Installation and Configuration Guide

English

Samba for Brisque 4.1, Brisque 5 and Brisque Serve

731-00281A-EN-Rev C

Copyright

Copyright © 2005 Creo Inc. All rights reserved. The Creo wordmark, Creo logo, and the names of the Creo products and services referred to in this document are trademarks of Creo Inc.

Adobe, Acrobat, Adobe Illustrator, Distiller, Photoshop, PostScript, and PageMaker are trademarks of Adobe Systems Incorporated. Apple, iMac, Power Macintosh, AppleShare, AppleTalk, TrueType, and ImageWriter are registered trademarks of Apple Computer, Inc. Macintosh is a trademark of Apple Computer, Inc., registered in the U.S.A. and other countries. PANTONE, Hexachrome, PANTONE Hexachrome, and PANTONE MATCHING SYSTEM are the property of Pantone, Inc. PEARL, PEARLsetter, PEARLhdp, PEARLdry, and PEARLgold are registered trademarks of Presstek, Inc. Xerox, DocuColor, and MajestiK Color Series are trademarks of Xerox Corporation in the U.S. and/or other countries. Other brand or product names are the trademarks or registered trademarks of their respective owners.

No copying, distribution, publication, modification, or incorporation of this document, in whole or part, is permitted without the express written permission of Creo Inc. In the event of any permitted copying, distribution, publication, modification, or incorporation of this document, no changes in or deletion of author attribution, trademark legend, or copyright notice shall be made. No part of this document may be reproduced, stored in a retrieval system, published, used for commercial exploitation, or transmitted, in any form by any means, electronic, mechanical, photocopying, recording, or otherwise, without the express written permission of Creo Inc. This document is distributed in Adobe Systems Incorporated's PDF (Portable Document Format). You may reproduce the document from the PDF file for internal use. Copies produced from the PDF file must be reproduced in whole.

Creo Inc.
3700 Gilmore Way
Burnaby, B.C., Canada
V5G 4M1
Tel: +1.604.451.2700
Fax:+1.604.437.9891

http://www.creo.com

Internal 731-00281A-EN-Rev C

Revised April 2005

Contents

Samba Server Installation 1

1.1 Overview 2
1.2 For Brisque 4.1 and Brisque Serve Only—Server Installation 4
1.2.1 Automatic Installation and Configuration 4
1.2.2 Installation Verification 4
1.3 For Brisque 5 Only—Samba Activation 6
1.4 Accessing Samba Web Administration Tool (SWAT) 7

Known Limitations 9

2.1 Extensions 10
2.1.1 Unsupported Characters 10
2.1.2 Usernames 10
2.2 Other Limitations 11
2.2.1 Brisque Station (AIX Operating System) 11
2.2.2 Windows Stations 13

Troubleshooting 15

A.1 Known Issues 16
A.2 Checking Configuration 16
A.3 Checking Connectivity 17
A.4 Protocol Overview 18
A.4.1 TCP/IP Protocols 19
A.4.2 SMB Protocols 19
A.5 Generic TCP/IP Utilities 19
A.6 Troubleshooting Utilities on Windows NT 20
A.6.1 NetBIOS Over TCP/IP Troubleshooting 21
A.7 Troubleshooting Utilities on AIX 26
A.7.1 TCP/IP Configuration Checking 26
A.8 Common Problems 30
A.8.1 NetBIOS Name Resolution 30
A.8.2 Browsing 31
A.8.3 Authentication 31

Inter-connectivity Between Different Operating Systems 33

B.1 Overview 34
B.2 AppleShare, AppleTalk, and Windows–Mac–LAN 34
B.3 TCP/IP NFS 35
B.4 FTP (File Transfer Protocol) 35
B.5 RPC 36
B.6 Samba (SMB) 36
B.6.1 SMB Networking Overview 37

Using SWAT 39

C.1 Overview 40
C.2 The Samba SWAT Interface 40

1

Samba Server Installation

Overview 2
For Brisque 4.1 and Brisque Serve Only—Server Installation 4
For Brisque 5 Only—Samba Activation 6
Accessing Samba Web Administration Tool (SWAT) 7

