

To the Student	xxxi
To the Instructor	xxxiii
Highlights of the Text	xxxv
Organization Supports both Hybrid and Other Well-Known Approaches	xxxvii
Pedagogy	xli
Supplements	xlili
Acknowledgments	xlvi

An Introduction to Information Networks	1
I.1 Introduction	1
I.2 The Internet Architecture	2
I.2.1 A Hierarchical Structure	2
I.2.2 Internet Standards and the Internet Corporation for Assigned Names and Numbers (ICANN)	3
I.3 Access Networks	4
I.3.1 Digital Subscriber Lines (DSL)	4
I.3.2 Hybrid Fiber Coax (HFC)	5
I.3.3 Fiber in the Loop (FITL)	6
I.3.4 Broadband over Power Lines (BPL) and HomePlug	6
I.3.5 A Typical Home Network	7
I.3.6 Local Area Networks (LAN)	8
I.3.7 Wireless Access Networks	8
I.3.8 The Transmission Media	8
I.4 The Network Core	9
I.4.1 Internet eXchange Points (IXPs)	9
I.4.2 Tier-1 Internet Service Providers (ISPs)	9
I.4.3 The Internet2 Network	10
I.5 Circuit Switching vs. Packet Switching	12
I.5.1 Circuit Switching	12
I.5.2 A Comparison of Circuit Switching with Packet Switching Using Statistical Multiplexing	12
I.6 Packet Switching Delays and Congestion	14
I.6.1 Packet Switching Delays	14
I.6.2 Packet Loss and Delay	15
I.6.3 Congestion and Flow Control	19
I.7 The Protocol Stack	20
I.7.1 The US DoD Protocol Stack	20
I.7.2 The OSI Protocol Stack	21
I.7.3 Packet Headers and Terms	21
I.7.4 The Layer 2 (L2) to Layer 5 (L5) Operations	22
I.7.5 A User's Perception of Protocols	26
I.7.6 A Comparison of the Connection-Oriented and Connectionless Approaches	27
I.8 Providing the Benefits of Circuit Switching to Packet Switching	28
I.9 Cybersecurity	29
I.9.1 Attacks and Malware	29
I.9.1.1 The Zero-Day Attack and Mutation in Delivery	29
I.9.1.2 Crimeware Toolkits and Trojans	30
I.9.1.3 Sophisticated Malware	31

I.9.2	Defensive Measures for Cybersecurity	32
I.9.2.1	The Firewall, the Intrusion Detection System (IDS) and the Intrusion Prevention System (IPS)	32
I.9.2.2	Virtual Private Networks (VPN) and Access Control.....	33
I.9.2.3	Integrated Defense for an Enterprise Network.....	34
I.10	History of the Internet	34
I.10.1	The Development of the Internet.....	34
I.10.2	The Global Information Grid (GIG) of the US Department of Defense (DoD)	34
I.11	Concluding Remarks	36
References		36
Problems		37

SECTION 1 — Applications

Chapter 1	The Application Layer	49
1.1	Overview	49
1.2	Client/Server and Peer-to-Peer Architectures	50
1.3	Inter-process Communication through the Internet	51
1.4	Sockets.....	52
1.5	Transport Layer Services	53
1.6	The Hypertext Transfer Protocol (http).....	54
1.6.1	An Overview of HTTP	54
1.6.2	HTTP Messages	55
1.6.3	The Uniform Resource Identifier (URI).....	56
1.6.4	The GET and POST Methods	58
1.6.5	The HTTP Response Message	61
1.6.6	Persistent and Non-persistent HTTP	61
1.6.7	TCP Fast Open (TFO).....	68
1.6.8	Using HTTP for a Video Progressive Download.....	68
1.7	Cookies: Providing States to HTTP	69
1.7.1	The Operation of Setting Cookies	69
1.7.2	The Details Associated with Cookies	71
1.8	The Design of Efficient Information Delivery through Use of a Proxy	73
1.8.1	The Web Cache	73
1.8.2	Proxy Roles and Limitations.....	74
1.8.3	An Investigation of Access Link Bandwidth Issues.....	75
1.8.4	The Wide Area Application Service (WAAS) and Content Delivery Networks (CDNs).....	77
1.9	The File Transfer Protocol (FTP).....	77
1.9.1	Passive and Active FTP Data Connections.....	78
1.9.2	The Secure File Transfer Protocol (SFTP)	79
1.10	Electronic Mail.....	79
1.10.1	The Simple Mail Transfer Protocol (SMTP)	79
1.10.2	Mail Access Protocols.....	81
1.10.3	Microsoft Exchange and Outlook	82
1.10.3.1	The Messaging Application Programming Interface (MAPI).....	82
1.10.3.2	The RPC over HTTP or Outlook Anywhere.....	82
1.10.3.3	The Exchange Server Messaging System	84
1.11	Concluding Remarks.....	85
References		85
Chapter 1	Problems.....	86

Chapter 2	DNS and Active Directory.....	95
2.1	The Domain Name Service (DNS)	95
2.1.1	Overview	95
2.1.2	Recursive and Iterative Queries	98
2.1.3	Recursive or Caching DNS Server.....	99
2.1.4	The Resource Record (RR) and DNS Query.....	101
2.1.4.1	The RR Format	101
2.1.4.2	The Insertion of a Specific Type of RR.....	102
2.1.4.3	The Mail Exchange Resource Record (MX RR) and Canonical Name (CNAME)	104
2.1.4.4	A Zone File	104
2.1.4.5	The BIND 9 DNS Server Configuration.....	106
2.1.4.6	The nslookup Command	107
2.1.5	The DNS Protocol.....	109
2.1.6	The Whois Service	112
2.1.7	Server Load Balancing.....	112
2.1.8	A Detailed Illustration of DNS Query and Response Messaging.....	114
2.1.9	Reverse DNS Lookup.....	115
2.1.10	The Berkeley Internet Name Domain (BIND) Server	116
2.2	Active Directory (AD).....	116
2.2.1	An Overview Including the Applications of AD.....	116
2.2.2	The Hierarchical Structure of AD	116
2.2.3	Active Directory's Structure and Trust.....	117
2.2.4	The AD Objects and Their Domain.....	118
2.2.5	Sites within an Active Directory (AD) Domain	122
2.2.6	The Service Resource Record (SRV RR).....	122
2.2.7	The Open Directory (OD)	124
2.3	Concluding Remarks.....	124
	References.....	124
	Chapter 2 Problems.....	125
 Chapter 3	 XML-Based Web Services	 131
3.1	Overview of XML-Based Web Applications.....	131
3.2	Client/Server Web Application Development	131
3.3	The PHP Server Script	132
3.4	AJAX.....	134
3.4.1	The Client Side Script.....	135
3.4.2	Server Side Script.....	137
3.5	XML.....	140
3.5.1	XML Benefits	142
3.5.2	Minor Problems in Editors.....	142
3.6	XML Schema	143
3.6.1	A Simple Element.....	144
3.6.2	Attributes	144
3.6.3	Complex Element	145
3.6.4	XSD Declaration in an XML File	145
3.6.5	Validating a XML against a xsd File.....	146
3.7	The XML Document Object Model (DOM)	147
3.7.1	The Client Side	150
3.7.2	Server Side.....	152
3.8	Concluding Remarks.....	155
	References.....	155
	Chapter 3 Problems.....	155

