

Introduction to Computer Networks and Cybersecurity

Introduction to Computer Networks and Cybersecurity

Chwan-Hwa (John) Wu
Auburn University

J. David Irwin
Auburn University



CRC Press

Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2013 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Version Date: 20121210

International Standard Book Number-13: 978-1-4665-7214-0 (eBook - PDF)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>

and the CRC Press Web site at
<http://www.crcpress.com>

*To Professor Erich Kunhardt and all my teachers who inspired me to
devote and share life, as well as be peaceful and patient*

To my loving family

Edie

Geri, Bruno, Andrew and Ryan

John, Julie, John David and Abi

Laura

Contents

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	xliii
Acknowledgments	xlv

An Introduction to Information Networks

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 (FTL)	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	802.11iWi-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 CCMPNonce	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 (NISSIE)	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... <td>1098</td>	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

To the Student

It is difficult to overstate the importance of computer networks and cybersecurity in today's world. They have become such an integral part of our existence that only a moment's reflection is required to delineate the many ways in which they impact essentially every aspect of our lives. For example, from a personal point of view one need only consider the impact that such things as wireless phones, texting, Facebook, Twitter, online billing and the like have had on the way we interact with one another and conduct various aspects of our lives. From a business perspective, it is clear that commerce is an ever growing global enterprise, dominated by digital transactions and conducted at unbelievable speeds via the Internet. In this environment, paper transactions are rapidly disappearing, and thus there is an expanding need for individuals who understand computer networks and their many facets and ramifications. This knowledge is becoming a prerequisite for living and working effectively in today's highly technical environment in which advances in

computer networks and security technology change almost daily.

The field of cybersecurity is composed of the body of technologies, processes and practices designed to protect networks, computers, programs and data from attacks, which result in damage or unauthorized access. The protection of data and systems within networks connected to the Internet is of preeminent importance in today's global communication environment. One need only recall the enormous problems incurred by individuals and corporations when their computer systems are hacked, which may pale in comparison to those encountered by government agencies such as the Department of Defense. The presentation of this area will not only include the standards and practices required to protect the entire information infrastructure but the fundamental concepts of malware and its tactics. In addition, an analysis of the tactics will be examined by illustrating typical attack methods and their associated defense mechanisms.

To the Instructor

This text has been prepared in full view of the current state-of-the-art of computer networks and cybersecurity. The book has been designed as carefully as possible to be a sort of “bible” for this area by uncovering numerous salient features of the various topics and providing clear and detailed explanations of concepts that are difficult to grasp. The book is organized into six parts that essentially walk the reader through this area in a straightforward and logical manner.

The book begins with a presentation of the Internet architecture in the Introduction because that is the normal way in which people first encounter computer networks, and then proceeds to Internet applications and the development of application software in Part 1, which represents the manner in which the Internet is used. This unique presentation sequence thus leverages the subjects with which readers are at least partially familiar. The application layer is used by students on an everyday basis and most of them have experience in setting up a home network using a wireless or Ethernet local area network (LAN). The book then addresses the link and physical layers in Part 2, which makes it easy for students to grasp the concepts surrounding LANs. Layer

2 switches are then extended to layer 3 switches and their attendant design issues.

The network layer including IPv4, IPv6, routers and the various design issues are covered in Part 3. Part 4 then addresses the transport layer, which is the layer of the protocol stack that provides a mechanism for efficient transport. The details surrounding the modern congestion control algorithms available in the newest operating systems (OS’s), together with their pros and cons, are also illustrated in detail.

The analysis of these layers is followed by an in-depth presentation of the numerous aspects of the information infrastructure and computer security in Part 5. The development of Internet applications covered in detail in Part 1 provides the student with the tools necessary to comprehend the vulnerabilities associated with each OS and the typical applications. Therefore, this book enables students to understand the defense methods as well as their weaknesses. Furthermore, this book provides a complete and seamless view of an information infrastructure in which security capabilities are built in rather than treated as an add-on feature. Finally, the emerging technologies that will alter the current state of multimedia communication and datacenter/cloud computing are addressed in Part 6.

Highlights of the Text

- The book is a complete presentation of the area of computer networks and cybersecurity encompassing 29 chapters so that every important aspect of the area is addressed.
- Learning goals for each chapter outline the topics that will be addressed and provide motivation for studying the material. The key concepts are summarized as bridges to new concepts.
- The color presentation is designed to enhance the clarity of the numerous diagrams and complex illustrations in order to improve the presentation.
- Recent and emerging IETF and IEEE standards and drafts are included and illustrated using real-world examples. As an example, the performance of congestion control in both Microsoft Windows and Linux is compared and discussed in detail.
- The design of Layer 2-7 switches is illustrated using the newest Cisco technology in order to facilitate an understanding of the algorithms and their related limitations.
- Complicated operations involving the Internet and cybersecurity are illustrated through step-by-step examples that employ diagrams and screen captures to explain in detail the configuration of critical parameters. The examples contained within each chapter are carefully designed to provide a detailed understanding of the manner in which the topic under discussion can be used. Some of these examples are quite extensive and employ numerous screen shots to enhance the learning process.
- A very complete presentation of Cybersecurity, encompassing 10 chapters, address every aspect of this subject including cryptography, firewalls, IDS/IPS, VPN, SSL, access control, wireless network security, endpoint security, malware defense and web security.
- The newest features of this technology are addressed and include virtualization, datacenter and cloud computing, unified communication, VoIP, and multimedia communication.
- The text contains over 1600 end-of-chapter problems and questions that are designed to test the reader's understanding of the material in each chapter.
- PowerPoint animations for critical operations are provided and have proved to be very useful for teaching and self-paced learning.

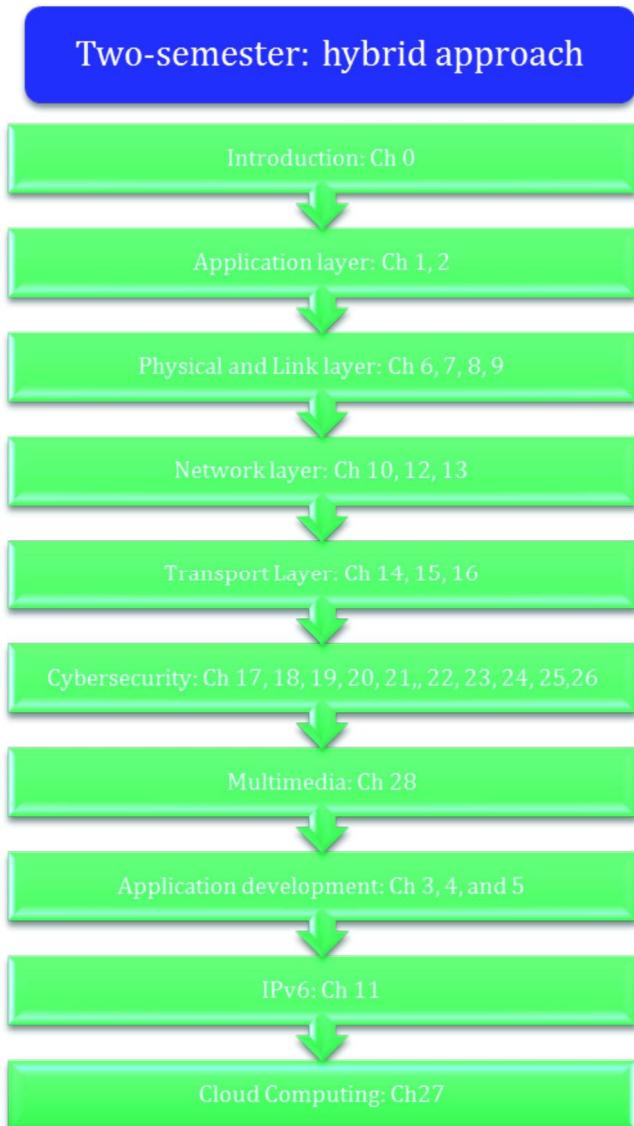
Organization Supports both Hybrid and Other Well-Known Approaches

The book is organized in a manner that provides the instructor with great flexibility in designing the manner in which they address the wide spectrum of topics contained herein. For example,

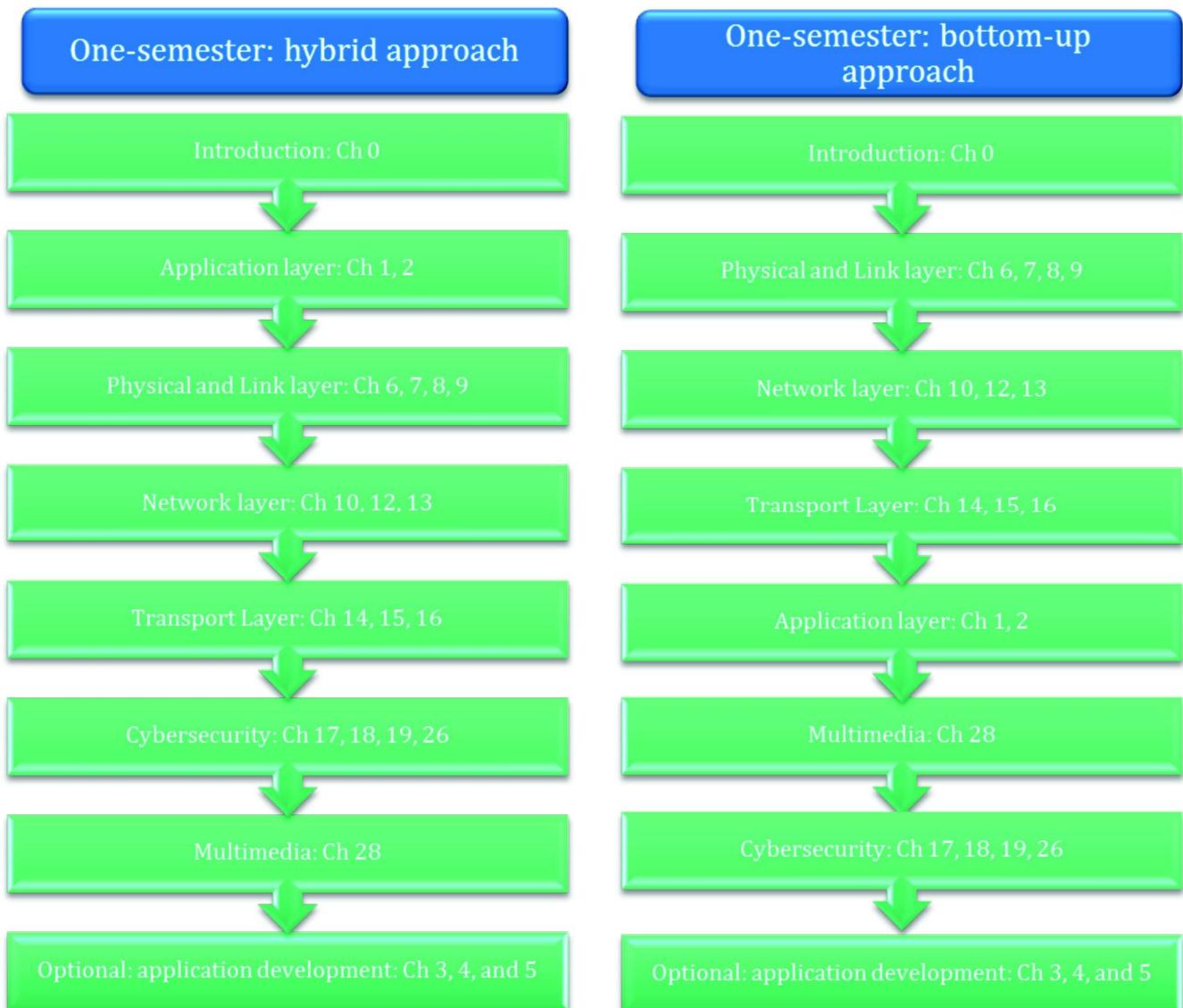
- The entire book can be covered in a two-semester course or selected chapters could be strategically covered in a one-semester course.
- The Introduction through Part 4 along with chapters 17-20 represent a typical one semester course.
- Network and computer security in Part 5, with the inclusion of the Introduction and Part 1 and the optional inclusion of chapters 10 and 14, may be used as a standalone cybersecurity course because the topics contained in these sections provide sufficient detail for comprehending the important vulnerabilities and defensive measures.

