

# Table of Contents

PREFACE.....	xxxi
--------------	------

## Section A - Introduction

<b>INTRODUCTION – CHAPTER 1.....</b>	<b>3</b>
1.1 What is TCP/IP?.....	4
1.1.1 A Brief History of TCP/IP.....	4
1.1.2 The Internet Protocol Suite.....	5
1.2 The Internet.....	8
1.2.1 The Growth of the Internet.....	8
1.3 Summary.....	11
<b>STANDARDIZATION - CHAPTER 2.....</b>	<b>13</b>
2.1 The Internet Architecture Board (IAB).....	13
2.1.1 The Internet Engineering Task Force (IETF).....	14
2.1.2 The Internet Research Task Force (IRTF).....	15
2.1.3 Internet Corporation For Assigned Names and Numbers (ICANN).....	15
2.1 Internet Protocol Standards.....	15
2.2.1 Protocol States.....	16
2.2.2 Protocol Status.....	18
2.2.3 The Request for Comments (RFC).....	19
2.3 Internet Protocol Architecture.....	20
2.3.1 The Open Systems Interconnection (OSI) Reference Model.....	20
2.3.2 The OSI Model and IEEE LANs.....	23
2.3.3 The Physical and Data Link Layers.....	26
2.3.4 The Internet Protocol Suite Model.....	27
2.4 Summary.....	30
<b>AN OVERVIEW OF UNDERLYING NETWORK TECHNOLOGIES - CHAPTER 3....</b>	<b>31</b>
3.1 Ethernet and IEEE 802.3.....	31
3.1.1 Ethernet/802.3 Standards.....	31
3.1.2 Ethernet/802.3 Frame Structures.....	36
3.1.3 Ethernet/802.3 Operation.....	39
3.2 Token Ring and IEEE 802.5.....	41
3.2.1 Token Ring/802.5 Specifications.....	41
3.2.2 Token Ring/802.5 Frame Structure.....	43
3.2.3 Token Ring/802.5 Basic Operation.....	45
3.2.4 Early Token Release.....	46
3.3 Wireless Local Area Networks (Wireless LANs) and IEEE 802.11.....	47
3.3.1 Wireless LAN/802.11 Standards.....	48
3.3.2 Wireless LAN/802.11 Operation.....	49
3.3.3 IEEE 802.11 Basic Frame Format.....	50
3.3.4 IEEE 802.11 Control Frame Formats.....	53
3.3.5 IEEE 802.11 Management Frame Formats.....	54
3.3.6 IEEE 802.11 Data Frame Formats.....	59
3.4 Relay Systems.....	60
3.4.1 Repeaters/Hubs.....	61

3.4.2	Bridges and Switches.....	62
3.4.3	Routers .....	66
3.5	WAN Links .....	67
3.6	Summary .....	68

## Section B – The Internet Protocol

<b>IP ADDRESSING - CHAPTER 4 .....</b>	<b>71</b>	
4.1	The Need for an Addressing Scheme .....	71
4.2	The Internet Protocol Version 4 (IPv4) Addressing Scheme.....	72
4.2.1	Dotted Decimal Notation .....	74
4.2.2	Identifying IP Addresses and Rules .....	75
4.2.3	Choosing the Right Addressing Scheme.....	77
4.2.3	Private Address Space .....	78
4.2.4	Automatic Private IP Addressing (APIPA) .....	79
4.3	Routing Fundamentals.....	79
4.3.1	Direct and Indirect Routing .....	80
4.4	The Resolution of MAC Addresses in IPv4 Environments .....	81
4.4.1	The Address Resolution Protocol (ARP).....	82
4.4.2	The ARP Packet Format .....	84
4.4.3	Gratuitous ARP .....	87
4.4.4	Problems with Address Resolution.....	87
4.4.5	Address Resolution for Non-Broadcast Networks .....	87
4.5	The Reverse Address Resolution Protocol (RARP) .....	87
4.5.1	Dynamic RARP .....	89
4.6	Subnetting .....	92
4.6.1	Natural Subnet Masks .....	95
4.6.2	Subnet Mask Representation .....	96
4.6.3	Obtaining and Implementing Subnet Masks .....	97
4.6.4	More Complex Subnet Mask Examples .....	98
4.6.5	Further Guidelines in Implementing Subnet Masks.....	98
4.7	Classless Inter-Domain Routing (CIDR) and Supernetting .....	102
4.7.1	Address Aggregation .....	102
4.8	Multi-Homing and Assigning Multiple IP Addresses.....	103
4.8.1	Assigning Multiple IP Addresses to a Single Physical Connection .....	103
4.9	The Internet Protocol Version 6 (IPv6) Addressing Scheme.....	104
4.9.1	Representing IPv6 Addresses .....	105
4.9.2	IPv6 Address Type Representation.....	107
4.9.3	Unicast Addresses.....	107
4.9.4	IPv6 Addresses with Embedded IPv4 Addresses.....	110
4.9.5	Provider Based Global Unicast Addresses.....	111
4.9.6	Aggregatable Global Unicast Addresses.....	111
4.9.7	Local Use IPv6 Unicast Addresses .....	112
4.9.8	The Anycast Address.....	112
4.9.9	Multicast Addresses.....	113
4.9.10	Required Addresses for an IPv6 Node.....	115
4.9.11	Stateful and Stateless Auto-Address Configuration .....	116
4.10	The Future of Internet Addressing.....	116
4.11	Summary .....	117
<b>THE INTERNET PROTOCOL VERSION 4 (IPv4) - CHAPTER 5.....</b>	<b>119</b>	

5.1	The IPv4 Datagram .....	120
5.2	IPv4 Datagram Options .....	123
5.2.1	End of Option List .....	125
5.2.2	No Operation .....	125
5.2.3	Security.....	125
5.2.4	Loose and Strict Source Routing .....	125
5.2.5	Internet Timestamp.....	126
5.2.6	Record Route .....	127
5.2.7	Router Alert.....	128
5.2.8	Sender Directed Multi-Destination Delivery .....	128
5.3	Type-of-Service.....	129
5.3.1	Applying Monetary Cost .....	129
5.3.2	Implementing Other Service Types (Differentiated Services).....	130
5.4	Datagram Fragmentation in IPv4 .....	131
5.5	Summary .....	135
<b>THE INTERNET PROTOCOL VERSION 6 (IPv6) - CHAPTER 6.....</b>		<b>137</b>
6.1	IPv6 Header Format .....	137
6.2	Extension Headers.....	139
6.2.1	Extension Header Options .....	140
6.2.2	The Hop-by-Hop Options Header.....	141
6.2.3	The Routing Header.....	144
6.2.4	The Fragment Header .....	146
6.2.5	The Destination Options Header.....	148
6.2.6	No Next Header .....	148
6.3	Packet Size Issues.....	148
6.3.1	Path MTU Discovery .....	149
6.4	Flow Labels.....	149
6.5	Traffic Classes.....	150
6.6	Using IPv6 With Upper Layer Protocols.....	152
6.6.1	Checksum Considerations .....	152
6.6.2	Maximum Packet Lifetime .....	153
6.6.3	Maximum Upper Layer Payload Size.....	153
6.6.4	Packets Carrying Routing Headers .....	153
6.7	Summary .....	154
<b>THE INTERNET CONTROL MESSAGE PROTOCOL for IPv4 - CHAPTER 7 .....</b>		<b>155</b>
7.1	ICMPv4 Message Types.....	156
7.1.1	Destination Unreachable.....	157
7.1.2	Time Exceeded .....	159
7.1.3	Parameter Problem .....	160
7.1.4	Source Quench.....	160
7.1.5	Redirect .....	161
7.1.6	Echo Request/Reply .....	163
7.1.7	Timestamp Request/Reply.....	165
7.1.8	Information Request/Reply.....	165
7.1.9	Address Mask Request/Reply.....	166
7.1.10	Router Discovery Advertisement and Solicitation.....	167
7.2	Summary .....	169
<b>THE INTERNET CONTROL MESSAGE PROTOCOL for IPv6 - CHAPTER 8 .....</b>		<b>171</b>