Chapter 4	Socket Programming	159
4.1	Motivation	159
4.2	Socket Concepts.....	160
4.3	TCP Socket Programming.....	160
4.4	Single-Thread TCP Socket Programming	161
4.4.1	The Server Side.....	162
4.4.2	The Client Side	163
4.4.3	The TCP Server Socket.....	163
4.4.4	The TCP Client Socket.....	164
4.4.5	The TCP Output Stream	165
4.4.6	The TCP Input Stream.....	165
4.4.7	The Console Input and Output.....	166
4.4.8	Closing the TCP Socket.....	166
4.4.9	Get localhost IP Address.....	167
4.4.10	The TCP Connection between Two Hosts.....	168
4.5	Multi-thread TCP Socket Programming.....	170
4.5.1	The Multi-threaded TCP Server.....	170
4.5.2	The Server Side.....	171
4.6	UDP Socket Programming	174
4.6.1	The Server Side.....	175
4.6.2	The Client Side.....	176
4.6.3	The UDP Socket.....	176
4.6.4	Obtaining the Client's IP Address and Port Number	176
4.6.5	The UDP Send	177
4.6.6	The UDP Receive	177
4.6.7	The Console Input.....	178
4.6.8	The Console Output.....	178
4.7	Multi-thread UDP Socket Programming.....	179
4.8	IPv6 Socket Programming	181
4.9	Concluding Remarks.....	183
	References.....	183
	Chapter 4 Problems.....	184
Chapter 5	Peer-to-Peer (P2P) Networks and Applications.....	187
5.1	P2P-vs-Client/Server.....	187
5.2	Types of P2P Networks	187
5.3	Pure P2P: Gnutella Networks.....	189
5.4	Partially Centralized Architectures	190
5.5	Hybrid Decentralized (or Centralized) P2P	192
5.6	Structured vs. Unstructured P2P.....	192
5.7	Skype	193
5.8	P2P Client Software.....	197
5.9	Peer-to-Peer Name Resolution (PNRP).....	197
5.9.1	PNRP Clouds.....	198
5.9.2	Peer Names and PNRP IDs	198
5.9.3	PNRP Name Resolution	199
5.9.4	PNRP Name Publication	199
5.10	Apple's Bonjour.....	199
5.11	Wi-Fi Direct Devices and P2P Technology.....	200
5.11.1	Device Discovery and Service Discovery.....	200
5.11.2	Groups and Security.....	200
5.11.3	Concurrent Connections and Multiple Groups	202
5.12	P2P Security	202
5.13	Internet Relay Chat (IRC)	203
5.14	Concluding Remarks.....	203

References.....	204
Chapter 5 Problems.....	204

SECTION 2 — Link and Physical Layers

Chapter 6	The Data Link Layer and Physical Layer.....	211
6.1	The Physical Layer.....	211
6.1.1	Modems.....	211
6.1.2	Pulse Code Modulation (PCM) and Codec.....	214
6.1.2.1	Analog-to-Digital (A/D) Conversion.....	214
6.1.2.2	Digital-to-Analog (D/A) Conversion.....	215
6.1.3	Data Compression.....	215
6.1.4	Digital Transmission of Digital Data.....	216
6.1.4.1	Baseband Transmission.....	216
6.1.4.2	Line Codes.....	216
6.1.4.3	Block Coding.....	219
6.1.5	Synchronization and Clock Recovery.....	220
6.1.6	Channel Multiplexing for Multiple Access.....	221
6.1.7	Error Control and Shannon's Capacity Theorem.....	223
6.1.7.1	Error Detection.....	224
6.1.7.2	Forward Error Correction.....	224
6.1.8	Organization for the Physical Layer Presentation.....	225
6.2	Link Layer Functions.....	225
6.2.1	Link Layer in Protocol Stack.....	225
6.2.2	Medium Access Control (MAC) and Logical Link Control (LLC) Sublayers.....	227
6.2.3	Data Rate Comparison among MAC and Associated Physical Layers.....	228
6.3	Link Layer Realization.....	229
6.4	Multiple Access Protocols.....	230
6.4.1	Point-to-Point Protocol (PPP).....	230
6.4.2	MAC Protocols.....	231
6.4.2.1	Channel Partitioning MAC Protocols.....	232
6.4.2.2	Shared Ethernet and Wireless LAN Using Random Access.....	232
6.4.2.3	Token Ring.....	239
6.5	The Link Layer Address.....	242
6.5.1	The MAC Address.....	242
6.5.2	The Address Resolution Protocol (ARP).....	243
6.6	MAC Layer Frame Format.....	243
6.6.1	Ethernet DIX V2.0.....	243
6.6.2	802.3 MAC Layer.....	244
6.6.3	802.11 MAC Layer.....	245
6.7	The 802.2 Logic Link Control (LLC) Sublayer.....	245
6.7.1	The LLC Header.....	245
6.7.2	The LLC PDU.....	246
6.7.3	The LLC Types.....	246
6.7.4	The Subnetwork Access Protocol (SNAP).....	247
6.7.5	NetBIOS/NetBEUI.....	249
6.8	Loop Prevention and Multipathing.....	252
6.8.1	The Spanning Tree Protocol (STP).....	252
6.8.2	The Rapid Spanning Tree Protocol (RSTP).....	253
6.8.3	Layer 2 Multipathing (L2MP).....	254
6.9	Error Detection.....	256
6.10	Concluding Remarks.....	258
	References.....	258
	Chapter 6 Problems.....	259

Chapter 7	The Ethernet and Switches	269
7.1	Ethernet Overview	269
7.2	The 802.3 Medium Access Control and Physical Layers	269
7.3	The Ethernet Carrier Sense Multiple Access/Collision Detection Algorithm	271
7.4	Ethernet Hubs	271
7.5	Minimum Ethernet Frame Length	272
7.6	Ethernet Cables and Connectors	273
7.7	Gigabit Ethernet and Beyond	275
7.7.1	Gigabit Ethernet (GE)	275
7.7.2	The Physical Layer for GE and Faster Technologies	276
7.7.3	Ten Gigabit (10G) Ethernet	278
7.7.4	40 Gbps and 100 Gbps Ethernet	279
7.8	Bridges and Switches	280
7.8.1	The Learning Function	280
7.8.2	The Switch Fabric in Full Duplex Operation	281
7.8.3	The Switch Table	282
7.8.4	An Interconnected Switch Network	283
7.9	A Layer 2 (L2) Switch and Layer 3 (L3) Switch/Router	285
7.9.1	A Multilayer Switch	286
7.9.2	A Simple View of Internet Switches/Routers	287
7.9.3	The Architecture of High-Performance Internet Routers	289
7.9.4	A Multilayer Switch Chassis and Blades for a Campus Network	291
7.9.4.1	The Cisco Catalyst 6500 Switch Chassis	291
7.9.4.2	The Crossbar Switch Fabric and Supervisor Engine	292
7.9.4.3	Line Cards/Blades	293
7.9.4.4	Centralized Switching by the Supervisor Engine in a 6500 Chassis	294
7.9.4.5	The Central Forwarding Operation of a Cisco 6500 Multilayer Switch	295
7.10	Design Issues in Network Processors (NPs) and ASICs	300
7.10.1	Forwarding and Policy Engine Design Issues	300
7.10.2	Network Processors (NPs) and Application-Specific Integrated Circuits (ASICs)	300
7.10.3	ASIC + General-Purpose Processors	301
7.10.3.1	The Cisco Nexus 7000 Series Switches	301
7.10.3.2	The Cisco Nexus 5500 Switch	302
7.10.4	The Use of a Cisco QuantumFlow Processor in Internet Backbone Routers	302
7.10.4.1	New Ethernet Switch/Router Technology	303
7.10.4.2	The Multi-Service Network Infrastructure	303
7.10.4.3	Aggregation or Edge Routers	303
7.10.4.4	The Carrier Ethernet Network	304
7.10.4.5	The Core Network Router	304
7.11	Design Issues for the Packet Buffer/Memory and Switch Fabric	305
7.11.1	Switch Fabric Design Issues	305
7.11.1.1	Input Queuing (IQ) vs. Output Queuing (OQ)	305
7.11.1.2	Shared-Output Queuing (SQ)	306
7.11.1.3	Virtual Output Queuing (VOQ)	307
7.11.1.4	The Combined Input/Output Queue (CIOQ)	309
7.11.2	Design Issues for Buffers/Queues	310
7.11.3	Design Issues for Sizing Buffers in Switches	310
7.12	Cut-Through or Store-and-Forward Ethernet for Low-Latency Switching	311
7.12.1	Traditional L2 and L3 Forwarding	311
7.12.2	The Mechanisms That Make Cut-Through Forwarding Versatile	312
7.12.3	The Design Issues Associated with Cut-Through Forwarding	312
7.13	Switch Management	313
7.13.1	The Simple Network Management Protocol (SNMP)	313
7.13.2	Remote Monitoring (RMON)	314
7.14	Concluding Remarks	315