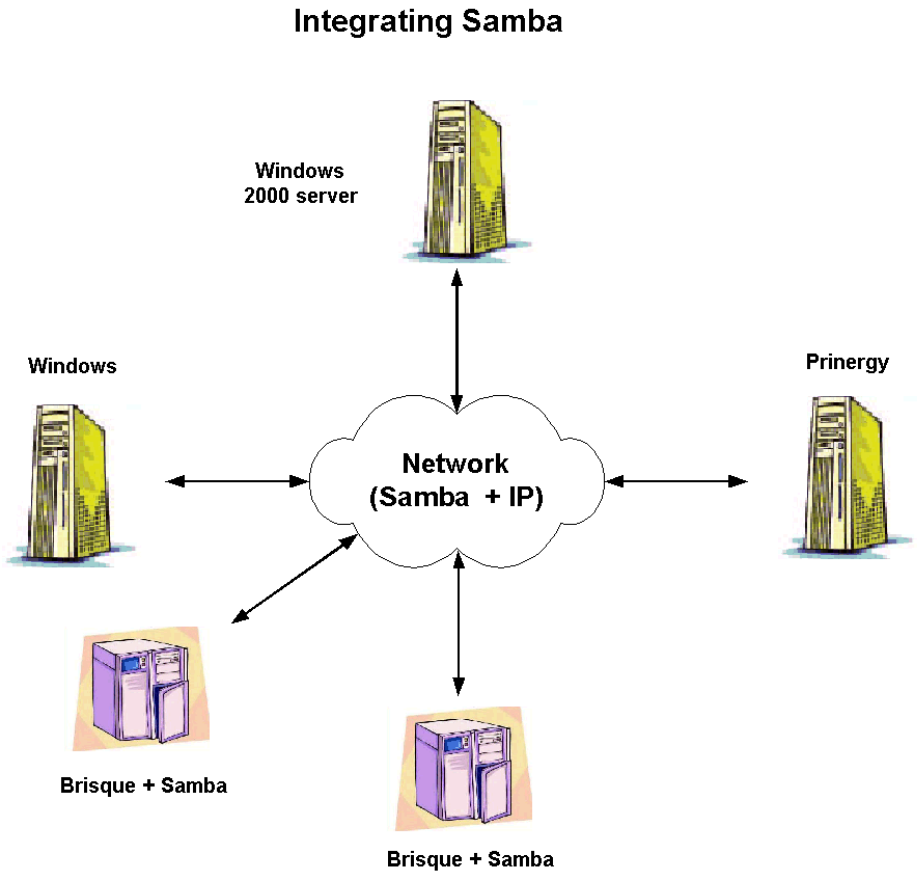
1.1 Overview

Samba is a suite of UNIX®/AIX® applications that uses the SMB (Server Message Block) protocol. Because many operating systems, including Windows® and OS/2®, use the SMB protocol to perform client–server networking, Samba enables UNIX systems to act as file and print servers for Windows client systems. In addition, Samba includes UNIX SMB client utilities. Windows 95/98, Windows NT, Windows 2000, Window XP and OS/2 Warp clients do not require additional software to access a Samba server.

With Samba, a UNIX/AIX server can offer the following services:

- Share one or more filesystems
- Share printers installed on both the server and its clients
- Assist clients with network neighborhood browsing
- Authenticate clients logging onto a Windows domain
- Provide or assist with WINS name server resolution.

The diagram on the following page illustrates Samba integration within a Brisque® site.


Integrating Samba
Windows
2000 server
Windows
Prinergy
Network
(Samba + IP)
Brisque + Samba
Brisque + Samba

1.2 For Brisque 4.1 and Brisque Serve Only—Server Installation

1.2.1 Automatic Installation and Configuration

To install the Samba server:

1. Insert the Creo *Samba Connectivity to Brisque Serve and Brisque 4.1* CD (part number 651-00173A) into the CD drive.
2. From the terminal, type: `smit install_latest`.
3. Select the CD as the installation source, and then select **ALL** for the installed software.

The Samba software will be automatically installed and configured.

1.2.2 Installation Verification

This section describes how to verify that the installation was successful. Basically there is no need to change any configuration file in order to start using Samba.

- Verify that the **smb.conf** file has the correct hostname that is necessary to start SWAT
- Verify that the **/etc/services** file contains a **swat 901/tcp** line.
- Verify that the **/etc/inetd.conf** file includes **SWAT** entries.

After installation, the following directory structure exists:

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

The following scripts are useful for Samba debugging (start/stop Samba daemons):

- **/scitex/version/scripts/startsmb**
- **/scitex/version/scripts/stopsmb**

If your machine is correctly installed and configured, it can now perform as a SMB server and provide information about the available shares. The **installp** installation starts **smbd** and **nmbd** daemons, and adds a default **smb.conf** configuration file in the **/usr/local/lib** file.

To test the installation, use the smbclient command:

Type: `/usr/local/bin/smbclient -L [yourhostname]` (use **root** and **ripro** as username and login).



Note: If after the first installation, the test file (**smbclient**) failed due to missing nmbd and smbd daemons, try restarting them by typing:

```
/scitex/version/scripts/startsmb
/scitex/version/scripts/stopsmb
```

If the `/usr/local/bin/smbclient -L [yourhostname]` command displays a list of the resources configured in **smb.conf**, this indicates that you have a properly–running Samba server. You should now be able to access the shared resources from your clients.

1.3 For Brisque 5 Only—Samba Activation

The Samba server is installed and configured during Brisque version 5 installation, but it is not activated upon reboot.

To activate Samba and keep it activated on each system boot:

Run this script once: `/scitex/version/scripts/installSmb`.

Running the `installSmb` script causes the following processes to be active on each reboot:

- **/usr/local/samba/bin/smbd**
- **/usr/local/samba/bin/nmbd**



Important: All dataVolumes are published for mounting by Samba after installation and activation.

To deactivate Samba from running on each boot:

Run this script once: `/scitex/version/scripts/remSmb`.

1.4 Accessing Samba Web Administration Tool (SWAT)

The Samba Web Administration Tool (SWAT) is a common method to set up and maintain the **smb.conf** configuration file, using your standard web browser. All pages have a similar look and feel, and it is easy to learn to use SWAT.

SWAT is a small web server and CGI scripting application that is designed to run from **inetd**, and provide access to the **smb.conf** configuration file.

Authorized users can configure the **smb.conf** file via a web interface. SWAT has a built-in Help system for each option on all pages.



Note: We recommend that you use SWAT carefully !
Normally the engineer will not be using SWAT, since the configuration is fully automatic—all dataVolume are published by Samba after installation and activation. SWAT will probably be used only when shares other than the standard ones are added (specific folders within dataVolumes).
DO NOT CHANGE THE SECURITY OF ANY FOLDER !
See *Using SWAT* on page 39 for details.

To access the SWAT interface using a web browser:

1. Verify that the following entries are located in **/etc/inetd.conf**:

   ```
   # The following three lines are for the Samba SMB server
   (freeware)
   swat stream tcp nowait.400 root /usr/local/samba/bin/swat swat
   ```

   If the lines are missing, add them to the **/etc/inetd.conf** file.

2. Type `refresh -s inetd` to refresh the Samba configuration.



Note: SWAT modifies the Samba configuration file, which is stored **/usr/local/samba/lib/smb.conf**. It rearranges the entries, and deletes all **include=** and **copy=** options and comments that may be included in the file. If you want to save any or all of these items, you must either back up the file or not use SWAT

3. Using a web browser, go to the following site: **http://yourhostname:901**, and log in as root using the standard AIX root password.

2

Known Limitations

Extensions.....10
Other Limitations 11

2.1 Extensions

Windows cannot handle files without extensions. This is because Windows cannot handle resources, and this is not a Samba-related problem. Resources do not exist on Windows, and one file always contains all information such as, preview and creator.

2.1.1 Unsupported Characters

Windows does not support the following characters: \ / : * ? “ < > |

2.1.2 Usernames

Invalid characters for usernames are listed below.