The modular approach embedded within the structure of this book permits its use in a wide variety of ways. Some suggested outlines for specific courses are shown in the following figures:

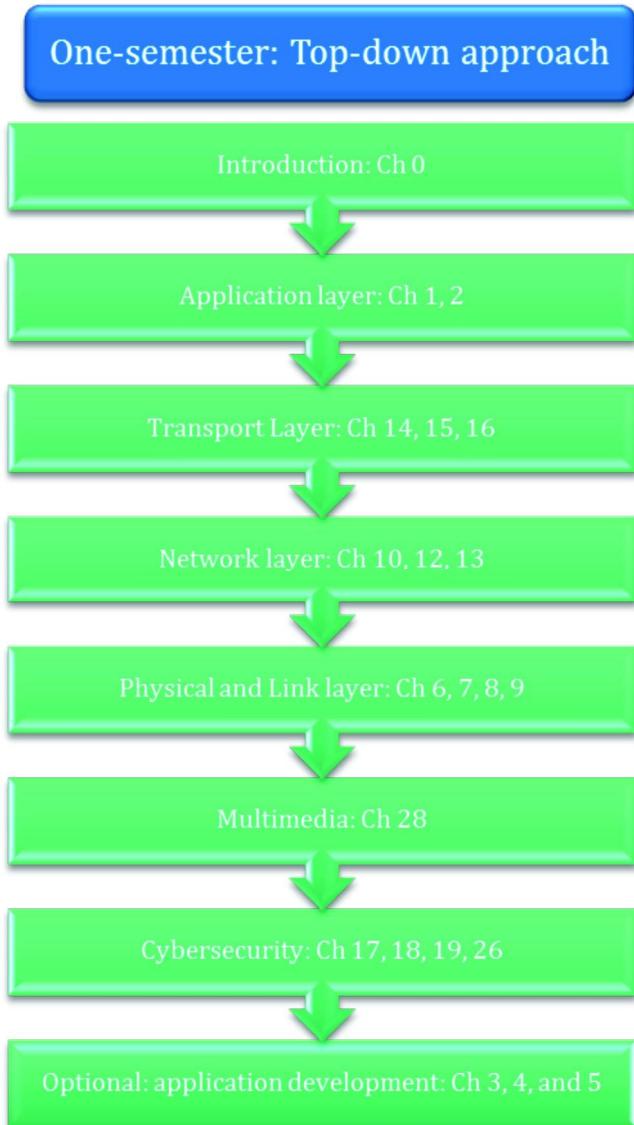
1. A two-semester computer networking course using a hybrid approach:



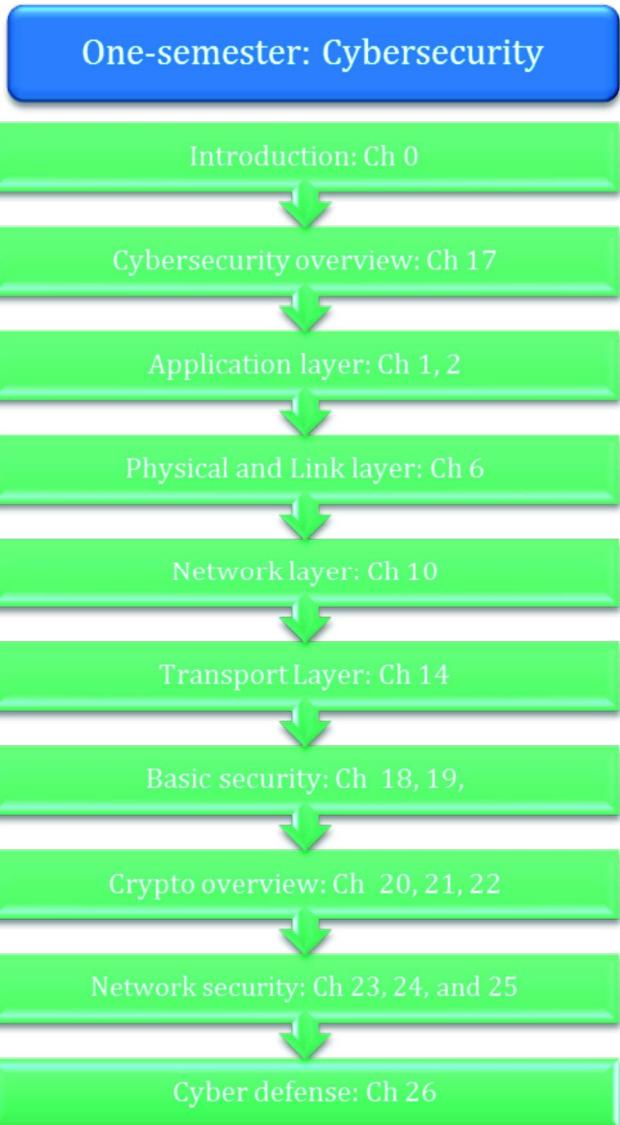
2. A one-semester computer networking course using a hybrid approach:
3. A one-semester computer networking course using a bottom-up approach:



4. A one-semester computer networking course using a top-down approach:



5. A one-semester cybersecurity course:



Pedagogy

In an attempt to provide the best possible learning experience for the student, the text is prepared as an integration of various elements that work in harmony. The learning goals, numerous examples and end-of-chapter problems and questions are all part of a synchronized whole designed for

maximum student understanding. In addition, the details contained within the plethora of figures, diagrams and illustrations support the rapid assimilation of the material. No stone has been left unturned in the presentation in an attempt to help the student grasp the concepts quickly.

Supplements

The following supplements are available for an instructor:

- A solutions manual that provides solutions and answers to all of the end-of-chapter problems and questions
- Professionally prepared PowerPoint lecture slides that are true lecture tools, which in addition to

figures and diagrams, provide the key learning issues for each topic under investigation. The most difficult concepts are illustrated using animations in order to foster a complete and easy grasp of the material. These slides are designed to both amplify and simplify an instructor's lecture material.

Acknowledgments

The authors would like to express their deep appreciation to their colleagues, the staff in the Office of Information Technology at Auburn University, especially Director Bliss Bailey and Manager Mark Wilson, and the numerous students who have contributed to the development of this book over a 16 year period. This book is based upon the

contributions of numerous researchers in this area, and while an effort has been made to reference every contributor to a key concept, some may have been omitted and for this we apologize. In addition, a real effort has been made to make this book error-free. However, if errors are found, they will be corrected as soon as possible on the website.

An Introduction to Information Networks

The learning goals for this chapter are as follows:

- Understand the structure of the worldwide information superhighway, commonly known as the Internet, as well as the various components that are inherent to its operation.
- Explore the numerous ways in which the Internet can be accessed through a variety of networks and transmission media
- Learn the composition of the network core that forms the Internet backbone and the organizations that support its continued development
- Learn the difference between packet switching and circuit switching, as well as the ramifications of each
- Understand the layers of the protocol stack that are used to support the interaction of computers connected to the Internet
- Learn the operations performed by the various layers of the protocol stack and the manner in which they affect the data, traveling in packets
- Obtain an overview of the role of security in the Internet
- Learn the manner in which the Internet has developed throughout its history

I.1 INTRODUCTION

There are three primary goals for this book: (1) understand the many facets and ramifications of the Internet and the wide spectrum of applications that it affords, (2) obtain a thorough grasp of computer networks, the various structures and myriad ways in which they are applied, and finally (3) learn how to apply the latest advances in Internet security in order to protect the networks and the large variety of applications running on them. Every attempt will be made to present the material in an easily understandable fashion. As such, the book will contain a plethora of aids that support the rapid assimilation of the material so that the reader can apply it as quickly as possible.

The goals of this text will be accomplished through a systematic progression of material that supports a rapid learning process. The book will be divided into parts, each of which will consist of several chapters. The different parts and the subjects that will be addressed in each are listed in Table I.1.

In this initial chapter we begin to lay the groundwork for our analysis of the concepts that form the foundation of our study of the Internet and the plethora of ways in which they can be employed. We will provide an overview of the Internet architecture and then zoom in on the access networks with which Internet users are typically familiar, together with the backbone that supports them.

The Internet contains a constant flow of information and this information is contained in packets. The manner in which these packets are switched is fundamental to the operation of the Internet. The Internet protocols, software, hardware, commands and similar functions that support packet switching are modularized in what are called protocol stacks and each layer of the stack performs a specific and vital function. These functions will be discussed in detail as we progress through the book. As will be indicated later, packet switching is a best effort delivery

TABLE I.1 The Six Parts of This Book

Introduction	The Internet architecture, together with the various protocols, protocol layers and service models
Part 1	The most important Internet applications and the methods used to develop them
Part 2	The network edge consisting of hosts, access networks, local area networks (LANs) and the various physical media used in conjunction with the Physical and Link Layers; including multiple layer (layer 2 and layer 3) switches and their design
Part 3	The network core, with all the elements that reside there such as packet/circuit switches, routers and the Internet backbone
Part 4	The transport and management of datagrams with the attendant issues of loss, delay, flow and congestion control
Part 5	Cybersecurity mechanisms and their application
Part 6	Emerging technologies

and suffers from the fact that delay jitter is inherent in its operation. In contrast, circuit switching does not have this drawback and therefore is best for voice and video. Packet switching requires the use of protocols to reserve bandwidth and resources in order to mimic circuit-switching operations.

Finally, a basic overview of various types of malware will be presented together with the various security systems, containing such things as firewalls, intrusion detection systems and the like. Network security is a fundamental issue and plays a vital role in the construction and operation of viable computer networks.

Given this conceptual view of the material to follow, let us now begin our presentation by first providing a global picture of the Internet.

I.2 THE INTERNET ARCHITECTURE

I.2.1 A HIERARCHICAL STRUCTURE

A global view of the Internet architecture is shown in Figure I.1. It is in essence a network of networks with a hierarchical structure and is reminiscent of the plain old telephone service (POTS) in which a call went from your phone to a central office by wire, then perhaps to a regional office by radio and finally cross-country by microwave then back down through a similar path to the receiver. The path through the Internet is similar in which a message from one host, e.g., PC, smartphone, etc. to another traverses a similar path, e.g., from sender to Regional ISP to Global ISP to Regional ISP to receiver. In this case, the figure indicates the path that would be traversed by sending a message from one host, e.g., PC, smartphone, etc. to another. The path into the Internet backbone could be wired, e.g., Digital Subscriber Line (DSL), Hybrid Fiber Coax (HFC), etc. or wireless. The backbone itself consists of global Internet Service Providers (ISPs) and several regional ISPs that are all interconnected to provide a path from sender to receiver. The communication path may typically contain a variety of switches and routers that facilitate and direct the flow of information through the network.

A moment's reflection indicates that the Internet is used to connect billions of hosts throughout the world running a wide spectrum of applications. It is absolutely mindboggling to envision the traffic that exists on this ubiquitous network at any given instant. Hosts, e.g., clients or servers, are connected through communication links and information passes through routers, switches and access points on a pathway of such things as fiber, copper or radio. The communication links, regardless of whether they are wired or wireless, are defined by a transmission rate and bandwidth. Access networks are used to connect a host or Local Area Network (LAN) to the Internet. Routers connect local area networks, generate routing tables and forward packets of data on their path from source to destination. The Internet backbone is basically a group of routers interconnected by optical fiber as well as DNS servers containing infrastructure name servers, such as root Domain Name Servers (DNSs) employed for naming. The remaining com-

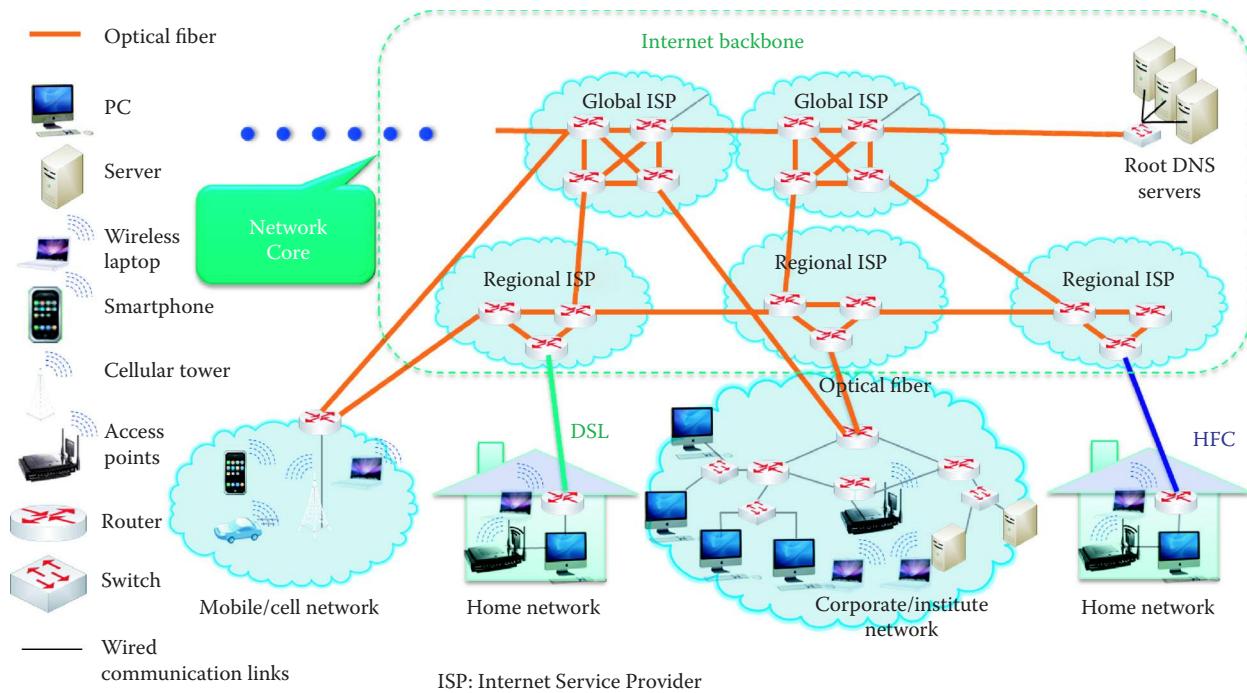


FIGURE I.1 The Internet architecture.

ponents in the Internet structure that lie outside the network core, are simply access networks as indicated in Figure I.1.