8.1	ICMPv6 Message Header General Format.....	171
8.2	ICMPv6 Message Types.....	173
8.2.1	Destination Unreachable.....	173
8.2.2	Packet Too Big .....	174
8.2.3	Time Exceeded .....	175
8.2.4	Parameter Problem .....	175
8.2.5	Echo Request/Reply .....	176
8.2.6	Group Membership Messages .....	176
8.3	The Neighbor Discovery Protocol.....	177
8.3.1	Router Solicitation Message .....	179
8.3.2	Router Advertisement Message.....	180
8.3.3	Neighbor Solicitation Message.....	181
8.3.4	Neighbor Advertisement Message.....	182
8.3.5	Redirect Message.....	183
8.4	Neighbor Discovery Option Formats.....	184
8.4.1	Source and Target Link-Layer Address Options .....	184
8.4.2	Prefix Information Option .....	185
8.4.3	Redirected Header Option .....	186
8.4.4	Maximum Transmission Unit (MTU) Option.....	187
8.5	Summary .....	187
<b>NETWORK ADDRESS TRANSLATION - CHAPTER 9 .....</b>		<b>189</b>
9.1	An Introduction to Traditional NAT.....	189
9.2	Basic Network Address Translation (NAT) .....	189
9.3	Network Address Port Translation (NAPT) .....	191
9.3.1	ICMP Queries in a NAPT Environment .....	192
9.4	Header Manipulation.....	193
9.4.1	Basic NAT.....	193
9.4.2	NAPT .....	193
9.4.3	IP Option Handling.....	193
9.4.4	Fragmented Packets.....	194
9.5	ICMP Error Packet Manipulation.....	194
9.6	Network Address Translation and Security .....	194
9.7	Summary .....	195
<b>TRANSITIONING FROM IPv4 to IPv6 - CHAPTER 10 .....</b>		<b>197</b>
10.1	Dual IP Layer Operation .....	198
10.2	IPv4/v6 Addresses .....	199
10.2.1	IPv4 Compatible Address Configuration.....	200
10.3	Tunneling Mechanisms .....	200
10.4	Automatic Tunnels .....	204
10.5	Configured Tunnels.....	205
10.5.1	The 'Default' Configured Tunnel .....	205
10.6	Issues Surrounding Tunneling .....	205
10.6.1	MTU and Fragmentation .....	205
10.6.2	ICMP Issues .....	206
10.6.3	Hop Limits.....	207
10.6.4	Neighbor Discovery Over Tunnels.....	207
10.7	Summary .....	208

## Section C – Reliable and Unreliable Data Delivery

<b>THE TRANSMISSION CONTROL PROTOCOL (TCP) - CHAPTER 11 .....</b>	<b>211</b>
11.1 TCP Operation.....	212
11.1.1 Basic Data Transfer .....	212
11.1.2 Reliability .....	212
11.1.3 Flow Control.....	215
11.1.4 Multiplexing .....	217
11.1.5 Connections .....	217
11.2 The TCP Segment Header .....	217
11.2.1 Explicit Congestion Notification (ECN) in IP .....	222
11.3 TCP Options.....	223
11.4 TCP Connection Management.....	224
11.4.1 Connection Establishment .....	224
11.4.2 Connection Maintenance .....	229
11.4.3 Connection Termination .....	229
11.4.4 The TCP Finite State Machine.....	232
11.5 Summary .....	234
<b>THE USER DATAGRAM PROTOCOL (UDP) - CHAPTER 12 .....</b>	<b>235</b>
12.1 UDP Multiplexing .....	236
12.2 The UDP Datagram Header.....	236
12.2.1 UDP and ICMP.....	240
12.3 Summary .....	241

## Section D – Quality of Service

<b>QUALITY OF SERVICE (QOS), DIFFERENTIATED and INTEGRATED SERVICES (DiffServ &amp; IntServ) - CHAPTER 13 .....</b>	<b>245</b>
13.1 Differentiated Services (DiffServ).....	245
13.1.1 The Differentiated Services (DS) Field .....	246
13.1.2 Class Selector Codepoints .....	247
13.1.3 Explicit Congestion Notification (ECN) in IP .....	248
13.2 Implementing Differentiated Services (DiffServ).....	249
13.2.1 DiffServ and Other/Traditional Flow Handling .....	249
13.2.2 The DiffServ Model.....	250
13.3 Traffic Classification and Conditioning .....	251
13.4 Per-Hop Behaviors (PHBs) .....	253
13.5 Bandwidth Reservation and Integrated Services (IntServ) .....	254
13.5.1 Implementing IntServ .....	257
13.5.2 Traffic Control.....	258
13.5.3 IntServ versus DiffServ .....	259
13.6 Summary .....	260
<b>THE RESOURCE RESERVATION PROTOCOL (RSVP) - CHAPTER 14 .....</b>	<b>261</b>
14.1 RSVP Reservation Styles .....	263
14.2 RSVP Protocol Overview .....	264
14.2.1 Host Operation.....	266
14.2.2 Merging Flowspecs.....	266
14.2.3 RSVP Reservation State .....	266
14.2.4 State Teardown .....	267
14.2.5 Errors and Error Handling .....	267

14.2.6	Confirmation.....	268
14.2.7	Policy and Security Control.....	268
14.2.8	Linking RSVP Domains Through non-RSVP Clouds .....	269
14.3	RSVP Message Formats .....	269
14.3.1	RSVP Object Formats .....	270
14.3.2	RSVP Object Classes.....	271
14.3.3	Path Messages .....	281
14.3.4	Resv Messages.....	281
14.3.5	PathTear Messages .....	282
14.3.6	ResvTear Messages .....	282
14.3.7	PathErr Messages .....	282
14.3.8	ResvErr Messages.....	283
14.3.9	ResvConf Messages.....	283
14.4	Summary .....	283

## Section E – IP Application Services

<b>THE DOMAIN NAME SYSTEM (DNS) - CHAPTER 15.....</b>	<b>287</b>
15.1 The Domain Name Space.....	288
15.1.1 Aliases .....	290
15.1.2 The Internet Mail System and DNS.....	290
15.2 Domain Name System Standardization .....	290
15.3 Resource Records.....	291
15.3.1 A (Address) Type Resource Record .....	293
15.3.2 CName (Canonical Name) Type Resource Record.....	293
15.3.3 HInfo (Host Information) Type Resource Record .....	293
15.3.4 MB/MD/MF/MG/MInfo/MR and MX (Mail) Type Resource Records.....	294
15.3.5 NS (Name Server) Type Resource Records.....	295
15.3.6 PTR (Pointer) Type Resource Records.....	295
15.3.7 SOA (Start of Authority) Type Resource Records.....	295
15.3.8 TXT (Text) Type Resource Records.....	296
15.3.9 WKS (Well Known Service) Type Resource Records.....	296
15.3.10 NULL (Null) Type Resource Records .....	297
15.4 Domain Name System Operation .....	297
15.4.1 Name Server Operation .....	298
15.5 The Domain Name System Protocol Format .....	300
15.5.1 The DNS Header Section.....	301
15.5.2 The Question Section.....	303
15.5.3 The Answer, Authority, and Additional Information Sections .....	303
15.5.4 Message Compression .....	303
15.6 Inverse Queries.....	304
15.7 The Notify Mechanism.....	305
15.7.1 Notify Operation.....	306
15.8 Zone Transfers.....	307
15.8.1 IXFR Operation .....	308
15.9 Dynamic DNS Updates .....	308
15.10 Security Extensions for DNS.....	310
15.10.1 Key Distribution .....	310
15.10.2 The Signature (SIG) Resource Record .....	312
15.10.3 Non-Existent Names and Types .....	313
15.11 Representing IPv6 Addresses in DNS .....	314

