TCP/IP - The Ultimate Protocol Guide

TCP/IP - The Ultimate Protocol Guide

Volume 2 - Applications, Access and Data Security

Philip M. Miller

BrownWalker Press
Boca Raton

TCP/IP - The Ultimate Protocol Guide: Volume 2 - Applications, Access and Data Security

BrownWalker Press
Boca Raton, Florida
USA • 2009

ISBN-10: 1-59942-493-2 *(paper)*
ISBN-13: 978-1-59942-493-4 *(paper)*

ISBN-10: 1-59942-494-0 *(ebook)*
ISBN-13: 978-1-59942-494-1 *(ebook)*

www.brownwalker.com

Cover Design by Shereen Siddiqui

Library of Congress Cataloging-in-Publication Data

Miller, Philip, 1956-
TCP/IP : the ultimate protocol guide / Philip Miller.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-1-59942-491-0 (vol. 1 : alk. paper)
ISBN-10: 1-59942-491-6 (vol. 1 : alk. paper)
ISBN-13: 978-1-59942-493-4 (vol. 2 : alk. paper)
ISBN-10: 1-59942-493-2 (vol. 2 : alk. paper)
1. TCP/IP (Computer network protocol) I. Title.

TK5105.585.M5643 2009
004.6'2--dc22

2009004906

To my wife Karen and my children Stuart and Nicole.

No man can be complete without the love of his family.

In memory of Brian Hill (1950-2006).

More than a colleague – Brian was a friend and a mentor.
Without him, this book would never have been completed.

Table of Contents

Volume 1 – Data Delivery & Routing

Preface ..... **xxxi**

Section A – Introduction **1**

Chapter 1 - Introduction **3**
1.1 What is TCP/IP? 3
1.1.1 A Brief History of TCP/IP 4
1.1.2 The Internet Protocol Suite 4
1.2 The Internet 6
1.2.1 The Growth of the Internet 7
1.3 Summary 9

Chapter 2 - Standardization **11**
2.1 The Internet Architecture Board (IAB) 11
2.1.1 The Internet Engineering Task Force (IETF) 12
2.1.2 The Internet Research Task Force (IRTF) 12
2.1.3 Internet Corporation for Assigned Names and Numbers (ICANN) 13
2.2 Internet Protocol Standards 13
2.2.1 Protocol States 13
2.2.2 Protocol Status 15
2.2.3 The Request for Comments (RFC) 15
2.3 Internet Protocol Architecture 16
2.3.1 The Open Systems Interconnection (OSI) Reference Model 17
2.3.2 The OSI Model and IEEE LANs 19
2.3.3 The Physical and Data Link Layers 21
2.3.4 The Internet Protocol Suite Model 22
2.4 Summary 24

Chapter 3 - An Overview of Underlying Network Technologies **25**
3.1 Ethernet and IEEE 802.3 25
3.1.1 Ethernet/802.3 Standards 25
3.1.2 Ethernet/802.3 Frame Structures 29
3.1.3 Ethernet/802.3 Operation 32
3.2 Token Ring and IEEE 802.5 33
3.2.1 Token Ring/802.5 Specifications 33
3.2.2 Token Ring/802.5 Frame Structure 35
3.2.3 Token Ring/802.5 Basic Operation 36
3.2.4 Early Token Release 37
3.3 Wireless Local Area Networks (Wireless LANs) and IEEE 802.11 37
3.3.1 Wireless LAN/802.11 Standards 39
3.3.2 Wireless LAN/802.11 Operation 39
3.3.3 IEEE 802.11 Basic Frame Format 40
3.3.4 IEEE 802.11 Control Frame Formats 43
3.3.5 IEEE 802.11 Management Frame Formats 44
3.3.6 IEEE 802.11 Data Frame Formats 48
3.4 Relay Systems 48
3.4.1 Repeaters/Hubs 49
3.4.2 Bridges and Switches 50
3.4.3 Routers 54
3.5 WAN Links 54
3.6 Summary 55

Section B – The Internet Protocol 57

Chapter 4 - IP Addressing 59
4.1 The Need for an Addressing Scheme 59
4.2 The Internet Protocol Version 4 (IPv4) Addressing Scheme 59
4.2.1 Dotted Decimal Notation 61
4.2.2 Identifying IP Addresses and Rules 62
4.2.3 Choosing the Right Addressing Scheme 63
4.2.4 The Private Address Space 64
4.2.5 Automatic Private IP Addressing (APIPA) 65
4.3 Routing Fundamentals 65
4.3.1 Direct and Indirect Routing 66
4.4 The Resolution of MAC Addresses in IPv4 Environments 67
4.4.1 The Address Resolution Protocol (ARP) 67
4.4.2 The ARP Packet Format 68
4.4.3 Gratuitous ARP 71
4.4.4 Problems with Address Resolution 71
4.4.5 Address Resolution for Non-Broadcast Networks 71
4.5 The Reverse Address Resolution Protocol (RARP) 71
4.5.1 Dynamic RARP 73
4.6 Subnetting 75
4.6.1 Natural Subnet Masks 78
4.6.2 Subnet Mask Representation 79
4.6.3 Obtaining and Implementing Subnet Masks 79
4.6.4 More Complex Subnet Mask Examples 80
4.6.5 Further Guidelines in Implementing Subnet Masks 80
4.7 Classless Inter-Domain Routing (CIDR) and Supernetting 83
4.7.1 Address Aggregation 84
4.8 Multi-Homing and Assigning Multiple IP Addresses 84
4.8.1 Assigning Multiple IP Addresses to a Single Physical Connection 85
4.9 The Internet Protocol Version 6 (IPv6) Addressing Scheme 85
4.9.1 Representing IPv6 Addresses 86
4.9.2 IPv6 Address Type Representation 87
4.9.3 Unicast Addresses 88
4.9.4 IPv6 Addresses with Embedded IPv4 Addresses 90
4.9.5 Provider Based Global Unicast Addresses 91
4.9.6 Aggregatable Global Unicast Addresses 91
4.9.7 Local Use IPv6 Unicast Addresses 91
4.9.8 The Anycast Address 92
4.9.9 Multicast Addresses 93
4.9.10 Required Addresses for an IPv6 Node 94
4.9.11 Stateful and Stateless Auto-Address Configuration 95
4.10 The Future of Internet Addressing 95
4.11 Summary 96

