## SMB Request and Message layouts

NetBIOS Header (4 byte)					S Header byte)			NetBIOS Header (4 byte)			
{0xFF, 'S', 'M', 'B'} (4 byte)					S','M','B'} byte)			{0xFE, 'S', 'M', 'B'} (4 byte)			
Command (1 byte)				Command (1 byte)				Header Length (2 byte)			
Status code (4 byte)					Status code (4 byte)			Epoch (2 byte)			
Flags (1 byte) Flags2 (2 byte)					(1 byte)			Status code (4 byte)			
Pad 12 byte	Pid high			Pad 12 byte	Pid high (2 byte)  Signature (8 byte)  Pad (2 byte)			Command (2 byte)			
	(2 byte)					S M	s	Credits (2 byte)			
	Signature (8 byte)		S			B R E	M B	Flags (4 byte)			
	Pad (2 byte)	-	B M			Q U E	M E S	Chain Offset (4 byte)			
Tree Id (2 byte)			E S	Tree Id	I (2 byte)	S T	A				
Pid low (2 byte)		S M	S	Pid low (2 byte)  Uid (2 byte)		L	E	Command Sequence	S M B 2 R E		
Uid (2 byte)		B	G E			E N G	L	(8 byte)			S M B
Mid (2 byte) Word count (1 byte)		R	L	Mid (2 byte) Word count (1 byte)		T	N G				2
ANDX command (1 byte) ANDX Reserved (1 byte)		Q U	N G		Byte count (1 byte)		T H	Pid (4 byte)	Q		M E S S A G
ANDX Offset (2 byte)  Byte count (1 byte)		E S	T H		Parameters			Tid	E		
Byte count (1 byte)		T       ,		(size matches word count)				(4 byte)	Т		
Parameters (size matches word count)		E N G		Optiona	Optional Padding				E N		L
Optional Padding		H		Data ( size matches byte count)				Session Id (8 byte)	G T H		E N G T
Data ( size matches byte count)											Н
				SMB1 Non-chained							
			message								
Optional Padding Word count (1 byte) ANDX command (1 byte) ANDX Reserved (1 byte) ANDX Offset (2 byte) Byte count (1 byte)  Parameters (size matches word count)			S				Signature (16 byte)				
			M B								
			M								
			E								
			S A					Length (2 byte)			
			G E								
Optional Padding  Data ( size matches byte count)			L				Doulood				
			E N G T					Payload			
SMB1 (	Oh o in o d				© 2010 Likewise S			SMB2 Non-chained			

SMB1 Chained Message

Copyright © 2010 Likewise Software

SMB2 Non-chained message