15.11.1	AAAA Resource Records .....	314
15.11.2	The IP6.ARPA Domain .....	315
15.12	Looking up DNS Information.....	315
15.13	Summary .....	316
<b>HOST CONFIGURATION - CHAPTER 16 .....</b>		<b>317</b>
16.1	BootP/DHCP Operation Compared to RARP/ICMP.....	318
16.2	BootP Basic Operation .....	319
16.3	DHCP Basic Operation .....	320
16.3.1	An Overview of DHCP Address Allocation .....	320
16.4	BootP/DHCP Protocol Format .....	321
16.5	DHCP Client/Server Transactions.....	332
16.5.1	DHCP Address Allocation Process.....	333
16.5.2	Reusing a Previously Allocated Address .....	335
16.5.3	Obtaining Parameters With a Configured Address .....	336
16.5.4	DHCP Lease Times .....	336
16.6	BootP/DHCP Protocol Anomalies.....	337
16.6.1	Interaction Between the Client & the Your IP Address Fields .....	337
16.6.2	Bit Ordering of the Client Hardware Address Field .....	337
16.6.3	Using BootP/DHCP in Token Ring Environments .....	338
16.6.4	The Broadcast Flag.....	338
16.7	Constructing the BootP/DHCP Request .....	339
16.7.1	Re-Transmitting BootP/DHCP Requests.....	339
16.8	Using BootP/DHCP with Relay Agents .....	339
16.8.1	BootP/DHCP Boot Request Message Handling .....	340
16.8.2	BootP/DHCP Boot Reply Message Handling.....	341
16.9	BootP/DHCP Configuration.....	342
16.9.1	BootP Configuration Files.....	342
16.9.2	DHCP Configuration Files .....	342
16.10	Summary .....	344
<b>TELNET and RLOGIN - CHAPTER 17.....</b>		<b>345</b>
17.1	The Telnet Protocol - An Introduction .....	345
17.2	Telnet Option Negotiation.....	346
17.2.1	Telnet Commands and Responses .....	346
17.2.2	Telnet Control Functions .....	348
17.3	Standard NVT Characters.....	349
17.4	Telnet Commands and Options .....	349
17.4.1	RFCs Related to Telnet Options .....	350
17.4.2	A Sample Telnet Session .....	353
17.5	Other Telnet Options.....	356
17.5.1	Telnet Environment Option .....	356
17.5.2	Telnet 3270 Commands .....	358
17.5.3	Telnet Window Size Option .....	359
17.5.4	Telnet Terminal Speed Option.....	360
17.5.5	Telnet Flow Control Options .....	361
17.6	Rlogin .....	362
17.6.1	Rlogin Commands .....	362
17.7	Telnet and Rlogin Security Considerations .....	363
17.7.1	Telnet Authentication Option .....	363
17.7.2	Telnet Data Encryption.....	367

17.8	Summary .....	369
<b>FILE TRANSFER PROTOCOLS - CHAPTER 18.....</b>		<b>371</b>
18.1	The Trivial File Transfer Protocol (TFTP).....	371
18.2	TFTP Operation.....	372
18.3	TFTP Protocol Format.....	372
18.3.1	The Determination of UDP Port Numbers.....	374
18.4	TFTP Security .....	375
18.5	Directed TFTP.....	376
18.6	TFTP Extensions .....	376
18.6.1	TFTP Option Extension.....	376
18.6.2	TFTP Block Size Option .....	379
18.6.3	TFTP Time-out Interval Option.....	379
18.6.4	TFTP Transfer Size Option .....	379
18.6.5	TFTP Multicast Option.....	380
18.7	The File Transfer Protocol (FTP) .....	381
18.8	FTP Basic Operation .....	381
18.9	FTP Data Transfer Functions .....	383
18.9.1	FTP Data Types.....	383
18.9.2	FTP Data Structures.....	384
18.10	FTP Transmission Modes.....	385
18.10.1	Stream Mode .....	385
18.10.2	Block Mode .....	385
18.10.3	Compressed Mode .....	386
18.11	FTP File Transfer Functions.....	387
18.11.1	Access Control Commands.....	387
18.11.2	Transfer Parameters .....	388
18.11.3	FTP Service Commands .....	388
18.11.4	FTP Responses .....	389
18.12	FTP Security Considerations.....	391
18.12.1	Proxy FTP.....	392
18.12.2	Restricting Access .....	392
18.12.3	Protecting Usernames .....	393
18.12.4	Protecting Passwords.....	393
18.12.5	Port Stealing .....	393
18.12.6	Software Based Security Issues .....	393
18.13	FTP Security Extensions .....	394
18.13.1	Authentication .....	395
18.13.2	Protecting the Command and Data Channels.....	396
18.14	FTP Extensions for IPv6 and Network Address Translation .....	398
18.14.1	EPRT Command.....	398
18.14.2	EPSV Command.....	399
18.14.3	FTP and Network Address Translation.....	400
18.15	A Complete FTP Example.....	400
18.16	Summary .....	408
<b>WEB OPERATIONS - CHAPTER 19.....</b>		<b>411</b>
19.1	URIs, URLs and URNs .....	411
19.1.1	Universal Resource Identifiers (URIs).....	412
19.1.2	Uniform Resource Locators (URLs).....	414
19.1.3	Uniform Resource Names (URNs).....	415

19.2	An Introduction to the Hypertext Transfer Protocol (HTTP)	416
19.2.1	Basic Operation	416
19.3	Protocol Basics	418
19.3.1	An Overview of HTTP Messages	418
19.4	HTTP Messages and Message Headers	418
19.4.1	General Headers	418
19.4.2	Requests and Request Headers	419
19.4.3	Responses and Response Headers	420
19.4.4	Entities and Entity Headers	422
19.4.5	HTTP Message Body	423
19.5	HTTP Connection Persistence	424
19.6	Using Transport Layer Security (TLS) with HTTP Connections	424
19.6.1	Upgrading to TLS within HTTP/1.1	425
19.6.2	Client Requested Upgrades to TLS	425
19.6.3	Server Requested Upgrades to TLS	425
19.6.4	Upgrading across Proxies	426
19.7	Summary	426
<b>THE SIMPLE MAIL TRANSFER PROTOCOL (SMTP) - CHAPTER 20</b>		<b>427</b>
20.1	An Introduction to The Simple Mail Transfer Protocol	427
20.2	Defining Senders and Recipients	429
20.3	Sending Mail Messages	429
20.4	Standard SMTP Commands and Responses	430
20.4.1	SMTP Commands	430
20.4.2	SMTP Replies	431
20.4.3	Verifying and Expanding	432
20.4.4	Message Header Format	432
20.5	Returning Mail to the Sender	433
20.6	SMTP Service Extensions	433
20.6.1	SMTP Message Size Declaration	435
20.6.2	SMTP Delivery Status Notifications	436
20.6.3	Returning Enhanced SMTP Error Codes	437
20.6.4	SMTP Remote Message Queue Starting	440
20.6.5	On Demand Mail Relay Through Dynamic IP Addresses	441
20.6.6	Delivery by SMTP Service Extensions	443
20.6.7	SMTP Command Pipelining	444
20.6.8	Extensions for Transmitting Large & Binary MIME Messages	445
20.7	SMTP Security Considerations	447
20.7.1	Extensions to SMTP for Authentication	447
20.7.2	SMTP extensions for Transport Layer Security (TLS)	448
20.7.3	Anti-Spam Recommendations for SMTP	448
20.8	Mail Encoding	450
20.8.1	Multi-Purpose Internet Mail Extensions (MIME)	450
20.8.2	UUencode	451
20.8.3	BinHex	452
20.9	Summary	453
<b>EMAIL DELIVERY POP3 and IMAP - CHAPTER 21</b>		<b>455</b>
21.1	An Introduction to The Post Office Protocol Version. 3 (POP3)	455
21.1.1	POP3 Basic Operation	455
21.2	POP3 Commands and Responses	456

