The Samba SMB File and Print Program - 1.9.18 and beyond

By Jeremy Allison

SAMBA Development Team

email: jeremy@netcom.com

Introduction
What is Samba ?

- Samba is an SMB file and print server for UNIX systems.
- SMB is the file sharing protocol built into Windows and OS/2, developed by 3COM and Microsoft. It has been built into all Windows OS's since Windows for Workgroups.
- SMB has recently been renamed CIFS by Microsoft, CIFS, or Common Internet File System is part of the attempt to make Windows 'Internet friendly'.
- Samba takes the view it is better to make the UNIX box talk the PC's protocol, than make the PC's talk the UNIX protocol (PC/NFS). It is much less hassle.

What is Samba

- Samba was originally developed by Andrew Tridgell, working at an Australian University.
- Samba was extended and is now maintained by a loosely connected group of people on the Internet, known as the Samba Team. This development model is similar to the one that works for the Linux Kernel.
- Like Linux, Samba is available 'without cost' under the GNU GPL license.
- The GPL allows anyone to use Samba for any purpose, but not to deny access to the source code.

The SMB/CIFS protocol

- The SMB protocol is the 'Swiss army knife' of protocols. It has a huge range of functions. It is complex and has changed much over time to fit Microsoft's needs.
- It has been specified by X/Open, but not completely. Microsoft have now made most of the protocol documents available on the Internet - but not some critical Windows NT components.
- Samba implements SMB over TCP for file sharing and UDP for browsing. SMB can run over other transports, notably IPX and NetBEUI.
- Microsoft is deprecating these other protocols and concentrating on TCP/IP.

The SMB/CIFS Protocol

- SMB is also known as the 'Lanman' protocol or 'Windows Networking'.
- The protocol has some advanced features such as command chaining and extensive option negotiation.
- The TCP/IP ports used are UDP 137 (browsing), UDP 138 (mailslots) and TCP 139 (filesharing).
- An example of a session will illustrate some concepts.

SMB/CIFS example

- Here is a client connecting to a server, doing a directory listing, reading a file and then disconnecting.

UDP-137	Name registration.
UDP-137	Name query request.
UDP-137	Positive name query response.
TCP-139	SMBnetgprot (negotiate protocol).
TCP-139	SMBsessetupX (session setup).
TCP-139	SMBtcon (tree connect).
TCP-139	SMBsearch (directory listing).
TCP-139	SMBopenX + SMBreadbraw (open and read file).
TCP-139	SMBclose (close file).
TCP-139	SMBtdis (tree disconnect).

SMB/CIFS - Advanced Features.

- SMB has some very advanced features (chaining, oplocks) added for speed purposes that make it faster than NFS (although not as safe for data sharing).
- Main feature is 'opportunistic locking' (known as op-locks).
- Op-locks allow a client to be granted a 'token' guarenteeing exclusing use of file - server will notify on file change.
- Allows client to cache entire file locally - Microsoft clients are written to use this extensively.
- Potential for data loss if client fails.
- Samba (1.9.18) implements op-locks - large speed increase for some programs.

The NBT (NetBIOS over TCP) Protocol.

- NBT (NetBIOS over TCP) is the protocol used to encapsulate the older NetBIOS protocol into TCP.
- Also used to implement name registration and resolution. Specified by Internet RFC's 1001 and 1002.
- Name resolution can be by broadcast or via point-to-point to a 'WINS server'.
- Samba can act as a WINS server but cannot replicate names with a Microsoft WINS server - Microsoft will not document this protocol.

The NBT (NetBIOS over TCP) Protocol.

- NBT namespace is flat. It doesn't scale to Internet needs.
- Microsoft have changed to using Internet DNS names but this requires a 'hack' to let clients contact servers (use of '*SMBSERVER' name).
- Only works with Windows NT 4.0 and beyond.
- There is no security in the name registration. This is extremely dangerous (as some hacker code has demonstrated).

Samba Security

- Samba was written with security in mind. It offers many more security options than other file sharing packages.
- Security bug (buffer overrun) in versions prior to 1.9.17p2 - do not run earlier version of Samba.
- Supports SMB encrypted passwords or UNIX passwords.
- Supports remote authentication to an NT server.
- All file system operations are done as an authenticated user - by default no 'guest' user (this can be set up, though).
- Never overrides UNIX security mechanisms.
- Carefully checks packets. Client is a potential enemy.
- tcp-wrappers style of host allow/deny built in.