As shown in Figure I.1, the Internet is essentially a network of interconnected networks. There is a hierarchical structure in this enormous mass. From a top-down view the Internet consists of a backbone that connects Internet Service Provider (ISP) backbones; the ISP backbones connect the backbones of various organizations; an organization's backbone is used to connect LANs; and finally, the LANs connect the hosts that are running such things as HyperText Transmission Protocol (HTTP) or mail.

I.2.2 INTERNET STANDARDS AND THE INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN)

Given the enormous number of players and the phenomenal amount of information in play at any given time, clearly there must be standards that control the use of the Internet and these standards are listed in what are called Requests For Comments (RFCs) and the organization that oversees this business is the Internet Engineering Task Force (IETF) [1]. All the RFCs can be downloaded free at rfc-editor.org; however, references are provided for them as they are encountered in this text.

As indicated in Figure I.1, the network edge (or access networks) consists of hosts, i.e., servers and clients, and the various applications that are running in the network, e.g., HTTP, mail and the like as well as access links. The network core is composed of edge routers that connect an organization/ISP to the Internet, and these routers are typically interconnected with fiber. The access networks that are present may be either wired, or wireless, communication links.

The internal structure of the Internet Corporation for Assigned Names and Numbers (ICANN) [2] is shown in Figure I.2. Of particular interest is the Internet Engineering Task Force (IETF), which is the standards body for the organization and controls the standards under which the development of the Internet proceeds. The funding for ICANN is obtained through the collection of registration fees from the various domains, which include .com, .net, .uk, .cn, etc. These fees support ICANN in its efforts to provide various services including a DNS database for all Internet users.

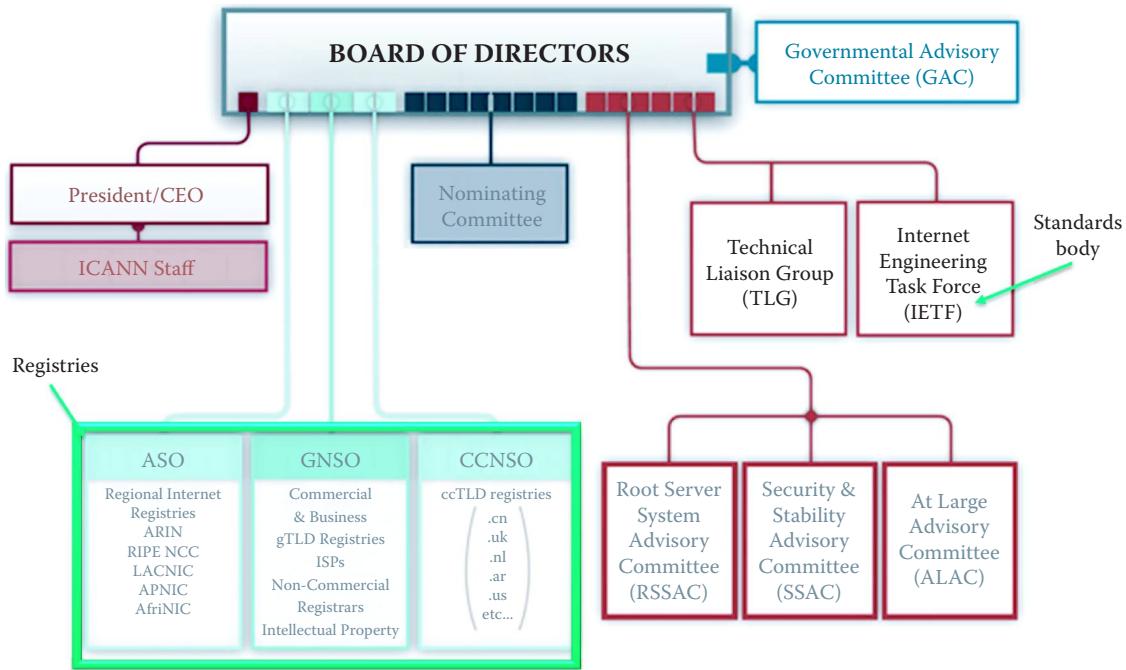


FIGURE I.2 The Internet Corporation for Assigned Names and Numbers (ICANN).

I.3 ACCESS NETWORKS

Given the massive configuration of the Internet, let us now examine the manner in which various hosts of any kind connect into this structure. An individual, home network or business network, e.g., local area network (LAN) can be considered a small network or subnet. The Internet uses a gateway, also known as an edge router, as the vehicle for entrance into the hierarchical network. Such an arrangement is shown in Figure I.3.

The Internet has become an integral part of most people's lives, and therefore households everywhere have Internet access. The point-to-point access between a residence and an ISP can be obtained in a variety of ways. For example, residential Internet access can be obtained via a dialup modem, a digital subscriber line (DSL), a cable modem, fiber in the loop, broadband over a power line, and broadband wireless such as a Wireless Metropolitan Area Network (WiMAX) or satellite. Let's examine each of these in some detail.

A dialup connection to the Internet will operate at a speed of up to 56 Kbps. If a poor quality line is involved, the speed may be less and surfing the Internet can be a slow and tedious process. If compression is employed the speed may reach 320 Kbps. However, surfing the Internet and talking on the phone at the same time are not allowed.

I.3.1 DIGITAL SUBSCRIBER LINES (DSL)

The digital subscriber line is defined by a dedicated physical line between a residential telephone and the telephone company's central office. This line is supplied by the telephone company and is not shared with anyone else. The DSL line speed is controlled by the distance between the phone and the central office, or the telephone company's Digital Subscriber Line Access Multiplexer (DSLAM). The standard for this technology in the U.S. is defined by ANSI T1.413-1998 Issue 2 [3], where ANSI is the American National Standards Institute. This standard defines the upstream rate to be a maximum of 1 Mbps, typically less than 256 Kbps, and the downstream rate to be a maximum of 8 Mbps, typically less than 6 M bps. Frequency Division Multiplexing (FDM) can be used with this technology, and in this mode one can surf the Internet and use the phone at the same time. In this mode, the upstream rate is 4 KHz to 50 KHz, the downstream rate is 50 KHz to 1 MHz, while the ordinary telephone employs the range between 0 KHz to 4 KHz.

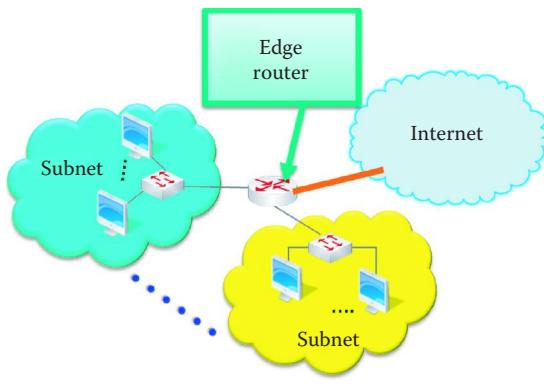


FIGURE I.3 A router with subnet.

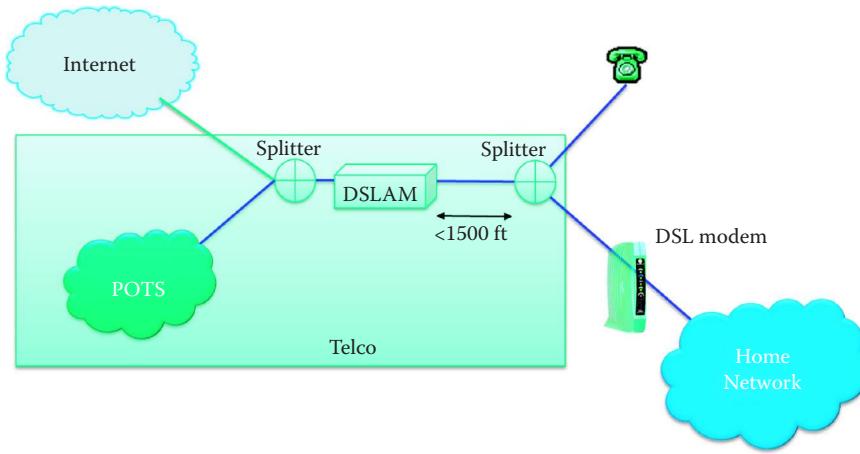


FIGURE I.4 The Digital Subscriber Line's (DSL) function in the network.

The network, shown in Figure I.4, illustrates some of the various components typically connected to the telephone company. The telephone company contains the Plain Old Telephone Service (POTS), the DSLAM and the splitters employed to connect the outside components such as the Internet, with a telephone and/or home network that connects through the DSL modem. It is important to note that the splitters must be less than 1500 feet from the DSLAM.

I.3.2 HYBRID FIBER COAX (HFC)

Most people are familiar with another technology that is employed for residential Internet access and that is the cable modem. The present technology is hybrid fiber coax (HFC), shown in Figure I.5, in which fiber is extended into a neighborhood and then coax is used to connect individual homes. In this manner, a number of homes share a coax cable in order to obtain Internet access. This technology deployed by the TV cable companies, uses fiber to the neighborhood and coax to the home in order to connect to an ISP router. This HFC technology is deployed by cable companies that supply TV, and this network of coax and fiber connects homes to the ISP router. The standards for this service are called the Data Over Cable Service Interface Specification (DOCSIS) and are developed by Cable Labs. The newest versions are DOCSIS 2.0 and 3.0 [4]. In North America, DOCSIS 2.0 provides for an asymmetric rate of up to 38 Mbps downstream and 27 Mbps upstream, and DOCSIS 3.0 provides for 304 Mbps downstream and 108 Mbps upstream when grouping multiple DOCSIS 2.0 channels. The coax signal downstream in a 6 MHz channel uses a frequency range from 54 to 108 MHz at the lower end and up to 300 MHz, or as much as 1002 MHz, on the upper end. The maximum number of channels is 158 and they are shared by

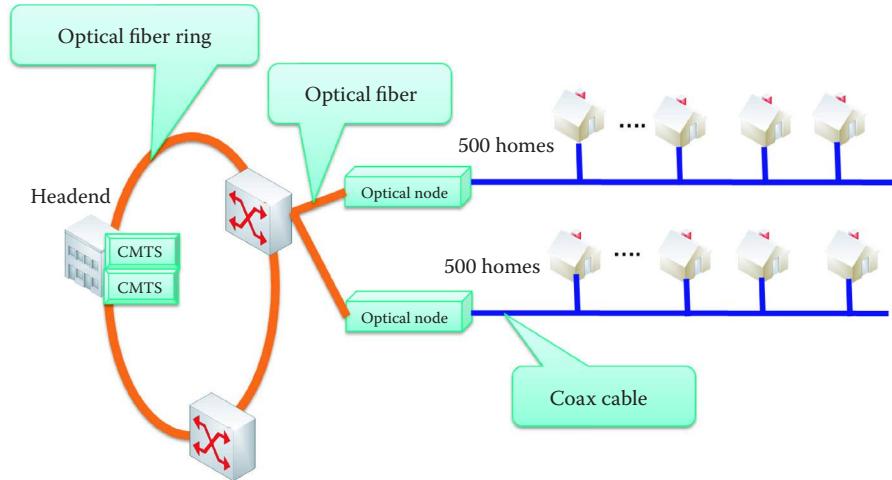


FIGURE I.5 A hybrid fiber coax network.

the neighborhood. In addition, there is a reverse/return path in the frequency range that extends from 5 MHz to either 42 or 85 MHz. More typical rate numbers in this environment are 5 Mbps downstream and 256 Kbps upstream.