Chapter 5 - The Internet Protocol Version 4 (IPv4) 97
5.1 The IPv4 Datagram 98
5.2 IPv4 Datagram Options 100
5.2.1 End of Option List 101
5.2.2 No Operation 101
5.2.3 Security 101
5.2.4 Loose and Strict Source Routing 102
5.2.5 Internet Timestamp 102
5.2.6 Record Route 103
5.2.7 Router Alert 104

5.2.8 Sender Directed Multi-Destination Delivery 104
5.3 Type-of-Service 104
5.3.1 Applying Monetary Cost 105
5.3.2 Implementing Other Service Types (Differentiated Services) 106
5.4 Datagram Fragmentation in IPv4 106
5.5 Summary 110

Chapter 6 - The Internet Protocol Version 6 (IPv6) 111
6.1 IPv6 Header Format 111
6.2 Extension Headers 112
6.2.1 Extension Header Options 114
6.2.2 The Hop-by-Hop Options Header 114
6.2.3 The Routing Header 116
6.2.4 The Fragment Header 118
6.2.5 The Destination Options Header 120
6.2.6 No Next Header 120
6.3 Packet Size Issues 120
6.3.1 Path MTU Discovery 120
6.4 Flow Labels 121
6.5 Traffic Classes 121
6.6 Using IPv6 with Upper Layer Protocols 123
6.6.1 Checksum Considerations 123
6.6.2 Maximum Packet Lifetime 124
6.6.3 Maximum Upper Layer Payload Size 124
6.6.4 Packets Carrying Routing Headers 124
6.7 Summary 124

Chapter 7 - The Internet Control Message for IPv4 (ICMPv4) 125
7.1 ICMPv4 Message Types 126
7.1.1 Destination Unreachable 126
7.1.2 Time Exceeded 128
7.1.3 Parameter Problem 129
7.1.4 Source Quench 129
7.1.5 Redirect 130
7.1.6 Echo Request/Reply 131
7.1.7 Timestamp Request/Reply 133
7.1.8 Information Request/Reply 133
7.1.9 Address Mask Request/Reply 134
7.1.10 Router Discovery Advertisement and Solicitation 134
7.2 Summary 136

Chapter 8 - The Internet Control Message for IPv6 (ICMPv6) 137
8.1 ICMPv6 Message Header General Format 137
8.2 ICMPv6 Message Types 139
8.2.1 Destination Unreachable 139
8.2.2 Packet Too Big 140
8.2.3 Time Exceeded 140
8.2.4 Parameter Problem 141
8.2.5 Echo Request/Reply 141
8.2.6 Group Membership Messages 142
8.3 The Neighbor Discovery Protocol 142
8.3.1 Router Solicitation Message 143
8.3.2 Router Advertisement Message 144
8.3.3 Neighbor Solicitation Message 145
8.3.4 Neighbor Advertisement Message 146

8.3.5 Redirect Message 146
8.4 Neighbor Discovery Option Formats 147
8.4.1 Source and Target Link-Layer Address Options 148
8.4.2 Prefix Information Option 148
8.4.3 Redirected Header Option 149
8.4.4 Maximum Transmission Unit (MTU) Option 149
8.5 Summary 150

Chapter 9 - Network Address Translation (NAT) 151
9.1 An Introduction to Traditional NAT 151
9.2 Basic Network Address Translation (NAT) 151
9.3 Network Address Port Translation (NAPT) 152
9.3.1 ICMP Queries in a NAPT Environment 154
9.4 Header Manipulation 154
9.4.1 Basic NAT 154
9.4.2 NAPT 154
9.4.3 IP Option Handling 154
9.4.4 Fragmented Packets 154
9.5 ICMP Error Packet Manipulation 155
9.6 Network Address Translation and Security 155
9.7 Summary 155

Chapter 10 - Transitioning from IPv4 to IPv6 157
10.1 Dual IP Layer Operation 158
10.2 IPv4/v6 Addresses 159
10.2.1 IPv4 Compatible Address Configuration 159
10.3 Tunneling Mechanisms 160
10.4 Automatic Tunnels 163
10.5 Configured Tunnels 163
10.5.1 The 'Default' Configured Tunnel 163
10.6 Issues Surrounding Tunneling 163
10.6.1 MTU and Fragmentation 164
10.6.2 ICMP Issues 164
10.6.3 Hop Limits 165
10.6.4 Neighbor Discovery over Tunnels 165
10.7 Summary 165

Section C – Reliable and Unreliable Data Delivery 167

Chapter 11 - The Transmission Control Protocol (TCP) 169
11.1 TCP Operation 169
11.1.1 Basic Data Transfer 169
11.1.2 Reliability 170
11.1.3 Flow Control 172
11.1.4 Multiplexing 173
11.1.5 Connections 174
11.2 The TCP Segment Header 174
11.2.1 Explicit Congestion Notification (ECN) in IP 178
11.3 TCP Options 178
11.4 TCP Connection Management 179
11.4.1 Connection Establishment 179
11.4.2 Connection Maintenance 183
11.4.3 Connection Termination 183
11.4.4 The TCP Finite State Machine 186
11.5 Summary 188

Chapter 12 - The User Datagram Protocol (UDP) 189
12.1 UDP Multiplexing 189
12.2 The UDP Datagram Header 190
12.2.1 UDP and ICMP 194
12.3 Summary 194

