contents** text.
4. Click the **Microsoft Windows Network** icon.

5. Click the domain of your Samba server.
You will find the servers on the domain you have selected as shown in Figure 32.



Locating the server with the Search for Computer option You can use the Find computer option to find the Samba server on the network. Complete the following steps:
1. Click the **My Network Places** icon.
2. Click the **Entire Network** icon.
3. Click the **Search for Computer** text.

4. Enter the computer name.
5. Click the **Search Now button** shown in Figure 33 on page 34.



5.9.3 Locating the server from the command line

You can locate the server with the net view command. The net view command displays a list of computers in the specified domain, or shared resources available on the specified computer. Complete the following steps:
1. Select **Start -> Programs -> Accessories -> Command Prompt**.
2. At the command prompt, type: net view \\<server name> (server name being the name of the Samba server whose resources you want to view), or type net view /DOMAIN:<domain name> (domain name being the name of the domain of your Samba server).
If you use the net view command without command line parameters, you see a list of computers with computer names in the left column and remarks in the right column.
If you use the net view command with a NetBIOS computer name (Windows server), you will see a list of available resources on that computer.

Note

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

Accessing resources from the Samba server
The following sections describe how to connect a Windows 2000 client to a Samba server.

5.10 Accessing Files

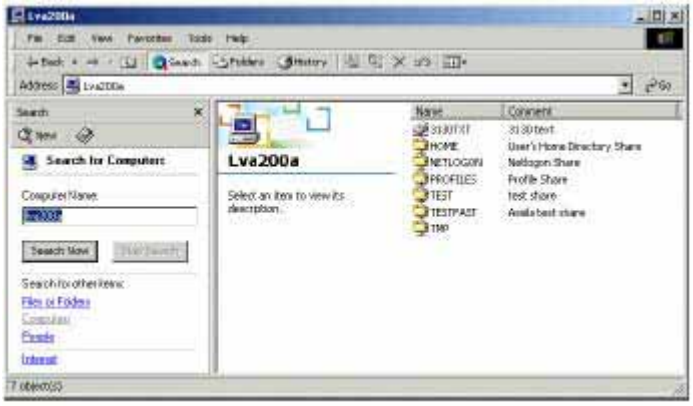
You can access the Samba shares from your Windows 2000 client from the GUI interface or the command line interface.

5.10.1 Using the GUI interface

When you want to access the network shared resource from your Windows 2000 client, you can create a mapping to this shared resource. You can use the My Network Places icon or the Search for Computers panel to do this. In this example, we use the Search for Computers option. You can perform the following steps to map a network drive to Samba shared resources:

1. Click the **My Network Places** icon.
2. Click the **Entire Network** icon.
3. Click the **Search for Computers** text.

4. Enter the computer name and click the **Search Now** button.
5. Double-click the computer name (lva200a in this example) .
6. You will see the shared resources of the lva200a server (see Figure 34).
7. Click the shared resource (for example, TEST) and select **File -> Map Network Drive...** or right-click the shared resource and select **Map Network Drive...**.
8. Select the desired drive (for example **G:**).
9. Click the **Finish** button.





5.10.2 Using the command line interface

Windows 2000 can also define drive mapping to the shared resources from the DOS command prompt. You have to use the net use command to define mappings between the PC drive letters and the Samba shared resource. You can use the net use command without parameters to see the current status of mapped shares.

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

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

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

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

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

You can delete network mapping with the /delete option.

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

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

5.11 Accessing printers

If you want to access a Samba server printer from Windows 2000, you will need to install the appropriate printer driver and map it to the network printer.
You have two ways of configuring a network printer on the Windows 2000 client:

- From the GUI interface
- From the command line interface

5.11.1 Using the GUI interface

You can perform the following steps to configure a network printer from the GUI interface:
1. Select **Start -> Settings -> Printers -> Add Printer**.
2. Press the **Next** button.
3. Select the Network printer server and press the **Next** button.
4. Select the network printer from a list or enter its path directly (for example, \\lva200a\3130TXT). See Figure 36 on page 39.
5. Select the proper Windows printer driver from the list (for example, select **Lexmark Optra N**), and install it from the Windows installation media (see Figure 37).