SMB/CIFS Security

- SMB/CIFS is vulnerable to a 'man-in-the-middle' attack. Hackers have demonstrated this.
- Microsoft's response for Windows NT service pack 3 is to add a 'MAC' or cryptographic message integrity check to SMB packets.
- Samba doesn't currently implement this MAC (no user demand).
- SMB/CIFS is also vulnerable to a 'downgrade' attack. Windows 95 is particularly vulnerable.
- Microsoft have now released a fix for Windows95.
- With NT service pack 3 NT will no longer send unencrypted passwords - needs registry change to fix this (or set up Samba with encrypted password support).

Samba Portability

- Samba is written to be portable and needs no kernel modifications.
- It has been ported to non-UNIX platforms such as OS/2, Novell NetWare, VMS and AmigaOS.
- Some large sites run it on Cray and Convex supercomputers.
- File locking causes the most problems. Windows apps use complex file locking as a form of IPC (inter-process communication). Samba tries to cope by implementing locking on top of UNIX mechanisms. Thus locking is only as good as these mechanisms on the underlying platform.

Samba Scalability

- Samba uses one UNIX process per connected user.
- Current estimates of working memory set are around 600-800k per user - depends on usage.
- Commercial companies have run large scale Samba systems with over 500 concurrent users (in some cases replacing their own SMB server software with Samba).
- Samba can be run as a stand-alone daemon at system start-up or from the inetd server.
- Recommend that Samba be run as a daemon at larger installations for speed.

Samba Configuration

- Samba uses one configuration file smb.conf.
- Based on a similar format to the old WINDOWS.INI system.
- Many complicated options, however most default sensibly, allowing simple config files. An example :

```
[global]
  security = user
  workgroup = CYGNUS-WEST
  encrypt passwords = yes
  hosts allow = 192.168.2. localhost
  include = /usr/local/samba/lib/smb.conf.%m
[homes]
  browseable = no
  guest ok = no
  read only = no
  create mask = 0755
```

Samba Configuration

- Samba config file (smb.conf) continued..

```
[printers]
  guest ok = no
  path = /var/spool/smbprint
  print ok = yes
[cdrom]
  comment = Jeremy's CDROM
  path = /mnt/cdrom
  read only = yes
  locking = no
```

- One thing Samba needs is a graphical smb.conf configuration tool. This is being worked on - no availability date yet.
- Commercial Samba vendors ship graphical tools.

Samba and Browsing

- Browsing protocols allow the 'Network Neighborhood' to see all available servers.
- Browsing protocols are very complex and involve an election system to choose a 'browse master' that keeps the list of servers visible in 'Network Neighborhood'.
- Browse protocol principally uses UDP port 138.
- Samba browsing daemon has been completely re-written for 1.9.18. Now supports multi-homed hosts correctly.
- Samba (1.9.17 and above) supports browsing correctly on subnetted networks.
- Samba WINS server still not as scalable to as many entries as the MS one. This is being worked on.

Samba and Domain Protocols

- The Windows NT 'Domain' system is the heart of the NT networking model.
- Fulfills the same function as NIS/NIS+ but considerably more complex - uses DCE-RPC.
- Windows 95 only partly participates.
- Samba supports Windows 95 logons and logon scripts.
- Microsoft released details of these protocols after Samba code was released.
- If site has Windows 95 clients only Samba can act as a complete replacement for Windows NT Server.

Samba and Domain Protocols

- Windows NT Domain protocols are still undocumented. Microsoft have no plans to do so. NT Logon protocol was published in August 1997 on comp.protocols.smb.
- Main advantage of Domain protocols is account replication - single sign on.
- Samba Team has code that can dump Windows NT passwords into a Samba password file.
  - As featured in the 'Wall Street Journal'.
- A documented protocol has been proposed to allow all other SMB/CIFS vendors to synchronize account databases with Windows NT systems.
- This is partially implemented in Cygnus Solutions 'KerbNet' Kerberos 5 software. Available in source code form.

Samba and Domain Protocols.

