[Index] [Feedback]

Just what is SMB?

V1.2
Richard Sharpe
8-Oct-2002

Copying
Please see the section on Copying this document for details of my policy on use of this document.

Disclaimer
This document attempts to provide a service to people involved with the SMB (soon to be CIFS) protocol in some way. Every attempt has been made to ensure that the information is correct, but no warranties are implied. Richard Sharpe can not be held liable for any loss or consequences resulting from your use or misuse of this information.

If you have any comments, please send me mail at sharpe@ns.aus.com. ## Acknowledgments
I would like to thank Andrew Tridgell for getting me started in this area by suggesting that I might like to start on smblib, Dan Shearer for much encouragement and information, Paul Blackman for helping with this page, and a number of other people who have not given me approval to name them.

I would also like to thank the many people who have sent me positive comments and constructive feedback.

Trademarks
Microsoft, MS, Windows, Windows 95, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation. Microsoft Corporation in no way endorses this document, nor is the author in any way affiliated with Microsoft Corporation.

All other trademarks are the sole property of their respective owners.

Table of Contents

Introduction
This document explains what the SMB protocol is and discusses the many client and server implementations of SMB that are available. The document grew out of my interest in implementing SMBlib, a portable library of SMB client routines.

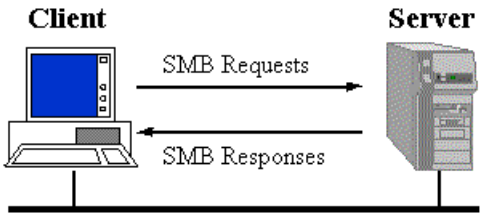
SMB is an important protocol because of the large number of PCs out there that already have client and server implementations running on them. All Windows for Workgroups, Windows 95 and Windows NT systems are (or are capable of) running SMB as either a client, a server, or both.

What's New
While there are many things out there that are new, perhaps the thing of greatest interest as far as the SMB protocol is concerned is CIFS, the Common Internet File System.

What is SMB?
SMB, which stands for Server Message Block, is a protocol for sharing files, printers, serial ports, and communications abstractions such as named pipes and mail slots between computers.

The earliest document I have on the SMB protocol is an IBM document from 1985. It is a copy of an IBM Personal

Computer Seminar Proceedings from May 1985. It contains the **IBM PC Network SMB Protocol**. The next document I have access to is a Microsoft/Intel document called **Microsoft Networks/OpenNET-FILE SHARING PROTOCOL** from 1987. The protocol was subsequently developed further by Microsoft and others. Many of the documents that define the SMB protocol(s) are available at ftp.microsoft.com in the SMB documentation area.



SMB is a client server, request-response protocol. The diagram to the left illustrates the way in which SMB works. The only exception to the request-response nature of SMB (that is, where the client makes requests and the server sends back responses) is when the client has requested opportunistic locks (oplocks) and the server subsequently has to break an already granted oplock because another client has requested a file open with a mode that is incompatible with the granted oplock. In this case, the server sends an unsolicited message to the client signalling the oplock break.

Servers make file systems and other resources (printers, mailslots, named pipes, APIs) available to clients on the network. Client computers may have their own hard disks, but they also want access to the shared file systems and printers on the servers.

Clients connect to servers using TCP/IP (actually NetBIOS over TCP/IP as specified in RFC1001 and RFC1002), NetBEUI or IPX/SPX. Once they have established a connection, clients can then send commands (SMBs) to the server that allow them to access shares, open files, read and write files, and generally do all the sort of things that you want to do with a file system. However, in the case of SMB, these things are done over the network.