21.2.1	Authorization using the USER and PASS Commands .....	457
21.2.2	Authorization using the APOP Command .....	457
21.2.3	Transaction Commands .....	458
21.2.4	Update Commands .....	463
21.3	A complete POP3 Example .....	463
21.4	POP3 Extensions .....	464
21.4.1	The CAPA Command .....	464
21.4.2	The TOP Capability .....	464
21.4.3	The USER Capability .....	465
21.4.4	The SASL Capability .....	465
21.4.5	The RESP-CODES Capability .....	465
21.4.6	The LOGIN-DELAY Capability .....	465
21.4.7	The PIPELINING Capability .....	466
21.4.8	The EXPIRE Capability .....	466
21.4.9	The UIDL Capability .....	466
21.4.10	The IMPLEMENTATION Capability .....	466
21.5	The Internet Message Access Protocol (IMAP) version 4 .....	466
21.5.1	IMAPv4 Basic Overview .....	467
21.6	IMAPv4 Message Attributes .....	467
21.6.1	IMAPv4 Message Texts .....	469
21.7	IMAPv4 Server and Client States .....	469
21.7.1	Non-Authenticated State .....	470
21.7.2	Authenticated State .....	470
21.7.3	Selected State .....	470
21.7.4	Logout State .....	470
21.8	IMAPv4 Data Formats .....	470
21.9	Operational Considerations .....	471
21.9.1	Mailbox Naming .....	471
21.9.2	Mailbox Size and Message Status Updates .....	471
21.9.3	Responses When no Command is in Progress .....	472
21.9.4	Inactivity Timers .....	472
21.9.5	Multiple Commands in Progress .....	472
21.10	IMAPv4 Client Commands .....	472
21.10.1	Client Commands - Any State .....	473
21.10.2	Client Commands - Non-Authenticated State .....	474
21.10.3	Client Commands - Authenticated State .....	475
21.10.4	Client Commands - Selected State .....	479
21.10.5	Client Commands - Experimental/Expansion .....	486
21.11	IMAPv4 Server Responses .....	486
21.11.1	Server Status Responses .....	487
21.11.2	Server and Mailbox Status Responses .....	489
21.11.3	Server Mailbox Size Responses .....	490
21.11.4	Server Message Status Responses .....	490
21.11.5	Command Continuation Request .....	492
21.12	Push Email - IMAPv4 Idle .....	492
21.13	POP3/IMAP Security Considerations .....	493
21.13.1	POP3 AUTH Command .....	494
21.13.2	AUTHorize Extension for IMAP and POP .....	494
21.13.3	Transport Layer Security (TLS/SSL) in POP3 & IMAP .....	495
21.14	Summary .....	496

<b>THE SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) - CHAPTER 22</b>	<b>497</b>
22.1 An Overview of Management Tasks	499
22.2 An Overview of SNMP	499
22.3 SNMP Architecture	500
22.4 The Structure of Management Information (SMI)	501
22.5 The Management Information Base (MIB)	503
22.5.1 RFCs Relating to Other MIBs	505
22.6 The Simple Network Management Protocol version 1 (SNMPv1)	506
22.6.1 Authentication	507
22.6.2 An Introduction to the SNMPv1 Protocol Format	508
22.6.3 The GetRequest PDU	511
22.6.4 The GetNextRequest PDU	511
22.6.5 The GetResponse PDU	512
22.6.6 The SetRequest PDU	512
22.6.7 The TRAP PDU	512
22.6.8 SNMPv1 PDU Format	513
22.7 SNMP Version 2 (SNMPv2)	514
22.7.1 SNMPv2 PDU Construct	514
22.7.2 The GetBulkRequest PDU	516
22.7.3 The InformRequest PDU	517
22.7.4 The Report PDU	517
22.7.5 SNMPv1 and SNMPv2 Co-existence	517
22.8 SNMP Version 3 (SNMPv3)	518
22.8.1 The SNMPv3 Message Format	519
22.8.2 User Based Security Model (USM) For SNMPv3	521
22.8.3 View Based Access Control Model (VACM) For SNMPv3	522
22.8.4 SNMPv1, SNMPv2 and SNMPv3 Co-existence	523
22.9 The Remote Monitoring MIB (RMON)	523
22.10 The Future of SNMP and Network Monitoring	524
22.11 Summary	524
<b>MISCELLANEOUS PROTOCOLS and SERVICES - CHAPTER 23</b>	<b>527</b>
23.1 The Echo Protocol	527
23.2 The Discard Protocol	528
23.3 The Character Generator Protocol (CHARGEN)	528
23.4 Quote of the Day (Quote)	529
23.5 Users	530
23.6 Finger	530
23.7 The Daytime Protocol	532
23.8 The Time Server Protocol	532
23.9 The Network Time Protocol (NTP)	533
23.10 The Line Printer Daemon Protocol (LPD)	533
23.11 SYSLOG	535
23.12 WHOIS/nickname	536
23.13 Summary	537

## Section F – Routing

<b>IPv4 ROUTING PRINCIPLES - CHAPTER 24</b>	<b>541</b>
24.1 Direct and Indirect Routing	541
24.1.1 Routing Protocols	544

24.1.2	Static and Default Routes .....	545
24.2	Routing in the Presence of Subnets .....	545
24.2.1	Variable Length Subnet Masks.....	546
24.3	ARP and Subnetted Environments .....	549
24.3.1	Proxy ARP.....	549
24.4	Policy Based Routing .....	551
24.5	Summary .....	552
<b>THE ROUTING INFORMATION PROTOCOL (RIP) - CHAPTER 25 .....</b>		<b>553</b>
25.1	Gauging Route Quality.....	553
25.2	Protocol Operation .....	555
25.2.1	Handling Topology Changes .....	557
25.2.2	Split Horizon .....	560
25.2.3	Poison Reverse .....	561
25.2.4	Triggered Updates .....	562
25.2.5	Route States and Timers .....	563
25.3	RIP Version 1 Protocol Format and Operation.....	563
25.3.1	RIP Response Datagram Processing.....	565
25.3.2	RIPv1 Router Operation at Start-up.....	570
25.4	RIP Version 1 Pros and Cons .....	570
25.4.1	RIPv1 Limitations.....	571
25.4.2	RIPv1 Strengths.....	572
25.5	RIP Version 2 .....	572
25.5.1	RIPv2 Protocol Format .....	572
25.6	Authentication with RIPv2 .....	575
25.6.1	Simple Password Authentication .....	575
25.6.2	Keyed MD5 Authentication.....	576
25.7	Using Multicast Datagrams with RIP .....	577
25.8	RIPv1/v2 Compatibility in an IPv4 Environment.....	577
25.9	Using RIP with Demand Circuits - (Low Demand RIP).....	578
25.9.1	Reducing Routing Updates .....	579
25.9.2	Reliable Delivery of Triggered Routing Updates .....	580
25.10	Triggered RIP .....	582
25.10.1	Triggered RIP Packet Types .....	582
25.10.2	Triggered RIP Packet Formats.....	583
25.11	RIP for IPv6 (RIPng).....	584
25.11.1	RIPng Message Format.....	585
25.11.2	RIPng Next Hop Information .....	587
25.11.3	RIPng MTU Considerations .....	587
25.12	Summary .....	588
<b>IGRP and EIGRP - CHAPTER 26 .....</b>		<b>589</b>
26.1	The Interior Gateway Routing Protocol (IGRP).....	589
26.1.1	IGRP Metrics.....	590
26.1.2	IGRP Holddown and Other Timers .....	590
26.1.3	IGRP Message Formats .....	591
26.1.4	IGRP Protocol Operation.....	592
26.2	The Enhanced Interior Gateway Routing Protocol (EIGRP).....	593
26.2.1	EIGRP Metrics .....	593
26.2.2	EIGRP Message Formats.....	594
26.2.3	EIGRP Operation.....	597