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

2.2 Other Limitations

2.2.1 Brisque Station (AIX Operating System)

- Folder/file names can't start with: - (dash), + (plus sign), @ (at sign), ~ (tilde)
- Tar files cannot be uncompressed after copying to Windows and cannot be uncompressed after copying back to Brisque
- Hot folders can be deleted or moved from Windows, including their enclosing folders.



Note: Hot folders cannot be moved/deleted from the Macintosh®.

- When jobs are copied to Windows (or to Mac® OS® X) and then back to the Brisque, their owner changes from root to macuser. However, this does not affect user access to the job, since the permissions remain 777.
- When 10 Windows stations are connected to the same Brisque, the Copy performance drops by 10%.
- A second file is created for each file that is copied from OS X. For example, if the original file is **test.job**, the second file is **._test.job**. A rsrc is also created for the second file.
  Note: The second files are ignored by the Brisque 5 application and are not RIPed.
- Not all hidden files are in fact hidden. For example, **.jt** files.
  To resolve this issue, in **OS X only**, open the **/etc/smb.conf** file and add the following line:
  `hide files = /*.assg/*.db/*jt/`

- Brisque 5 looses Samba shares after application login.
  The cause of this issue is that the current syntax [**brisque04.1.0**] in the **smb.conf** file is faulty.
  The recommended syntax is [**brisque04.brisque04.1.0**] (mandatory for proper Samba operation). The application checks this file upon each login (not reboot) and removes incorrect mounts.
  Note: In OS X environment, there is a limitation of maximum 12 characters. This limitation is irrelevant in the Insight environment.

Synapse® InSite considerations:

- Synapse InSite supports the Synapse Director style path naming convention. InSite does not use hardcoded paths to page elements. The **etc\otherhosts** file must be configured correctly to ensure that pages registered from a Macintosh can be mapped properly into UNC paths. For example, **brisque4.brisque4.1.0** would be accessed from Windows as: `\\brisque4\brisque4.brisque4.1.0\`
- If the path to pages is changed *and* auto-page registration is used in InSite, then the auto-page registration settings must reflect the correct UNC path.
- **Problem:** Pages registered with the old pathname are *not* accessible after changing to the new path. InSite stores the registered path in the database.
  Workaround: You can write a database script on Synapse that will modify the old style paths to new style paths.

Synapse Director considerations:

Synapse Director does require the **brisque4.brisque4.1.0** share name for Brisque dataVolumes.
When Samba is enabled on Brisque 5, a Samba share is automatically created via the Brisque during startup for all mounted volumes in the file browser in this format.
In this example, the share is accessible from Windows as:
`\\brisque4\brisque4.brisque4.1.0`

2.2.2 Windows Stations

- Folder/file names must include more than only periods (.) and spaces.
- AIX usernames are case-sensitive, limited to no more than eight characters in length, and can include double-byte characters.
  AIX passwords are case-sensitive and are not limited in length.
  However, **only the first eight characters are considered distinct, and the extra characters are ignored at the logon.**



Note: The best solution for these incompatibilities is planning ahead when designing your user account policies. In addition, Samba also offers mechanisms for mapping the AIX and Windows standards.

A

Troubleshooting

Known Issues 16
Checking Configuration 16
Checking Connectivity 17
Protocol Overview 18
Generic TCP/IP Utilities 19
Troubleshooting Utilities on Windows NT 20
Troubleshooting Utilities on AIX 26
Common Problems 30

A.1 Known Issues

Windows client browses incorrect Brisque shares

Problem: This issue may occur when browsing the Brisque 5 shares using run: `\\Brisque5_name` from the Windows client, and the incorrect shares will be shown in the browsing window. These could the NFS volumes, instead of the Samba ones.

Possible cause: The fact that the Windows client has an SFU client installed on the same computer. If at any point the Samba server is down and the client tries to browse the Brisque 5 workstation, incorrect NFS published volumes will be shown.

Workaround: The problem won't be solved by starting the Samba server on the Brisque 5 workstation or restarting Windows—the browsing will still be incorrect.

The workaround is to browse the Brisque 5 workstation using the IP address, instead of the hostname.
For example: instead of
run: `\\timna1`
use the following command:
run: `\\10.4.27.181`.
This will reset the Windows browsing to the correct state.

A.2 Checking Configuration

If Samba doesn't operate properly, check the following:

- Verify that the **/scitex/version/usr/local/samba/lib/smb.conf** file has the correct hostname to start SWAT
- Verify that the **/etc/services** file contains a line such as `swat 901/tcp`
- Verify that **/etc/inetd.conf** includes the smbd, nmbd, and SWAT entries:
  ```
  swat stream tcp nowait.400 root /usr/local/samba/bin/
  swat swat
  ```
- Verify that the **/etc/rc** script includes the following line:
  `/scitex/version/scripts/startsmb`

The following scripts can be useful for Samba debugging (starts/stops samba daemons):

- **/scitex/version/scripts/startsmb**
- **/scitex/version/scripts/stopsmb**

A.3 Checking Connectivity

If you cannot browse any Samba shares via Windows, check the following steps:

- Ping your Samba server from **itself** (that is, not across the network) using the **loopback address**.
- Ping your Samba server from **itself** (that is, not across the network) using its **IP address**.
- Ping your Samba server from **itself** (that is, not across the network) using its **FQDN** (**Fully Qualified Domain Name**).
- Ping your Samba server from another machine using the **loopback address**.
- Ping your Samba server from another machine using its **IP address**
- Ping your Samba server from another machine using its **FQDN** (**Fully Qualified Domain Name**).
- Run the `testparm` command to validate the syntax of your smb.conf file.
- Verify that smbd and nmbd are both running.
- From the Samba server, verify that you can query the nmbd server for **its own** NetBIOS name using:
  ```
  nmblookup -Bmyserver  __SAMBA__
  ```
- From the Samba server, verify that you can query the nmbd server for **any** NetBIOS client name using:
  ```
  nmblookup -B example-client
  ```
- From the Samba server, verify that you can **query your subnet** for any NetBIOS client name using:
  ```
  nmblookup -d 2
  ```

- Use the `smbclient` command to test 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**, the Samba server is running properly. You should now be able to access the shared resources from your clients.
- From a Windows client, try to generate a list of valid shares using: `NET VIEW \\myserver`
- From the Samba server, verify that you can query the Domain Master browser (probably itself) for the Samba server IP address using: `nmblookup -M myworkgroup`
- From the Samba server, try to connect to one of its own shares using: `smbclient //myserver/myshare -Umyusername`
- From a Windows client, try to connect to one of the shares using: `NET USE X: \\myserver\myshare`

A.4 Protocol Overview

It is difficult to define how to identify problems in a domain as large as the combined SMB and TCP/IP protocols. The following sections provide steps and guidelines for troubleshooting the SMB protocol.