As mentioned, SMB can run over multiple protocols. The following diagram shows this:

<table>
<tr><td>OSI</td><td colspan="4"></td><td>TCP/IP</td></tr>
<tr><td>Application
Presentation</td><td colspan="4">SMB</td><td rowspan="2">Application</td></tr>
<tr><td>Session</td><td>NetBIOS</td><td rowspan="3">NetBEUI</td><td>NetBIOS</td><td>NetBIOS</td></tr>
<tr><td>Transport</td><td rowspan="2">IPX[1]</td><td rowspan="2">DECnet</td><td>TCP&UDP</td><td>TCP/UDP</td></tr>
<tr><td>Network</td><td>IP</td><td>IP</td></tr>
<tr><td rowspan="2">Link</td><td rowspan="2">802.2,
802.3,802.5</td><td>802.2</td><td rowspan="2">Ethernet V2</td><td rowspan="2">Ethernet V2</td><td rowspan="2">Ethernet or
others</td></tr>
<tr><td>802.3,802.5</td></tr>
<tr><td>Physical</td><td colspan="4"></td></tr>
</table>

SMB can be used over TCP/IP, NetBEUI and IPX/SPX. If TCP/IP or NetBEUI are in use, the NetBIOS API is being used.

SMB was also sent over the DECnet protocol. Digital (now Compaq) did this for their PATHWORKS product.

NetBIOS over TCP/IP seems to be referred to by many names. Microsoft refers to it as NBT in some places and NetBT in others (specifically in their Windows NT documentation and in the Windows NT registry). Others refer to it as RFCNB. NetBEUI is sometimes refered to as NBF (NetBIOS Frame Format?) by Microsoft.

NetBIOS Names
If SMB is used over TCP/IP, DECnet or NetBEUI, then NetBIOS names must be used in a number of cases. NetBIOS names are up to 15 characers long, and are usually the name of the computer that is running NetBIOS. Microsoft, and some other implementors, insist that NetBIOS names be in upper case, especially when presented to servers as the CALLED NAME.

When NetBIOS names are sent over the wire they are padded to 15 characters with spaces and a 16th character is added that specifies the type of NetBIOS name. Microsoft refers to these as NetBIOS Suffixes. A complete list can be found in the Microsoft Knowledge Base article Q163409.

There are two classes of NetBIOS names, Unique names and Global Names. However, Microsoft also defines a few other classes: Internet Group, Domain, and Multihomed.

SMB Protocol Variants
Since the inception of SMB, many protocol variants have been developed to handle the increasing complexity of the environments that it has been employed in.

The actual protocol variant client and server will use is negotiated using the *negprot* SMB which must be the first SMB sent on a connection.

The first protocol variant was the Core Protocol, known to SMB implementations as PC NETWORK PROGRAM 1.0. It could handle a fairly basic set of operations that included:

- connecting to and disconnecting from file and print shares
- opening and closing files
- opening and closing print files
- reading and writing files
- creating and deleting files and directories
- searching directories
- getting and setting file attributes
- locking and unlocking byte ranges in files

Subsequent variants were introduced as more functionality was needed. Some of these variants and the related version of LAN Manager are:

SMB Protocol Variant	Protocol Name	Comments
PC NETWORK PROGRAM 1.0	Core Protocol	The original version of SMB as defined in IBM's PC Network Program. Some versions were called PCLAN1.0
MICROSOFT NETWORKS 1.03	Core Plus Protocol	Included Lock&Read and Write&Unlock SMBs with different versions of raw read and raw write SMBs
MICROSOFT NETWORKS 3.0	DOS LAN Manager 1.0	The same as LANMAN1.0, but OS/2 errors must be translated to DOS errors.
LANMAN1.0	LAN Manager 1.0	The full LANMAN1.0 protocol.
DOS LM1.2X002	LAN Manager 2.0	The same as LM1.2X002, but errors must be translated to DOS errors.
LM1.2X002	LAN Manager 2.0	The full LANMAN2.0 protocol.
DOS LANMAN2.1	LAN Manager 2.1	The same as LANMAN2.1, but errors must be translated to DOS errors.
LANMAN2.1	LAN Manager 2.1	The full LANMAN2.1 protocol.
Windows for Workgroups 3.1a	LAN Manager 2.1?	Windows for Workgroups 1.0?
NT LM 0.12	NT LAN Manager 1.0?	Contains special SMBs for NT
Samba	NT LAN Manager 1.0?	Samba's version of NT LM 0.12?
CIFS 1.0	NT LAN Manager 1.0	Really NT LM 0.12 plus a bit?

