Samba and SMB Tutorial

Andrew Tridgell
E-mail: tridge@samba.anu.edu.au

July 7, 1998

This tutorial will be divided into four sections:

- The SMB protocol - what's on the wire
- Configuring Samba - installing and tuning Samba
- The future of SMB - where the protocol is going
- Discussion - we discuss your SMB needs

1 The SMB Protocol

Samba implements the SMB protocol and a number of associated protocols. It is sometimes useful to compare SMB to NFS

- SMB has scores of top level commands some with dozens of subcommands and subsubcommands
- NFS has around a dozen commands in total
- SMB is connection oriented with a client-maintains-state architecture to handle reconnect
- NFS is stateless
- SMB has sophisticated command chaining, client caching and locking capabilities.
- NFS is well documented and was designed before being implemented
- SMB is badly documented with the documentation being written retrospectively from the existing implementations

1.1 The anatomy of SMB

The SMB protocol can work over many transports, but the most interesting these days is TCP/IP. SMB on TCP/IP uses three ports:

- UDP/137 is used for name resolution and registration
- UDP/138 is used for browsing
- TCP/139 is used for the main file and print sharing transactions

This is a simplification, but it is close

1.2 NBT on UDP/137

UDP/137 carries name registrations and name queries. When the queries are unicast this protocol if often referred to as WINS (or Windows Internet Name Server). It is a inappropriate name as WINS does not work at all well on large WANs.

We will now observe a Win95 machine called VAAREKE starting up and watch the traffic on UDP/137. Note particularly the differences in the startup for WINS and non-WINS.

1.3 NBT on UDP/138

UDP/138 carries browsing traffic. This is mostly local broadcast traffic with the occasional message between subnets for cross subnet browsing.

We will take a look at the following situations:

- a browse client (such as a win95 PC) boots up
- a browse server restarts

One thing to note about these packets is that they actually have a mixed byte order! It is a rare thing for a internet protocol to mix byte orders. Can you work out how it happened?

2 SMB on TCP/139

TCP/139 is where the main action happens with the SMB protocol. All file and printer sharing happens on this port. It is a complex protocol but its structure is fairly easy to understand. We will look at a number of situations:

- connecting to a SMB server

- copying a file
- obtaining and breaking oplocks
- printing a file

2.1 SMB authentication

SMB authentication is a thorny issue. There are two main authentication models available but unfortunately many people want something that is a combination of the two.

We will examine the authentication process for the two security models:

- user level security - where the client first authenticates then chooses a share to access
- share level security - where the client authenticates as part of accessing a share

2.2 Domain logons

The SMB protocol (or more accurately the MS implementations) support two quite different methods for "network logons", one being used by Windows95 and the other by WindowsNT.

The Windows95 domain logon protocol is fairly simple but is a useful way of allowing users to move between workstations while maintaining a single point of logon and single place where profiles are stored.

A Windows95 domain logon works by:

- The client doing a broadcast on UDP/138 to ask for a logon server
- The logon server responding with its netbios name
- The client doing a SMB connect to the logon server
- The client asking the logon server for information on its domain logon configuration, such as logon scripts, home directories and profile paths.

A WindowsNT domain logon works by:

- The client doing a broadcast on UDP/138 to ask for a NT domain server
- The domain server responding with its netbios name
- The client doing a SMB connect to the logon server

- The client establishes an encrypted secure pipe using a shared secret key and a RC4 encryption stream
- The client asks the logon server for information on its domain logon configuration, such as logon scripts, home directories and profile paths.

The NT domain protocol may look a lot more secure, but it actually has some major flaws. unfortunately we have been forced to reproduce some of those flaws in the Samba implementation in order to remain compatible with NT clients.

2.3 Locking and client caching

One area where SMB is particularly rich is in the range of locking capabilities available. They are divided into 3 types of locks:

- byte range locking - for locking records in a file
- share modes - for specifying what other users can do with a file at the same time
- opportunistic locks - not really locking at all, oplocks are a safe client caching mechanism

3 Configuring Samba

Samba is really fairly easy to install as long as you read the documentation. Unfortunately most people seem to skip the documentation and instead write to us (hint: read the docs first!).

3.1 Installing Samba

It's simple:

- unpack the archive
- read the documentation
- edit the Makefile
- compile - use "make"
- install - use "make install"
- build a config file, starting with the sample

I'll give a quick demo

3.2 The smb.conf file

The smb.conf file should be familiar to anyone who has dealt with the old win.ini style config files.

Here are some tips:

- don't just guess the meaning of an option from its name. Look in the man page!
- take advantage of the % macros to allow for per host and per user customization
- smb.conf access controls are not a replacement for good unix file permissions
- use the include option and macros to allow you to test configs on one guinea pig machine

3.3 performance tuning

Lots of people ask how to tune Samba performance. The best way to tune anything is to first understand why is is running slower than you expect. For this I suggest you use a sniffer and your system trace utility.

There are some common "quick fixes" however:

- socket options, particularly TCP_NODELAY
- client TCP tuning options
- oplocks

The biggest problem with SMB performance is the way that MS have written their clients. A less efficient client is hard to imagine. Let's look at a couple of examples:

- file properties
- copying a file

3.4 SWAT - the Samba Web Administration Tool

Samba is finally coming out of the dark ages as far as GUI administration tools are concerned. The next major release will come with a web based GUI config tool called SWAT.

I'll give you a quick demo to whet your appetites

4 The future of SMB and Samba

SMB and Samba are rapidly evolving things. While Samba is constantly improving we also have to track major changes in the SMB protocol.

4.1 CIFS specification effort

A couple of years ago MS started a standardization effort for CIFS. The motivations for this are sure to be complex but the result is definitely a good thing for the SMB community. The SMB protocol is finally being (at least partly) documented!

The protocol is still really defined by the MS implementations, but at least its a start.

4.2 What's new in CIFS

CIFS adds a few new things

- formalizes the new "NT LM 0.12" subprotocol
- adds some rather unsatisfactory methods for solving the flat name space issue using DNS
- finally removes some SMB commands - some bloat is removed

4.3 LDAP

Microsoft have stated that LDAP is the way of the future for name resolution and some other aspects of SMB. It is still very unclear exactly how this will work.

4.4 Kerberos

Microsoft have decided that the proprietary domain protocols will be replaced with Kerberos. This is certainly a good thing, but there are some gotchas.

4.5 netbios-less operation

NT5 will include netbios-less operation on a new TCP port number. This sparked the most heated debate we have yet seen in the CIFS community. I'll try to explain the issues as I see them.

4.6 PDC support in Samba

Samba is continuing to develop NT4 style Primary Domain Controller support. I'll give a demo and a brief rundown on why this is important.

5 Discussion

This final section I'd like to leave open ended. I'm hoping that a number of the tutorial attendees will describe their network setup so that we can discuss the role that SMB and Samba plays in their network.

I'm hoping to learn as much from this section as you do! I'm always looking for feedback on Samba so I know where effort needs to be concentrated.

6 Further info

There is lots of Samba info available!

- The first stop for Samba info is the Samba web site at http://samba.anu.edu.au/samba/
- John Blair has written a Samba book. It is well worth reading if you run a Samba server. See the Samba web site for details. More books are being written as well.
- The Samba mailing lists, see http://samba.anu.edu.au/listproc/
- you can contact me at tridge@samba.anu.edu.au, but please be patient in waiting for a reply, I get far more email than I can handle.