Figure I.5 illustrates a typical HFC cable network. The headend is the generation/coordination point and it exists on the optical fiber ring. The headend also contains the Cable Modem Termination System (CMTS), which is equivalent to a DSLAM. As the network grows, the CMTS can be upgraded with more downstream and upstream ports. If the HFC network is very large, the CMTS can be grouped into hubs to support a more efficient management of the system. Some users have attempted to override the bandwidth cap and gain access to the full bandwidth of the system, often as much as 38 Mbps, by uploading their own configuration file to the cable modem. This process, called uncapping, is almost always a violation of the Terms of Service agreement. As a result, there is the risk of being dropped from the ISP service. At the optical node, the conversion between light pulses and electrons is done. As indicated, all transmission for some set of homes takes place on the same coax cable.

I.3.3 FIBER IN THE LOOP (FITL)

The ideal manner in which to employ optical fiber is to run it directly from the telephone company's central office to the home, and in this case this Fiber in the Loop (FITL) replaces the POTS, which is composed of copper. A remote Serving Area Interface (SAI) is located in the neighborhood, and an Optical Network Unit (ONU) is located at either the customer's home or premises, i.e., Fiber to the Home (FTTH) or Fiber to the Premises (FTTP). The fiber to the premises is a point-to-multipoint Passive Optical Network (PON). Later versions of this technology are Gigabit PON and Ethernet PON. In early 2008, Verizon deployed Gigabit PON (GPON), and it expanded to more than 800 thousand lines by mid-year. The GPON standard is ITU-T G.984 [5]. Ethernet PON (EPON) enables service providers to deliver up to 100 Mbps full-duplex over a single-mode optical fiber to the premises. The EPON standard is IEEE 802.3ah [6]. China was expected to deploy EPON to approximately 20 million subscribers by the end of 2008.

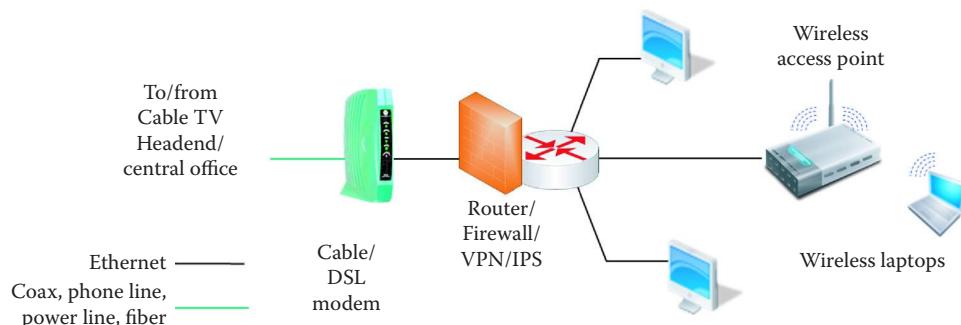
I.3.4 BROADBAND OVER POWER LINES (BPL) AND HOMEPLUG

Broadband over Power Lines (BPL) is an interesting technology since every home has a power line connection. The power-line Internet, aka Powerband, provides broadband Internet access through ordinary power lines using a BPL modem.

The standard for this technology is IEEE P1901 [7], which was developed in collaboration with the HomePlug Alliance. It includes residential access to the Internet using BPL, typically at

TABLE I.2 Various HomePlug Standards

Standard	Peak data rate
HomePlug Access BPL	A peak data rate of a few Mbps for Internet access
HomePlug 1.0	A peak data rate of 14 Mbps at the physical layer
HomePlug AV	A peak data rate of 200 Mbps at the physical layer
HomePlug AV2	A peak data rate of 600 Mbps at the physical layer
HomePlugGreen PHY	A peak data rate of 10 Mbps at the physical layer for smart meters and smaller appliances with a 256 Kbps minimum effective throughput

**FIGURE I.6** A home network configuration.

10 Mbps, as well as HomePlug AV (HPAV) for an in-home LAN to support Voice over Internet Protocol (VoIP) and video. The HomePlug standards are listed in Table I.2.

This HomePlug AV technology specifies speeds up to 600 Mbps at the physical layer and 500 Mbps at the application layer. Products based on HomePlug AV2 are currently available. Typical rates are much lower, but the upstream and downstream rates are the same. HomePlug AV provides a powerline network with a peak rate of 200 Mbps for video, audio and data. HomePlug AV employs BPL Coexistence through one of two methods: *Coexistence of Services*, and *Coexistence of Technologies*. The *Coexistence of Services* method uses time division multiplexing (TDM) with beacon signaling and messaging to coordinate the in-home and BPL networks, while the *Coexistence of Technologies* method uses frequency division multiplexing (FDM) to permit different technologies to coexist. It is worth noting that the city of Manassas Virginia was the first to deploy a wide-scale BPL service in the U.S in October 2005. They use the MainNet BPL technology and offer a 10 Mbps service for under \$30 U.S. per month to approximately 35,000 residents.

The IEEE P1901.2 standard (aka HomePlugGreen PHY) was developed for utility companies and makers of smart meters to support their ability to send data from the smart grid through existing electrical wiring. It is a new narrow band powerline communications standard with a low data rate. Power-line technology is also a viable means of supplying in-vehicle network communication of data, voice, music and video by digital means over a direct current (dc) power line.

I.3.5 A TYPICAL HOME NETWORK

A typical home network may be represented by the configuration shown in Figure I.6. As indicated, the cable TV headend or telephone company central office is connected to the home network by a modem. Powerline or fiber is also applicable in this environment. The router shown in the figure does not perform a routing function, such as, generating a routing table, but is referred to as a router because it performs the network address translation, e.g., it may provide the address 192.168.y.x, as a typical example of a given IP address from the ISP. The router may contain a firewall/virtual private network (VPN) or intrusion prevention system (IPS). The router may also contain a built-in Ethernet switch and a wireless access point.

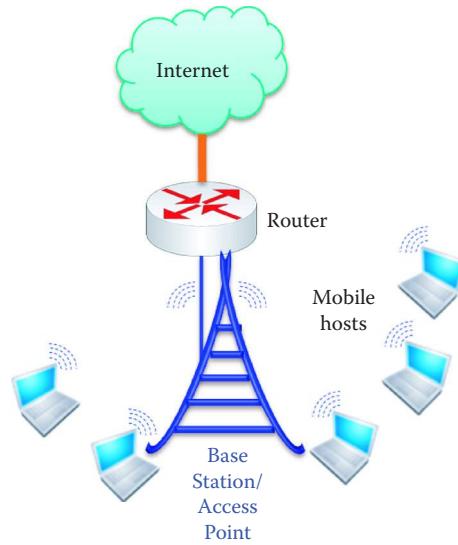


FIGURE I.7 Wireless access networks.

I.3.6 LOCAL AREA NETWORKS (LAN)

As was indicated in Figure I.3, a LAN or subnet containing various hosts is connected to the Internet via an edge router. If the subnet is in an Ethernet LAN, hosts are connected to an Ethernet switch and operate at speeds of 10 Mbps, 100 Mbps, 1 Gbps or 10 Gbps. Each LAN must connect to a router interface in order to connect to the Internet. In the Internet community, the router interface is also called a gateway, and an organization typically uses an asynchronous transfer mode (ATM) leased line via an optical fiber link to connect to an ISP. This router at the edge, i.e., edge router, began as simply a representation for a switch with Ethernet on one end and an ATM line on the other, and thus it is essentially a router connected to a cloud of ATM switches.

I.3.7 WIRELESS ACCESS NETWORKS

As illustrated in Figure I.6 and again in Figure I.7, mobile hosts are connected to the router via an access point or base station. The wireless LANs (WLANs) are governed by the standards 802.11a/b/g (WiFi) [8] operating at between 11 and 54 Mbps, or 802.11n [9] with speeds greater than 100 Mbps. The new standards, 802.11ac and 802.11ad, will operate at rates of up to 1.7 and 7 Gbps, respectively. The wide-area wireless access, provided by the telephone company, has a speed of approximately 1 Mbps over the cellular system, or one can use WiMAX [10] at speeds of 10 Mbps or greater, over a wide area. In free space the signals propagate as radio waves. In this environment, the transmission vehicles are wireless LANs (802.11), 3G wireless (HSDPA and EV-DO) [11][12][13][14], WiMAX and satellite., where HSDPA is High-Speed Downlink Packet Access and EV-DO is Evolution-Data Optimized.

I.3.8 THE TRANSMISSION MEDIA

The transmission media may be physical wires (transmission lines) or free space. The physical links used between the transmitter and receiver are typically a twisted pair (Ethernet 100BASET or 1000BASET), coax (10BASE2) or fiber (100BASEF, 1000BASEX, or 10GBASE-R) [6]. The radio wave propagated in free space suffers more loss than wired transmission media, while fiber is the best medium in terms of data rate and transmission distance.

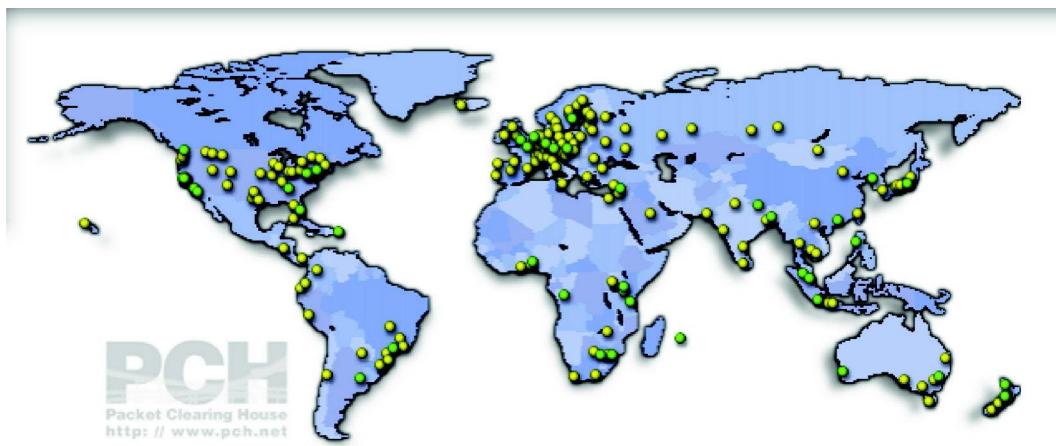


FIGURE I.8 The Internet eXchange points throughout the world. (Courtesy of <https://prefix.pch.net/applications/ixpdir/>)

I.4 THE NETWORK CORE

Having now examined the means employed to access the Internet, let us now turn our attention to the structure that comprises the heart of the Internet, i.e., the network core as illustrated in Figure I.1. The core of the Internet is composed of a set of routers and fiber links, shown in Figure I.1 in orange. The routers work together to determine the most efficient routing path for a packet from source to destination. A distributed algorithm is used that provides the flexibility to adapt to changing conditions, and routing tables are generated and maintained in real time. The ISPs that form the network core interconnect multiple continents. These ISPs are Global ISPs, also known as Tier-1 ISPs, whereas the Regional ISPs are known as Tier-2 ISPs.

I.4.1 INTERNET EXCHANGE POINTS (IXPS)

The Tier-1 ISPs that form the Internet backbone are Verizon, AT&T, Qwest, Level 3 Communications, and the like. These Tier-1 ISPs are interconnected at various access points called Internet eXchange Points (IXPs). There are approximately 300 IXPs in 86 countries. The U.S. has about 88 of them. At these various ISP locations, under bilateral and multilateral agreements, the major ISPs agree to accept traffic from one another and route it to its downstream destination without charge. In addition, the major ISPs also have private agreements between one another in locations where two or more carriers have switching points in close proximity.

Figure I.8 provides a global view of the Internet eXchange Points. The source for this figure is [15]. Clearly, these points have a direct relationship to the population centers of the world.