Some variants introduced new SMBs, some simply changed the format of existing SMBs or responses, and some variants did both.

Security
The SMB model defines two levels of security:

- **Share level**. Protection is applied at the share level on a server. Each share can have a password, and a client only needs that password to access all files under that share. This was the first security model that SMB had and is the only security model available in the Core and CorePlus protocols. Windows for Workgroups' vserver.exe implements share level security by default, as does Windows 95.
- **User Level**.Protection is applied to individual files in each share and is based on user access rights. Each user (client) must log in to the server and be authenticated by the server. When it is authenticated, the client is given a UID which it must present on all subsequent accesses to the server. This model has been available since LAN Manager 1.0.

Browsing the network
Having lots of servers out in the network is not much good if users cannot find them. Of course, clients can simply be configured to know about the servers in their environment, but this does not help when new servers are to be introduced or old ones removed.

To solve this problem, browsing has been introduced. Each server broadcasts information about its presence. Clients listen

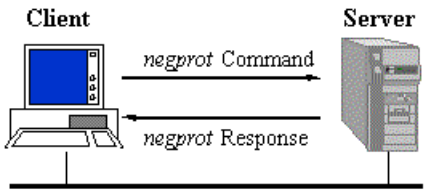
for these broadcasts and build up browse lists. In a NetBEUI environment, this is satisfactory, but in a TCP/IP environment, problems arise. The problems exist because TCP/IP broadcasts are not usually sent outside the subnet in which they originate (although some routers can selectively transport broadcasts to other subnets).

Microsoft have introduced browse servers and the Windows Internet Name Service (WINS) to help overcome these problems.

CIFS: The latest incarnation?
Microsoft and a group of other vendors (Digital Equipment, Data General, SCO, Network Appliance Corp, etc) are engaged in developing a public version of the SMB protocol. It is expected that CIFS 1.0 will be essentially NT LM 0.12 with some modifications for easier use over the Internet.

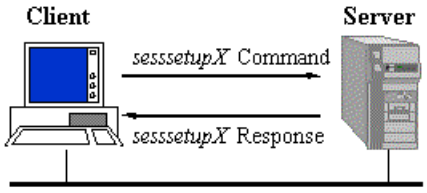
An Example SMB Exchange
The protocol elements (requests and responses) that clients and servers exchange are called SMBs. They have a specific format that is very similar for both requests and responses. Each consists of a fixed size header portion, followed by a variable sized parameter and data portion.

After connecting at the NetBIOS level, either via NBF, NetBT, etc, the client is ready to request services from the server. However, the client and server must first identify which protocol variant they each understand.

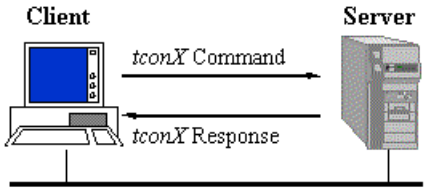


The client sends a *negprot* SMB to the server, listing the protocol dialects that it understands. The server responds with the index of the dialect that it wants to use, or 0xFFFF if none of the dialects was acceptable.

Dialects more recent than the Core and CorePlus protocols supply information in the negprot response to indicate their capabilities (max buffer size, canonical file names, etc).



Once a protocol has been established. The client can proceed to logon to the server, if required. They do this with a *sesssetupX* SMB. The response indicates whether or not they have supplied a valid username password pair and if so, can provide additional information. One of the most important aspects of the response is the UID of the logged on user. This UID must be submitted with all subsequent SMBs on that connection to the server.



Once the client has logged on (and in older protocols-Core and CorePlus-you cannot logon), the client can proceed to connect to a tree.

The client sends a *tcon* or *tconX* SMB specifying the network name of the share that they wish to connect to, and if all is kosher, the server responds with a TID that the client will use in all future SMBs relating to that share.

Having connected to a tree, the client can now open a file with an open SMB, followed by reading it with read SMBs, writing it with write SMBs, and closing it with close SMBs.

SMB Clients and Servers Currently Available

There are a few SMB clients available today and a relatively large number of servers available from a range of vendors.