The TCP/IP protocol is divided into separate independent levels. This architecture is helpful because normally there's a problem only in one level. Following is a simplified version of these levels that can help you locate the problem. You should try to locate the lowest network level with the problem. For example, in a name resolution problem, the access to the shares will probably not work.

A.4.1 TCP/IP Protocols

- **Address resolution:** conversion from the hardware network address to the IP address and back. The utilities are **arp** and **ping**.
- **Routing:** 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:** conversion from the domain name to the IP address. The utilities are **nslookup** and **host**.

A.4.2 SMB Protocols

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

A.5 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 don't know the network organization, use the same tools to find it. These utilities are available on AIX and also on Windows NT.



Note: Some utilities may be missing on Windows 95 systems.

The following utilities are available:

- **ipconfig** shows the IP configuration on Windows NT stations.
- **ping** 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** checks the route from one computer in a TCP/IP network to another (use **tracert** on client).
- **route** prints out the routing table. You can also add and delete routes.
- **netstat** shows the status of the network, such as routing table, port allocation, and statistics.
- **nslookup** checks the Domain Name Service (DNS)— TCP/IP name resolution. You can locate the IP address from the computer name, and vice versa.
- **arp** shows and modifies the IP address to adapter address translation table. Try to determine if there's a problem with only one computer.

A.6 Troubleshooting Utilities on Windows NT

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

TCP/IP configuration

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

```
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 obtain similar information.
You can use other commands to help you analyze the configuration, routing, DNS, and other TCP/IP-related problems, such as hostname, ping, netstat, route, arp.
You may try using *Solving Basic TCP/IP Problems* procedure at the following web site: **http://support.microsoft.com/support/tshoot/nt4_tcp.asp**.

A.6.1 NetBIOS Over TCP/IP Troubleshooting

To analyze NetBIOS over TCP/IP configuration, you can use various utilities that check your NetBIOS name resolution, routing, and browsing.

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` defines the maximum number of hops to reach the destination
- `-j` specifies loose source route along host-list
- `-w` specifies the wait time for each reply

The output shows the steps to reach the destination. Each 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.
```

nbtstat

`nbtstat` is used for troubleshooting NetBIOS name resolution. The name resolution on Windows NT clients uses one of the following methods:

- Local cache lookup
- WINS server
- broadcast
- DNS
- LMHOSTS
- HOSTS lookup

`nbtstat` can analyze name resolution problems with the following options:

-n 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 list the remote computer name table (similar to **-n** option for local computer)

c shows the content of the NetBIOS name cache

r shows the name resolution and registration statistics, and names resolved by broadcast

R clears the local cache and reloads it from the LMHOSTS file

s, -S list the NetBIOS sessions. The first option shows NetBIOS names and the second one shows 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
```

browstat

The *Microsoft Windows NT Server Resource Kit 4.0* includes the `browstat` utility that can be used for analyzing SMB network.

`browstat` shows browsers and the domain organization of a network. It is a command line utility. Some of the command options require a transport parameter which you can retrieve 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

...
```

There are two transports in this example: NetBF_Ibmtok51 and Nbf_Ibmtok51.

`browstat` includes the following options:

status [**-V**] [**domain**] shows the status of the domain. The **–V** switch shows extended information. The following sample output shows basic browsing and domain information:

```
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**] shows the browsing statistics of the computer.

get pdc transport domain shows the NetBIOS name of the primary domain controller for the domain.

getmaster transp. domain shows the master browser name for the domain.

getblist transport lists master and backup browser servers.

listwfw domain lists WFW servers that are running browser.

view transp. [**srv | dom**] requests a browse list for the 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 viewed by entering the `browstat` command without parameters. An output example is shown below:

```
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 forces an election on the selected domain.

tickle forces a remote master to stop.

A.7 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. However, you can still obtain valuable information from standard TCP/IP tools.

A.7.1 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
...
```

tcpdump

The `tcpdump` command prints 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 exits after receiving count packets.

f prints the foreign Internet address numerically, not symbolically.

i interface defines the interface. If not defined, `tcpdump` will select an available interface.

I (uppercase i) specifies immediate packet capture mode without waiting for the buffer to fill up.

N omits printing domain part of the host name (for example, lv3030c instead of lv3030c.itsc.austin.ibm.com).

q quits output. Output lines contain less protocol information and are therefore shorter.

t omits printing a timestamp on each line.

-tt prints an unformatted timestamp on each line.

v prints more packet information (TTL and the type of service).

We need to define expressions to filter incoming packets. When the expression is true, the packet is accepted. An 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 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
```