26.3	Summary .....	598
<b>OPEN SHORTEST PATH FIRST (OSPF) PROTOCOL for IPv4 - CHAPTER 27 .....</b>		
27.1	Enhancements Over Other IGPs .....	600
27.2	Metrics 602	
27.2.1	Type-of-Service Routing .....	603
27.2.2	Equal Cost Paths .....	605
27.3	An Overview of OSPF for IPv4 .....	605
27.3.1	OSPF Terminology .....	605
27.3.2	OSPF Areas, Area Types, and Network Types .....	607
27.3.3	Designated and Backup Designated Routers .....	609
27.3.4	Router Adjacency and Network Types .....	610
27.4	OSPF Protocol Operation for IPv4 .....	610
27.4.1	A Simplified View of OSPF Database Synchronization .....	610
27.4.2	Carrying OSPF Packets .....	611
27.4.3	A Simple OSPF internet .....	615
27.4.4	The Hello Protocol .....	616
27.4.5	Exchanging Database Information and Creating Adjacencies .....	621
27.4.6	Exchanging Database Description Packets .....	622
27.4.7	Requesting Additional Information Through Link State Requests (LSRs) .....	625
27.4.8	Link State Updates .....	627
27.5	Link State Advertisements for IPv4 .....	628
27.5.1	Router Links (Type 1) LSAs .....	628
27.5.2	Network Links (Type 2) LSAs .....	630
27.5.3	Summary Links (Type 3 and Type 4) LSAs .....	631
27.5.4	Autonomous System (AS) External Links (Type 5) LSAs .....	631
27.5.5	Not-So-Stubby-Area (NSSA) Links (Type 7) LSAs .....	633
27.5.6	Opaque Links (Types 9, 10, and 11) LSAs .....	633
27.5.7	Sample Trace Demonstrating Router Adjacency .....	634
27.6	Creating the Shortest Path Tree .....	638
27.6.1	The Routing Table .....	639
27.7	OSPF for IPv4 and Demand Circuits - (Low Demand OSPF) .....	639
27.7.1	Do-Not-Age Link State Advertisements .....	639
27.7.2	Suppressing OSPF Hellos .....	640
27.7.3	Demand Circuit Example .....	640
27.8	Using Areas .....	642
27.8.1	The Backbone Area .....	643
27.8.2	Virtual Links .....	644
27.8.3	Intra-Area and Inter-Area Routing .....	646
27.9	Joining Autonomous Systems Together .....	650
27.10	Summary .....	651
<b>OPEN SHORTEST PATH FIRST (OSPF) PROTOCOL for IPv6 - CHAPTER 28 .....</b>		
28.1	Detailed Differences Between OSPF for IPv4 and IPv6 .....	653
28.2	Carrying OSPF Information for IPv6 .....	657
28.2.1	The OSPF Packet Header for IPv6 .....	657
28.2.2	The Hello Packet .....	658
28.2.3	Database Description Packets .....	660
28.2.4	Link State Requests .....	661
28.2.5	Link State Updates .....	662
28.2.6	Link State Acknowledgements .....	663

28.3	OSPF Link State Advertisements for IPv6 .....	663
28.3.1	The IPv6 LSA Header .....	663
28.3.2	Router (Type 1) LSAs .....	665
28.3.3	Network (Type 2) LSAs .....	666
28.3.4	Inter-Area-Prefix (Type 3) LSAs.....	667
28.3.5	Inter-Area-Router (Type 4) LSAs.....	668
28.3.6	AS-External (Type 5) LSAs .....	668
28.3.7	Group Membership (Type 6) LSAs .....	670
28.3.8	Not-So-Stubby-Area (Type 7) LSAs .....	670
28.3.9	Link (Type 8) LSAs.....	670
28.3.10	Intra-Area-Prefix (Type 9) LSAs.....	671
28.4	Summary .....	672
<b>THE BORDER GATEWAY PROTOCOL (BGP) - CHAPTER 29.....</b>		<b>673</b>
29.1	BGP Operation .....	674
29.2	BGP Message Formats .....	675
29.2.1	The BGP Message Header.....	676
29.2.2	Open Messages.....	677
29.2.3	Update Messages .....	680
29.2.4	Notification Messages .....	686
29.2.5	KeepAlive Messages .....	689
29.2.6	Route-Refresh Messages .....	690
29.3	Multi-Protocol Extensions to BGPv4 .....	690
29.3.1	Multi-Protocol Reachable NLRI (MP_REACH_NLRI) Attribute.....	691
29.3.2	Multi-Protocol Unreachable NLRI (MP_UNREACH_NLRI) Attribute .....	692
29.3.3	Handling Errors with Multi-Protocol Extensions .....	693
29.4	Using BGP with IP version 6 (IPv6) .....	693
29.5	A Simple BGPv4 Example .....	694
29.6	Summary .....	698
<b>HIGH AVAILABILITY ROUTING - CHAPTER 30.....</b>		<b>699</b>
30.1	Virtual Router Redundancy Protocol (VRRP) Overview .....	700
30.2	VRRP Configurations.....	700
30.2.1	Single Virtual Router.....	700
30.2.2	Multiple Virtual Routers and Load Balancing .....	701
30.3	VRRP Protocol .....	702
30.4	VRRP Protocol Operation .....	704
30.4.1	VRRP Router Start-up .....	705
30.4.2	VRRP Router Operation in the Backup State .....	705
30.4.3	VRRP Router Operation in the Master State .....	706
30.5	VRRP Operational Issues.....	707
30.5.1	Virtual Router Interface Failure.....	707
30.5.2	Virtual Router MAC Addresses and ARP .....	708
30.5.3	VRRP Operation over Token Ring.....	709
30.5.4	ICMP Redirection.....	710
30.5.5	Proxy ARP.....	710
30.6	VRRP Security Considerations .....	710
30.7	VRRP Operation With Firewalls.....	711
30.8	The Cisco Hot Standby Router Protocol (HSRP).....	713
30.8.1	Similarities to VRRP .....	713
30.8.2	Differences to VRRP .....	713

30.9	HSRP Protocol Format and Operation .....	714
30.9.1	HSRP Operational Parameters .....	715
30.9.2	HSRP Timers .....	716
30.10	HSRP Operational Issues .....	716
30.10.1	HSRP MAC Addresses and ARP .....	716
30.10.2	HSRP Over Token Ring .....	716
30.10.3	ICMP Re-Directs .....	716
30.10.4	Proxy ARP .....	717
30.11	HSRP Security Considerations .....	717
30.12	Summary .....	717