Section D – Quality of Service 195

Chapter 13 - Quality of Service (QoS), Differentiated and Integrated Services (DiffServ & IntServ) ... 197
13.1 Differentiated Services (DiffServ) 197
13.1.1 The Differentiated Services (DS) Field 197
13.1.2 Class Selector Codepoints 199
13.1.3 Explicit Congestion Notification (ECN) in IP 199
13.2 Implementing Differentiated Services (DiffServ) 200
13.2.1 DiffServ and Other/Traditional Flow Handling 200
13.2.2 The DiffServ Model 201
13.3 Traffic Classification and Conditioning 202
13.4 Per-Hop Behaviors (PHBs) 203
13.5 Bandwidth Reservation and Integrated Services (IntServ) 204
13.5.1 Implementing IntServ 206
13.5.2 Traffic Control 207
13.5.3 IntServ versus DiffServ 208
13.6 Summary 208

Chapter 14 - The Resource Reservation Protocol (RSVP) 211
14.1 RSVP Reservation Styles 212
14.2 RSVP Protocol Overview 214
14.2.1 Host Operation 215
14.2.2 Merging Flowspecs 215
14.2.3 RSVP Reservation State 215
14.2.4 State Teardown 216
14.2.5 Errors and Error Handling 216
14.2.6 Confirmation 216
14.2.7 Policy and Security Control 216
14.2.8 Linking RSVP Domains Through non-RSVP Clouds 217
14.3 RSVP Message Formats 217
14.3.1 RSVP Object Formats 218
14.3.2 RSVP Object Classes 219
14.3.3 Path Messages 227
14.3.4 Resv Messages 227
14.3.5 PathTear Messages 227
14.3.6 ResvTear Messages 228
14.3.7 PathErr Messages 228
14.3.8 ResvErr Messages 228
14.3.9 ResvConf Messages 229
14.4 Summary 229

Section E – Routing 231

Chapter 15 - IPv4 Routing Principles 233
15.1 Direct and Indirect Routing 233
15.1.1 Routing Protocols 236
15.1.2 Static and Default Routes 236
15.2 Routing in the Presence of Subnets 236
15.2.1 Variable Length Subnet Masks 237

15.3 ARP and Subnetted Environments....239
15.3.1 Proxy ARP....240
15.4 Policy Based Routing....241
15.5 Summary....242

Chapter 16 - The Routing Information Protocol (RIP)....243
16.1 Gauging Route Quality....243
16.2 Protocol Operation....245
16.2.1 Handling Topology Changes....247
16.2.2 Split Horizon....249
16.2.3 Poison Reverse....249
16.2.4 Triggered Updates....250
16.2.5 Route States and Timers....251
16.3 RIP Version 1 Protocol Format and Operation....251
16.3.1 RIP Response Datagram Processing....253
16.3.2 RIPv1 Router Operation at Start-up....257
16.4 The Pros and Cons of RIP Version 1....257
16.4.1 RIPv1 Limitations....257
16.4.2 RIPv1 Strengths....258
16.5 RIP Version 2....259
16.5.1 RIPv2 Protocol Format....259
16.6 Authentication with RIPv2....261
16.6.1 Simple Password Authentication....261
16.6.2 Keyed MD5 Authentication....262
16.7 Using Multicast Datagrams with RIP....262
16.8 RIPv1/v2 Compatibility in an IPv4 Environment....263
16.9 Using RIP with Demand Circuits - (Low Demand RIP)....263
16.9.1 Reducing Routing Updates....264
16.9.2 Reliable Delivery of Triggered Routing Updates....265
16.10 Triggered RIP....266
16.10.1 Triggered RIP Packet Types....267
16.10.2 Triggered RIP Packet Formats....267
16.11 RIP for IPv6 (RIPng)....268
16.11.1 RIPng Message Format....269
16.11.2 RIPng Next Hop Information....270
16.11.3 RIPng MTU Considerations....271
16.12 Summary....271

Chapter 17 - IGRP and EIGRP....273
17.1 The Interior Gateway Routing Protocol (IGRP)....273
17.1.1 IGRP Metrics....273
17.1.2 IGRP Holddown and Other Timers....274
17.1.3 IGRP Message Formats....275
17.1.4 IGRP Protocol Operation....275
17.2 The Enhanced Interior Gateway Routing Protocol (EIGRP)....276
17.2.1 EIGRP Metrics....276
17.2.2 EIGRP Message Formats....276
17.2.3 EIGRP Operation....279
17.3 Summary....280

Chapter 18 - The Open Shortest Path Protocol (OSPF) for IPv4....281
18.1 Enhancements over Other IGPs....282
18.2 Metrics 283
18.2.1 Type-of-Service Routing....284
18.2.2 Equal Cost Paths....285

18.3 An Overview of OSPF for IPv4 285
18.3.1 OSPF Terminology 286
18.3.2 OSPF Areas, Area Types, and Network Types 287
18.3.3 Designated and Backup Designated Routers 288
18.3.4 Router Adjacency and Network Types 289
18.4 OSPF Protocol Operation for IPv4 290
18.4.1 A Simplified View of OSPF Database Synchronization 290
18.4.2 Carrying OSPF Packets 290
18.4.3 A Simple OSPF internet 293
18.4.4 The Hello Protocol 294
18.4.5 Exchanging Database Information and Creating Adjacencies 298
18.4.6 Exchanging Database Description Packets 299
18.4.7 Requesting Additional Information through Link State Requests (LSRs) 302
18.4.8 Link State Updates 304
18.5 Link State Advertisements for IPv4 305
18.5.1 Router Links (Type 1) LSAs 305
18.5.2 Network Links (Type 2) LSAs 306
18.5.3 Summary Links (Type 3 and Type 4) LSAs 307
18.5.4 Autonomous System (AS) External Links (Type 5) LSAs 308
18.5.5 Not-So-Stubby-Stub-Area (NSSA) Links (Type 7) LSAs 308
18.5.6 Opaque Links (Types 9, 10, and 11) LSAs 309
18.5.7 Sample Trace Demonstrating Router Adjacency 310
18.6 Creating the Shortest Path Tree 313
18.6.1 The Routing Table 314
18.7 OSPF for IPv4 and Demand Circuits - (Low Demand OSPF) 315
18.7.1 Do-Not-Age Link State Advertisements 315
18.7.2 Suppressing OSPF Hellos 315
18.7.3 Demand Circuit Example 316
18.8 Using Areas 317
18.8.1 The Backbone Area 318
18.8.2 Virtual Links 318
18.8.3 Intra-Area and Inter-Area Routing 320
18.9 Joining Autonomous Systems Together 324
18.10 Summary 325