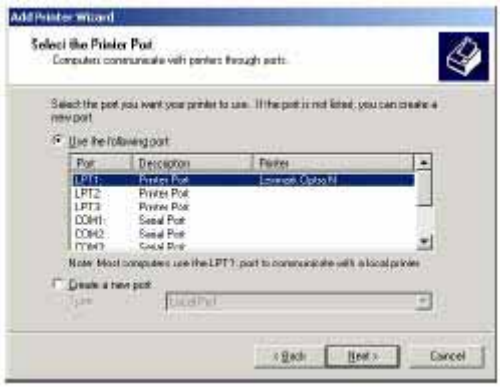




5.11.2 Command line interface

For DOS application, you can map the network printer to local printer devices (for example, LPT1). You can use the following simple device mapping on Windows 2000 client:
net use LPT1: \\lva200a\3130txt

If you want to print from a Windows application, a windows printer driver must be installed and mapped to the network printer. You must perform the following steps:
1. Select **Start -> Settings -> Printers -> Add Printer** .
2. Click the **Next** button.
3. Select **Local Printer** and deselect **Automatically detect and install my Plug and Play printer** option.
4. Select the port you want to use (see Figure 38), and press the **Next** button.
5. Select the proper windows driver from the list (for example, select **Lexmark Optra N**) and install it from the windows installation media.
6. Press the **Next** Button.
7. Enter the name of the printer, and press the **Next** button.
8. Press the **Next** button three times, and then press the **Finish** button.



6 Appendix A. Troubleshooting

This appendix describes the basic tools for locating problems with Samba, clients, and SMB/CIFS protocols and how to narrow them down.

6.1 Protocol levels

It is hard to define, in a very strict way, how to find the problems in a domain as large as the combination of the SMB and TCP/IP protocols. The following sections provide some steps and hints you should not forget when troubleshooting the SMB protocol.
The TCP/IP protocol is divided into separate independent levels. This architecture helps us because, normally, we only have a problem in one level and must locate it. Here is a simplified version of these levels that can help you locate the problem. You should try to locate the lowest network level with the problem. If you have, for example, a problem with name resolution, access to the shares will probably not work.

• **TCP/IP protocols**

- **Address resolution** - This is the conversion from the hardware network address to the IP address and back. The utilities are arp and ping.
- **Routing** - This is a mechanism for transferring traffic (packets) from one network to another, that is, out of your local network and back. The utilities are traceroute, route, ping, netstat, and tracert.
- **Name resolution** - This is the conversion from the domain name to the IP address. The utilities are nslookup and host.

• **SMB protocols**

- **Name resolution** - This is the conversion from the SMB name to the IP address. The utility is nbtstat.
- **Browsing** - This is the function on the SMB network that provides a list of accessible computers and resources to the clients. The utilities are browstat and smbclient.
- **Authentication** - This is the verification of the client on the SMB server.
- **Access** - This is the access of the client to the shared resources.
- **Netlogon** - This is the network logon feature of the SMB server.

6.2 Generic TCP/IP utilities

If you know your network organization, use the following tools to check the status of the TCP/IP level of the network. If you do not know the network organization, use the same tools to find it. These utilities are available on AIX and also on Windows NT. Some of them may be missing on the Windows 95 system. These utilities are:

ipconfig This shows the IP configuration on Windows NT machines.
ping This checks the IP connectivity. Try to ping to localhost (127.0.0.1), local IP address, gateway, and remote computer. Try it with computer name and IP address.
traceroute This checks the route from one computer in a TCP/IP network to another (use tracert on client).
route This prints out the routing table. You can also add and delete routes.
netstat This shows the aspects of the status of the network, such as routing table, port allocation, and statistics.
nslookup This checks the Domain Name Service (DNS) - TCP/IP name resolution. You can find IP address from the computer name and vice versa.
arp This shows and modifies the table for IP address to adapter address translation.
Try to determine if the problem is only one computer.

