

Contents

Foreword	xxi
Introduction	xxiii
PART I NBT: NetBIOS over TCP/IP	I
Chapter 1 A Short Bio of NetBIOS	3
1.1 NetBIOS and DOS: The Early Years	4
Chapter 2 Speaking NetBIOS	5
2.1 Emulating “NetBIOS LANs”	6
2.1.1 <i>The NetBIOS Name Service</i>	7
2.1.2 <i>The NetBIOS Datagram Service</i>	10
2.1.3 <i>The NetBIOS Session Service</i>	11
2.2 Scope: The Final Frontier	12
2.3 Thus Endeth the Overview	16

Chapter 3	The Basics of NBT Implementation	17
3.1	You Got the Name, Look Up the Number	18
3.1.1	<i>Encoding NetBIOS Names</i>	19
3.1.2	<i>Fully Qualified NBT Names</i>	22
3.1.3	<i>Second Level Encoding</i>	22
3.1.4	<i>Name Service Packet Headers</i>	25
3.1.5	<i>The Query Entry</i>	28
3.1.6	<i>Some Trouble Ahead</i>	29
3.1.7	<i>Finally! A Simple Broadcast Name Query</i>	32
3.2	Interlude	38
Chapter 4	The Name Service in Detail	41
4.1	NBT Names: Once More with Feeling	42
4.1.1	<i>Valid NetBIOS Name Characters</i>	42
4.1.2	<i>NetBIOS Names within Scope</i>	44
4.1.3	<i>Encoding and Decoding NBT Names</i>	45
4.2	NBT Name Service Packets	48
4.2.1	<i>Name Service Headers</i>	48
4.2.2	<i>Name Service Question Records</i>	53
4.2.3	<i>Name Service Resource Records</i>	55
4.3	Conversations with the Name Service	61
4.3.1	<i>Name Registration</i>	62
4.3.1.1	Broadcast Name Registration	66
4.3.1.2	Unicast (NBNS) Name Registration	75
4.3.1.3	M and H Node Name Registration	80
4.3.1.4	Registering Multi-Homed Hosts	81
4.3.2	<i>Name Query</i>	85
4.3.2.1	Negative Query Response	89
4.3.2.2	Positive Query Response	91
4.3.2.3	The Redirect Name Query Response	93
4.3.2.4	A Simple Name Query Revisited	93
4.3.3	<i>Name Refresh</i>	98
4.3.4	<i>Name Release</i>	100
4.3.4.1	Name Release Response	102

4.3.5	<i>Node Status</i>	103
4.3.5.1	Node Status Response	104
4.3.6	<i>Name Conflict Demand</i>	111
4.3.6.1	Name Release Demand Revisited	112
4.4	Enough Already	113
Chapter 5	The Datagram Service in Detail	115
5.1	Datagram Distribution over Routed IP Internetworks	117
5.2	The NBDD and the Damage Done	119
5.3	Implementing a Workable Datagram Service	120
5.3.1	<i>Fragmenting Datagrams</i>	125
5.3.2	<i>Receiving Datagrams</i>	126
5.3.3	<i>Querying the NBDD</i>	127
5.3.4	<i>The Second Least Well Understood Aspect of NBT</i>	128
Chapter 6	The Session Service in Detail	129
6.1	Session Service Header	129
6.2	Creating an NBT Session	130
6.3	Maintaining an NBT Session	139
6.4	Closing an NBT Session	140
Chapter 7	Where It All Went Wrong	141
7.1	The 0x1Dirty Little Secret	141
7.2	Twenty-five IPs or Less	142
7.3	Special Handling Required for 0x1B Names	142
7.4	Alternate Name Resolution	143
7.5	The Awful Truth	144
PART II	SMB: The Server Message Block Protocol	145
Chapter 8	A Little Background on SMB	147
8.1	Getting Started	149