Or: (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

For example, to see the packet traffic between client and server, when the client runs the net view command, the client output on screen is as follows:

```
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, the network traffic can be viewed 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. Currently, no compiled version of this utility is available for the AIX system.

A.8 Common Problems

The following sections list common problems and tips regarding the Samba server.

A.8.1 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, then you have a name resolution problem.
- Use the ping command with the WINS server IP address to see if 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.
  To enable LMHOSTS for name resolution select:
  Start > **Settings** > **Control Panel** > **Network** > **Protocols** > **TCP/IP Protocol** > **Properties** > **WINS Address**.
  Then select the **Enable LMHOSTS Lookup** check box.
  To resolve the host name of a machine, lv3030c, with IP address 9.3.187.213, add `9.3.187.213 lv3030c` to the following line **C:\winnt\system32\drivers\etc\LMHOSTS**
- Use the `nbtstat` command on the client to check NetBIOS name resolution.

A.8.2 Browsing

Check the resource browsing on the client 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 resources on single server
- Use `browstat` for detailed information

A.8.3 Authentication

Checks if the guest account is enabled and if the guest user name is appropriate for an AIX user.

Netlogon

Occasionally you may experience problems when working with the User profiles and System policies. The following tools and tips can be useful for dealing with these problems.

Check 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. A window at the login, waits on your input.

Disable the local profile

If you are not sure if your local or remote profile is used, change the registry as follows 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

To remove a complete profile for a user on a single computer, use the `delprof` command. It is located on a *Windows NT Server Resource Kit 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

B

Inter-connectivity Between Different Operating Systems

Overview 34
AppleShare, AppleTalk, and Windows–Mac–LAN 34
TCP/IP NFS 35
FTP (File Transfer Protocol) 35
RPC 36
Samba (SMB) 36

B.1 Overview

Inter–connectivity crosses the borders between different communication protocols. Many types of protocols are used, but there is no accepted standard. However, the way of using the protocols is standardized. Users on the same operating system can talk to each other. However, users on different operating systems use a client application to emulate the other network protocol. Compared to other operating systems, Windows seems to be the most sensitive to changes in the default behavior when the network client software is from a non-Windows source. The most common protocols are detailed on the following pages.