## Section G – Multicasting in IP Environments

### **BROADCASTING, MULTICASTING and the INTERNET GROUP MANAGEMENT PROTOCOL (IGMP) - CHAPTER 31**.....721

31.1	Broadcasting in IPv4 Environments .....	721
31.1.1	Using Broadcasts in the Presence of Subnets .....	724
31.2	Multicasting in IP Environments .....	725
31.2.1	Host Group Addresses .....	726
31.2.2	Mapping IPv4 Multicasts to Local Network Multicasts .....	727
31.2.3	Multicasts and IPv6 .....	728
31.3	The Internet Group Management Protocol (IGMP) for IPv4 .....	728
31.3.1	IGMP Message Types .....	729
31.4	The Internet Group Management Protocol Version 3 (IGMPv3) for IPv4 .....	729
31.4.1	IGMPv3 Membership Query Messages .....	729
31.4.2	IGMPv3 Membership Report Messages .....	731
31.5	IGMP Versions 1 and 2 (IGMPv1 and IGMPv2) for IPv4 .....	734
31.5.1	IGMPv2 Message Formats .....	734
31.5.2	IGMPv1 Message Formats .....	735
31.5.3	Differentiating Queries Between IGMP Versions .....	735
31.6	IGMP Operation for IPv4 .....	735
31.6.1	IGMP Host States .....	737
31.7	Allocating Transient Host Group Addresses .....	738
31.8	The Multicast Listener Discovery (MLD) Protocol for IPv6 .....	738
31.9	MLDv2 Message Formats .....	738
31.9.1	MLDv2 Multicast Listener Query Messages .....	739
31.9.2	MLDv2 Multicast Listener Report Messages .....	741
31.10	MLDv1 Message Formats .....	744
31.11	Propagating Multicast Routing Information .....	745
31.12	Summary .....	746

### **DISTANCE VECTOR MULTICAST ROUTING PROTOCOL (DVMRP).....749 - CHAPTER 32** .....

32.1	An Introduction DVMRP .....	749
32.2	DVMRP Message Types and Formats .....	750
32.2.1	DVMRP Commands .....	751
32.3	Sending and Receiving DVMRP Messages .....	755
32.3.1	Sending DVMRP Messages .....	755
32.3.2	Receiving DVMRP Messages .....	756
32.4	DVMRP Tunnels .....	757
32.5	DVMRP Examples .....	758

32.6	Summary .....	758
<b>MULTICAST OSPF (MOSPF) - CHAPTER 33 .....</b>		<b>761</b>
33.1	Propagating Routing Information .....	761
33.2	MOSPF Operation .....	763
33.2.1	MOSPF Link State Advertisements (LSAs) .....	764
33.3	Pruned Shortest Path Trees .....	766
33.4	Summary .....	767
<b>PROTOCOL INDEPENDENT MULTICAST - CHAPTER 34.....</b>		<b>769</b>
34.1	Common PIM Definitions .....	769
34.1.1	A Brief Overview of PIM Message Types .....	771
34.2	An Overview of PIM .....	772
34.3	PIM-SM Operation .....	773
34.3.1	The RP Tree .....	773
34.3.2	Register Stop .....	774
34.3.3	The Shortest Path Tree (SPT) .....	774
34.3.4	Source-Specific Joins and Prunes .....	775
34.3.5	Obtaining Rendezvous Point (RP) Information .....	775
34.3.6	Multicast Data Packet Processing .....	776
34.4	PIM Protocol Format .....	777
34.4.1	PIM Header Format .....	777
34.4.2	Encoding Source and Group Addresses .....	778
34.4.3	Hello Message .....	780
34.4.4	Register Message .....	782
34.4.5	Register-Stop Message .....	783
34.4.6	Join/Prune Message .....	783
34.4.7	Bootstrap Message .....	785
34.4.8	Assert Message .....	785
34.4.9	Candidate RP Advertisement Message .....	787
34.4.10	State Refresh Message .....	788
34.4.11	Graft Message .....	789
34.4.12	Graft-Ack Message .....	789
34.5	Inter-operation of PIM-SM with Other Dense Mode Protocols (DVMRP) .....	789
34.6	Operation over Multi-Access Networks .....	790
34.6.1	Electing the Designated Router .....	790
34.6.2	Avoiding Parallel Paths to a Source .....	790
34.7	Dense Mode PIM (PIM-DM) .....	791
34.8	Bi-Directional PIM (BiDir) .....	792
34.8.1	BiDir PIM Neighbor Discovery .....	792
34.8.2	BiDir PIM Data Packet Forwarding .....	793
34.8.3	Designated Forwarder (DF) Election Process .....	793
34.8.4	Message Formats for BiDir PIM .....	795
34.9	Summary .....	797

## Section H – Securing the Communication Channel

<b>AUTHENTICATION, AUTHORIZATION, and ACCOUNTING - CHAPTER 35.....</b>		<b>801</b>
35.1	Kerberos .....	801
35.1.1	Kerberos Realms .....	802
35.2	Kerberos Tickets.....	803

35.2.1	Initial and Pre-Authenticated Tickets .....	803
35.2.2	Invalid Tickets .....	803
35.2.3	Renewable Tickets.....	803
35.2.4	Post-dated Tickets.....	804
35.2.5	Proxiable and Proxy Tickets.....	804
35.2.6	Forwardable and Forwarded Tickets .....	804
35.3	Kerberos Protocol Exchanges.....	804
35.3.1	The Authentication Service Exchange.....	805
35.3.2	The Client/Server Authentication Exchange.....	805
35.3.3	The Ticket Granting Service (TGS) Exchange .....	805
35.4	RADIUS 806	
35.4.1	Basic Radius Operation .....	807
35.4.2	RADIUS Challenges and Responses .....	809
35.4.3	Interoperability with the Point-to-Point Protocol's PAP and CHAP .....	809
35.4.4	Using RADIUS with Proxies.....	810
35.5	RADIUS Protocol.....	810
35.5.1	RADIUS Packet Format .....	811
35.5.2	RADIUS Authentication Packet Types .....	812
35.6	RADIUS Protocol Attributes.....	814
35.6.1	RADIUS Attribute Details.....	815
35.7	RADIUS Accounting .....	825
35.7.1	RADIUS Accounting Packet Types.....	825
35.7.2	RADIUS Accounting Attributes Details.....	826
35.8	RADIUS Extensions For Tunneling with IPv4 .....	829
35.8.1	Using RADIUS with Tunneling Protocols.....	829
35.8.2	RADIUS Attributes for Tunnel Protocol Support.....	830
35.8.3	Other Attribute Changes Allowing RADIUS Accounting in Tunnels .....	834
35.9	RADIUS Extensions.....	834
35.9.1	General RADIUS Extensions .....	834
35.9.2	Dynamic Authorization Extensions .....	837
35.10	RADIUS Attribute Inter-Operation .....	838
35.11	RADIUS and IP Version 6 (IPv6) .....	840
35.11.1	RADIUS Attributes for IPv6 Operation .....	841
35.11.2	IPv6 Attribute Inter-Operation and Usage .....	842
35.12	Summary 842	
<b>DIGITAL SIGNATURES, CERTIFICATES and PUBLIC KEY INFRASTRUCTURE .....</b>		
<b>(PKI) – CHAPTER 36..... 843</b>		
36.1	An Introduction to Digital Signatures and Certificates.....	843
36.2	The MD5 Message Digest Algorithm.....	846
36.2.1	MD5 Operation.....	846
36.2.2	The Differences Between MD5 and Previous Versions.....	849
36.3	Digital Signatures .....	849
36.4	Certificates .....	850
36.5	The X.509 Certificate Standard .....	851
36.5.1	tbsCertificate.....	852
36.6	Revoking Certificates .....	857
36.6.1	Certificate Revocation Lists (CRLs).....	858
36.6.2	TBSCertList.....	859
36.7	Self Signed Certificates .....	861
36.8	Public Key Infrastructure (PKI) .....	862