8.2	NBT or Not NBT	150
Chapter 9	An Introductory Tour of SMB	153
9.1	The Server Identifier	154
9.2	The Directory Path	155
9.3	The File	156
9.4	The SMB URL	157
9.5	Was That Trip Really Necessary?	158
Chapter 10	First Contact: Reaching the Server	159
10.1	Interpreting the Server Identifier	160
10.2	The Destination Port	162
10.3	Transport Discovery	163
10.3.1	<i>Run Naked</i>	163
10.3.2	<i>Using the NetBIOS Name</i>	164
10.3.3	<i>Reverse Mapping a NetBIOS Name</i>	166
10.4	Connecting to the Server	167
Chapter 11	SMB in Its Natural Habitat	177
11.1	Our Very First Live SMBs	179
11.2	SMB Message Structure	180
11.2.1	<i>SMB Message Header</i>	181
11.2.2	<i>SMB Message Parameters</i>	185
11.2.3	<i>SMB Message Data</i>	186
11.3	Case in Point: NEGOTIATE PROTOCOL	186
11.4	The AndX Mutation	188
11.5	The Flow of Conversation	192
11.6	A Little More Code	193
11.7	Take a Break	196
Chapter 12	The SMB Header in Detail	197
12.1	The SMB_HEADER.STATUS Field Exposed	198
12.2	The FLAGS and FLAGS2 Fields Tell All	202
12.3	EXTRA! EXTRA! Read All About It!	208

12.4	TID and UID: Separated at Birth?	209
12.5	PID and MID Revealed	211
12.5.1	EXTRA.PidHigh <i>Dark Secrets Uncovered</i>	214
12.6	SMB Header Final Report	215
Chapter 13	Protocol Negotiation	221
13.1	A Smattering of SMB Dialects	222
13.2	Greetings: The NEGOTIATE PROTOCOL REQUEST	224
13.3	Gesundheit: The NEGOTIATE PROTOCOL RESPONSE	227
13.3.1	<i>NegProt Response Parameters</i>	227
13.3.2	<i>NegProt Response Data</i>	235
13.4	Are We There Yet?	237
Chapter 14	Session Setup	239
14.1	SESSION SETUP ANDX REQUEST Parameters	239
14.1.1	<i>Virtual Circuits</i>	242
14.1.2	<i>Capabilities Bits</i>	245
14.2	SESSION SETUP ANDX REQUEST Data	251
14.3	The SESSION SETUP ANDX RESPONSE SMB	255
Chapter 15	Authentication	257
15.1	Anonymous and Guest Login	258
15.2	Plaintext Passwords	259
15.2.1	<i>User Level Security with Plaintext Passwords</i>	261
15.2.2	<i>Share Level Security with Plaintext Passwords</i>	264
15.3	LM Challenge/Response	265
15.3.1	<i>DES</i>	266
15.3.2	<i>Creating the Challenge</i>	267
15.3.3	<i>Creating the LM Hash</i>	268
15.3.4	<i>Creating the LM Response</i>	270
15.3.5	<i>LM Challenge/Response: Once More with Feeling</i>	272
15.4	NTLM Challenge/Response	275
15.5	NTLM Version 2	276
15.5.1	<i>The NTLMv2 Toolbox</i>	277

15.5.2	<i>The NTLMv2 Password Hash</i>	279
15.5.3	<i>The NTLMv2 Response</i>	281
15.5.4	<i>Creating The Blob</i>	282
15.5.5	<i>Improved Security Through Confusion</i>	284
15.5.6	<i>Insult to Injury: LMv2</i>	286
15.5.7	<i>Choosing NTLMv2</i>	287
15.6	Extended Security: That Light at the End of the Tunnel	289
15.6.1	<i>The Extended Security Authentication Toolkit</i>	291
15.7	Kerberos	294
15.8	Random Notes on W2K and NT Domain Authentication	295
15.8.1	<i>A Quick Look at W2K Domains</i>	296
15.8.2	<i>A Few Notes about NT Domains</i>	296
15.8.3	<i>It's Good to Have a Backup</i>	298
15.8.4	<i>Trust Me on This</i>	299
15.9	Random Notes on Message Authentication Codes	300
15.9.1	<i>Generating the Session Key</i>	302
15.9.2	<i>Sequence Numbers</i>	304
15.9.3	<i>Calculating the MAC</i>	304
15.9.4	<i>Enabling and Requiring MAC Signing</i>	306
15.10	Non Sequitur Time	307
15.11	Further Study	308
Chapter 16	Building Your SMB Vocabulary	309
16.1	That TREE CONNECT Thingy	310
16.2	SMB Echo	312
16.3	Readin', Writin', and 'Rithmetic	315
16.4	Transaction SMBs	318
16.4.1	<i>Mailslots and Named Pipes</i>	321
Chapter 17	The Remaining Oddities	323
17.1	Opportunistic Locks (OpLocks)	323
17.1.1	<i>OpLock Breaks</i>	325
17.2	Distributed File System (DFS)	326
17.3	DOS Attributes, Extended File Attributes, Long Filenames, and Suchlike	328