References.....	315
Chapter 7 Problems.....	317

Chapter 8	Virtual LAN, Class of Service, and Multilayer Networks	323
8.1	The Virtual LAN (VLAN-802.11q).....	323
8.1.1	VLAN Switches and Trunks.....	323
8.1.1.1	VLANs Connected by a L3 Switch/Router for Inter VLAN Communication.....	323
8.1.1.2	VLANs Connected without a L3 Switch/Router for Intra VLAN Communication	324
8.1.1.3	The Access Mode or Trunk Mode	324
8.1.2	The VLAN Registration Protocol.....	325
8.1.3	The VLAN Tag	325
8.1.4	VLAN Forwarding.....	327
8.2	Class of Service (CoS-802.11p).....	327
8.2.1	The Quality of Service (QoS) on L2.....	327
8.2.2	Priority Classification and Queues in Frame Forwarding.....	328
8.2.3	Class of Service Scheduling Methods.....	328
8.3	Switch Design Issues in CoS, Queues and Switch Fabric	330
8.3.1	ASICs for Forwarding Based on CoS at Wire Speed.....	330
8.3.2	The Unified Forwarding Engine (UFE) in Unified Port Controller (UPC)	331
8.3.3	Meeting CoS Requirements through the Use of Virtual Output Queues.....	331
8.4	Asynchronous Transfer Mode (ATM)	332
8.4.1	The ATM Network Architecture.....	332
8.4.2	The Adaptation Layer (AAL).....	333
8.4.3	Virtual Circuits (VCs).....	335
8.4.4	The ATM Cell	335
8.4.5	The ATM Physical Layer	335
8.5	Classical IP over ATM	336
8.6	Multiprotocol Label Switching (MPLS).....	338
8.6.1	The Multiprotocol Label Switching (MPLS) Network.....	338
8.6.2	The MPLS Header and Switching.....	338
8.7	Multilayer Network (MLN) Architectures.....	340
8.7.1	The Motivating Factors for MLN.....	340
8.7.2	The Architecture of the CapabilityPlanes.....	341
8.7.3	The DataPlane and Its Provisioning.....	342
8.8	Concluding Remarks.....	343
	References.....	343
	Chapter 8 Problems.....	344

Chapter 9	Wireless and Mobile Networks.....	353
9.1	An Overview of Wireless Networks.....	353
9.2	802.11 Wireless LANs	355
9.2.1	The Infrastructure Mode.....	355
9.2.2	The Ad Hoc Mode	356
9.2.3	The Basic Service Set (BSS) and the Independent BSS (IBSS).....	357
9.2.4	The Distribution System (DS) and the Extended Service Set (ESS).....	357
9.2.5	Passive and Active Scanning.....	359
9.2.6	Robust Security Network Associations (RSNAs)	359
9.2.7	Wireless Challenges	360
9.2.8	The 802.11 Physical Layer.....	360
9.2.9	The 802.11n Physical Layer	361
9.2.9.1	MIMO.....	361
9.2.9.2	Space Division Multiplexing (SDM).....	362
9.2.9.3	Antenna Diversity or Space-Time Coding (STC).....	363
9.2.9.4	MIMO Summary	364

9.2.10	The MAC Layer.....	364
9.2.10.1	Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA).....	364
9.2.10.2	The Unicast Frame.....	365
9.2.10.3	The Distributed Coordination Function (DCF).....	365
9.2.10.4	The Broadcast Frame.....	366
9.2.10.5	Virtual Carrier Sensing.....	366
9.2.10.6	The Point Coordination Function (PCF).....	368
9.2.10.7	Random Back-off Time and Error Recovery.....	369
9.2.10.8	MAC Frames and MAC Addresses.....	370
9.2.10.9	MAC Frame Types.....	373
9.2.11	Frequency Reuse, Power and Data Rates.....	381
9.2.11.1	Frequency Reuse.....	381
9.2.11.2	802.11h: Dynamic Frequency Selection (DFS) and Transmitter Power Control (TPC).....	382
9.2.11.3	The Number of Stations in a BSS.....	384
9.2.12	Power over Ethernet.....	384
9.3	Wireless Personal Area Network (WPAN).....	385
9.3.1	Bluetooth.....	385
9.3.1.1	Data Rates and Range.....	385
9.3.1.2	The Piconet.....	387
9.3.1.3	The States and Modes of Piconet.....	387
9.3.1.4	Types of Links.....	388
9.3.1.5	Packet Format.....	389
9.3.1.6	Time Division Duplex (TDD) and Frequency Hopping (FH).....	390
9.3.1.7	The Scatternet.....	392
9.3.2	Ultra Wideband (802.15.3).....	392
9.3.3	ZigBee (802.15.4).....	394
9.4	WLANs and WPANs Comparison.....	396
9.5	WiMAX (802.16).....	396
9.6	Cellular Networks.....	398
9.6.1	CDMA2000.....	399
9.6.2	The Universal Mobile Telecommunication Service (UMTS).....	400
9.6.3	Long Term Evolution.....	400
9.6.4	Mobility.....	401
9.7	Concluding Remarks.....	402
	References.....	402
	Chapter 9 Problems.....	404

SECTION 3 — Network Layer

Chapter 10	The Network Layer.....	417
10.1	Network Layer Overview.....	417
10.1.1	The Need for Network and Link Layers.....	417
10.1.2	Network Layer Functions.....	418
10.2	Connection-Oriented Networks.....	419
10.3	Connectionless Datagram Forwarding.....	420
10.4	Datagram Networks vs. Virtual Circuit ATM Networks.....	422
10.5	Network Layer Functions in the Protocol Stack.....	423
10.6	The IPv4 Header.....	423
10.7	IP Datagram Fragmentation/Reassembly.....	425
10.8	Type of Service (ToS).....	427
10.8.1	ToS, IP Precedence and DSCoDe Points (DSCP).....	427
10.8.2	Queuing/Scheduling Methods.....	428

10.9	The IPv4 Address	429
10.9.1	Network Interface and IP address	429
10.9.2	Subnet.....	430
10.9.3	Network ID, Subnet ID and Host ID.....	432
10.9.4	Private IP Addresses.....	433
10.9.5	Classless Inter-Domain Routing.....	434
10.9.6	ARP Cache.....	435
10.9.7	Optimal use of IP addresses.....	436
10.10	The Dynamic Host Configuration Protocol (DHCP)	438
10.10.1	The DHCP Server and Routers.....	438
10.10.2	DHCP Protocol	438
10.10.3	The Reuse of a Previously Allocated Network Address.....	439
10.11	IP Multicast.....	443
10.11.1	The IP Multicast Advantage.....	443
10.11.2	Routing for Multicast	444
10.11.3	The Protocol Independent Multicast (PIM).....	446
10.12	Routing between LANs.....	447
10.13	Network Address Translation (NAT)	450
10.13.1	Address and Port Translation	450
10.13.2	NAPT Mapping/Binding Classifications	454
10.13.2.1	NAT Behavior Related to UDP Bindings in RFC3489.....	454
10.13.2.2	Address and Port Mapping Behavior in RFC 4787 and RFC 5382.....	457
10.13.3	NAPT for Incoming Requests.....	458
10.13.3.1	Application Level Gateways (ALGs).....	459
10.13.3.2	The Static Port Forwarding.....	460
10.13.3.3	The Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol.....	461
10.13.3.4	Traversal Using Relays around NAT (TURN).....	462
10.13.3.5	The Session Traversal Utilities for NAT (STUN).....	464
10.13.3.6	The Interactive Connectivity Establishment (ICE).....	465
10.14	The Internet Control Message Protocol (ICMP).....	469
10.14.1	The ICMP Packet.....	469
10.14.2	Echoes and Replies	470
10.14.3	The Destination Unreachable Message	471
10.14.4	The Traceroute	472
10.14.4.1	A Traceroute in UNIX-like OSs.....	472
10.14.4.2	The Microsoft Windows Tracert.....	475
10.15	The Mobile Internet Protocol.....	478
10.16	Concluding Remarks.....	481
	References.....	481
	Chapter 10 Problems.....	483