Chapter 19 - The Open Shortest Path Protocol (OSPF) for IPv6 327
19.1 Detailed Differences between OSPF for IPv4 and IPv6 327
19.2 Carrying OSPF Information for IPv6 330
19.2.1 The OSPF Packet Header for IPv6 330
19.2.2 The Hello Packet 331
19.2.3 Database Description Packets 332
19.2.4 Link State Requests 333
19.2.5 Link State Updates 334
19.2.6 Link State Acknowledgements 335
19.3 OSPF Link State Advertisements for IPv6 335
19.3.1 The IPv6 LSA Header 335
19.3.2 Router (Type 1) LSAs 337
19.3.3 Network (Type 2) LSAs 338
19.3.4 Inter-Area-Prefix (Type 3) LSAs 338
19.3.5 Inter-Area-Router (Type 4) LSAs 339
19.3.6 AS-External (Type 5) LSAs 339
19.3.7 Group Membership (Type 6) LSAs 340
19.3.8 Not-So-Stubby-Area (Type 7) LSAs 340
19.3.9 Link (Type 8) LSAs 341
19.3.10 Intra-Area-Prefix (Type 9) LSAs 341

19.4 Summary 342

Chapter 20 - The Border Gateway Protocol (BGP) 343
20.1 BGP Operation 344
20.2 BGP Message Formats 345
20.2.1 The BGP Message Header 345
20.2.2 Open Messages 346
20.2.3 Update Messages 349
20.2.4 Notification Messages 353
20.2.5 KeepAlive Messages 356
20.2.6 Route-Refresh Messages 356
20.3 Multi-Protocol Extensions to BGPv4 357
20.3.1 Multi-Protocol Reachable NLRI (MP_REACH_NLRI) Attribute 357
20.3.2 Multi-Protocol Unreachable NLRI (MP_UNREACH_NLRI) Attribute 358
20.3.3 Handling Errors with Multi-Protocol Extensions 359
20.4 Using BGP with IP version 6 (IPv6) 359
20.5 A Simple BGPv4 Example 360
20.6 Summary 364

Chapter 21 - High Availability Routing 365
21.1 Virtual Router Redundancy Protocol (VRRP) Overview 365
21.2 VRRP Configurations 366
21.2.1 Single Virtual Router 366
21.2.2 Multiple Virtual Routers and Load Balancing 366
21.3 VRRP Protocol 367
21.4 VRRP Protocol Operation 369
21.4.1 VRRP Router Start-up 369
21.4.2 VRRP Router Operation in the Backup State 370
21.4.3 VRRP Router Operation in the Master State 371
21.5 VRRP Operational Issues 371
21.5.1 Virtual Router Interface Failure 371
21.5.2 Virtual Router MAC Addresses and ARP 372
21.5.3 VRRP Operation over Token Ring 372
21.5.4 ICMP Redirection 373
21.5.5 Proxy ARP 374
21.6 VRRP Security Considerations 374
21.7 VRRP Operation with Firewalls 374
21.8 The Cisco Hot Standby Router Protocol (HSRP) 376
21.8.1 Similarities to VRRP 376
21.8.2 Differences to VRRP 376
21.9 HSRP Protocol Format and Operation 376
21.9.1 HSRP Operational Parameters 378
21.9.2 HSRP Timers 378
21.10 HSRP Operational Issues 378
21.10.1 HSRP MAC Addresses and ARP 378
21.10.2 HSRP over Token Ring 378
21.10.3 ICMP Re-Directs 379
21.10.4 Proxy ARP 379
21.11 HSRP Security Considerations 379
21.12 Summary 379

Section F – Mulicasting in IP Environments 381

Chapter 22 - Broadcasting, Multicasting, IGMP and Multicast Listener Discovery (MLD) 383
22.1 Broadcasting in IPv4 Environments 383

22.1.1 Using Broadcasts in the Presence of Subnets 385
22.2 Multicasting in IP Environments 386
22.2.1 Host Group Addresses 387
22.2.2 Mapping IPv4 Multicasts to Local Network Multicasts 388
22.2.3 Multicasts and IPv6 389
22.3 The Internet Group Management Protocol (IGMP) for IPv4 389
22.3.1 IGMP Message Types 389
22.4 IGMP Version 3 (IGMPv3) for IPv4 389
22.4.1 IGMPv3 Membership Query Messages 390
22.4.2 IGMPv3 Membership Report Messages 391
22.5 IGMP Versions 1 and 2 (IGMPv1 and IGMPv2) for IPv4 393
22.5.1 IGMPv2 Message Formats 393
22.5.2 IGMPv1 Message Formats 394
22.5.3 Differentiating Queries Between IGMP Versions 394
22.6 IGMP Operation for IPv4 394
22.6.1 IGMP Host States 395
22.7 Allocating Transient Host Group Addresses 396
22.8 The Multicast Listener Discovery (MLD) Protocol for IPv6 396
22.9 MLDv2 Message Formats 397
22.9.1 MLDv2 Multicast Listener Query Messages 397
22.9.2 MLDv2 Multicast Listener Report Messages 399
22.10 MLDv1 Message Formats 401
22.11 Propagating Multicast Routing Information 402
22.12 Summary 403