B.2 AppleShare, AppleTalk, and Windows–Mac–LAN

AppleShare®, AppleTalk®, and Windows–Mac–LAN are used for communicating between Macintoshes, Windows, and UNIX systems, which are based on the AppleTalk protocol that runs over TCP/IP. Previously, this protocol was inconvenient and resulted in slow performance.

This protocol is responsible for **resource** (rsrc), and saves information such as creator and file-type. This implies that two files are located on an AppleShare volume: the file itself and the resource file. If a Macintosh or Windows station connects to such volume, this information defines how to handle the file on the Macintosh or Windows desktop.



Note: The Macintosh cannot handle two files at the same time (namely, file and rsrc).

The rsrc file is constantly updated with changes to the file. In a way, the rsrc directory is a mirror of the real file but much smaller in size. The desktop information is automatically updated whenever a file arrives, is modified, deleted, or moved.

Desktop corruption occurs when there is inconsistency between the information in the file–system and the desktop. Rebuilding the desktop usually corrects the problem by comparing file–system information and desktop information (rsrc directory).

Files stored on such volumes do not require a file extension in order to identify the file type.

Another aspect is the length of the filename displayed on a Macintosh using AppleShare. The limit is 31 characters. Longer filenames are visible on UNIX and Windows , but not on Macintosh other than Mac OS X.

Customers can use any file and folder names, but are restricted by the delimiters, which are letters and signs that are used by the operating system. For example, / or \ define a path from or to. In Windows, **C:** or in UNIX, **/backup/nsr**.

Not confirming to the above rules may result in functionality problems.

B.3 TCP/IP NFS

TCP/IP NFS is the most common communication protocol, originally designed by the US army as the internet protocol for communicating with their own protocol.

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. A network set-up is required for access by IP, Router, Gateway and DNS. The network is based on TCP/IP, underlying NFS.

NFS requires export and access, and both computers need to be defined in each other (/etc/hosts).

The subnet masks the IP network into ranges of Class A, B, and C, where class A covers the first 8 bits of the mask: 255.0.0.0, class B covers the first 16 bit of the mask: 255.255.0.0, and class C covers the first 24 bit of the mask: 255.255.255.0.