6.3 Troubleshooting utilities on Windows NT

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

6.4 TCP/IP configuration

The TCP/IP configuration of the Windows NT system can be obtained with the `ipconfig` command. You can use the /all switch to see detailed information about IP address, netmask, gateway address, and so forth.

```
Windows NT IP Configuration
Host Name . . . . . . . . . : lv3030b.itsc.austin.ibm.com
DNS Servers . . . . . . . . : 9.3.240.2
Node Type . . . . . . . . . : Hybrid
NetBIOS Scope ID. . . . . . :
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
NetBIOS Resolution Uses DNS : Yes
Token Ring adapter Ibmtok51:
Description . . . . . . . . : IBM Token Ring Network Card for PC I/O bus.
Physical Address. . . . . . : 00-06-29-68-8B-2E
DHCP Enabled. . . . . . . . : Yes
IP Address. . . . . . . . . : 9.3.240.123
Subnet Mask . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . : 9.3.240.1
DHCP Server . . . . . . . . : 9.3.240.2
Primary WINS Server . . . . : 9.3.1.81
Lease Obtained. . . . . . . : Monday, February 15, 1999 3:05:31 PM
Lease Expires . . . . . . . : Tuesday, February 16, 1999 9:05:31 AM
```

You can use the `winipcfg` command on Windows 95 systems to get similar information.
You can use other commands that can help you analyze the configuration,

routing, DNS, and other TCP/IP-related problems, such as `hostname`, `ping`, `netstat`, `route`, `arp`
You may try using Solving Basic TCP/IP Problems procedure at the following Web site: `http://support.microsoft.com/support/tshoot/nt4_tcp.asp`

6.5 NetBIOS over TCP/IP troubleshooting

When you want to analyze NetBIOS over TCP/IP configuration, you have different utilities to check your NetBIOS name resolution, routing, and browsing.

6.5.1 tracert

The `tracert` command is a route tracing utility similar to the trace utility in UNIX. It determines a route to a destination by sending ICMP echo packets with varying time-to-live values (TTL). You can use the following options:
-
d IP addresses are not resolved to hostnames.
-h This defines the maximum number of hops to reach the destination.
-j This specifies loose source route along host-list.
-w This specifies the wait time for each reply.
The output shows the steps to reach the destination. Every line shows the hop number, three round-trip times for three attempts, and the hostname (or IP address) of the system that was reached in this hop. An asterisk (`*`) means that the attempt timed out.

```
C:\>tracert lv3030c
Tracing route to lv3030c.itsc.austin.ibm.com [9.3.187.213]
over a maximum of 30 hops:
1 10 ms * <10 ms itso240.itsc.austin.ibm.com [9.3.240.1]
2 <10 ms <10 ms <10 ms lv3030c.itsc.austin.ibm.com [9.3.187.213]
Trace complete.
```

6.5.2 nbtstat

This tool is used for troubleshooting NetBIOS name resolution. The name resolution on Windows NT client uses one of the following methods: Local cache lookup, WINS server, broadcast, DNS, LMHOSTS, or HOSTS lookup. nbtstat can help you analyze name resolution problems with the following options:
`-n` This lists local registered NetBIOS names.

```
C:\>nbtstat -n
Node IpAddress: [9.3.240.113] Scope Id: []
NetBIOS Local Name Table
Name Type Status
---------------------------------------------
AUSRES10 <00> UNIQUE Registered
ITSOAUSNT <00> GROUP Registered
AUSRES10 <03> UNIQUE Registered
AUSRES10 <20> UNIQUE Registered
INet~Services <1C> GROUP Registered
IS~AUSRES10....<00> UNIQUE Registered
ITSOAUSNT <1E> GROUP Registered
```

a, -A These list the remote computer's name table (similar to what option -n does for a local computer).
-
c This shows the content of the NetBIOS name cache.
-
r This shows the name resolution and registration statistics and also names resolved by broadcast.
-
R This clears the local cache and reloads it from the LMHOSTS file.
-
s, -S These list the NetBIOS sessions. The first option will show NetBIOS names and the second one IP addresses.

```
C:\>nbtstat -S
NetBIOS Connection Table
Local Name State In/Out Remote Host Input Output
---------------------------------------------------------------------------
LV3030B <00> Connected Out ITSONT00 <20> 105KB 105KB
LV3030B <00> Connected Out LV3030C <20> 11KB 1KB
LV3030B <03> Listening
LV3030B Connected In AUSRES10 <00> 2MB 1MB
ADMINISTRATOR <03> Listening
```