Chapter 23 - The Distance VectorMulticast Routing Protocol (DVMRP) 405
23.1 An Introduction DVMRP 405
23.2 DVMRP Message Types and Formats 406
23.2.1 DVMRP Commands 407
23.3 Sending and Receiving DVMRP Messages 410
23.3.1 Sending DVMRP Messages 410
23.3.2 Receiving DVMRP Messages 411
23.4 DVMRP Tunnels 411
23.5 DVMRP Examples 412
23.6 Summary 412

Chapter 24 - Multicast OSPF (MOSPF) 413
24.1 Propagating Routing Information 413
24.2 MOSPF Operation 414
24.2.1 MOSPF Link State Advertisements (LSAs) 416
24.3 Pruned Shortest Path Trees 417
24.4 Summary 418

Chapter 25 - Protocol Independent Multicast (PIM) 419
25.1 Common PIM Definitions 419
25.1.1 A Brief Overview of PIM Message Types 421
25.2 An Overview of PIM 421
25.3 PIM-SM Operation 422
25.3.1 The RP Tree 422
25.3.2 Register Stop 423
25.3.3 The Shortest Path Tree (SPT) 423
25.3.4 Source-Specific Joins and Prunes 423
25.3.5 Obtaining Rendezvous Point (RP) Information 424
25.3.6 Multicast Data Packet Processing 424
25.4 PIM Protocol Format 425

25.4.1 PIM Header Format 425
25.4.2 Encoding Source and Group Addresses 426
25.4.3 Hello Message 427
25.4.4 Register Message 429
25.4.5 Register-Stop Message 430
25.4.6 Join/Prune Message 430
25.4.7 Bootstrap Message 432
25.4.8 Assert Message 433
25.4.9 Candidate RP Advertisement Message 434
25.4.10 State Refresh Message 434
25.4.11 Graft Message 435
25.4.12 Graft-Ack Message 435
25.5 Inter-operation of PIM-SM with Dense Mode Protocols (DVMRP) 435
25.6 Operation over Multi-Access Networks 436
25.6.1 Electing the Designated Router 436
25.6.2 Avoiding Parallel Paths to a Source 436
25.7 Dense Mode PIM (PIM-DM) 437
25.8 Bi-Directional PIM (BiDir) 437
25.8.1 BiDir PIM Neighbor Discovery 438
25.8.2 BiDir PIM Data Packet Forwarding 438
25.8.3 Designated Forwarder (DF) Election Process 438
25.8.4 Message Formats for BiDir PIM 440
25.9 Summary 441

Section G – Appendices 443

Appendix A - A Glossary of Networking Terms 445
A.1 Networking Terms 445

Appendix B - Official Internet Protocol Standards 463
B.1 Standard Protocols Ordered By Standard (STD) Number 463
B.2 Best Current Practices (BCP) Documents 464
B.3 For Your Information (FYI) Documents 467

Appendix C - Official IP Protocol Identifiers 469
C.1 Protocol Numbers 469

Appendix D - Address Family Identifiers 473
D.1 Address Family Numbers 473
D.2 Ethernet Type Codes 473

Appendix E - Official TCP/UDP Port Numbers 477
E.1 Well Known Port Numbers 477

Appendix F - Multicast and Anycast Address Allocation 489
F.1 IPv4 Multicast Address Allocation 489
F.1.1 IPv4 Multicast Address Allocation - 224.0.0.0 - 224.0.0.255 489
F.1.2 IPv4 Multicast Address Allocation - 224.0.1.0 - 224.0.1.255 490
F.1.3 IPv4 Multicast Address Allocation - 224.0.2.0 - 224.0.255.255 493
F.1.4 IPv4 Multicast Address Allocation - 224.1.0.0 - 224.1.255.255 494
F.1.5 IPv4 Multicast Address Allocation - 224.2.0.0 - 224.2.255.255 494
F.1.6 IPv4 Multicast Address Allocation - 224.3.0.0 - 239.255.255.255 495
F.2 IPv6 Multicast Address Allocation 495
F.2.1 IPv6 Fixed Scope Multicast Addresses 495
F.2.2 IPv6 Variable Scope Multicast Addresses 496

F.3 IPv6 Anycast Address Allocation 497
F.3.1 IPv6 Subnet-Router Anycast Address 497

Appendix G - Bibliography 499
G.1 Request For Comments (RFCs) 499

Index 513

Volume 2 – Applications, Access & Data Security

Preface ..... **xxxi**

Section H - An Introduction to Applications & Security in the TCP/IP Suite **531**

Chapter 26 - Introduction **533**
26.1 Application Support in the IP Suite 533
26.1.1 End User Application Protocols 533
26.1.2 End User Services 534
26.2 Network Management, Diagnostic Protocols and Services 534
26.3 Authentication and Security 535
26.4 Wide Area Connectivity 535
26.5 Summary 536