B.4 FTP (File Transfer Protocol)

FTP is mostly used for moving files through the internet from an ftp server to the final location, and the transfer rate is fast. However, you can connect to a local machine by using for example: **ftp://10.3.1.47/**.
After authentication you can access all folders and file.

B.5 RPC

RPC is used for the **Send** operation on Brisque. NFS is not used for this operation.

B.6 Samba (SMB)

Samba connects between Windows and UNIX platforms.

Samba is a suite of programs that work together to allow clients to access to 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 Windows client systems. Although Samba is primarily used for providing Windows–like file and print services under UNIX, it also includes UNIX SMB client utilities.

Windows 95/98, Windows NT, Windows XP, Windows 2000, and OS/2 Warp clients do not require additional software to access a Samba server, since these operating systems support NetBIOS over TCP/IP (NBT), which is required in order 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 Windows stations.

B.6.1 SMB Networking Overview

Before installing Samba it is important to understand Windows networking concepts since Windows SMB file and print services differ from UNIX files and print services.

In 1984, IBM and Sytec coauthored a simple **API** called Network Basic Input/Output System (NetBIOS). This was extended in 1985 to **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 hosted on top of IPX, DECNet, and TCP/IP, and as TCP/IP gained popularity, NetBIOS over TCP/IP (NBT) became the most common implementation. Samba only implements NetBIOS over TCP/IP.

Meanwhile, Microsoft developed the **Server Message Block** (SMB) protocol which 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 other features.

NetBIOS name resolution varies depending on the type of node and client configuration. 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.

The Microsoft NetBIOS name server is **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 security models:

- In the original model, **share level security**, the client only provides a password to access a share, and a username is not required. Once a client has access to a share, any files contained within that share can be accessed.
- The more recent model, **user level security**, requires the client to provide a username and password in order to access a share. Individual files within a share may also be further protected.