36.8.1	X.509 PKI Certificate Management Operations .....	862
36.8.2	Diffie-Hellman (DH) Key Agreement Protocol.....	865
36.8.3	Security Associations (SAs) .....	865
36.9	PKI Data Structures.....	866
36.9.1	PKI Message Header .....	866
36.9.2	PKI Message Body .....	867
36.9.3	PKI Message Protection .....	874
36.10	Summary .....	876
<b>INTERNET PROTOCOL SECURITY (IPsec) and DATA ENCRYPTION STANDARDS</b>		
<b>(DES) – CHAPTER 37..... 877</b>		
37.1	IPsec, a Basic Definition .....	877
37.1.1	IPsec Components .....	877
37.2	Basic IPsec Operation .....	878
37.2.1	Security Associations (SAs) .....	879
37.3	IP Authentication Header (AH).....	880
37.3.1	Positioning of the Authentication Header.....	880
37.3.2	Authentication Header Format .....	881
37.3.3	Mutable and Immutable Fields for IPv4 .....	884
37.3.4	Mutable and Immutable Fields for IPv6 .....	885
37.3.5	AH Authentication Algorithms.....	886
37.3.6	AH and Fragmentation .....	887
37.4	IP Encapsulating Security Payload (ESP) .....	887
37.4.1	Positioning of the Encapsulating Security Payload Header .....	887
37.4.2	Encapsulating Security Payload Header Format.....	889
37.4.3	ESP Encryption Algorithms .....	890
37.4.4	ESP Authentication Algorithms .....	891
37.4.5	ESP and Fragmentation .....	891
37.5	Data Encryption Standard (DES) and Triple DES (3DES).....	891
37.5.1	A Brief History of Encryption .....	891
37.5.2	The History of the Data Encryption Standard (DES).....	892
37.5.3	The Data Encryption Standard (DES).....	893
37.5.4	Triple DES (3DES).....	896
37.6	Advanced Encryption Standard (AES).....	896
37.7	Blowfish and Twofish .....	897
37.7.1	Blowfish .....	897
37.7.2	Twofish.....	899
37.8	Summary .....	899
<b>VIRTUAL PRIVATE NETWORKS (VPNs) – CHAPTER 38..... 901</b>		
38.1	What are VPNs? .....	901
38.1.1	Remote Access VPNs.....	903
38.1.2	Site-to-Site VPNs .....	903
38.2	VPN Tunnels .....	903
38.3	Types of VPN.....	903
38.3.1	IPSec vs SSL VPNs.....	904
38.4	Other Components.....	905
38.5	Summary .....	906
<b>SECURE CONNECTIONS TLS/SSL/HTTPS/SSH – CHAPTER 39..... 907</b>		
39.1	The Relationship Between SSL, TLS and HTTPS .....	907

39.2	An Introduction to TLS .....	908
39.3	The TLS Record Protocol.....	909
39.3.1	The Record Layer .....	909
39.4	An Overview of the TLS Handshake Protocol .....	912
39.4.1	The Change Cipher Spec Protocol.....	912
39.4.2	The Alert Protocol .....	913
39.4.3	The Handshake Protocol.....	914
39.5	TLS Handshake Protocol Messages .....	916
39.5.1	Hello Messages.....	917
39.5.2	Server Certificate.....	919
39.5.3	Server Key Exchange .....	920
39.5.4	Certificate Request .....	921
39.5.5	Server Hello Done .....	921
39.5.6	Client Certificate .....	921
39.5.7	Client Key Exchange.....	921
39.5.8	Certificate Verify.....	922
39.5.9	Finished .....	923
39.6	TLS Extensions .....	923
39.6.1	Extended Client and Server Hello Message Structures.....	924
39.6.2	Specific Extensions .....	925
39.6.3	Error Alerts.....	929
39.7	Secure Shell (SSH).....	930
39.7.1	The Transport Layer Protocol.....	930
39.7.2	The User Authentication Protocol .....	932
39.7.3	The Connection Protocol .....	932
39.8	Summary .....	933
<b>FIREWALLS and FIREWALLING – CHAPTER 40 .....</b>		<b>935</b>
40.1	The De-Militarized Zone (DMZ) .....	938
40.2	Packet Filtering .....	939
40.3	Internet Protocols and Packet Filtering.....	940
40.3.1	Data-Link Layer Protocols .....	940
40.3.2	Transport Layer Protocols .....	940
40.3.3	Management and Informational Protocols.....	941
40.3.4	Routing Protocols .....	943
40.3.5	Application Protocols .....	944
40.4	Designing Secure Filters.....	945
40.4.1	Telnet Filters.....	946
40.4.2	Simple Mail Transport Protocol (SMTP) Filters .....	947
40.4.3	File Transfer Protocol (FTP) Filters .....	947
40.4.4	DNS Filtering .....	951
40.4.5	ICMP Filtering.....	952
40.4.6	SNMP Filtering and Management .....	954
40.5	Filter Types .....	954
40.5.1	IP Fragmentation and the SYN Flag.....	955
40.6	Stateful Inspection .....	956
40.6.1	Basic Operation of Stateful Inspection .....	957
40.6.2	Stateful Inspection and Connectionless Protocols .....	958
40.7	High Availability Stateful Inspection .....	958
40.8	Proxy Services.....	959
40.9	Network Address Translation (NAT) .....	960

40.10	Other Considerations .....	961
40.10.1	Unauthorized Routers .....	961
40.10.2	Dial In Access.....	961
40.11	Summary .....	962

**INTRUSION DETECTION, ACTIVITY MONITORING, VIRUS PROTECTION and SPAM – CHAPTER 41 .....963**

41.1	Firewalls and Intrusion Detection Systems .....	964
41.2	Intrusion Detection Defined .....	965
41.3	IDS Implementation .....	966
41.4	Common Detection Methodologies and Techniques .....	967
41.5	Detection Categories .....	969
41.6	False Positives and False Negatives .....	970
41.6.1	Noise and False Positives .....	971
41.6.2	Sensor Positioning .....	972
41.6.3	Alarm Levels .....	973
41.7	The Anatomy of Attacks .....	974
41.7.1	The Attack .....	974
41.8	Penetration Testing.....	975
41.8.1	Penetration Testing Requirements .....	976
41.9	Virus Scanning .....	976
41.10	SPAM.....	978
41.11	Summary .....	979

**DENIAL of SERVICE (DoS) – CHAPTER 42 .....935**

42.1	TCP SYN Flooding .....	981
42.1.1	Restricting Forged Traffic .....	982
42.2	UDP and Broadcast Flooding .....	983
42.3	Smurf and Fraggle Attacks .....	984
42.4	The Ping of Death.....	984
42.5	Other Fragmentation Attacks.....	984
42.6	Connection Killing .....	985
42.7	Land .....	986
42.8	Out of Band .....	986
42.9	Stacheldraht and Trinity DDoS Attacks .....	987
42.10	Summary .....	988