The IXP typically consists of a centralized Ethernet switching fabric, together with all the supporting infrastructure that permits companies to interconnect with one another at anywhere from 1 Gbps to multiples of 10 Gbps. Because of its strategic importance in the Internet, the ISP carefully monitors all mission critical systems, has a sophisticated fire protection system, and is equipped with ac and dc power, a generator and an uninterruptable power supply. As indicated, these facilities are located throughout the United States and one of them is located at 56 Marietta St, NW, Atlanta, GA 30303.

I.4.2 TIER-1 INTERNET SERVICE PROVIDERS (ISPS)

Tier-1 ISPs typically have backbones that cover the globe. For example, the Verizon backbone is shown in Figure I.9. It is a graphic picture of the manner in which the Internet has developed worldwide. The source for this figure is [16]. Note the relationship between this network and the population centers of the world.

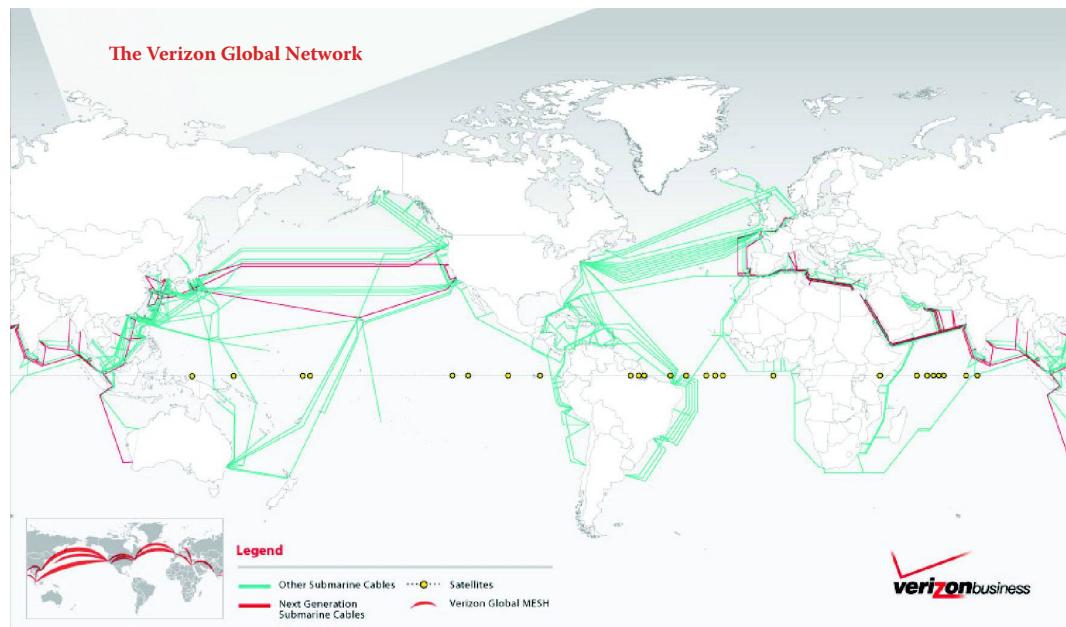


FIGURE I.9 Verizon backbone. (Courtesy of Verizon.)

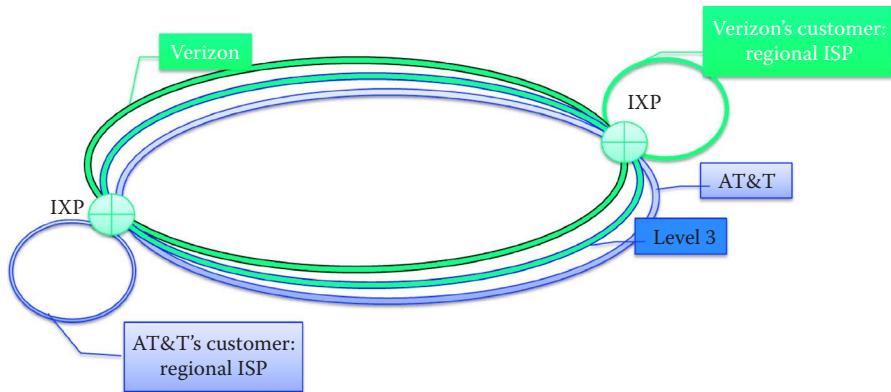


FIGURE I.10 The regional ISP structure.

The manner in which the various regional ISPs connect their customers to the network through an IXP is shown in Figure I.10. In this manner the regional ISPs work in conjunction with other Tier-1 and Tier-2 ISPs to provide the service required by their customer base.

I.4.3 THE INTERNET2 NETWORK

There is a U.S. centric nationwide network that is unique in its mission. This network, known as the Internet2 network [17], shown in Figure I.11, provides the education and research community within the U.S. with a dynamic, innovative and cost-effective hybrid optical and/or packet network. Its backbone network, operating at 10 Gbps and known as the Abilene network, is shown in Figure I.12. In contrast to the Internet2 backbone, which only covers major cities, the network itself covers the entire nation. Internet2 supports research facilities throughout the nation in their development of advanced Internet applications, as well as their enhancement through the deployment of vanguard services, such as IPv6. This IP network, is built over a carrier-class infrastructure, and provides support for the most advanced networking protocols. It is a dynamic circuit network that enables short-term or point-to-point circuits that are established in response to an application in the standard synchronous optical network bandwidth at increments of up to

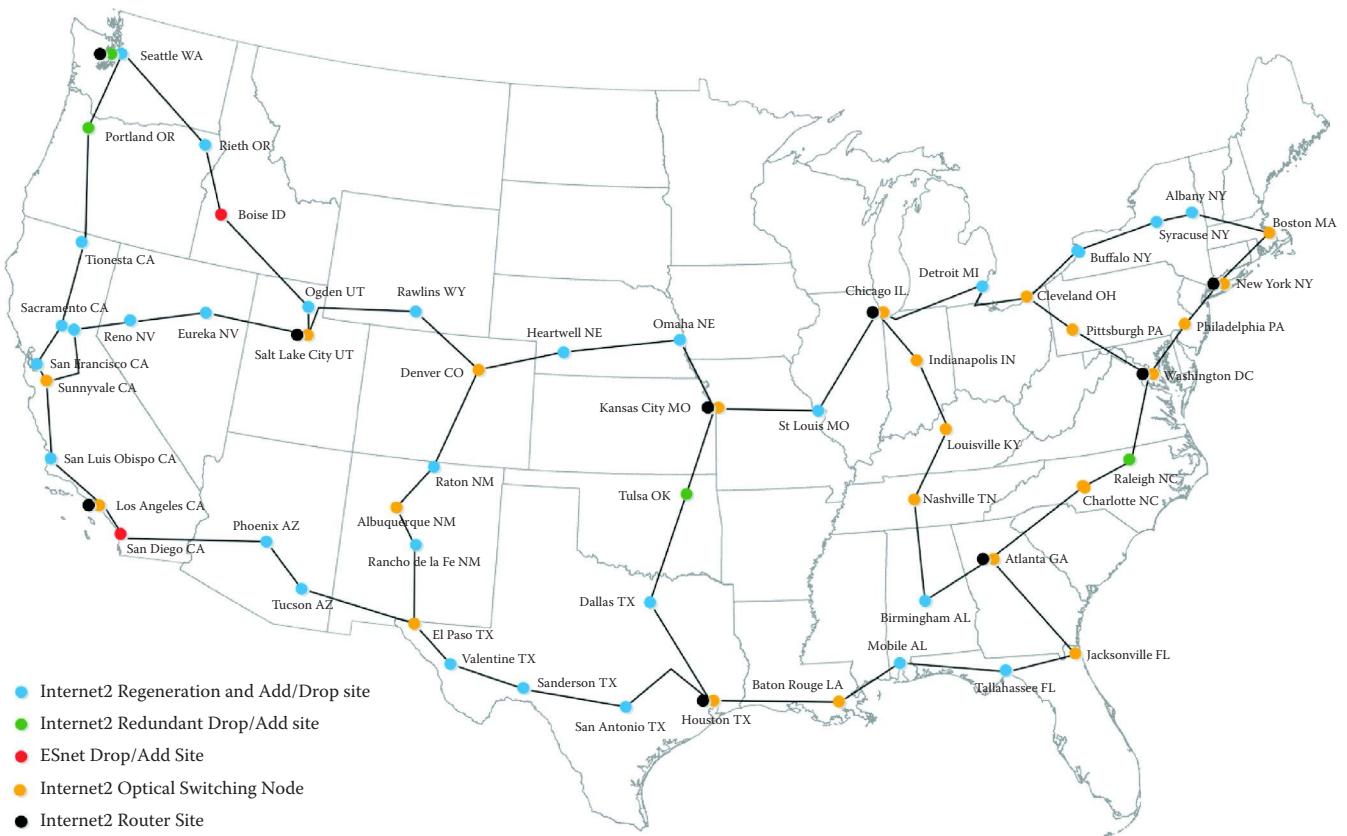


FIGURE I.11 The Internet2 network.

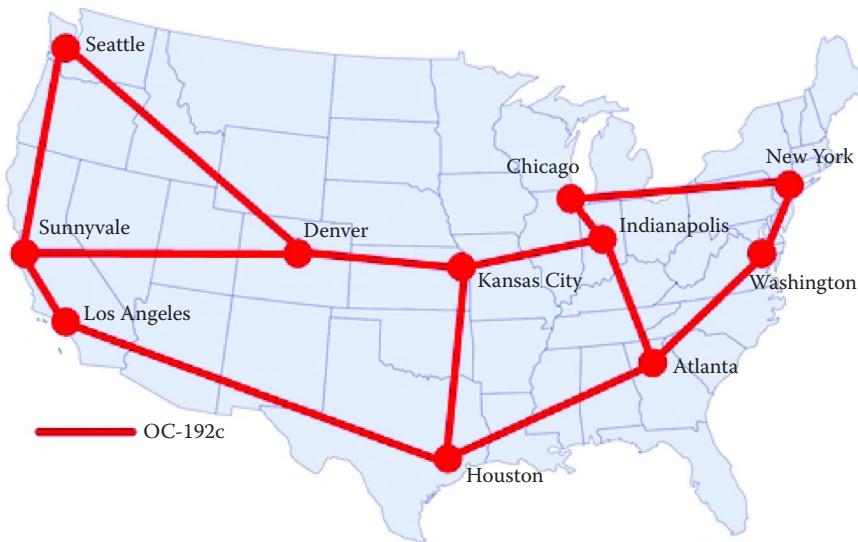


FIGURE I.12 The Internet2 backbone.

10 Gbps. Static networks are provided by either the Internet2-controlled optical infrastructure or the Level 3 Communications network (an ISP network).

Internet2 announced on 11/15/2010 that it will begin deployment of a new, nationwide 100 Gigabit per second (Gbps) Ethernet backbone network using 100 Gbps core routers. The complete deployment of this new network is scheduled for 2013. Internet2 has a long-term partnership with the router/switch vendor, Juniper Networks.

I.5 CIRCUIT SWITCHING VS. PACKET SWITCHING

I.5.1 CIRCUIT SWITCHING

The information organized within the protocols must be switched as it travels from source to destination. The switching function is performed in one of two ways: *Packet switching* or *circuit switching*. In the former case, the header contains the source and destination IP addresses, and the delivery is best effort. Thus, packets may be lost, corrupted or may be delivered out of order. Circuit switching on the other hand uses a dedicated circuit for each call, e.g., when using a dial-up modem, or a virtual circuit, examples of which are the classic IP over Asynchronous Transmission Mode (ATM) or leased lines.

Another way of looking at the difference between circuit switching and packet switching is the following scenario. Consider the difference between a paying airline customer and an airline employee who flies for free. The customer who pays for a round-trip ticket and obtains a reserved seat is analogous to circuit switching, while packet switching is analogous to the airline employee who uses free, open tickets to fly but the seats are not reserved and boarding is only permitted if the seats are available just prior to takeoff.

With circuit switching the end-to-end resources are reserved for the connection, i.e., the connection is established before any data is transferred. Given the dedicated link bandwidth and switch circuit capacity, the performance is guaranteed. Because the resources are dedicated, there is no sharing. So, if Frequency Division Multiplexing (FDM) or Time Division Multiplexing (TDM) is used, a portion of the end-to-end resource will be idle if one of the hosts is not active. Call setup and teardown are required when either modems or constant bit rate (CBR) ATM on leased lines, are used.