The main clients are from Microsoft, and are included in Windows for WorkGroups 3.x, Windows 95, and Windows NT. They are most evident when you use the File Manager or the Windows 95 Explorer, as these allow you to connect to servers across the network. However they are also used when you open files using a UNC (universal naming convention).

Some other clients that I am aware of are:

- smbclient from Samba
- smbfs for Linux
- SMBlib (an SMB client library that is in development)

Server implementations are available from many sources. Some that I am aware of are:

- Samba
- Microsoft Windows for Workgroups 3.x
- Microsoft Windows 95

- Microsoft Windows NT
- The PATHWORKS family of servers from Digital
- LAN Manager for OS/2, SCO, etc
- VisionFS from SCO
- TotalNET Advanced Server from Syntax
- Advanced Server for UNIX from AT&T (NCR?)
- LAN Server for OS/2 from IBM

The next two sections will discuss each of the above in turn.

SMB Servers

Before discussing SMB servers, it is useful to discuss the difference between Workgroups and Domains.

Workgroups
A workgroup is a collection of computers that each maintain their own security information. With Windows for Workgroups, each server is pretty much in share level security. Windows 95 can pass user authentication off to an NT or LAN Manager server.

However, the point of a workgroup is that security is distributed, not centralized.

Domains
A domain is a collection of computers where security is handled centrally. Each domain has one or more domain controllers. There is usually a primary domain controller and several backup domain controllers. The domain controllers maintain account style information related to users (clients), like account names, encrypted passwords, authorized hours of use, groups the user belongs to, etc.

Samba
Samba is a freely available SMB server for UNIX, OpenVMS (recently ported and maybe not very stable) developed by Andrew Tridgell and maintained by a loosely knit group of people all over the world. Samba runs on a great many UNIX variants (Linux, Solaris, SunOS, HP-UX, ULTRIX, DEC OSF/1, Digital UNIX, Dynix (Sequent), IRIX (SGI), SCO Open Server, DG-UX, UNIXWARE, AIX, BSDI, NetBSD, NEXTSTEP, A/UX, etc).

Samba implements the NT LM 0.12 protocol dialect. Samba can now participate in a domain (both as a PDC and a Member of a domain), and it can participate in browsing and can be a browse master. Samba can also process logon requests for Windows 95 systems

Samba implements user level security, but shares can be public where access is mapped to the owner etc of the share.

Microsoft Windows Servers
Microsoft has a number of SMB server implementations for the Windows range of operating systems. These are not separate products, rather, they are integral to the appropriate version of the Windows operating system. However, they can be switched off either though the Control Panel or at the command line (**net stop server** at DOS prompt).

It is clear from the fact that the Windows 95 and Windows NT SMB servers react differently to certain sequences of SMBs, that Microsoft do not use the same code for each of these servers (although the Windows for Workgroups and Windows 95 implementations may be derived from the same code).

Windows for Workgroups 3.11 implements the Windows for Workgroups 3.0a protocol variant, and implements share level security.

Windows 95 implements the NT LM 0.12 protocol level and implements both share and user level security.

Windows NT implements the NT LM 0.12 protocol level and implements both share and user level security.

LAN Manager and LAN Manager for UNIX (LM/X)
Microsoft and AT&T GIS ported various LAN Manager versions to the UNIX operating system. This code formed the basis of many SMB servers available for UNIX operating systems from many vendors.

Some examples are: LM/X for SCO, LM Server for HP-UX (Advanced Server/9000), etc.

The most recent version of this software seems to be LAN Manager for UNIX Version 2.2, which implements the LANMAN2.1 protocol variant.

VisionFS
VisionFS is a written-from-scratch SMB server from SCO. It is available for Solaris 2.x, HP-UX and SCO (both SCO

OpenServer and UNIXware).

TotalNET Advanced Server
This product is from Syntax. It is a completely independently written SMB server, that was perhaps the first SMB server for UNIX. These days, it comes with additional modules providing AppleShare and NetWare serving all in the one product.