6.5.3 browstat

The Microsoft Windows NT Server Resource Kit 4.0includes the browstat utility, which can be used for analyzing SMB network.
The browstat utility can show you browsers and the domain organization of a network. It is a command line utility. Some options of the command require a transport parameter. You can retrieve it with browstat status (this is part of the output):

```
Status for domain ITSOAUSNT on transport \Device\NetBT_Ibmtok51
...
Status for domain ITSOAUSNT on transport \Device\Nbf_Ibmtok51
...
```

You can see two transports in this example: `NetBF_Ibmtok51` and `Nbf_Ibmtok51`.
Browstat has the following options:
status [-V] [domain] This shows the status of the domain. The –V switch shows us extended information. You can see basic browsing and domain information on this sample output:

```
Status for domain ITSOAUSNT on transport \Device\NetBT_Ibmtok51
Browsing is active on domain.
Master browser name is: AUSRES05
Master browser is running build 1381
3 backup servers retrieved from master AUSRES05
\\AUSRES05
\\AUSRES08
\\AUSRES06
There are 85 servers in domain ITSOAUSNT on transport \Device\NetBT_Ibmtok51
There are 32 domains in domain ITSOAUSNT on transport \Device\NetBT_Ibmtok51
Status for domain ITSOAUSNT on transport \Device\Nbf_Ibmtok51
Browsing is active on domain.
Master browser name is: AUSRES10
Master browser is running build 1381
```

```
3 backup servers retrieved from master AUSRES10

\\AUSRES03
\\AUSRES11
\\AUSRES10
There are 42 servers in domain ITSOAUSNT on transport \Device\Nbf_Ibmtok51
There are 2 domains in domain ITSOAUSNT on transport \Device\Nbf_Ibmtok51
```

stats [computer] This shows the browsing statistics of the computer.
get pdc transport domain This shows the NetBIOS name of the primary domain controller for the domain.
getmaster transp. domain This shows the master browser name for the domain.
getblist transport This lists master and backup browser servers.
listwfw domain This lists WFW servers that are running browser.
view transp. [srv | dom] This requests a browse list for selected transport. You can select the browse list from specific server (srv) or domain (dom). The flags that are used in this list can be seen by entering the browstat command without parameters. Here is an example of the output:

```
Remoting NetServerEnum to \\AUSRES15 on transport \device\netbt_ibmtok51 with flags
13 entries returned. 13 total. 10 milliseconds
\\AUSRES03 NT 04.00 (W,S,NT,SS,PBR,BBR)
\\AUSRES05 NT 04.00 (W,S,NT,SS,PBR,BBR,MBR)
\\AUSRES06 NT 04.00 (W,S,NT,SS,PBR,BBR)
\\AUSRES08 NT 04.00 (W,S,NT,SS,PBR,BBR)
\\AUSRES10 NT 04.00 (W,S,NT,SS,PBR)
\\AUSRES11 NT 04.00 (W,S,NT,SS,PBR)
\\ISHIIY W95 04.00 (W,S,WFW,PBR,W95)
\\ITSONICE NT 04.02 (W,S,PQ,XN,NT,SS) ITSO-Austin Samba Server
\\ITSONT00 NT 04.00 (W,S,PDC,NT,BBR,MBR) ITSO Austin NT PDC
\\ITSONT01 NT 04.00 (W,S,BDC,PQ,NT,BBR) ITSO Austin NT BDC
\\LV3030C NT 01.00 (W,S,PQ,XN,NT,SS) Fast Connect Server
\\LV3030D NT 04.02 (W,S,PQ,XN,NT,SS,PBR) Samba2 Server
\\VIPER NT 04.00 (W,S,NT,SS,PBR) ITSO Austin CD-ROM Burner system
```

elect transport domain This forces an election on the selected domain.
tickle This forces a remote master to stop.

6.6 Troubleshooting utilities on AIX

This section describes AIX tools for troubleshooting SMB protocol. SMB is not a native protocol on AIX; so, special utilities are not available, but you can still get valuable information from standard TCP/IP tools.