Example I.1: The Transmission Delays Inherent in Circuit Switching

For a moment, let's quantify some of the details of circuit switching using an example. Assume that Host A will send 1,000,000 bits to Host B over a switched network. Further assume that the links are T1 lines operating at 1.536 Mbps, each link uses TDM with 24 channels or slots, a single channel is to be used in transmission and 500 milliseconds is needed to establish the end-to-end circuit. Given this data, the time required is

$$[1M/(1.536M/24)] + 500 = 16.125 \text{ seconds.}$$

I.5.2 A COMPARISON OF CIRCUIT SWITCHING WITH PACKET SWITCHING USING STATISTICAL MULTIPLEXING

It is both interesting and instructive to understand the inherent advantages and disadvantages that attend circuit switching and packet switching. In the former case, the advantage is fixed delay jitter, while its main disadvantage is the fact that it cannot fully utilize the bandwidth and network resources that are assigned when a circuit is established. In contrast to circuit switching, packet switching with the use of statistical multiplexing allows heavier traffic for data of a bursty nature than circuit switching over the same links. Under normal demand, packet switching can serve more users, who can only produce bursty traffic, through the use of statistical multiplexing by fully utilizing the bandwidth and network resources that are available. Of course, packet switching is not without its problems either, e.g., packets may be lost and congestion will occur when the bandwidth and network resources are not able to meet the demand. In addition, variable delay jitter accompanies packet switching and thus it is not suitable for voice and video. In order to provide reliable video/voice transport, additional overhead must be paid by packet switch protocols in order to match circuit switching's performance.

Statistical multiplexing (SM), shown in Figure I.13, is an efficient method for packet switching. As indicated, packets from hosts A and B are generated randomly, and if there is no fixed priority, then packets are treated equally based on their order of arrival. Router 1's T1 link bandwidth

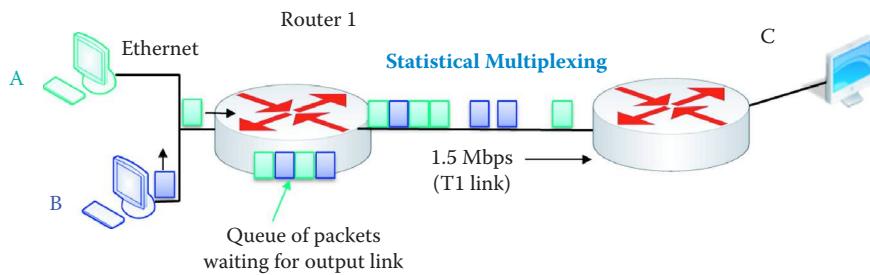


FIGURE I.13 Illustration of statistical multiplexing.

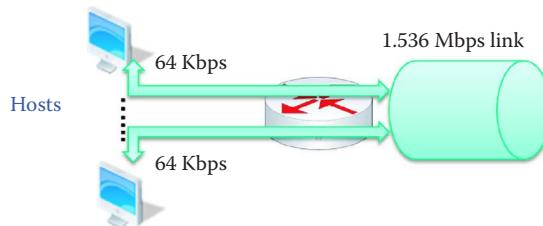


FIGURE I.14 Multiple hosts using a standard T1 link.

is shared by packets from both hosts A and B, and if the T1 link is overwhelmed with packets, they are queued up in the router and await time slots on the output link. This technique stands in sharp contrast to both FDM and TDM with dedicated slots and thus no resource contention.

Example I.2: A Comparison of Packet Switching vs. Circuit Switching Using a T1 Link

As a simple example comparison of packet switching versus circuit switching, consider the network in Figure I.14 where several hosts share a T1 (DS1) link. The T1 link to the Internet is 1.536 Mbps and a standard T1 circuit can be divided into 24 8-bit narrow-band DS0 circuits, sampled 8000 times per second and operating at 64 Kbps when active. In a switching circuit environment, a user is typically assigned a DS0 circuit. If it is assumed that the hosts are active on average 20% of the time, then 24 hosts can be circuit-switched since a fixed bandwidth is assigned to each host in spite of the fact that they may exhibit long inactive periods. In reality, when a user is surfing the web, it is impossible to keep a DS0 circuit active 100% of the time and inactive periods are a waste of resources.

However, with packet switching (or SM) approximately 120 hosts (24 x 5) or more can statistically be accommodated. SM is based on the average use of bandwidth in determining the number of hosts. No fixed bandwidth is assigned to a host and when a host has inactive periods, other hosts can make effective use of the bandwidth. In this latter case, some hosts may encounter contention and long delays, and thus while packet switching may serve more hosts it does so with some uncertainty due to statistical multiplexing.

Clearly, both packet switching and circuit switching possess some advantages and carry with them some attendant disadvantages. Packet switching is the best technique for bursty data. It provides a best effort delivery and better resource sharing. However, there is the problem of network congestion caused by packet delays in the queue of the routers and packet loss due to queue overflow. Therefore, packet-switching-based protocols carry overhead in order to provide reliable data transfer as well as congestion and flow control. On the other hand, circuit switching is best for voice and video. There is a guaranteed bandwidth as well as guarantees for timing, latency and latency jitter.

Packet switching is widely used for its flexibility and efficiency. For example, HyperTransport, which is an open-standard technology, is being used by Advanced Micro Devices to replace the Front-Side Bus in its multiprocessor interconnect, which includes the graphic processing unit

(GPU) located in the same die as the CPU. Intel's counterpart is called the QuickPath Interconnect. Other examples include Serial Advanced Technology Attachment (SATA), which is a computer bus interface for connecting to hard disk drives, Peripheral Component Interconnect Express bus (PCI Express bus), which is a motherboard-level interconnect to link motherboard-mounted peripheral cards, e.g., a graphics card, and USB.

I.6 PACKET SWITCHING DELAYS AND CONGESTION

I.6.1 PACKET SWITCHING DELAYS

A delay that is inherent in packet switching is the transmission delay. This delay is a direct result of the finite bandwidth of the link employed. The following example illustrates the effect of this delay.

Example I.3: The Transmission Delay Inherent in Packet Switching

With reference to Figure I.15, assume a packet length of L bits and a link rate of R bps. If the link between Router 1 and Router 2 is available, a transmission delay of L/R seconds is encountered in sending one packet over this link. Assuming store and forward routing, i.e., the entire packet must arrive at one router interface before it can be transmitted over the next link, the host-to-host transmission delay = $3L/R$; there will also be propagation and other delays. For example, if $L = 1000$ Mbits, $R = 100$ Mbps, e.g., Ethernet, then the transmission delay per link is 10 seconds. The total transmission delay is 30 seconds.

As indicated earlier, packets encounter both loss and delays as illustrated in Figure I.16. When the incoming packets rate exceeds the link data rate, the incoming packets must be queued in the buffer, and there is a resultant queuing delay. In addition, if there is no free space in the buffer the incoming packets are dropped, creating a loss.

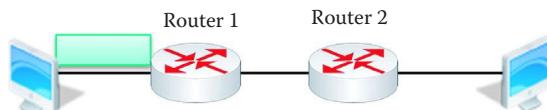


FIGURE I.15 The network used to examine packet transmission latency.

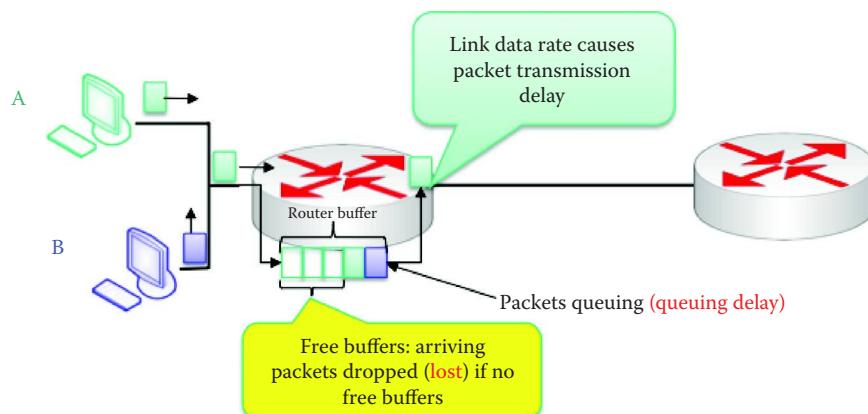


FIGURE I.16 Network illustrating packet loss and delay.

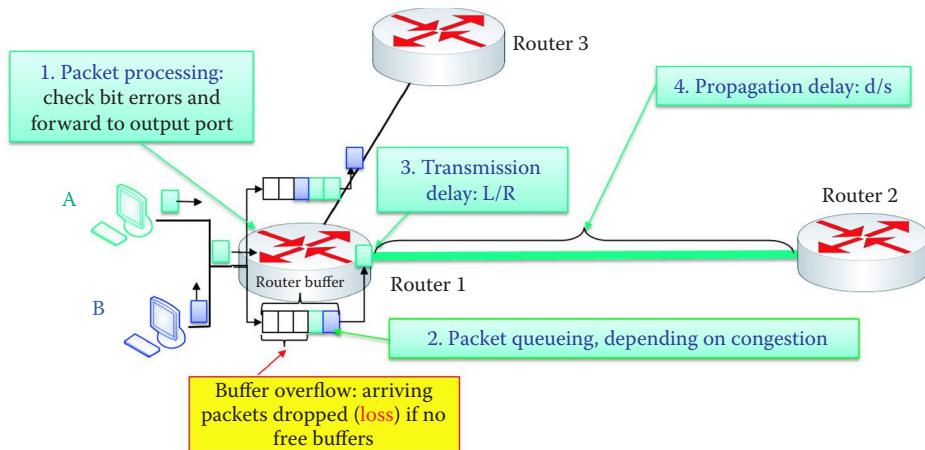


FIGURE I.17 Network used to identify packet delay factors.

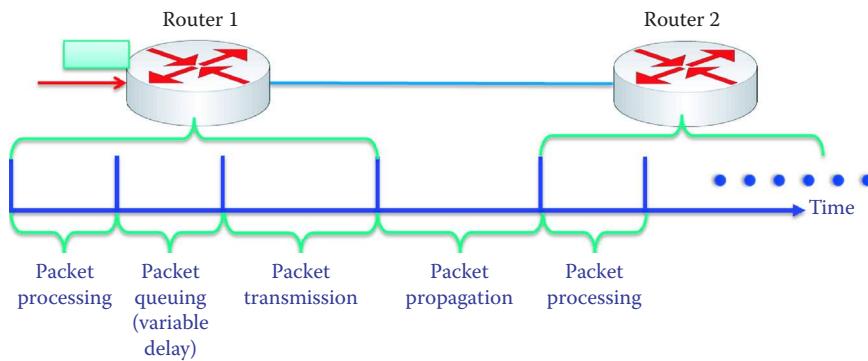


FIGURE I.18 The packet delays for a packet flowing through a router; the queuing delay is variable and depends on the availability of the output link and the other packets in the queue.

There are four delay factors that are encountered with packet switching, and they are labeled in Figure I.17. Thus, the total delay is the sum total of the individual delays. These individual delays are (1) the processing delay at the router input caused by packet processing in which bit errors are checked and the packet is forwarded through the router or into the buffer, (2) the queuing delay caused by packet queuing when congestion is present, (3) the transmission delay (L/R), and (4) the propagation delay (d/s) down the link, where d is the distance down the link and s is the propagation speed. Another view of the packet delays for a packet flowing through a router is shown in Figure I.18. All delays except queuing delay are almost a constant in a router. The queuing delay depends on the availability of the output link and the other packets in the queue.

Packets traveling in the Internet pass through numerous routers, and the routers in today's Internet backbone typically employ multi-threaded network processors or application-specific integrated circuits (ASICs) to perform the forwarding process. Each router processes multiple packets in a parallel fashion and it is impossible to ensure that the output packets have the same order as the input packets in this parallel processing environment. Hence packet switching cannot maintain packet order when a message contains multiple packets.

I.6.2 PACKET LOSS AND DELAY

A primary cause of packet loss is the finite size of the buffer involved. This loss, coupled with the delays outlined earlier, forces the sender to retransmit the data after timeout. The following example provides some insight on these issues.