**Section I – Wide Area Communications**

**COMMUNICATIONS OVER WIDE AREA LINKS – CHAPTER 43.....991**

43.1	Serial Line IP (SLIP).....	992
43.1.1	SLIP Encapsulation .....	992
43.1.2	SLIP Packet Size .....	993
43.2	Compression.....	993
43.2.1	Van Jacobson Compression.....	994
43.3	The Point-to-Point Protocol (PPP).....	996
43.3.1	PPP Encapsulation.....	997
43.4	PPP Link Operation.....	999
43.5	PPP Link Control Protocol (LCP) .....	1000
43.5.1	Link Control Protocol (LCP) General Packet Format.....	1000
43.5.2	LCP Configure Request.....	1001

43.5.3	LCP Configure Acknowledgement and Rejection.....	1007
43.5.4	LCP Terminate Request and Acknowledgement.....	1008
43.5.5	LCP Code Reject.....	1008
43.5.6	LCP Protocol Reject.....	1009
43.5.7	LCP Echo Request/Reply.....	1009
43.5.8	LCP Discard Request.....	1009
43.5.9	LCP Identification.....	1010
43.5.10	LCP Time Remaining.....	1010
43.5.11	Sample PPP Configuration Examples.....	1011
43.6	PPP Authentication Protocols.....	1013
43.6.1	The Password Authentication Protocol (PAP).....	1013
43.6.2	The Challenge Handshake Authentication Protocol (CHAP).....	1016
43.7	PPP Link Quality Monitoring (LQM).....	1018
43.7.1	The LQM Configuration Option.....	1019
43.7.2	Link Quality Report.....	1019
43.7.3	Gauging Link Quality.....	1020
43.8	PPP Multi-Link Operation.....	1021
43.8.1	Multi-Link Operation.....	1022
43.9	The Internet Protocol Control Protocol - IPCP.....	1023
43.9.1	IPCP Configuration Options.....	1024
43.9.2	Van Jacobson Compression over PPP.....	1025
43.10	The Internet Protocol Version 6 Control Protocol - IPV6CP.....	1025
43.10.1	IPV6CP Configuration Options.....	1026
43.11	PPP Compression Control Protocol (CCP).....	1027
43.11.1	CCP Operation.....	1028
43.11.2	CCP Configuration Options.....	1028
43.11.3	OUI Proprietary Compression.....	1029
43.11.4	Other Compression Types.....	1030
43.12	Vendor Extensions to PPP.....	1030
43.12.1	Vendor Specific Packets.....	1030
43.12.2	Vendor Specific Options.....	1031
43.13	PPP Framing over Serial Links.....	1032
43.13.1	Preserving Data Transparency.....	1033
43.13.2	PPP Example Using HDLC-Like Framing.....	1033
43.14	PPP over Ethernet (PPPoE).....	1035
43.14.1	An Overview of PPPoE Operation.....	1035
43.14.2	PPPoE Discovery Phase.....	1036
43.14.3	PPPoE Session Phase.....	1039
43.14.4	LCP Negotiation.....	1039
43.15	PPP over ATM (PPPoA).....	1039
43.15.1	Virtual Circuit Multiplexed PPP Over AAL5.....	1040
43.15.2	LLC Encapsulated PPP Over AAL5.....	1040
43.15.3	Control Signaling and LCP Negotiation.....	1041
44.16	Summary.....	1041
<b>TUNNELING PROTOCOLS – PPTP/L2TP and GRE – CHAPTER 44.....</b>		<b>1043</b>
44.1	An Overview of The Layer Two Tunneling Protocol (L2TP).....	1043
44.1.1	L2TP Protocol Overview.....	1044
44.2	L2TP Header Format.....	1045
44.3	L2TP Control Message Types.....	1046
44.4	An Overview of L2TP Control Message Attribute Value Pairs (AVPs).....	1047

44.4.1	Attribute Value Pair (AVP) Format .....	1047
44.5	L2TP Attribute Value Pairs (AVPs) .....	1049
44.5.1	General AVPs Applicable to All Control Messages .....	1049
44.5.2	Result and Error Codes .....	1050
44.5.3	Control Connection Management AVPs.....	1051
44.5.4	Call Management AVPs .....	1053
44.5.5	Proxy LCP and Authentication AVPs.....	1055
44.5.6	Call Status AVPs .....	1057
44.6	L2TP Protocol Operation .....	1058
44.6.1	L2TP Control Connection/Session Establishment and Teardown .....	1059
44.7	An Overview of The Point-to-Point Tunneling Protocol (PPTP) .....	1061
44.8	PPTP Protocol Overview.....	1062
44.8.1	PPTP Control Connection Message Header Format .....	1063
44.8.2	PPTP Control Connection Message Formats .....	1064
44.8.3	PPTP Control Connection Message General Error Codes .....	1074
44.9	PPTP Control Connection Protocol Operation .....	1075
44.9.1	The PPTP Control Connection .....	1075
44.10	Generic Router Encapsulation (GRE) .....	1077
44.11	The GRE Packet Header.....	1077
44.12	Forwarding and Delivery of GRE Packets .....	1079
44.13	Generic Routing Encapsulation Over IPv4 Networks .....	1080
44.13.1	Using IP as a Delivery Protocol.....	1080
44.13.2	IP as a Payload Protocol .....	1080
44.13.3	IP as the Delivery and Payload Protocols .....	1080
44.14	PPTP Tunnel Protocol Operation .....	1080
44.15	Summary .....	1081

## Section J – Appendices

<b>A GLOSSARY of NETWORKING TERMS – APPENDIX A .....</b>	<b>1085</b>
A.1 Networking Terms.....	1085
<b>OFFICIAL INTERNET PROTOCOL STANDARDS – APPENDIX B .....</b>	<b>1113</b>
B.1 Standard Protocols Ordered By Standard (STD) Number .....	1113
B.2 Best Current Practices (BCP) Documents .....	1115
B.3 For Your Information (FYI) Documents .....	1118
<b>OFFICIAL IP PROTOCOL IDENTIFIERS – APPENDIX C .....</b>	<b>1119</b>
C.1 Protocol Numbers.....	1119
<b>ADDRESS FAMILY IDENTIFIERS – APPENDIX D .....</b>	<b>1123</b>
D.1 Address Family Numbers .....	1123
D.2 Ethernet Type Codes .....	1124
<b>OFFICIAL TCP/UDP PORT NUMBERS – APPENDIX E .....</b>	<b>1129</b>
E.1 Well Known Port Numbers .....	1129
<b>MULTICAST/ANYCAST ADDRESS ALLOCATION – APPENDIX F .....</b>	<b>1145</b>
F.1 IPv4 Multicast Address Allocation.....	1145
F.1.1 IPv4 Multicast Address Allocation - 224.0.0.0 - 224.0.0.255.....	1146
F.1.2 IPv4 Multicast Address Allocation - 224.0.1.0 - 224.0.1.255.....	1147

F.1.3	IPv4 Multicast Address Allocation - 224.0.2.0 - 224.0.255.255.....	1150
F.1.4	IPv4 Multicast Address Allocation - 224.1.0.0 - 224.1.255.255.....	1151
F.1.5	IPv4 Multicast Address Allocation - 224.2.0.0 - 224.2.255.255.....	1151
F.1.6	IPv4 Multicast Address Allocation - 224.3.0.0 - 239.255.255.255.....	1151
F.2	IPv6 Multicast Address Allocation.....	1152
F.2.1	IPv6 Fixed Scope Multicast Addresses.....	1152
F.2.2	IPv6 Variable Scope Multicast Addresses.....	1153
F.3	IPv6 Anycast Address Allocation.....	1154
F.3.1	IPv6 Subnet-Router Anycast Address .....	1154
<b>BIBLIOGRAPHY – APPENDIX G.....</b>		<b>1157</b>
G.1	Request For Comments (RFCs).....	1157
<b>INDEX.....</b>		<b>1173</b>

Copyright