6.6.1 TCP/IP configuration checking

You can check the TCP/IP configuration on SMB server with the following standard utilities: ifconfig, ping, arp, netstat, route, nslookup.

```
<source port=1932, destination port=139(netbios-ssn) >
th_seq=216bef8, th_ack=3a349002
th_off=5, flags<PUSH | ACK>
th_win=5836, th_sum=d8ea, th_urp=0
00000000 0000009a ff534d42 72000000 00000000 |.....SMBr.......|
00000010 00000000 00000000 00000000 0000c11d |................|
00000020 00000132 00770002 5043204e 4554574f |...2.w..PC NETWO|
00000030 524b2050 524f4752 414d2031 2e300002 |RK PROGRAM 1.0..|
00000040 4d494352 4f534f46 54204e45 54574f52 |MICROSOFT NETWOR|
00000050 4b532033 2e300002 444f5320 4c4d312e |KS 3.0..DOS LM1.|
00000060 32583030 32000244 4f53204c 414e4d41 |2X002..DOS LANMA|
00000070 4e322e31 00025769 6e646f77 7320666f |N2.1..Windows fo|
00000080 7220576f 726b6772 6f757073 20332e31 |r Workgroups 3.1|
00000090 6100024e 54204c4d 20302e31 3200 |a..NT LM 0.12. |
====( 141 bytes transmitted on interface tr0 )==== 01:42:12.318337099
...
```

6.6.2 tcpdump

The `tcpdump` command prints out the headers of packets on a network interface. You can define expressions to select packets that you want to see.
The basic syntax of the `tcpdump` command is:
`tcpdump { flags } expression`
Important flags are:
-
c count This exits after receiving count packets.
-
f This prints the foreign Internet address numerically, not symbolically.
-
i interface This defines the interface to listen to. If not defined, tcpdump will select one available interface.
-
I This (uppercase i) specifies immediate packet capture mode without waiting for the buffer to fill up.
-
N This omits printing domain part of the host name (e.g. lv3030c instead of lv3030c.itsc.austin.ibm.com).
-
q This quiets output. Output lines contains less protocol information and are therefore shorter.
-
t This omits printing a timestamp on each line.
-tt This prints an unformatted timestamp on each line.
-
v This prints more packet information (TTL and the type of service).
We must define expressions to filter incoming packets. When expression is true, the packet is accepted. Expression consists of one or more primitives.
The following are the important primitives:
[`src` | `dst`] `host host` This is true if the source or destination is a host with a specified host name. You can limit selection to only source or destination host with src and dst qualifiers.

[`src` | `dst`] `net net` This is true if the source or destination is a network with a specified net number. You can limit the selection to only the source or destination network with src and dst qualifiers.
[`src` | `dst`] `port port` This is true if the source or destination is a port with a specified port number. You can limit the selection to only the source or destination port with src and dstqualifiers.

`ip broadcast` This is true if the packet is an IP broadcast packet.

`ip multicast` This is true if the packet is an IP multicast packet.

`ip`, `arp`, `rarp` This is true if the packet is of the selected protocol

type (ip, arp, or rarp).
`tcp`, `udp`, `icmp` This is true if the packet is of the selected IP protocol type (tcp, udp, or icmp).
You can combine these primitives together with the operators and, or, not and parentheses (they must be escaped - '`\)`'). The following are some examples of expressions.
To show all traffic to and from the lv3030c computer, use:

```
host lv3030c
```

To show traffic to and from a machine with a specified IP address, use:

```
ip host 9.3.187.21
```

To show traffic from lv3030c to ausres10, use:

```
srchost lv3030c and dst host ausres10
```

To show NetBIOS traffic involving host lv3030c, use:

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

Same as the previous example:

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

The important ports for diagnosing the SMB protocol are as follows:

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

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

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

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

```
C:\>net view \\lv3030c
Shared resources at \\lv3030c
Samba Server
Share name Type Used as Comment
```

```
FINAL1 Print Lexmark Optra N
HOME Disk User's Home Directory Share
TMP Disk X:
The command completed successfully.
```