Section I - IP Application Services **537**

Chapter 27 - The Domain Name System (DNS) **539**
27.1 The Domain Name Space 540
27.1.1 Aliases 541
27.1.2 The Internet Mail System and DNS 541
27.2 Domain Name System Standardization 541
27.3 Resource Records 542
27.3.1 A (*Address*) Type Resource Record 544
27.3.2 CName (*Canonical Name*) Type Resource Record 544
27.3.3 HInfo (*Host Information*) Type Resource Record 544
27.3.4 MB/MD/MF/MG/MInfo/MR and MX (*Mail)* Type Resource Records 544
27.3.5 NS (*Name Server*) Type Resource Records 545
27.3.6 SOA (*Start of Authority*) Type Resource Records 545
27.3.7 PTR (*Pointer*) Type Resource Records 546
27.3.8 TXT (*Text*) Type Resource Records 546
27.3.9 WKS (*Well Known Service*) Type Resource Records 546
27.3.10 NULL (*Null*) Type Resource Records 546
27.4 Domain Name System Operation 547
27.4.1 Name Server Operation 548
27.5 The Domain Name System Protocol Format 549
27.5.1 The DNS Header Section 550
27.5.2 The Question Section 551
27.5.3 The Answer, Authority, and Additional Information Sections 552
27.5.4 Message Compression 552
27.6 Inverse Queries 552
27.7 The Notify Mechanism 553
27.7.1 Notify Operation 554
27.8 Zone Transfers 555
27.8.1 IXFR Operation 555
27.9 Dynamic DNS Updates 556
27.10 Security Extensions for DNS 557
27.10.1 Key Distribution 557
27.10.2 The Signature (SIG) Resource Record 559
27.10.3 Non-Existent Names and Types 560
27.11 Representing IPv6 Addresses in DNS 561
27.11.1 AAAA Resource Records 561
27.11.2 The IP6.ARPA Domain 561
27.12 Looking up DNS Information 561
27.13 Summary 562

Chapter 28 - Host Configuration 563
28.1 BootP/DHCP Operation Compared to RARP/ICMP 564
28.2 BootP Basic Operation 564
28.3 DHCP Basic Operation 565
28.3.1 An Overview of DHCP Address Allocation 565
28.4 BootP/DHCP Protocol Format 566
28.5 DHCP Client/Server Transactions 574
28.5.1 DHCP Address Allocation Process 575
28.5.2 Reusing a Previously Allocated Address 576
28.5.3 Obtaining Parameters with a Configured Address 577
28.5.4 DHCP Lease Times 578
28.6 BootP/DHCP Protocol Anomalies 578
28.6.1 Interaction between the Client & the Your IP Address Fields 578
28.6.2 Bit Ordering of the Client Hardware Address Field 578
28.6.3 Using BootP/DHCP in Token Ring Environments 579
28.6.4 The Broadcast Flag 579
28.7 Constructing the BootP/DHCP Request 579
28.7.1 Re-Transmitting BootP/DHCP Requests 579
28.8 Using BootP/DHCP with Relay Agents 580
28.8.1 BootP/DHCP Boot Request Message Handling 580
28.8.2 BootP/DHCP Boot Reply Message Handling 581
28.9 BootP/DHCP Configuration 581
28.9.1 BootP Configuration Files 581
28.9.2 DHCP Configuration Files 582
28.10 Summary 583

Chapter 29 - Telnet and Rlogin 585
29.1 The Telnet Protocol - An Introduction 585
29.2 Telnet Option Negotiation 586
29.2.1 Telnet Commands and Responses 586
29.2.2 Telnet Control Functions 587
29.3 Standard NVT Characters 588
29.4 Telnet Commands and Options 588
29.4.1 RFCs Related to Telnet Options 589
29.4.2 A Sample Telnet Session 592
29.5 Other Telnet Options 594
29.5.1 Telnet Environment Option 594
29.5.2 Telnet 3270 Commands 596
29.5.3 Telnet Window Size Option 597
29.5.4 Telnet Terminal Speed Option 598
29.5.5 Telnet Flow Control Options 598
29.6 Rlogin 599
29.6.1 Rlogin Commands 600
29.7 Telnet and Rlogin Security Considerations 600
29.7.1 Telnet Authentication Option 600
29.7.2 Telnet Data Encryption 603
29.8 Summary 605

Chapter 30 - File Transfer Protocols 607
30.1 The Trivial File Transfer Protocol (TFTP) 607
30.2 TFTP Operation 607
30.3 TFTP Protocol Format 608
30.3.1 The Determination of UDP Port Numbers 610
30.4 TFTP Security 610
30.5 Directed TFTP 611

30.6 TFTP Extensions 611
30.6.1 TFTP Option Extension 611
30.6.2 TFTP Block Size Option 613
30.6.3 TFTP Time-out Interval Option 613
30.6.4 TFTP Transfer Size Option 613
30.6.5 TFTP Multicast Option 614
30.7 The File Transfer Protocol (FTP) 614
30.8 FTP Basic Operation 615
30.9 FTP Data Transfer Functions 616
30.9.1 FTP Data Types 616
30.9.2 FTP Data Structures 617
30.10 FTP Transmission Modes 618
30.10.1 Stream Mode 618
30.10.2 Block Mode 618
30.10.3 Compressed Mode 619
30.11 FTP File Transfer Functions 619
30.11.1 Access Control Commands 619
30.11.2 Transfer Parameters 620
30.11.3 FTP Service Commands 620
30.11.4 FTP Responses 621
30.12 FTP Security Considerations 623
30.12.1 Proxy FTP 623
30.12.2 Restricting Access 624
30.12.3 Protecting Usernames 624
30.12.4 Protecting Passwords 624
30.12.5 Port Stealing 624
30.12.6 Software Based Security Issues 625
30.13 FTP Security Extensions 625
30.13.1 Authentication 626
30.13.2 Protecting the Command and Data Channels 627
30.14 FTP Extensions for IPv6 and Network Address Translation 628
30.14.1 EPRT Command 628
30.14.2 EPSV Command 629
30.14.3 FTP and Network Address Translation 630
30.15 A Complete FTP Example 630
30.16 Summary 638