Chapter 11	IPv6.....	493
11.1	The Need for IPv6	493
11.2	The IPv6 Packet Format.....	494
11.3	IPv6 Addresses.....	494
11.3.1	Three Types of IPv6 Addresses.....	496
11.3.2	The Scope of Addresses.....	496
11.3.3	The Global Unicast Address.....	496
11.3.4	The Multicast Address.....	497
11.3.5	The Anycast Address.....	498
11.3.6	Special Addresses.....	499
11.4	The Transition from IPv4 to IPv6	500
11.4.1	The Double NAT: NAT 444.....	500

11.4.2	An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition.....	501
11.4.3	Address Family Translation	501
11.4.3.1	Stateful Address Family Translation (AFT)-(NAT 64)	502
11.4.3.2	Stateless AFT (IVI)	502
11.4.4	The Dual Stack	503
11.4.5	Dual-Stack Lite (DS-Lite).....	504
11.4.5.1	The Access Model.....	504
11.4.5.2	The Home Gateway	505
11.4.6	Tunneling.....	505
11.4.7	Encapsulating an IPv6 Datagram into IPv4.....	505
11.4.8	The 6To4 Scheme	506
11.4.9	6To4 Automatic Tunneling.....	506
11.4.10	A 6To4 Relay Router	507
11.4.11	The Rapid Deployment of IPv6 on the IPv4 Infrastructures (6rd).....	508
11.4.12	The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)	509
11.4.13	Teredo Tunneling.....	510
11.4.13.1	The Motivation for Teredo Tunneling.....	510
11.4.13.2	The Teredo Network Infrastructure	510
11.4.13.3	The Teredo Protocol.....	511
11.4.13.4	The Teredo IPv6 Addressing Scheme.....	512
11.4.13.5	Teredo Packet Encapsulation.....	513
11.5	IPv6 Configuration and Testing.....	513
11.5.1	OS X	513
11.5.2	Microsoft Windows.....	515
11.5.3	Pinging Windows 7/Vista from OS X.....	516
11.5.4	Installing IPv6 in Windows XP	518
11.5.5	The Firewall Configuration for Echo Reply in Windows XP.....	519
11.5.6	A Multicast Ping and the Replies.....	522
11.6	Concluding Remarks	524
	References.....	525
	Chapter 11 Problems	526

Chapter 12	Routing and Interior Gateways.....	531
12.1	Routing Protocol Overview.....	531
12.2	Configuring a Router	532
12.2.1	Static Route Configuration.....	532
12.2.2	Dynamic Routing Protocol Configuration	533
12.2.3	The RIP Configuration	533
12.2.4	The OSPF Configuration.....	534
12.2.5	The BGP Configuration	535
12.3	VLAN Routing.....	536
12.4	Open Shortest Path First (OSPF).....	537
12.4.1	OSPF Areas.....	538
12.4.2	OSPF Routing Table Construction.....	538
12.4.3	Type of Service (ToS) Support	540
12.5	The OSPF Routing Algorithm.....	540
12.5.1	A Graphical Representation.....	540
12.5.2	Dijkstra's Algorithm.....	540
12.5.3	Generating a Routing Table.....	542
12.5.4	Load-Sharing Multipath in OSPF	545
12.5.5	OSPF Properties.....	546
12.6	The Routing Information Protocol (RIP).....	547
12.6.1	The Distance Vector Algorithm.....	547
12.6.2	The Positive Aspects of Rapid Convergence.....	552

12.6.3	The Negative Aspects of Slow Convergence.....	555
12.6.4	Split Horizon with Poison Reverse.....	560
12.6.5	A Three-Node Loop Problem.....	563
12.7	OSPF-vs.-RIP.....	566
12.8	Concluding Remarks.....	567
	References.....	567
	Chapter 12 Problems.....	568

Chapter 13	Border Gateway Routing.....	575
13.1	Autonomous Systems.....	575
13.2	Border Gateway Protocol (BGP) Overview.....	577
13.2.1	A BGP Session.....	577
13.2.2	A BGP Route.....	578
13.2.3	The AS_Path Attribute.....	579
13.2.4	Path Attributes.....	580
13.3	A Real-World BGP Case.....	581
13.4	BGP Route Advertisements.....	583
13.4.1	The Next Hop Attribute in External BGP (eBGP) and Internal BGP (iBGP).....	583
13.4.2	AS_Path Attribute Propagation in Route Advertisements.....	584
13.5	BGP Route Selection.....	585
13.5.1	The BGP Policy.....	585
13.5.2	The Use of Attributes in Selecting Routes.....	590
13.5.3	The Integration of BGP and IGP.....	591
13.5.4	Local Preference.....	593
13.5.5	The Multi-Exit Discriminator (MED) Attribute.....	596
13.6	BGP Import and Export Policies.....	603
13.6.1	The import policy.....	603
13.6.2	The Export Policy.....	603
13.6.3	Bandwidth-Based Policy for Export Routes.....	603
13.7	BGP Security.....	605
13.8	Concluding Remarks.....	607
	References.....	607
	Chapter 13 Problems.....	608

SECTION 4 — Transport Layer

Chapter 14	The Transport Layer.....	615
14.1	Transport Layer Overview.....	615
14.1.1	The Function of the Transport Layer in the Protocol Stack.....	615
14.1.2	The Transmission Control and Stream Control Transmission Protocols.....	615
14.2	The Socket.....	616
14.3	The User Datagram Protocol (UDP).....	617
14.3.1	The Use of UDP.....	617
14.3.2	The UDP Packet Format.....	618
14.4	A Reliable Transport Protocol: TCP.....	619
14.4.1	TCP Overview.....	619
14.4.2	The 3-Way Handshake.....	619
14.4.3	Closing a TCP Connection.....	620
14.4.4	The Sequence and Acknowledgment (ACK) Numbers.....	620
14.4.5	A Simple Acknowledgment Scheme.....	622
14.4.6	Pipelined Protocols.....	623
14.4.7	A TCP Segment and Sequence Number.....	625
14.4.8	The Sliding Window.....	625

14.5	The TCP Packet Header and Options.....	626
14.5.1	The TCP Header Format.....	626
14.5.2	A 3-Way Handshake Analysis Using a Network Analyzer.....	628
14.5.3	The Half Close Analysis Using a Network Analyzer.....	630
14.5.4	Using a Network Analyzer to Obtain the Secure Shell (SSH) and HTTP Sequence and ACK Numbers.....	632
14.5.4.1	The Secure Shell Protocol.....	632
14.5.4.2	HTTP.....	633
14.5.5	Explicit Congestion Notification.....	634
14.5.6	Round Trip Time Measurement.....	634
14.5.7	Windows Scaling.....	636
14.5.8	Selective Acknowledgment.....	639
14.5.9	The Use of a Reset Flag.....	639
14.5.10	The Use of a Push Flag.....	640
14.6	The Buffer and Sliding Window.....	642
14.6.1	The Sender Side.....	642
14.6.2	The Receiver Side.....	642
14.6.3	Extending the Sequence Number to 64 Bits.....	644
14.7	Features of the Stream Control Transmission Protocol (SCTP).....	644
14.7.1	The Motivation for SCTP.....	644
14.7.2	SCTP vs. TCP.....	644
14.7.3	SCTP Streams and Services.....	645
14.8	The SCTP Packet Format.....	646
14.8.1	The Chunk Field.....	646
14.8.2	Chunk Types.....	647
14.8.3	The Payload Data Format.....	647
14.9	SCTP Association Establishment.....	648
14.10	The SCTP SHUTDOWN.....	648
14.11	SCTP Multi-Homing.....	649
14.12	Concluding Remarks.....	650
	References.....	650
	Chapter 14 Problems.....	651