On an AIX server, you can see the network traffic during this command as shown in the following screen:

```
$ tcpdump -t -N \(port 137 or port 138 or port 139\) and host lv3030c
LV3030B.1056 > lv3030c.netbios-ssn: P 841:945(104) ack 662 win 8099 (DF)
lv3030c.netbios-ssn > LV3030B.1056: P 662:701(39) ack 945 win 65535
lv3030c.netbios-ssn > LV3030B.1056: P 662:701(39) ack 945 win 65535
LV3030B.1056 > lv3030c.netbios-ssn: P 945:1060(115) ack 701 win 8060 (DF)
lv3030c.netbios-ssn > LV3030B.1056: P 701:992(291) ack 1060 win 65535
lv3030c.netbios-ssn > LV3030B.1056: P 701:992(291) ack 1060 win 65535
LV3030B.1056 > lv3030c.netbios-ssn: P 1060:1164(104) ack 992 win 7769 (DF)
lv3030c.netbios-ssn > LV3030B.1056: P 992:1031(39) ack 1164 win 65535
lv3030c.netbios-ssn > LV3030B.1056: P 992:1031(39) ack 1164 win 65535
LV3030B.1056 > lv3030c.netbios-ssn: P 1164:1279(115) ack 1031 win 7730 (DF)
lv3030c.netbios-ssn > LV3030B.1056: P 1031:1143(112) ack 1279 win 65535
lv3030c.netbios-ssn > LV3030B.1056: P 1031:1143(112) ack 1279 win 65535
LV3030B.1056 > lv3030c.netbios-ssn: . ack 1143 win 7618 (DF)
```

The `tcpdump` command does not support SMB protocol specifics. Extension to tcpdump source code is known under the name tcpdump-smb. At the time of this writing, no compiled version of this utility was available for the AIX system.

6.7 Common problems

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

6.7.1 NetBIOS name resolution

Check the NetBIOS name resolution (WINS service):
• Use the `ping` command on the client with its NetBIOS name, its TCP/IP name, and its IP address to see whether the name translation works. If the ping to IP address works, but not with the NetBIOS name, you have a name resolution problem.

• Use the `ping` command with the WINS server IP address to see whether you can reach the WINS server.

• Double check the WINS server settings on the client and the status of your WINS server. You can check the WINS server settings on your client by selecting **Start -> Settings -> Control Panel -> Network -> Protocols -> TCP/IP Protocol -> Properties -> WINS Address**. To find the WINS server status on Windows NT, select **Start -> Settings -> Control Panel -> Services**, and then locate the Windows Internet Name Service. If the Status field is Started, WINS is running on the server.

• Enable LMHOSTS for name resolution and add an entry to the LMHOSTS file. You will enable LMHOSTS for name resolution by selecting **Start -> Settings -> Control Panel -> Network -> Protocols -> TCP/IP Protocol -> Properties -> WINS Address**. Then, check the **Enable LMHOSTS Lookup** check box. If you want to resolve the host name of a machine, lv3030c, with IP address 9.3.187.213, you would add the following line into C:\winnt\system32\drivers\etc\LMHOSTS:

```
9.3.187.213 lv3030c
```

• Use the `nbtstat` command on the client for checking NetBIOS name resolution.

6.7.2 Browsing

Check the resource browsing on the client by using the following commands:

• Use `net view` to get the list of all visible computers on the network.
• Use `net view \\` NetBIOS_name to see the resources on single server.
• Use `browstat` for detailed information.

6.7.3 Authentication

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

6.7.4 Netlogon

Sometimes, you may experience problems when working with the User profiles and System policies. You can use some tools and hints to deal with this.

Checking if the startup script runs
If you are not sure if the startup script runs, when a user logs in, add the `pause` command to the script. You should see a window at the login, waiting on your input.

Disable the local profile
If you are not sure, whether your local or remote profile is used, make the following registry change to use only remote profile (clear local profile on exit):

```
My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current
Version\WinLogon\DeleteRoamingCache=1 (DWORD)
```

Remove profiles
If you want to remove a complete profile for a user on a single computer, you can use the `delprof` command. It is located on a Windows NT Server Resource Kit, version 4.0. The basic syntax for the `delprof` command is as follows:

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

The flags are:

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