Chapter 31 - Web Operations 641
31.1 URIs, URLs and URNs 641
31.1.1 Universal Resource Identifiers (URIs) 641
31.1.2 Uniform Resource Locators (URLs) 643
31.1.3 Uniform Resource Names (URNs) 644
31.2 An Introduction to the Hypertext Transfer Protocol (HTTP) 645
31.2.1 Basic Operation 645
31.3 Protocol Basics 646
31.3.1 An Overview of HTTP Messages 646
31.4 HTTP Messages and Message Headers 647
31.4.1 General Headers 647
31.4.2 Requests and Request Headers 648
31.4.3 Responses and Response Headers 649
31.4.4 Entities and Entity Headers 650
31.4.5 HTTP Message Body 651
31.5 HTTP Connection Persistence 651
31.6 Using Transport Layer Security (TLS) with HTTP Connections 652
31.6.1 Upgrading to TLS within HTTP/1.1 652

31.6.2 Client Requested Upgrades to TLS 652
31.6.3 Server Requested Upgrades to TLS 653
31.6.4 Upgrading across Proxies 653
31.7 Summary 653

Chapter 32 - The Simple Mail Transfer Protocol (SMTP) 655
32.1 An Introduction to the Simple Mail Transfer Protocol 655
32.2 Defining Senders and Recipients 656
32.3 Sending Mail Messages 656
32.4 Standard SMTP Commands and Responses 657
32.4.1 SMTP Commands 657
32.4.2 SMTP Replies 658
32.4.3 Verifying and Expanding 659
32.4.4 Message Header Format 659
32.5 Returning Mail to the Sender 660
32.6 SMTP Service Extensions 660
32.6.1 SMTP Message Size Declaration 661
32.6.2 SMTP Delivery Status Notifications 662
32.6.3 Returning Enhanced SMTP Error Codes 663
32.6.4 SMTP Remote Message Queue Starting 665
32.6.5 On Demand Mail Relay through Dynamic IP Addresses 666
32.6.6 Delivery by SMTP Service Extensions 668
32.6.7 SMTP Command Pipelining 669
32.6.8 Extensions for Transmitting Large & Binary MIME Messages 670
32.7 SMTP Security Considerations 671
32.7.1 Extensions to SMTP for Authentication 671
32.7.2 SMTP extensions for Transport Layer Security (TLS) 672
32.7.3 Anti-Spam Recommendations for SMTP 672
32.8 Mail Encoding 673
32.8.1 Multi-Purpose Internet Mail Extensions (MIME) 674
32.8.2 UUencode 675
32.8.3 BinHex 675
32.9 Summary 676

Chapter 33 - Email Delivery POP3 and IMAP4 677
33.1 An Introduction to the Post Office Protocol Version 3 (POP3) 677
33.1.1 POP3 Basic Operation 677
33.2 POP3 Commands and Responses 677
33.2.1 Authorization using the USER and PASS Commands 678
33.2.2 Authorization using the APOP Command 679
33.2.3 Transaction Commands 679
33.2.4 Update Commands 683
33.3 A complete POP3 Example 683
33.4 POP3 Extensions 684
33.4.1 The CAPA Command 684
33.4.2 The TOP Capability 685
33.4.3 The USER Capability 685
33.4.4 The SASL Capability 685
33.4.5 The RESP-CODES Capability 685
33.4.6 The LOGIN-DELAY Capability 686
33.4.7 The PIPELINING Capability 686
33.4.8 The EXPIRE Capability 686
33.4.9 The UIDL Capability 686
33.4.10 The IMPLEMENTATION Capability 686
33.5 The Internet Message Access Protocol (IMAP) version 4 686

33.5.1 IMAPv4 Basic Overview 687
33.6 IMAPv4 Message Attributes 687
33.6.1 IMAPv4 Message Texts 688
33.7 IMAPv4 Server and Client States 688
33.7.1 Non-Authenticated State 688
33.7.2 Authenticated State 689
33.7.3 Selected State 689
33.7.4 Logout State 689
33.8 IMAPv4 Data Formats 689
33.9 Operational Considerations 690
33.9.1 Mailbox Naming 690
33.9.2 Mailbox Size and Message Status Updates 690
33.9.3 Responses when no Command is in Progress 690
33.9.4 Inactivity Timers 691
33.9.5 Multiple Commands in Progress 691
33.10 IMAPv4 Client Commands 691
33.10.1 Client Commands - Any State 692
33.10.2 Client Commands - Non-Authenticated State 692
33.10.3 Client Commands - Authenticated State 693
33.10.4 Client Commands - Selected State 697
33.10.5 Client Commands - Experimental/Expansion 702
33.11 IMAPv4 Server Responses 702
33.11.1 Server Status Responses 702
33.11.2 Server and Mailbox Status Responses 704
33.11.3Server Mailbox Size Responses 705
33.11.4 Server Message Status Responses 705
33.11.5 Command Continuation Request 707
33.12 Push Email - IMAPv4 Idle 707
33.13 POP3/IMAP Security Considerations 708
33.13.1 POP3 AUTH Command 708
33.13.2 AUTHorize Extension for IMAP and POP 709
33.13.3 Transport Layer Security (TLS/SSL) in POP3 & IMAP 709
33.14 Summary 710

Chpater 34 - The Simple Network Management Protocol (SNMP) 711
34.1 An Overview of Management Tasks 712
34.2 An Overview of SNMP 713
34.3 SNMP Architecture 714
34.4 The Structure of Management Information (SMI) 714
34.5 The Management Information Base (MIB) 715
34.5.1 RFCs Relating to Other MIBs 717
34.6 The Simple Network Management Protocol version 1 (SNMPv1) 718
34.6.1 Authentication 719
34.6.2 An Introduction to the SNMPv1 Protocol Format 720
34.6.3 The GetRequest PDU 722
34.6.4 The GetNextRequest PDU 722
34.6.5 The GetResponse PDU 723
34.6.6 The SetRequest PDU 723
34.6.7 The TRAP PDU 723
34.6.8 SNMPv1 PDU Format 724
34.7 SNMP Version 2 (SNMPv2) 725
34.7.1 SNMPv2 PDU Construct 725
34.7.2 The GetBulkRequest PDU 727
34.7.3 The InformRequest PDU 727
34.7.4 The Report PDU 728