Chapter 15	Packet Loss Recovery.....	661
15.1	Packet Acknowledgment (ACK) and Retransmission.....	661
15.2	Round Trip Time and Retransmission Timeout.....	662
15.3	Cumulative ACK and Duplicate ACK.....	663
15.4	The Sliding Window and Cumulative ACK.....	666
15.5	Delayed ACK.....	671
15.6	Fast Retransmit.....	673
15.7	Synchronization (SYN) Packet Loss and Recovery.....	675
15.8	The Silly Window Syndrome/Solution.....	676
15.9	The TCP Selective Acknowledgment (SACK) Option.....	676
15.10	Concluding Remarks.....	684
	References.....	684
	Chapter 15 Problems.....	685

Chapter 16	TCP Congestion Control.....	689
16.1	TCP Flow Control.....	689
16.2	TCP Congestion Control.....	689
16.2.1	The Buffer Sizing Problem.....	691
16.2.2	Congestion Control Approaches.....	691
16.2.3	ATM Congestion Control.....	692

16.3	Standard TCP End-to-end Congestion Control Methods.....	693
16.3.1	The Congestion Window Size (CWND).....	693
16.3.2	Slow Start	694
16.3.3	The Effective Window	695
16.3.4	The Signs of Congestion.....	696
16.3.5	Additive Increase Multiplicative Decrease (AIMD) and Congestion Avoidance	696
16.4	TCP Tahoe and TCP Reno in Request for Comment (RFC) 2001	697
16.4.1	Slow Start and Timeout.....	697
16.4.2	Three or More Duplicate Acknowledgments (ACKs)	698
16.4.3	Congestion Avoidance	699
16.4.4	Fast Retransmit and Fast Recovery in RFC 2001	699
16.5	An Improvement for the Reno algorithm—RFC 2581 and RFC 5681	699
16.6	TCP NewReno.....	702
16.6.1	Filling Multiple Holes in the Receiver's Buffer.....	702
16.6.2	Fast Retransmit and Fast Recovery Algorithms in NewReno	702
16.7	TCP Throughput for a Real-World Download in Microsoft's Windows XP.....	704
16.8	A Selective Acknowledgment (SACK)-Based Loss Recovery Algorithm	706
16.8.1	A Conservative SACK-Based Loss Recovery Algorithm for TCP.....	706
16.8.2	Reno vs. NewReno vs. SACK.....	708
16.8.3	The CWND Slow Recovery Process.....	713
16.8.4	The "Limited Transmit" Algorithm.....	713
16.9	High-Speed TCP (HSTCP) Congestion Control Design Issues	713
16.9.1	The Design Issues Associated with TCP Congestion Control for High-Speed Networks	714
16.9.2	An Overview of HighSpeed TCP (HSTCP)	714
16.9.3	The Response Functions in HighSpeed TCP (HSTCP)	715
16.9.4	Limited Slow-Start in HSTCP.....	716
16.9.5	H-TCP	717
16.10	CUBIC TCP.....	718
16.10.1	CUBIC Window Adjustment	718
16.10.2	TCP CUBIC vs. TCP NewReno	719
16.10.3	The Performance of TCP CUBIC.....	719
16.11	Loss-Based TCP End-to-End Congestion Control Summary.....	721
16.12	Delay-Based Congestion Control Algorithms	723
16.13	Compound TCP (CTCP).....	723
16.13.1	The Compound TCP (CTCP) Control Law	724
16.13.2	The Compound TCP Response Function.....	725
16.13.3	CTCP Deployment and Performance	726
16.14	The Adaptive Receive Window Size	729
16.15	TCP Explicit Congestion Control and Its Design Issues.....	730
16.15.1	ECN-Capable Transport (ECT) and Congestion Experienced (CE)	730
16.15.2	The Explicit Congestion Notification (ECN) 3-Way Handshake.....	732
16.15.3	Congestion Experienced (CE) by Router and ECN-Echo (ECE) by Receiver	733
16.15.4	Weighted Random Early Detection (WRED) + Explicit Congestion Notification.....	733
16.15.5	A WRED and ECN Case Study.....	734
16.15.6	Performance Evaluation of Explicit Congestion Notification (ECN)	735
16.15.7	The ECN-Based Data Center TCP (DCTCP).....	736
16.16	The Absence of Congestion Control in UDP and TCP Compatibility.....	737
16.16.1	The Coexistence of TCP and UDP flows	738
16.16.2	The Coexistence of Multiple TCP Flows	738
16.16.3	Coexisting Heterogeneous TCP NewReno, CUBIC and CTCP Flows.....	739
16.17	Concluding Remarks.....	741
	References.....	741
	Chapter 16 Problems.....	743

SECTION 5 — Cybersecurity

Chapter 17	Cybersecurity Overview	749
17.1	Introduction	749
17.2	Security from a Global Perspective	749
17.3	Trends in the Types of Attacks and Malware	751
17.3.1	Malware Statistics and Detection Methods	752
17.3.2	Web-Based Malware	753
17.4	The Types of Malware	754
17.4.1	Worms	754
17.4.2	Phishing	756
17.4.3	Trojans	758
17.4.4	Botnets	759
17.4.5	Rootkits	764
17.4.5.1	User Mode Rootkits	765
17.4.5.2	Kernel Mode Rootkits	765
17.4.5.3	The Master Boot Record (MBR) Rootkit	766
17.4.5.4	A Real-World Rootkit/Trojan	766
17.4.6	Viruses	767
17.5	Vulnerability Naming Schemes and Security Configuration Settings	768
17.5.1	Common Vulnerabilities and Exposures (CVE)	768
17.5.2	Common Configuration Enumeration (CCE)	769
17.6	Obfuscation and Mutations in Malware	770
17.6.1	Executable Packing/Compression	771
17.6.2	Entry Point Obfuscation (EPO)	773
17.6.3	Polymorphism	774
17.6.3.1	Polymorphic Malware	774
17.6.3.2	The Detection of Polymorphic Malware	775
17.6.4	Metamorphism	776
17.6.4.1	Metamorphic Malware	776
17.6.4.2	The Detection of Metamorphic Malware: An Open Challenge	780
17.7	The Attacker's Motivation and Tactics	780
17.7.1	The Attack Motivation	780
17.7.2	Attack Tactics and Their Trends	781
17.8	Zero-Day Vulnerabilities	783
17.8.1	The History of Zero-Day Vulnerabilities	783
17.8.2	Defensive Measures for Zero-Day Vulnerabilities	785
17.9	Attacks on the Power Grid and Utility Networks	786
17.10	Network and Information Infrastructure Defense Overview	786
17.10.1	Defense for the Enterprise	786
17.10.2	Penetration Tests	790
17.10.3	Contingency Planning	790
17.10.4	The Critical Infrastructure Protection (CIP) Plan	791
17.10.5	Intelligence Collection for Defense of the Internet Community	791
17.10.6	The Eradication of Botnets	792
17.11	Concluding Remarks	793
	References	793
	Chapter 17 Problems	796
Chapter 18	Firewalls	807
18.1	Overview	807
18.2	Unified Threat Management	807
18.3	Firewalls	809
18.4	Stateless Packet Filtering	810

18.4.1	The Format for the Rule Used in Packet Filtering	810
18.4.2	The Manner in Which the Firewall ACL Is Processed.....	812
18.4.3	The Inherent Weaknesses of Stateless Filters	813
18.5	Stateful/Session Filtering.....	815
18.5.1	Stateful Inspection.....	815
18.5.2	Network Address Translation (NAT).....	815
18.6	Application-Level Gateways.....	816
18.7	Circuit-Level Gateways.....	816
18.8	A Comparison of Four Types of Firewalls	817
18.9	The Architecture for a Primary-Backup Firewall.....	818
18.10	The Windows 7/Vista Firewall as a Personal Firewall.....	818
18.11	The Cisco Firewall as an Enterprise Firewall.....	833
18.12	The Small Office/Home Office Firewall	839
18.13	Emerging Firewall Technology.....	842
18.14	Concluding Remarks.....	842
	References.....	843
	Chapter 18 Problems.....	843