Example I.4: Packet Processing within a Router and the Associated Delays and Losses

The following example will illustrate the effect that packet delay factors have on packet transmission. In this example, it is assumed that there are two hosts, A and B, each has an infinite buffer, is located zero distance from the first router, and will employ best effort transmission. Host A has 4 packets, A1, A2, A3 and A4 to send, and Host B has 5 packets, B1, B2, B3, B4 and B5, to send. The transmission path to be examined is that from the hosts through Router 1 to Router 2. Both routers have buffer space for 5 packets. The remaining parameters for the example are

Packet length = 7 Kbits
 Link rate R = 1 Mbps
 Packet processing time = 0.001 s
 Propagation speed s = 2×10^8 m/s
 Distance between routers d = 2×10^5 m

Therefore,

$$\text{Propagation delay} = d/s = (2 \times 10^5 \text{ m})/(2 \times 10^8 \text{ m/s}) = 0.001 \text{ s}$$

$$\text{Transmission delay} = L/R = (7 \text{ Kbits})/(1 \text{ Mbps}) = 0.007 \text{ s}$$

Initially, at time = 0, each host has a packet ready to send as indicated in Figure I.19. Packet B1 is sent first and takes 0.001 seconds to pass through the router. At time = 0.002 seconds, packet A1 is queued into the buffer, as shown in Figure I.20 and Figure I.21, because packet B1 is still in transmission.

At time = 0.003 seconds, packet B2 is queued into the buffer, as shown in Figure I.21 and Figure I.22, because packet B1 is still in transmission.

As Figure I.22 and Figure I.23 indicate, at time = 0.004 seconds, packet A2 is queued into the buffer.

As indicated in Figure I.24 and Figure I.25, when A3 is queued into the buffer the buffer will be full.

As Figure I.25 indicates, the buffer is full and packet B1 is still in transmission. Therefore, packet B4 is discarded.

Furthermore, since packet B1 will not complete transmission until time = 0.008 seconds (0.001 s for processing and 0.007 s for transmission), packet A4 will also be dropped, as shown in Figure I.26.

Finally, at time = 0.009 seconds, packet B1 has completed transmission to Router 2 and packet B5 is placed in the buffer, as shown in Figure I.27.

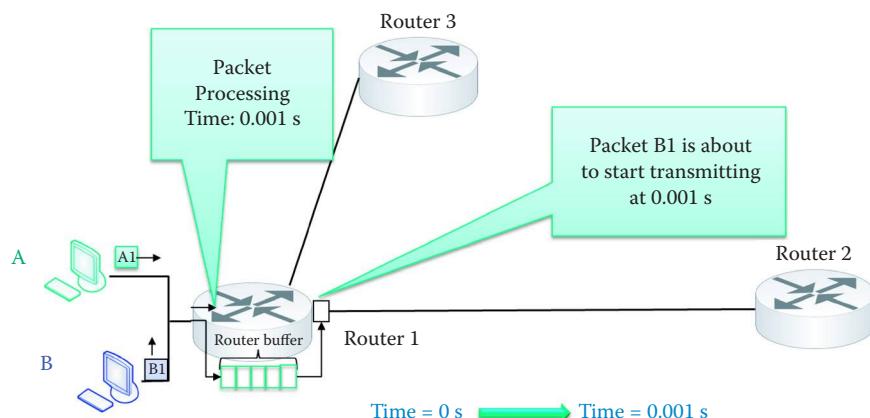


FIGURE I.19 Delay factor example at time 0 s.

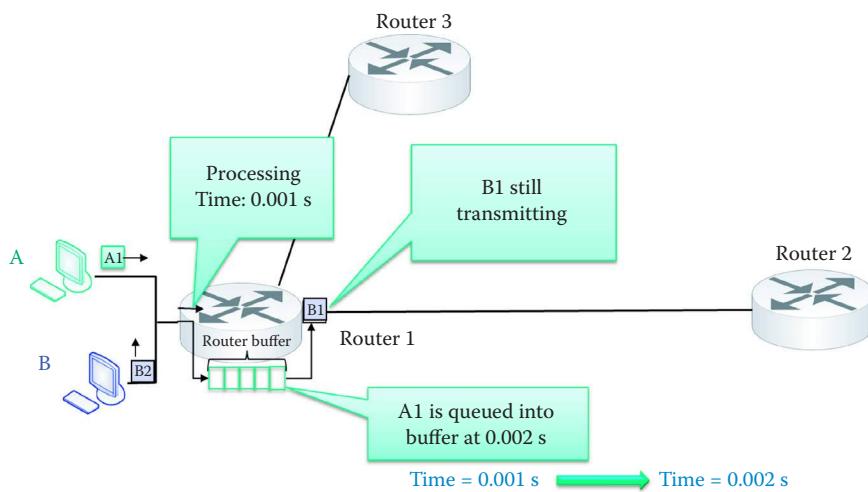


FIGURE I.20 Delay factor example at time 0.001 s.

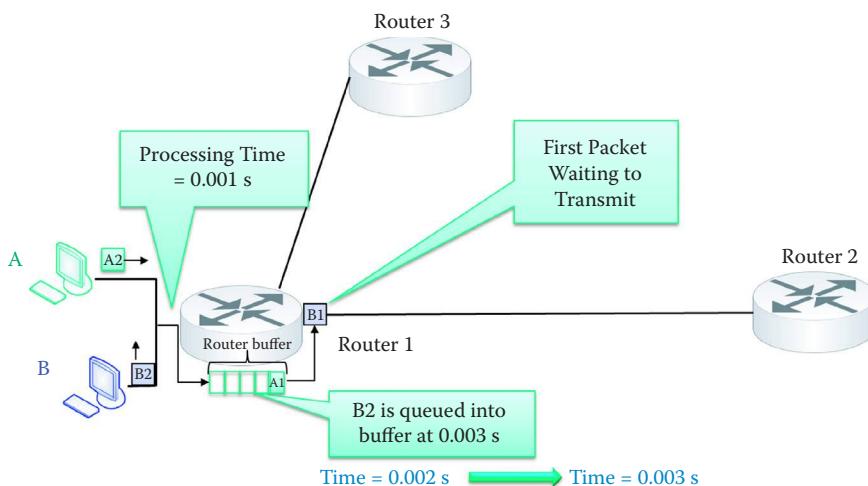


FIGURE I.21 Delay factor example at time 0.002 s.

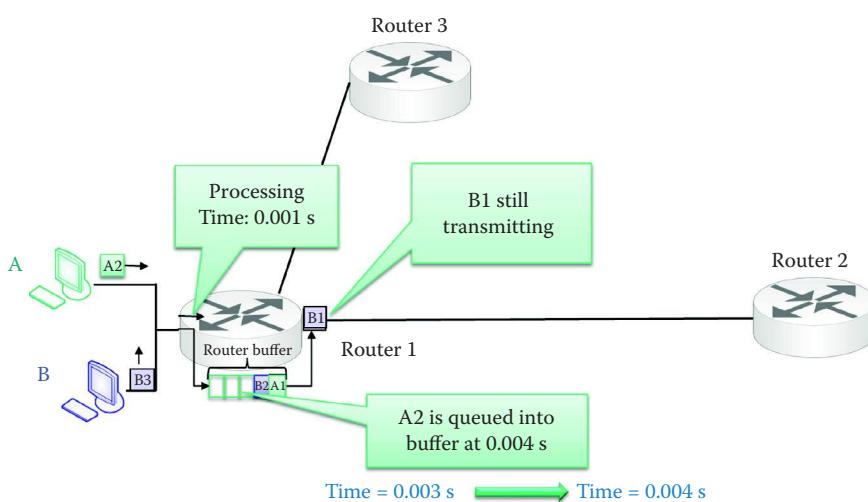
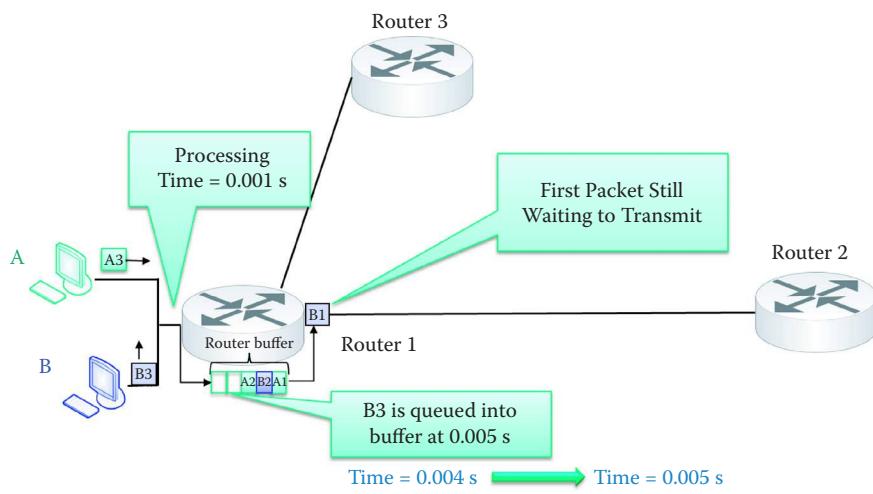
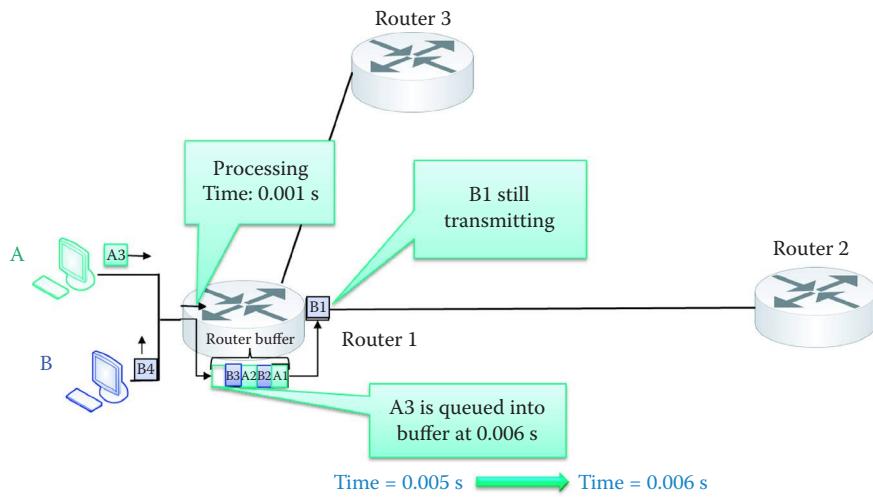
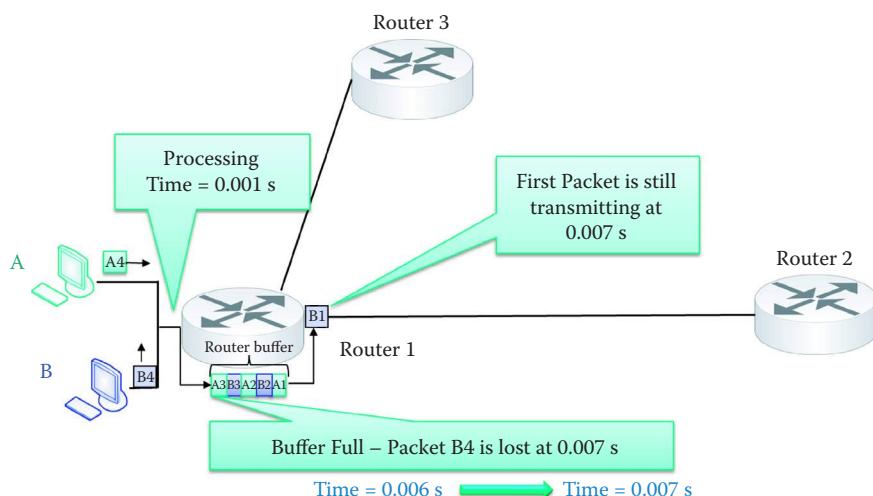


FIGURE I.22 Delay factor example at time 0.003 s.

**FIGURE I.23** Delay factor example at time 0.004 s.**FIGURE I.24** Delay factor example at time 0.005 s.**FIGURE I.25** Delay factor example at time 0.006 s.

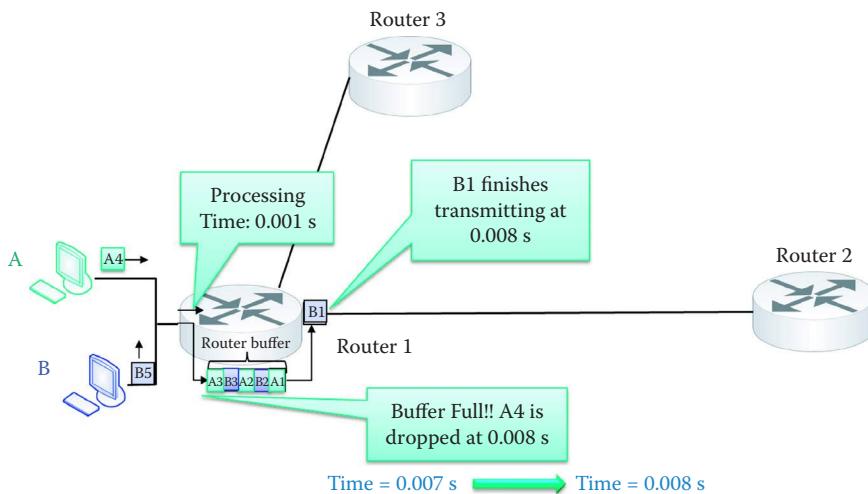


FIGURE I.26 Delay factor example at time 0.007 s.