A **Domain** is a collection of computers whose security information is centrally managed by a Domain controller. Within a given domain, there can only be one primary Domain controller and multiple Backup Domain controllers. In a Workgroup, each client maintains its own security information. Generally, a workgroup is restricted to a single subnet. As of Samba version 2.0, Samba can function as a primary Domain controller.

Recently, Microsoft 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).

C

Using SWAT

Overview 40
The Samba SWAT Interface 40

C.1 Overview

If set up and configured properly without errors, SWAT is ready to be used. To start SWAT, point your web browser to the Internet address of your Samba server on port 901. At authentication, type your username and password, as defined on your server. SWAT can be accessed with any AIX user, but you can make changes only when logged in as the root user.



Note: When 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 perform SWAT administration tasks locally on the server.

The Samba server will reread the file and pick up changes to the **smb.conf** file every 60 seconds. If you can't wait that long, you can send a HUP signal to the smbd and nmbd daemons to accept the changes. The SWAT opening page is shown on the screens on the following pages.

C.2 The Samba SWAT Interface

SWAT is the browser graphic interface of Samba that is used during configuration. To log on from the browser window, type:
`http://<ip address>:901.`

Alternatively, you can type the host name if the client address is located in the host file of the server.

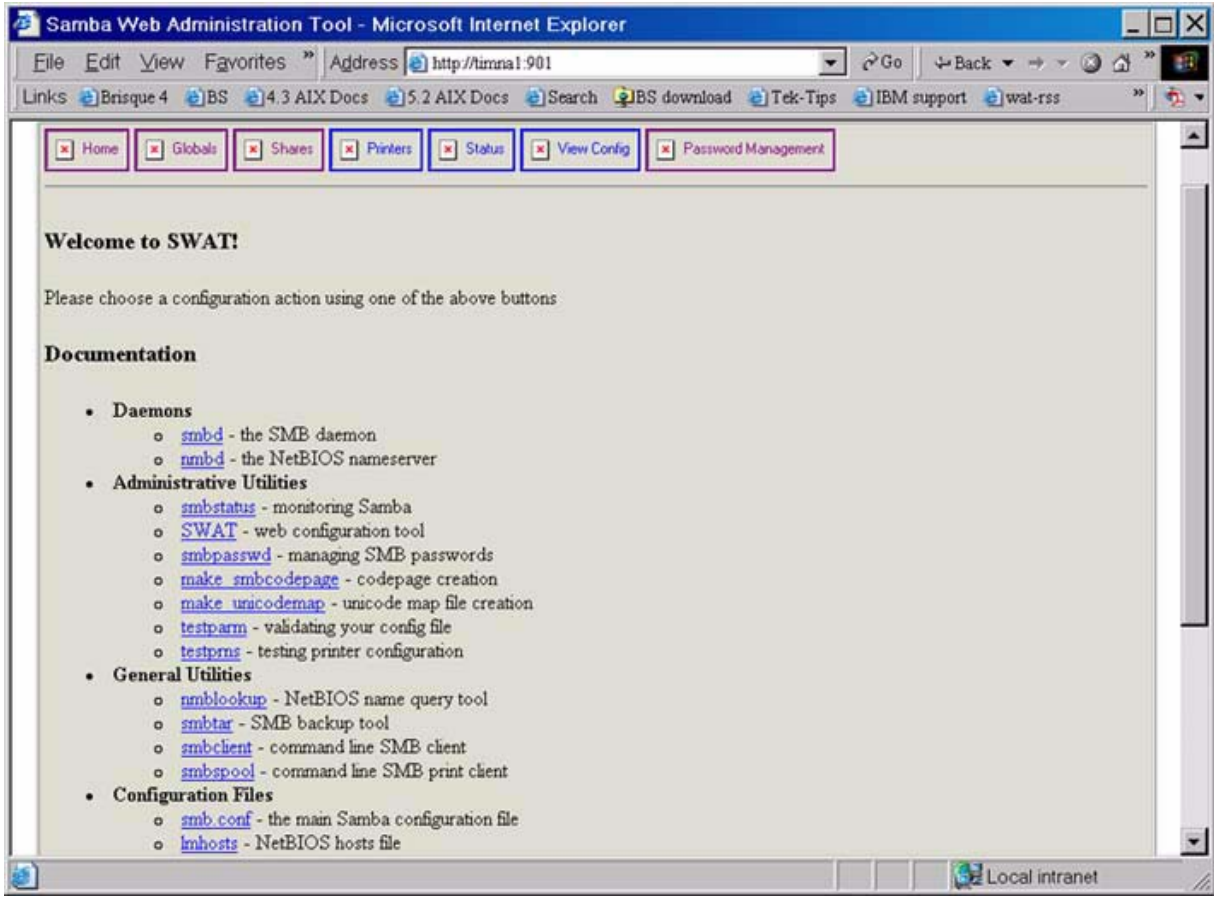


Figure 1: SWAT Home page.
7 categories are available at the top menu: Home, Globals, Shares, Printers, Status, View, and Passwords.

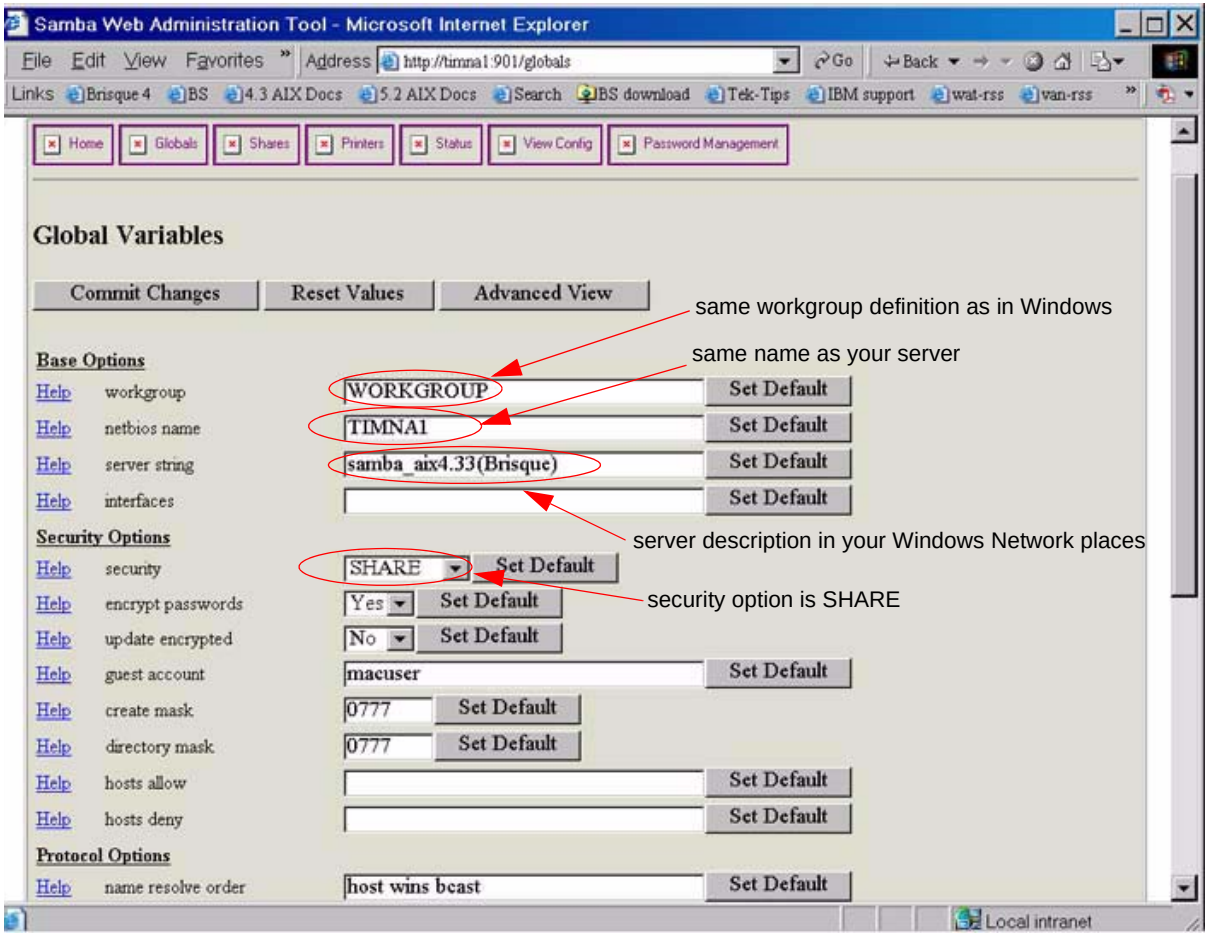


Figure 2: SWAT - Global Variables window

- **Home** links to the documentation section of Samba (**/usr/local/samba/man**).
- **Globals variables** are used to setup the base parameters for the Samba server.
- After performing changes, click the **Commit Changes** button.
- Guest account must be **macuser**

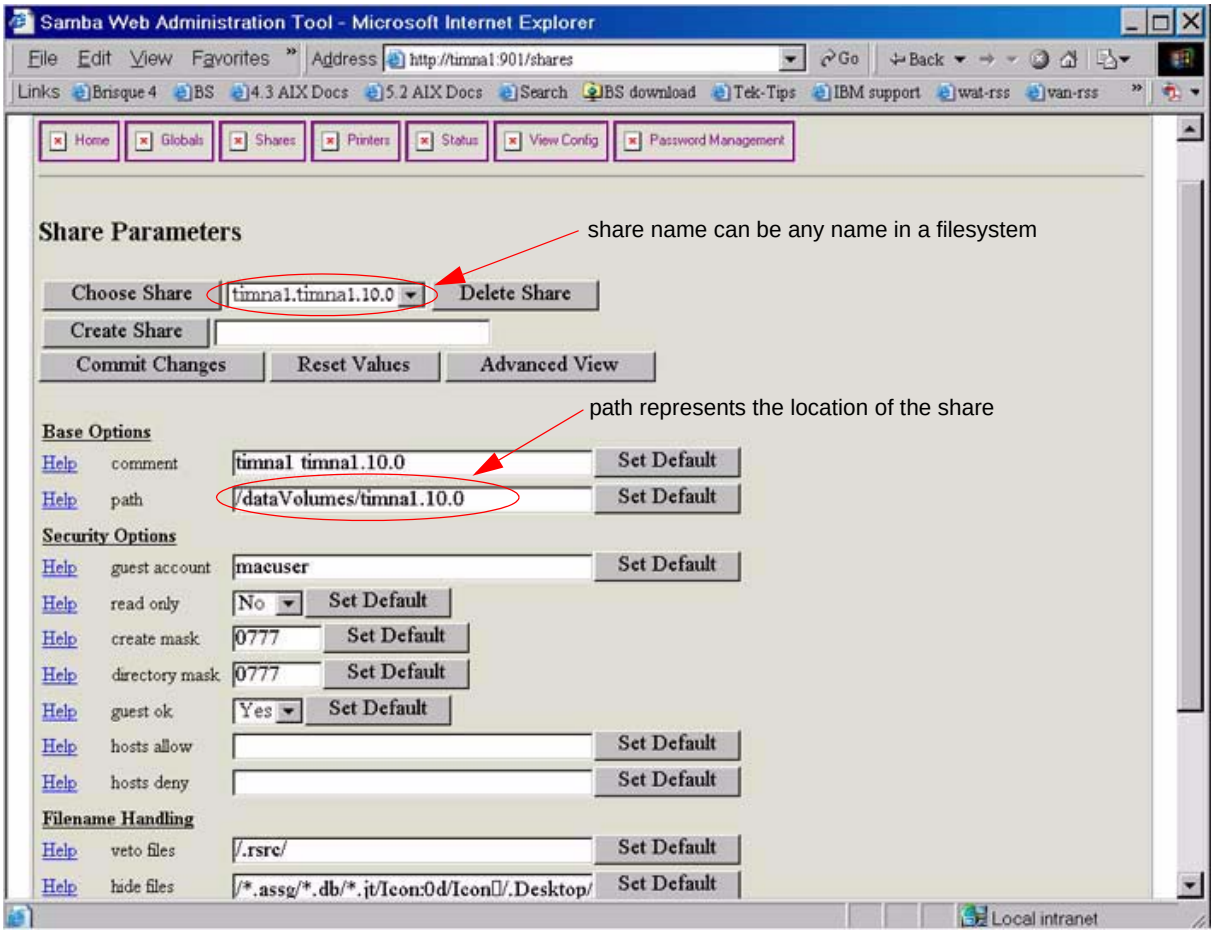


Figure 3: SWAT - Share Parameters window

- The above window is used to set up the share. All additional options were set up in the previous Globals Variables window.
- Click **Create Share**
- Click **Choose Share** to open the window.
- Guest account must be **macuser**

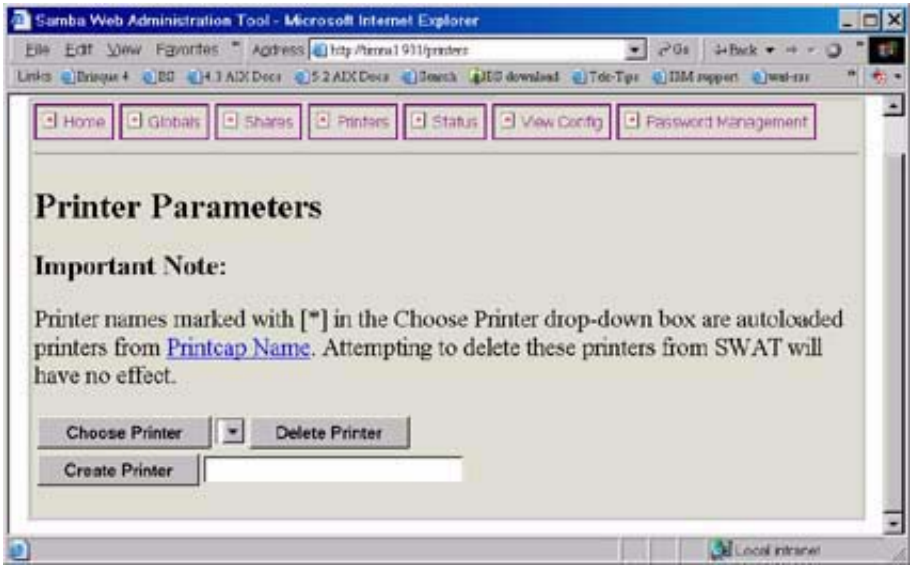


Figure 4: Printer setup to print via UNIX

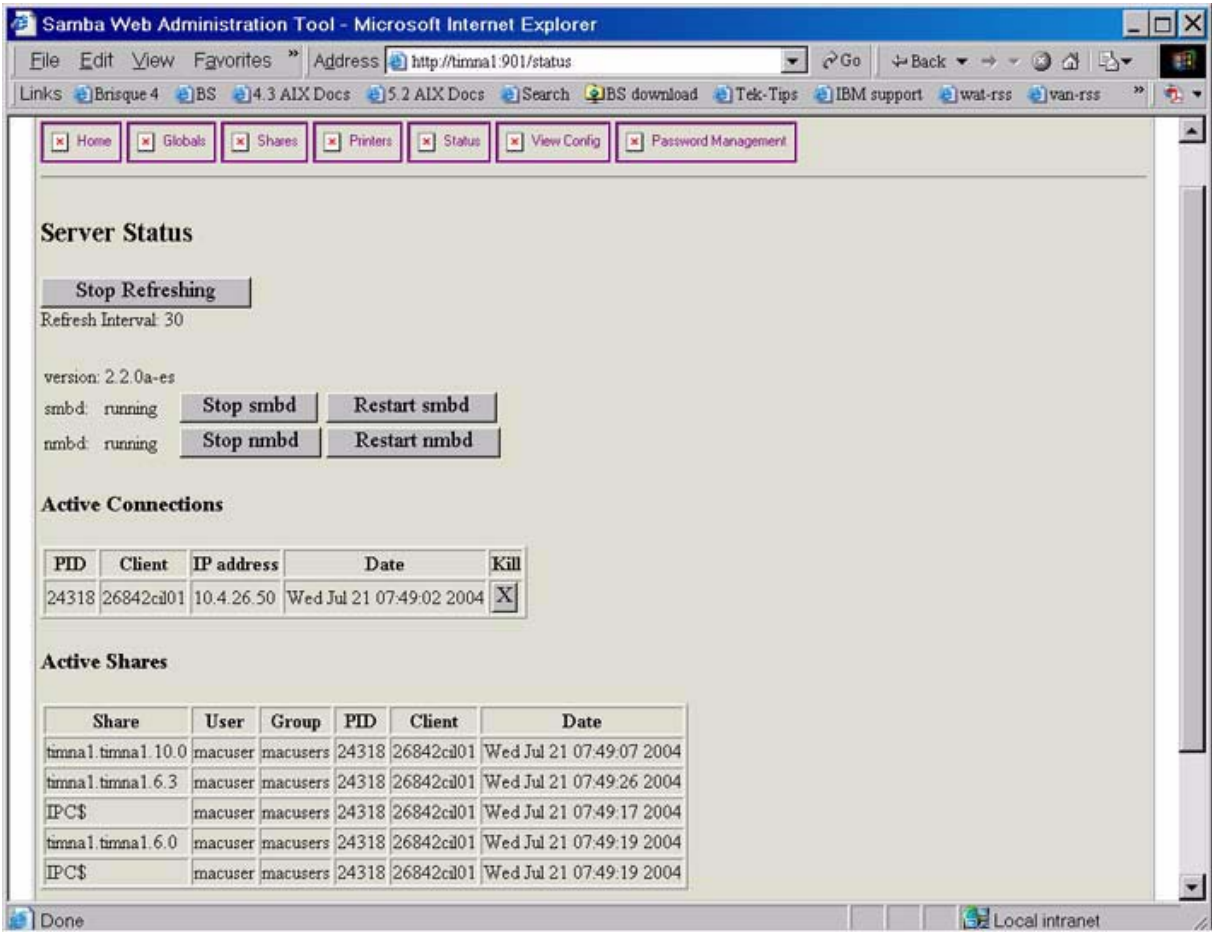


Figure 5: SWAT - Server Status window

The Server Status window provides information about connected clients and Server shares. To disconnect a client, click the **Kill** button. If needed, use the **Stop smbd**, **Restart smbd**, **Stop nmbd** and **Restart nmbd** buttons.



Figure 6: Password setup window