Chapter 19	Intrusion Detection/Prevention System	849
19.1	Overview.....	849
19.1.1	IDS/IPS Building Blocks	850
19.1.2	Host-Based or Network-Based IDS/IPS.....	850
19.2	The Approaches Used for IDS/IPS.....	852
19.2.1	Anomaly-Based Detection Methods	852
19.2.1.1	Statistical-Based IDS/IPS.....	852
19.2.1.2	Knowledge-/Expert-Based IDS/IPS.....	853
19.2.1.3	Machine Learning-Based IDS/IPS.....	854
19.2.2	Signature-Based IDS/IPS	854
19.2.3	Adaptive Profiles	856
19.3	Network-Based IDS/IPS.....	857
19.3.1	Network-Based IDS/IPS (NIDS/NIPS) Functions	857
19.3.2	Reputation-Based IPS	858
19.4	Host-Based IDS/IPS.....	859
19.5	Honeypots.....	859
19.6	The Detection of Polymorphic/Metamorphic Worms.....	861
19.7	Distributed Intrusion Detection Systems and Standards.....	861
19.7.1	Event Aggregation and Correlation.....	862
19.7.2	Security Information and Event Management (SIEM).....	863
19.7.3	Standards for Multiple Formats and Transport Protocols.....	864
19.8	SNORT.....	864
19.9	The TippingPoint IPS.....	870
19.10	The McAfee Approach to IPS.....	873
19.11	The Security Community's Collective Approach to IDS/IPS.....	876
19.12	Concluding Remarks.....	878
	References.....	878
	Chapter 19 Problems.....	880

Chapter 20	Hash and Authentication.....	885
20.1	Authentication Overview.....	885
20.2	Hash Functions.....	886
20.2.1	The Properties of Hash Functions.....	886
20.2.2	The History of Hash Functions.....	889
20.2.3	Secure Hash Algorithms 1 and 2 (SHA-1 and SHA-2).....	889

20.2.4	Feasible Attacks to a Hash	890
20.3	The Hash Message Authentication Code (HMAC)	891
20.3.1	The HMAC Algorithm	891
20.3.2	The Key Derivation Function (KDF) and the Pseudorandom Function (PRF)	893
20.4	Password-Based Authentication	893
20.4.1	Dictionary Attacks	894
20.4.2	The UNIX Encrypted Password System: CRYPT	894
20.4.3	The UNIX/Linux Password Hash	896
20.4.3.1	The MD5-Based Scheme	896
20.4.3.2	The SHA-Based Scheme	897
20.4.4	The Windows Password	897
20.4.4.1	The LM (LanManager) Hash	897
20.4.4.2	The Windows NT Hash	897
20.4.5	Cracking Passwords	898
20.5	The Password-Based Encryption Standard	898
20.6	The Automated Password Generator Standard	899
20.7	Password-Based Security Protocols	899
20.7.1	IEEE P1363.2	899
20.7.2	Online Authentication	900
20.7.3	ANSI X9.26-1990	901
20.7.4	Kerberos	901
20.8	The One-Time Password and Token	901
20.8.1	Two-Factor Authentication	902
20.8.2	The OTP Standards	903
20.8.3	RFC 2289: A One-Time Password System	903
20.8.4	RFC 2808: The SecurID Simple Authentication and Security Layer (SASL) Mechanism	904
20.8.5	RFC 4226: The HMAC-based One Time Password (HOTP)	904
20.8.6	A Time-Based One-time Password Algorithm (TOTP)	905
20.8.7	RFC 4758: The Cryptographic Token Key Initialization Protocol (CT-KIP)	905
20.8.8	IETF Draft: One Time Password (OTP) Pre-authentication	907
20.8.9	Intel Identity Protection Technology (Intel IPT)	908
20.9	Open Identification (OpenID) and Open Authorization (OAuth)	909
20.9.1	OpenID	909
20.9.2	OAuth	909
20.10	Concluding Remarks	910
	References	910
	Chapter 20 Problems	912

Chapter 21	Symmetric Key Ciphers and Wireless LAN Security	917
21.1	Block Ciphers	917
21.1.1	The Data Encryption Standard (DES)	917
21.1.2	Triple-DES	919
21.1.3	The Advanced Encryption Standard (AES)	920
21.1.4	Confidentiality Modes	922
21.1.4.1	The Electronic Codebook (ECB) Mode	922
21.1.4.2	The Cipher Block Chaining (CBC) Mode	923
21.2	Stream Ciphers	926
21.2.1	Rivest Cipher 4 (RC4)	926
21.2.2	WLAN Security Using Stream Cipher RC4	927
21.2.2.1	The Chronology of WLAN Security	927
21.2.2.2	The 802.11 WEP and 802.11i WPA Security Processes, and Their Weaknesses	927
21.2.2.3	Wired Equivalent Privacy (WEP)	928
21.2.2.4	802.11i Wi-Fi Protected Access (WPA)	929
21.2.2.5	802.11i Fresh Keying	930

21.2.3	The AES Counter Mode	937
21.2.4	802.11i Wi-Fi Protected Access 2 (WPA2)	938
21.2.4.1	An Overview of the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)	938
21.2.4.2	The CCMP Nonce	939
21.2.5	The Advanced Encryption Standard Counter Mode (AES-CTR)	940
21.2.5.1	The Cipher Block Chaining Message Authentication Code (CBC-MAC)	941
21.2.5.2	The CCMP Complete Scheme	942
21.2.6	WiFi Protected Setup (WPS)	943
21.3	The US Government's Cryptography Module Standards	944
21.3.1	Federal Information Processing Standard (FIPS) 140-2	944
21.3.2	FIPS 140-3	945
21.3.3	The New European Schemes for Signatures, Integrity and Encryption (NESSIE)	945
21.4	Side Channel Attacks and the Defensive Mechanisms	946
21.5	Concluding Remarks	947
	References	947
	Chapter 21 Problems	948
Chapter 22	Public Key Cryptography, Infrastructure and Certificates	955
22.1	Introduction	955
22.1.1	The Diffie-Hellman (DH) Protocol	957
22.1.1.1	Overview of the DH Key-Agreement Protocol	957
22.1.1.2	Diffie-Hellman Key-Agreement Protocol Security	959
22.1.1.3	The Use of a Diffie-Hellman Key-Agreement Protocol	959
22.1.1.4	Diffie-Hellman Groups	960
22.1.2	The Rivest, Shamir and Adleman (RSA) Public-Key Cryptography	961
22.1.2.1	The RSA Algorithm	961
22.1.2.2	Chinese Remainder Theorem (CRT) and RSA Decryption	964
22.1.2.3	RSA Security	967
22.2	The Digital Signature Concept	968
22.2.1	RSA Signatures	968
22.2.1.1	The RSA Signature Algorithm	968
22.2.1.2	The Security of RSA Signatures	968
22.2.1.3	An Example of Signing and Verifying a RSA Signature	969
22.2.2	The Digital Signature Standard (DSS)	970
22.3	Public Key Cryptography Characteristics	971
22.3.1	The Recommended Use of Public Key Cryptography	971
22.3.2	RSA vs. DH	972
22.3.3	The RSA Challenge	972
22.4	Elliptic Curve Cryptography (ECC)	972
22.4.1	The ECC Algorithms and Their Properties	972
22.4.2	The Elliptic Curve Discrete Logarithm Problem (ECDLP) and Its Applications	976
22.4.3	Elliptic Curve Diffie-Hellman (ECDH) Key-Agreement Protocol	976
22.4.4	Elliptic Curve Digital Signature Algorithm (ECDSA)	977
22.4.5	The Elliptic Curve Integrated Encryption Standard (ECIES)	978
22.4.6	Recommended Finite Fields and Elliptic Curves for Desired Security Strength	979
22.4.7	The ECC Challenge	980
22.5	Certificates and the Public Key Infrastructure	981
22.5.1	A Certificate Authority (CA) and the Public Key Infrastructure	981
22.5.2	The Secure Socket Layer (SSL) and Certificates	983
22.5.3	The X.509 Certificate Format	985
22.5.4	Classes of Certificates	988
22.5.5	Trusted Root Certificates	989
22.5.6	Certificate Revocation List (CRL)	990