34.7.5 SNMPv1 and SNMPv2 Co-existence 728
34.8 SNMP Version 3 (SNMPv3) 728
34.8.1 The SNMPv3 Message Format 729
34.8.2 User Based Security Model (USM) For SNMPv3 731
34.8.3 View Based Access Control Model (VACM) For SNMPv3 731
34.8.4 SNMPv1, SNMPv2 and SNMPv3 Co-existence 732
34.9 The Remote Monitoring MIB (RMON) 732
34.10 The Future of SNMP and Network Monitoring 733
34.11 Summary 734

Chapter 35 - Miscellaneous Protocols and Services 735
35.1 The Echo Protocol 735
35.2 The Discard Protocol 735
35.3 The Character Generator Protocol (CHARGEN) 736
35.4 Quote of the Day (Quote) 737
35.5 Users 737
35.6 Finger 737
35.7 The Daytime Protocol 739
35.8 The Time Server Protocol 739
35.9 The Network Time Protocol (NTP) 740
35.10 The Line Printer Daemon Protocol (LPD) 740
35.11 SYSLOG 742
35.12 WHOIS/nickname 743
35.13 Summary 743

Section J - Securing the Communications Channel 745

Chapter 36 - Authentication, Authorization and Accounting 747
36.1 Kerberos 747
36.1.1 Kerberos Realms 748
36.2 Kerberos Tickets 748
36.2.1 Initial and Pre-Authenticated Tickets 748
36.2.2 Invalid Tickets 749
36.2.3 Renewable Tickets 749
36.2.4 Post-dated Tickets 749
36.2.5 Proxiable and Proxy Tickets 749
36.2.6 Forwardable and Forwarded Tickets 749
36.3 Kerberos Protocol Exchanges 749
36.3.1 The Authentication Service Exchange 750
36.3.2 The Client/Server Authentication Exchange 750
36.3.3 The Ticket Granting Service (TGS) Exchange 750
36.4 RADIUS 750
36.4.1 Basic Radius Operation 751
36.4.2 RADIUS Challenges and Responses 753
36.4.3 Interoperability with the Point-to-Point Protocol's PAP and CHAP 753
36.4.4 Using RADIUS with Proxies 753
36.5 RADIUS Protocol 754
36.5.1 RADIUS Packet Format 755
36.5.2 RADIUS Authentication Packet Types 756
36.6 RADIUS Protocol Attributes 757
36.6.1 RADIUS Attribute Details 758
36.7 RADIUS Accounting 765
36.7.1 RADIUS Accounting Packet Types 766
36.7.2 RADIUS Accounting Attributes Details 766
36.8 RADIUS Extensions for Tunneling with IPv4 769

36.8.1 Using RADIUS with Tunneling Protocols 769
36.8.2 RADIUS Attributes for Tunnel Protocol Support 769
36.8.3 Other Attribute Changes Allowing RADIUS Accounting in Tunnels 773
36.9 RADIUS Extensions 773
36.9.1 General RADIUS Extensions 773
36.9.2 Dynamic Authorization Extensions 775
36.10 RADIUS Attribute Inter-Operation 776
36.11 RADIUS and IP Version 6 (IPv6) 778
36.11.1 RADIUS Attributes for IPv6 Operation 778
36.11.2 IPv6 Attribute Inter-Operation and Usage 779
36.12 Summary 779

Chapter 37 - Digital Signatures, Certificates and the Pblic Key Infrastructure (PKI) 781
37.1 An Introduction to Digital Signatures and Certificates 781
37.2 The MD5 Message Digest Algorithm 783
37.2.1 MD5 Operation 783
37.2.2 The Differences between MD5 and Previous Versions 786
37.3 Digital Signatures 786
37.4 Certificates 787
37.5 The X.509 Certificate Standard 787
37.5.1 tbsCertificate 789
37.6 Revoking Certificates 793
37.6.1 Certificate Revocation Lists (CRLs) 793
37.6.2 TBSCertList 794
37.7 Self Signed Certificates 796
37.8 Public Key Infrastructure (PKI) 796
37.8.1 X.509 PKI Certificate Management Operations 797
37.8.2 Diffie-Hellman (DH) Key Agreement Protocol 799
37.8.3 Security Associations (SAs) 799
37.9 PKI Data Structures 799
37.9.1 PKI Message Header 800
37.9.2 PKI Message Body 801
37.9.3 PKI Message Protection 807
37.10 Summary 808

Chapter 38 - Internet Protocol Security (IPsec), and Data Encryption Standards (DES) 809
38.1 IPsec, a Basic Definition 809
38.1.1 IPsec Components 809
38.2 Basic IPsec Operation 810
38.2.1 Security Associations (SAs) 810
38.3 IP Authentication Header (AH) 811
38.3.1 Positioning of the Authentication Header 811
38.3.2 Authentication Header Format 812
38.3.3 Mutable and Immutable Fields for IPv4 814
38.3.4 Mutable and Immutable Fields for IPv6 815
38.3.5 AH Authentication Algorithms 816
38.3.6 AH and Fragmentation 816
38.4 IP Encapsulating Security Payload (ESP) 817
38.4.1 Positioning of the Encapsulating Security Payload Header 817
38.4.2 Encapsulating Security Payload Header Format 818
38.4.3 ESP Encryption Algorithms 819
38.4.4 ESP Authentication Algorithms 820
38.4.5 ESP and Fragmentation 820
38.5 Data Encryption Standard (DES) and Triple DES (3DES) 820
38.5.1 A Brief History of Encryption 820