Chapter 18 That Just about Wraps Things Up for SMB 333**PART III The Browse Service 335****Chapter 19 A Beautiful Day in the Network Neighborhood 337**

19.1 History: From Frontier Town to Bustling Metropolis 338

19.2 Sociology 339

19.3 Politics 340

19.3.1 *When Is a Workgroup not a Workgroup?* 343

19.3.2 *Delegating Responsibility* 344

Chapter 20 Meet the Neighbors 347

20.1 Browse Service Clientele 348

20.1.1 *Providers* 348

20.1.2 *Consumers* 349

20.2 The Local Master Browser 351

20.3 Becoming a Backup Browser 354

20.4 Crossing the Street with the DMB 355

20.5 Elections 356

Chapter 21 Infrastructure: The Mailslot and Named Pipe Abstractions 359

21.1 Meet the Plumbing: Named Pipes 360

21.2 The Mailslot Metaphor 363

Chapter 22 The Talk on the Street 367

22.1 Making Sense of SMBtrans 368

22.2 Browse Service Mailslot Messages 377

22.2.1 *Announcement Request* 380

22.2.2 *Host Announcement* 381

22.2.3 *Election Request* 383

22.2.4 *Get Backup List Request* 384

22.2.5	<i>Get Backup List Response</i>	385
22.2.6	<i>Local Master Announcement</i>	387
22.2.7	<i>Master Announcement</i>	387
22.2.8	<i>Domain Announcement</i>	388
22.2.9	<i>Become Backup Request</i>	389
22.2.10	<i>The Undocumented Reset</i>	390
22.2.11	<i>It's All in the Delivery</i>	392
22.3	<i>RAPture</i>	393
22.3.1	<i>NetServerEnum2 Request</i>	395
22.3.2	<i>NetServerEnum2 Reply</i>	398
22.3.3	<i>On the Outskirts of Town</i>	406
22.3.4	<i>Transaction Fragmentation</i>	407
22.3.5	<i>RAP Annoyances</i>	408
Chapter 23	The Better Browser Bureau	411
23.1	Running an Election	411
23.1.1	<i>Voting</i>	412
23.1.2	<i>The Ballot</i>	413
23.2	Timing Is Everything	416
Chapter 24	Samba Browse Service Enhancements	419
24.1	Automatic LANMAN	419
24.2	UnBrowsable	420
24.3	NBNS Wildcard DMB Queries and Enhanced Browsing	420
24.4	Remote Announce	422
24.5	Remote Browse Sync	423
24.6	DMB != PDC	423
Chapter 25	It Can't Happen Here	425
25.1	Misconfigured Hosts	425
25.2	Misconfigured Networks	427
25.3	Implementation Bugs	428
25.4	Troublemakers	428
25.5	Design Flaws	429

Chapter 26 At Home in the Network Neighborhood	431
PART IV Appendices	433
Appendix A Making a Good Cup of Tea	435
A.1 Basics of Making Tea	435
A.2 About Tea	436
A.3 Nasty Habits	437
A.4 Decaffeinating Tea	438
Appendix B Known NetBIOS Suffix Values	439
B.1 NetBIOS Name Suffix Bytes	439
B.2 Special Handling of NetBIOS Names in WINS	447
Appendix C The SMB URL	451
C.1 The Origins of the SMB URL	451
C.2 Of Round Pegs, Square Holes, and Big Mallets	452
C.3 Form Versus Function	453
C.4 Additional Parts	456
C.5 A Simple SMB URL Parser	458
Appendix D SNIA CIFS Technical Reference	463
Glossary	613
References	623
Index	633