22.6	Public Key Cryptography Standards (PKCS)	990
22.7	X.509 certificate and Private Key File Formats	990
22.8	U.S. Government Standards.....	993
22.8.1	National Security Agency (NSA) Suite B.....	993
22.8.2	Suite B Cryptography Support in Windows	994
22.8.3	The Entity Authentication Standard	994
22.9	Attacks Which Target the Public Key Infrastructure and Certificates	995
22.10	Email Security.....	996
22.10.1	Pretty Good Privacy (PGP)	996
22.10.2	Secure/Multipurpose Internet Mail Extensions (S/MIME).....	998
22.11	Concluding Remarks.....	999
	References.....	999
	Chapter 22 Problems.....	1001

Chapter 23 Secure Socket Layer/Transport Layer Security (SSL/TLS) Protocols for Transport Layer Security 1009

23.1	Introductory Overview	1009
23.2	The Handshake Protocol.....	1010
23.3	Attacks on the Handshake Protocol	1016
23.3.1	A SSL Version 2 Rollback Attack.....	1016
23.3.2	Man-in-the-Middle Attacks.....	1017
23.3.3	Browser Exploits against SSL/TLS (BEAST).....	1018
23.4	The Record Protocol.....	1018
23.5	SSL/TLS Cryptography.....	1019
23.5.1	Key Generation	1019
23.5.2	Diffie-Hellman (DH) in SSL/TLS	1020
23.5.3	Elliptic Curve Cryptography (ECC) Cipher Suites for TLS.....	1021
23.6	Datagram Transport Layer Security (DTLS).....	1022
23.6.1	The Need to Protect UDP Communication	1022
23.6.2	The Features in DTLS.....	1023
23.6.3	Applications of DTLS.....	1023
23.7	US Government Recommendations	1024
23.8	Extended Validation SSL (EV-SSL)	1025
23.9	Establishing a Certificate Authority (CA).....	1025
23.10	Web Server's Certificate Setup and Client Computer Configuration	1027
23.10.1	Certificate Request and Generation	1027
23.10.2	The Apache Web Server	1030
23.10.3	Microsoft's Internet Information Services (IIS) Server.....	1031
23.11	A Certificate Authority's Self-Signed Root Certificate	1040
23.11.1	The Use of a Self-Signed Root CA Certificate with Windows	1041
23.11.2	The Use of a Self-Signed CA Certificate with Firefox	1043
23.12	Browser Security Configurations	1046
23.13	Concluding Remarks.....	1047
	References.....	1048
	Chapter 23 Problems.....	1049

Chapter 24 Virtual Private Networks for Network Layer Security.....1053

24.1	Network Security Overview.....	1053
24.2	Internet Protocol Security (IPsec)	1053
24.2.1	IPsec Security Services	1053
24.2.2	IPsec Modes.....	1054
24.2.3	Security Association (SA).....	1055
24.2.4	The Encapsulating Security Protocol (ESP)	1056
24.2.5	The Authentication Header (AH)	1058

24.2.6	The Anti-Replay Service	1060
24.3	The Internet Key Exchange (IKE)	1060
24.3.1	The IKE Components and Functions	1061
24.3.2	Distributed Denial of Service (DDoS) Resistance and Cookies	1062
24.3.3	IKEv2 Protocol	1063
24.3.3.1	IKE_SA_INIT and IKE_AUTH Exchanges	1063
24.3.3.2	Authentication (AUTH)	1067
24.3.3.3	The Traffic Selector	1067
24.3.4	The Two Phases of IKE	1067
24.3.5	Generating Keying Material	1069
24.3.6	The Pre-Shared Secret	1069
24.3.7	Extended Authentication (XAUTH)	1069
24.3.8	IKE Diffie-Hellman Groups	1071
24.3.9	Network Address Translation (NAT) Issues in an Authentication Header (AH) and Encapsulating Security Payloads (ESP)	1071
24.4	Data Link Layer VPN Protocols	1072
24.4.1	The Point-to-Point Tunneling Protocol (PPTP) Version 2	1073
24.4.2	The Layer 2 Tunneling Protocol (L2TP)	1073
24.5	VPN Configuration Procedure Examples	1074
24.5.1	The Use of a Pre-shared Secret for Authentication in Windows 7/Vista	1074
24.5.2	Windows 7/Vista Tunnel Using PKI Certificates for Authentication	1082
24.5.3	A VPN Server in Microsoft's Internet Security and Acceleration (ISA) Server	1087
24.5.4	Connecting a Windows 7/Vista to a Cisco VPN Appliance	1092
24.5.5	The Cisco VPN Appliance: Certificate-Based Authentication for a Gateway to Gateway Tunnel	1098
24.6	Concluding Remarks	1103
	References	1106
	Chapter 24 Problems	1106
Chapter 25	Network Access Control and Wireless Network Security	1113
25.1	An Overview of Network Access Control (NAC)	1113
25.1.1	NAC Policies	1113
25.1.2	The Network Access Control/Network Access Protection (NAC/NAP) Client/Agent	1114
25.1.3	The Enforcement Points	1115
25.1.4	The NAC/NAP Server	1115
25.1.5	NAC/NAP Product Examples	1116
25.1.6	Enforcement Point Action	1116
25.1.6.1	Case 1: Using a Dynamic Host Configuration Protocol (DHCP)	1116
25.1.6.2	Case 2: Using a VPN	1117
25.1.6.3	Case 3: Using 802.1X	1117
25.1.7	Authentication and Authorization	1117
25.2	Kerberos	1117
25.2.1	The Key Distribution Center (KDC)	1118
25.2.2	A Single Sign-On Authentication Process	1119
25.2.3	Access Resources	1120
25.2.4	The Use of Realms in a KDC	1123
25.2.5	Security Issues	1123
25.2.6	Implementations	1124
25.3	The Trusted Platform Module (TPM)	1124
25.3.1	An Overview of TPM	1124
25.3.2	The TPM Functional Blocks	1125
25.3.3	The Platform Configuration Register (PCR)	1125
25.3.4	The Endorsement Key (EK)	1126
25.3.5	The Attestation Identity Key (AIK)	1127
25.3.6	The Root of Trust for Storage (RTS) and the TPM Key Hierarchy	1127

25.3.6.1	The Storage Root Key (SRK)	1127
25.3.6.2	Sealing a Key	1127
25.3.6.3	The TPM Key Hierarchy	1128
25.3.6.4	Ownership of the Storage Root Key (SRK) in a TPM	1129
25.3.7	TPM Applications	1129
25.4	Multiple Factor Authentications: Cryptographic Tokens and TPM	1129
25.5	802.1X	1130
25.5.1	The Extensible Authentication Protocol (EAP)	1132
25.5.2	The Remote Authentication Dial-In User Service (RADIUS)	1135
25.6	Enterprise Wireless Network Security Protocols	1138
25.6.1	The Home Network Scenario	1138
25.6.2	The Enterprise Wireless Network Scenario	1138
25.6.3	Roaming and Reassociation	1142
25.6.4	Disassociation and Deauthentication	1143
25.6.5	Remote Access Security Solutions	1144
25.6.6	The Products for NAC/NAP Provided by Cisco and Microsoft	1144
25.7	Concluding Remarks	1146
	References	1146
	Chapter 25 Problems	1147

Chapter 26	Cyber Threats and Their Defense	1153
26.1	Domain Name System (DNS) Protection	1153
26.1.1	A Cache Poisoning Attack	1153
26.1.2	Domain Name Service Security Extensions (DNSSEC)	1157
26.1.2.1	The New Types of Resource Records (RRs) for DNSSEC	1158
26.1.2.2	Authenticated Denial of Existence for a DNS RR	1159
26.1.2.3	A Chain of Trust	1161
26.1.2.4	The Key Signing Key (KSK) and the Zone Signing Key (ZSK)	1163
26.1.2.5	Authentication Chains in DNS Parent and Child Zones	1164
26.1.3	DNSSEC Deployment	1166
26.1.3.1	The US Government Deployment Guidelines	1166
26.1.3.2	The DNSSEC Tools	1167
26.2	Router Security	1168
26.2.1	BGP Vulnerabilities	1168
26.2.2	BGP Security Measures	1169
26.3	Spam/Email Defensive Measures	1170
26.3.1	Email Blacklists	1170
26.3.2	The Sender Policy Framework (SPF)	1170
26.3.3	DomainKey Identified Mail (DKIM)	1170
26.3.4	Secure/Multipurpose Internet Mail Extensions (S/MIME)	1173
26.3.5	Domain-Based Message Authentication, Reporting and Conformance (DMARC)	1173
26.3.6	Certificate Issues for S/MIME and Open Pretty Good Privacy (OpenPGP)	1174
26.3.7	National Institute of Standards and Technology (NIST) SP 800-45 Version 2	1174
26.4	Phishing Defensive Measures	1174
26.4.1	Safe Browsing Tool	1175
26.4.2	Uniform Resource Locator (URL) Filtering	1175
26.4.3	The Obfuscated URL and the Redirection Technique	1181
26.5	Web-Based Attacks	1183
26.5.1	Web Service Protection	1183
26.5.2	Attack Kits	1185
26.5.3	HTTP Response Splitting Attacks	1185
26.5.4	Cross-Site Request Forgery (CSRF or XSRF)	1191
26.5.5	Cross-Site Scripting (XSS) Attacks	1192
26.5.6	Non-persistent XSS Attacks	1192