- One member of the Samba Team (Luke Leighton) is actively working on adding Primary Domain Controller support to Samba.
- Currently Windows NT Workstations and Servers can join a 'Samba' Domain, but there are still parts that don't work correctly.
- It appears that the Windows NT Domain protocols may have serious security flaws. The Samba implementation has crashed Windows NT PDC's many times.
- Current (Dec '97) status is that User Manager for Domains has started to work with a Samba PDC.
- This is slow, difficult work with an undoucumented protocol, additional help is welcome.

SMB/CIFS Futures

- Microsoft is trying to tidy up CIFS protocol and remove redundant calls.
- With Windows NT 5.0 security model will be Kerberos 5 (already available on UNIX).
- Microsoft claim their Kerberos will interoperate with UNIX Kerberos (developed by MIT). Specified in RFC 1510.
- CIFS Authentication will move to Kerberos ticket model - several changes needed - not yet documented.
- Critical question. Will Microsoft document what goes in 'application specific' field of their Kerberos 5 tickets ? Current answer is 'no'.
- This will mean UNIX Kerberos KDC's will not be able to create tickets for Microsoft clients - an example of a monopoly subverting an open standard.

What's new in Samba 1.9.18

- Opportunistic locking now supported - massive speed increase
- DES code for authentication now included with Samba. No longer necessary to link in external library.
- Internationalization support. Dynamic support for different client code pages within the same binary. Customizable by the administrator.
- Re-write of browsing/WINS code. Multi-homed host support.
- Re-write of share mode code to use faster locking semantics (same as those used by Oracle) - another portability win and speed increase.

What's new in Samba 1.9.18

- Ability to serve Windows 95 printer drivers automatically from a Samba share.
- System V printing support donated by Sun - as easy to use as the BSD printcap style code.
- Many flaws in browsing/name resolution fixed with the new nmbd code - new code easier to extend.
- Many small improvements and code enhancements.
- Many bugfixes from around the world (I think we fixed more than we broke :-).

Samba Futures - 1.9.19 and beyond.

- Add Windows NT specific SMB calls. This will ease adding NT RPC calls.
- Add 'change notify' support to Samba as part of the Windows NT specific SMB calls.
- Samba will track CIFS standards process. Implement new Windows NT Service pack 3 security model ?
- Move to Kerberos based authentication as soon as Microsoft specify the protocol changes and ship the clients.
- Add a graphical configure tool (at last !).
- Once Windows NT PDC support is available we will call it Samba 2 :-).

Samba Futures - 1.9.19 and beyond

- Blocking locks. As Samba is single threaded internally lock calls currently are non-blocking.
- Better Windows NT integration. Attempts are bing made to get Samba to map NT security descriptors into UNIX permissions and vica-versa. Not sure if this is possible yet (we may need POSIX acl support).
- UNICODE support - better internationalization.
- Remote administration of Samba servers.
- Samba book written by Samba Team member. Projected availability Jan/Feb '98. This book has been reviewed by Andrew and myself for accurary.

Samba futures - 1.9.19 and beyond.

- Updated WINS support - for large installations (University of Mitchigan needs to serve >35,000 machines - they are writing the code).
- Some form of WINS replication - either Microsoft (if documented) or Samba Team invented (if not).
- Better OS/2 support (Lanman announce, Workplace shell fixes) - large patch already written - needs integration.
- Samba code profiling - Samba Team want to be faster than NT on equivalent hardware with UNIX based OS Benchmarks with Samba on non-Intel hardware of equal price/performance show Samba is faster than NT !
- Whatever additions people send - remember - IT'S YOUR CODE !

References and code availability

- Samba Web site (SGI donated server):
  - http://samba.anu.edu.au/samba
  - FAQ and Manual pages available.
  - Mailing list archives
  - Source code and pre-compiled binaries for some systems available.
  - Survey page - remember to register ! You'll be surprised at some of the companies already there.
- Samba mailing list available.
- Newsgroup comp.protocols.smb

Commercial Support for Samba

- List of commercial companies supporting Samba available at the Samba Web site. Currently over 100 organizations offering support - still growing.
- World wide coverage (not one company, yet :-).
- Samba ships as standard with most Linux distributions, RedHat and Caldera for example support Samba commercially as part of their products.
- Report bugs to

  samba-bugs@samba.anu.edu.au