Advanced Server for UNIX
After LM/X, NCR (which used to be ATT GIS) (perhaps with help from Microsoft) ported the Windows NT SMB server code to UNIX to provide the same level of functionality as Windows NT.

PATHWORKS
PATHWORKS is the name of a product family from Digital equipment corporation. It included both servers and clients, with the servers running on:

- VAX and Alpha VMS
- VAX and MIPS ULTRIX
- DEC OSF/1 for AXP and Digital UNIX (DEC OSF/1 renamed)
- OS/2

The clients ran on DOS, Windows, Windows for Workgroups, Windows NT and Windows 95 and are explained below.

Digital's clients and server implement SMB over DECnet as well as TCP/IP and more recently, NetBEUI. The SMB over DECnet specification has never been released.

Digital's original PATHWORKS servers were for VAX/VMS and implemented the CorePlus protocol (MICROSOFT NETWORKS 1.03 dialect). This product went through several versions and culminated in version 4.2. After a time, a version was done for ULTRIX and called PATHWORKS for ULTRIX V1, the highest version of which was 1.3. Both of these product streams were internally developed.

Subsequently, Digital used the AT&T and Microsoft LAN Manager for UNIX (LM/X) code. This was released as PATHWORKS V5.0 for OpenVMS (LAN Manager) and PATHWORKS V5.0 for Digital UNIX (LAN Manager). This product implements LAN Manager for UNIX V2.2 and the highest SMB dialect that it recognizes is LANMAN2.1 (and DOS LANMAN2.1). The reason for the LAN Manager in brackets at the end of each product name is that the products also support NetWare functionality.

PATHWORKS V5 is able to participate in a Windows NT based domain, albeit only as a Backup Domain Controller or a member server.

Recently, Digital has announced PATHWORKS V6.0 for UNIX (Advanced Server), which is based on AT&T's ASU (Advanced Server for UNIX) product.

LAN Server for OS/2
This is an IBM product that seems to be derived in some way from Microsoft's LAN Manager code.

SMB Clients

There are several SMB clients out there:

- Microsoft Clients
  - Windows NT
  - Windows 95
  - Windows for Workgroups 3.11
- Digital's PATHWORKS clients
- Samba's smbclient
- Linux's smbfs
- SMBlib

Further Resources On The Web

The following are some other web pages that you can visit that are relevant to the SMB protocol:

- CIFS Explained by John Klevin
- Samba
- SMBlib
- SCO's VisionFS

- Syntax's TotalNET Advanced Server
- Digital's PATHWORKS products
- Microsoft's Windows NT products
- IBM's LAN Server products
- IBM's PC Integration with AIX
- Data General's Support of Advanced Server for UNIX
- smbfs LSM entry (and smbfs ftp location)
- CIFS Home page
- Network Appliance's Support for CIFS
- HP Ships NT Server Network Operating System on Enterprise-Class HP-UX Platform
- AT&T GIS announces Advanced Server for UNIX Systems
- Thursby's Dave, Macintosh Client Software for Microsoft Networking
- Solstice LM Server
- Triteal's TEDfs, an SMB server for CDE (Unix) machines.

Copying this document

I have had a number of requests for permission to use this document in other material. In one case, I was asked if someone could include this document as an appendix in a book. In another case, I was asked if the document could be handed to customers and potential customers. In both cases I felt that the request was reasonable.

My view on these matters is that this document was written to be read.

However, I would ask that you send me email stating your intended use and requesting my permission.

FeedBack

This document will be updated from time to time. If you have any comments, please feel free to send me email at *sharpe@ns.aus.com*

Visit me at RichardSharpe.com for more info on what I am currently doing.

Last updated 8-Oct-2002.

Introduction to Server Message Block (SMB). Server Message Block (SMB) protocol was first created by IBM in the 1980s. It is one of the versions of the Common Internet File System (CIFS) to transfer the files over the network. Server Message Block is a network communication transfer protocol to provide shared access to files, printers, ports between the networks. What is Server Message Block? SMB is a client-server interaction protocol where clients request a file and the server provides it to the client. It is now a Windows-based network that gives users to create, modify and delete the share