26.5.7	Persistent XSS Attacks	1196
26.5.8	Document Object Model (DOM) XSS Attacks.....	1198
26.5.9	JavaScript Obfuscation	1200
26.5.10	Asynchronous JavaScript and Extensible Markup Language (AJAX) Security	1201
26.5.11	Clickjacking	1202
26.6	Database Defensive Measures	1202
26.6.1	Structured Query Language (SQL) injection Attacks.....	1202
26.6.2	SQL injection Defense Techniques	1203
26.7	Botnet Attacks and Applicable Defensive Techniques	1204
26.7.1	Botnet Attacks.....	1204
26.7.2	Fast Flux DNS	1205
26.7.3	Well-Known Trojans and Botnets	1207
26.7.4	Distributed Denial of Service (DDoS) Attacks.....	1208
26.7.5	Botnet Control.....	1208
26.7.6	Botnet Defensive Methods That Use Intelligence and a Reputation-Based Filter	1210
26.8	Concluding Remarks.....	1211
	References.....	1211
	Chapter 26 Problems	1213

SECTION 6 — Emerging Technologies

Chapter 27	Network and Information Infrastructure Virtualization.....	1223
27.1	Virtualization Overview	1223
27.2	The Virtualization Architecture	1223
27.2.1	The Computer Hardware/Software Interface	1223
27.2.2	The Process Virtual Machine (VM) and System Virtual Machine (VM)	1224
27.2.3	The Virtual Machine Monitor	1225
27.2.4	Instruction Set Architecture (ISA) Emulation.....	1226
27.2.5	Security Domain Isolation.....	1226
27.3	Virtual Machine Monitor (VMM) Architecture Options	1226
27.3.1	Hosted Virtualization.....	1227
27.3.2	The Hypervisor	1227
27.3.3	Hosted Virtualization-vs.-Hypervisor.....	1228
27.4	CPU Virtualization Techniques	1228
27.4.1	Privileges Resident in the x86 Architecture	1228
27.4.2	CPU Virtualization	1229
27.4.3	Full Virtualization with Binary Translation.....	1229
27.4.4	Para-virtualization	1230
27.4.5	Hardware-Assisted Virtualization.....	1231
27.5	Memory Virtualization.....	1233
27.6	I/O Virtualization	1235
27.6.1	The Input Output Virtual Machine (IOVM) Model.....	1235
27.6.2	Intel Virtualization Technology for Directed I/O	1235
27.7	Server Virtualization.....	1236
27.7.1	Microsoft's Hyper-V.....	1236
27.7.2	Xen Virtualization	1238
27.7.3	VMware's ESX Server Architecture	1239
27.7.4	A Comparison of Xen with VMware.....	1240
27.7.5	The Virtual Appliance	1241
27.8	Virtual Networking.....	1241
27.8.1	Segmentation in Virtual Networking.....	1241
27.8.1.1	The VPN	1242
27.8.1.2	The Overlay Network.....	1244

27.8.2	Isolation/Segmentation in the Network Virtualization Environment	1244
27.8.3	Virtual Switches.....	1245
27.8.4	The VMware VirtualCenter.....	1246
27.8.5	Virtual Machine Migration	1247
27.8.6	VPN Routing and Forwarding (VRFs) Tables	1247
27.8.6.1	VRFs	1249
27.8.6.2	VRF Lite Traffic Routing with Segmentation	1250
27.8.7	Unified Access and Centralized Services	1250
27.9	Data Center Virtualization.....	1252
27.9.1	A Virtualized Data Center Architecture.....	1253
27.9.2	Storage Area Networks (SANs) Virtualization	1254
27.9.3	Fiber Channel (FC) and Fiber Channel over Ethernet (FCoE)	1256
27.9.3.1	Fiber Channel.....	1256
27.9.3.2	Fiber Channel over Ethernet (FCoE)	1257
27.9.4	The Converged Network Adapter (CNA).....	1258
27.9.5	The Cisco Unified Computing System (UCS)	1260
27.10	Cloud Computing.....	1261
27.11	Concluding Remarks.....	1263
	References.....	1263
	Chapter 27 Problems.....	1265

Chapter 28	Unified Communications and Multimedia Protocols.....	1271
28.1	Unified Communications (UC)/Unified Messaging (UM).....	1271
28.2	Internet Protocol Telephony and Public Service Telephone Network Integration	1271
28.2.1	The Media Gateway.....	1272
28.2.2	The Media Gateway Controller (MGC).....	1273
28.2.3	The Media Gateway Control Protocol Standards	1273
28.2.4	Integrated Services.....	1274
28.3	Implementations of Unified Communications	1275
28.3.1	The All-in-One Box	1275
28.3.2	The Microsoft Exchange Server	1275
28.4	The Session Initiation Protocol (SIP).....	1277
28.4.1	SIP Overview	1277
28.4.2	The SIP Standards Groups.....	1277
28.4.3	SIP Services.....	1277
28.4.4	SIP Addressing.....	1278
28.5	The SIP Distributed Architecture	1278
28.5.1	The User Agent (UA).....	1278
28.5.2	Locating a SIP Server.....	1278
28.5.3	The SIP Registrar	1279
28.5.4	Setting Up A Call	1279
28.6	Intelligence in Unified Communications	1286
28.7	The Media in a Session Initiation Protocol Session.....	1286
28.7.1	Quality of Service (QoS) Constraints.....	1287
28.7.2	The Multimedia Protocol Stack.....	1287
28.7.3	A Protocol Comparison (SIP vs. H.323).....	1288
28.8	The Real-Time Protocol (RTP) and Its Packet Format.....	1289
28.8.1	The RTP Header.....	1289
28.8.2	The Payload Type and Sequence Number.....	1289
28.8.3	The Timestamp	1290
28.9	The Real-Time Control Protocol (RTCP) and Quality of Service (QoS).....	1290
28.9.1	The Purpose of RTCP.....	1290
28.9.2	RTCP Packets	1292

28.9.3	The RTCP Extended Report Packet Format.....	1292
28.9.4	Audio/Video Conferencing.....	1293
28.10	Integrated Services in the Internet.....	1293
28.10.1	The Resource ReSerVation Protocol (RSVP).....	1293
28.10.2	RSVP's Role in Voice/Video Communication	1294
28.10.3	The RSVP Flow Descriptor.....	1294
28.10.4	RSVP Protocol Mechanisms.....	1295
28.11	The Real-Time Streaming Protocol (RTSP).....	1297
28.11.1	The Use of RTSP for Streaming Multimedia Control	1297
28.11.2	RTSP Functions	1298
28.11.3	A RTSP Session	1298
28.12	Unified Communication/Unified Messaging Security	1305
28.12.1	The National Institute of Standards and Technology (NIST)'s SP 800-58.....	1305
28.12.2	The International Telecommunications Union's H.323 Security Standard: H.325	1307
28.12.3	Session Initiation Protocol (SIP) Security	1307
28.13	Concluding Remarks.....	1308
	References.....	1309
	Chapter 28 Problems.....	1310
	Glossary of Acronyms	1315
	Index	1325