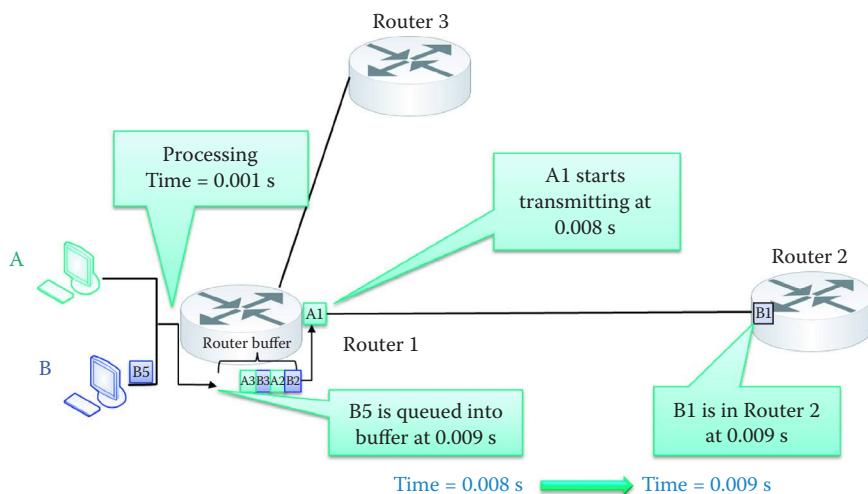


FIGURE I.27 Delay factor example at time 0.008 s.

I.6.3 CONGESTION AND FLOW CONTROL

Congestion is a natural consequence, which results when a source host sends out more data than the network and destination host can digest. This situation is even exacerbated by the fact that destination hosts can range from servers with fast Central Processing Units (CPUs) and high-speed links to smartphones with low-power CPUs and slower links. These situations can result in busy links and router/switch buffer overflow due to finite buffer size.

Given this situation, the obvious question is—how do we cope with this resulting congestion when the bandwidth and buffer size are unable to meet the required demand? When using Transmission Control Protocol (TCP) during congestion, resending packets, resulting from packet delay or loss, causes further loss and delay, and the negative feedback will cause even more congestion. So, the answer is flow and congestion control, which attempts to alleviate this condition by throttling back the output rate of the source host to relieve the congestion. The symptoms of congestion that trigger the congestion control are packet loss and delay, as well as buffer overflow. Flow control is used to tell the source host how much information the destination host can digest. The goal of this process is to optimize the throughput rate (bits/sec) between source and destination without causing congestion.

I.7 THE PROTOCOL STACK

It would certainly appear that the intercommunication among computers would require some standardization that would facilitate their successful interactions. There should be some “protocol” that defines the manner in which they talk to each other so that messages are clearly understood. It is this “protocol”, documented in a stack that is accomplished through modularization, development and upgrades that support operations such as web surfing, email and the like.

Prior to addressing the many facets and ramifications of the protocol stack, it is important to note that activities within the Internet can be approached in a modular fashion and this modularization is accomplished through layering. As a result, numerous aspects and technologies that are applicable are being developed by many diverse individuals and groups through a divide-and-conquer strategy. By its very structure it is clear that the stack consists of different layers, each of which performs a special function.

Modularization of the Internet is accomplished through layering. As a result, the Internet is being developed by many people, and institutions through a divide-and-conquer strategy. For example, using modularization, one company can tackle the development, maintenance, and updating of a single module. There is strong interaction between layers in that each layer relies on the services of the layer below and exports services to the layer above. It is the interface between layers that defines the interaction, e.g., implementation details can be hidden and layers can change without affecting other layers.

I.7.1 THE US DOD PROTOCOL STACK

When computers are connected within a network, guidelines must be established that support their interaction. The architecture that defines the network functionality is split into layers that collectively form what is commonly known as a protocol stack. The U.S. Department of Defense (DoD) model for the Internet protocol stack is shown in Figure I.28. The International Standards Organization also developed a separate protocol stack containing two additional layers, and known as the Open Systems Interconnection model, but that model was never completed.

Each layer of the protocol stack may employ several protocols to implement the functionality of that particular layer. In a natural progression up the stack, the physical layer deals with the transmission of bits that are propagating over such media as copper, fiber or radio. The data link layer aggregates the bits, e.g., into a frame, and performs the data transfer between neighboring network elements using as an example, Ethernet or WiFi. The network layer handles the routing of datagrams, in packet form, from source to destination using routing protocols. The transport layer performs the process-to-process communication using segments, i.e., message transfer using for example (a) Transmission Control Protocol (TCP) for reliable transport with overhead, (b) User Datagram Protocol (UDP) for best effort delivery with little overhead, or (3) Stream Control Transmission Protocol (SCTP) for reliable transport based upon the nature of the transaction. Finally, the application layer, containing the message, supports the various network applications, such as transferring files (File Transfer Protocol, FTP), data transfer on the world wide web (HyperText Transfer Protocol, HTTP), or electronic mail (Simple Mail Transfer Protocol, SMTP).

The various applications performed on the network can be typically categorized as either Web-based applications or new protocol/technology development. In the former case, scripts are used for rapid development. For example, JavaScript is employed on the client side and PHP is used on the server side for HTTP applications. There are many other script languages, e.g., Perl, asp, Ruby, and the like. In the latter case, sockets which provide an Application Programming Interface (API) are used by programmers to invoke TCP or UDP. Inter Process Communication (IPC) is extended to the other host in the Internet connection, and information is virtually stored in the device’s memory. Socket programming uses Java or C++, and the OS as well as the related firmware/hardware support IPC. The applications invoke protocols for information exchange and, as a result, information is virtually resident in memory with access latency and loss.

Application	Layer 5
Transport	Layer 4
Network	Layer 3
Data Link	Layer 2
Physical	Layer 1

FIGURE I.28 The U.S. DoD model for the Internet protocol stack.

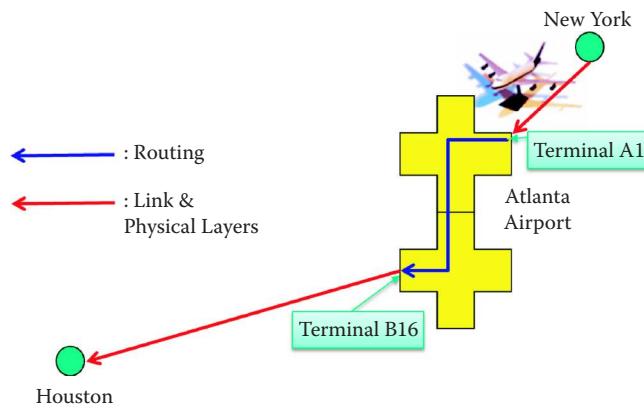


FIGURE I.29 Comparing routing/forwarding with the data link layer.

Example I.5: Network Layer Routing/Forwarding Functions and the Link and Physical Layers

Figure I.29 is used as a vehicle to compare the actions of network layer routing/forwarding with the data link layer. As an analogy, assume someone comes in on a flight and enters terminal A at Gate 1 and must leave on a plane from terminal B, Gate 16. Routing/forwarding from one gate to another would involve moving from one terminal to another terminal using the flight number and monitor guide as aids. The data link is the flight from one airport to another, and the physical layer is invoked by the Link layer.

The Physical Layer defines the means by which bits rather than packets are transmitted over a physical link connecting two network nodes. This bit stream may be grouped into code words or symbols and converted to a physical signal that is conveyed over a transmission medium. The Physical Layer performs character/symbol encoding, transmission, reception and decoding. The transmission media include such things as copper, twisted pairs or coax, fiber and radio. The encoding of the physical layer defines the manner in which each bit/symbol can be represented as voltage, current, phase, frequency, or photons.

I.7.2 THE OSI PROTOCOL STACK

The International Standards Organization (ISO) [24] has developed the protocol stack shown in Figure I.30, referred to as the Open Systems Interconnection (OSI) model. In contrast to the DoD Internet stack, this latter model has seven layers. The two additional layers that lie between the transport and application layers are the session and presentation layers. The session layer aggregates connections for efficiency, synchronization, and recovery in data exchange. The presentation layer permits applications to deal with coding, encryption, compression and the like. If these services are needed in the DoD model, they must be implemented in the application layer. The OSI stack was never completed, but the U.S. DoD had sufficient funding to complete the development of its protocol stack.

I.7.3 PACKET HEADERS AND TERMS

Each layer in the stack, with the exception of the physical layer, has a header. These headers facilitate the communication of information and are analogous to an envelope that contains both source and destination addresses. The link layer has a header containing Media Access Control (MAC) addresses, the network layer has a header containing Internet Protocol (IP) addresses and the transport layer has a header containing the port, i.e., service number.



FIGURE I.30 The ISO protocol stack.

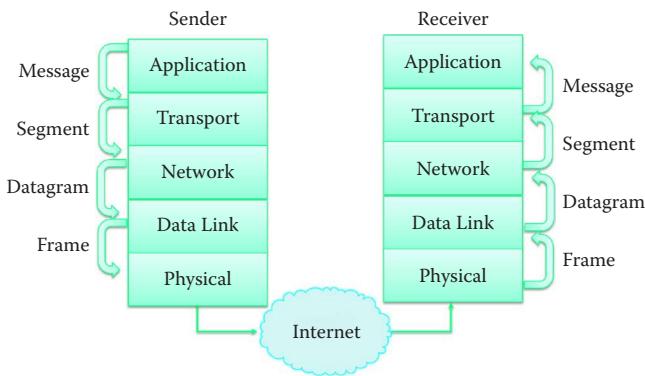


FIGURE I.31 The Internet protocol stack and associated packet identifiers.

The Internet protocol stack and associated packet identifiers are shown in Figure I.31, where the terms *message*, *segment*, *datagram*, and *frame* are used for the following corresponding layers: application, transport, network and data link.

I.7.4 THE LAYER 2 (L2) TO LAYER 5 (L5) OPERATIONS

Given the protocol stack and the manner in which a packet of information progresses through this stack with the attendant headers that are applied at each level, let us now consider in some detail the switching that takes place as the packet moves from layer to layer.

Example I.6: An Overview of Layer 2 to Layer 5 Operations Performed at the Source Host, L2 Switch, L3 Router and Destination Host

The manner in which a message is sent from source to destination over the network is illustrated in the figures that range from Figure I.32 to Figure I.35. As indicated earlier and illustrated in Figure I.32, the protocol stack consists of layers, with one or more protocols supporting each layer. Each protocol may be implemented in a combination of hardware and software.

Suppose now that an application has a message to send to a destination. This message employs application protocols such as HTTP and FTP. The message is passed to the transport layer. For Internet use, the protocols used at this layer are TCP or UDP. At this point, the message is segmented and a transport header is attached to each segment, which contains the port number of the transport layer, i.e., both source and destination port numbers. The port number of a server indicates the application layer protocol, e.g., port 80 for HTTP. The transport layer segments are then passed to the network layer where the destination's IP address is added. At this point, the message has, in essence, a destination IP address and a source IP address. It is the responsibility of the network layer of the source host and involved routers as well as the destination host's network layer to deliver the segments, also known as packets or datagrams, to the transport layer at the destination. The network layer of hosts and routers contains the routing protocols necessary for this delivery. The destination IP address is obtained through DNS from a URL. The network layer passes the datagram on to the link layer. While the network layer routes the packets from source to destination through one or more routers, the link layer only knows how to progress from one interface to the next interface connected by a physical link. The link layer creates a frame containing the datagram, and is responsible for moving this frame to the next adjacent interface in the transmission path. The link layer adds the MAC address of the next interface, e.g., the router interface, and passes it on to the physical layer. The network layer of the source host knows the destination IP address belonging to another subnet and delivers the frame to the router interface (aka. gateway to the Internet). The destination MAC address is obtained using the ARP (Address Resolution Protocol) from the IP address of the

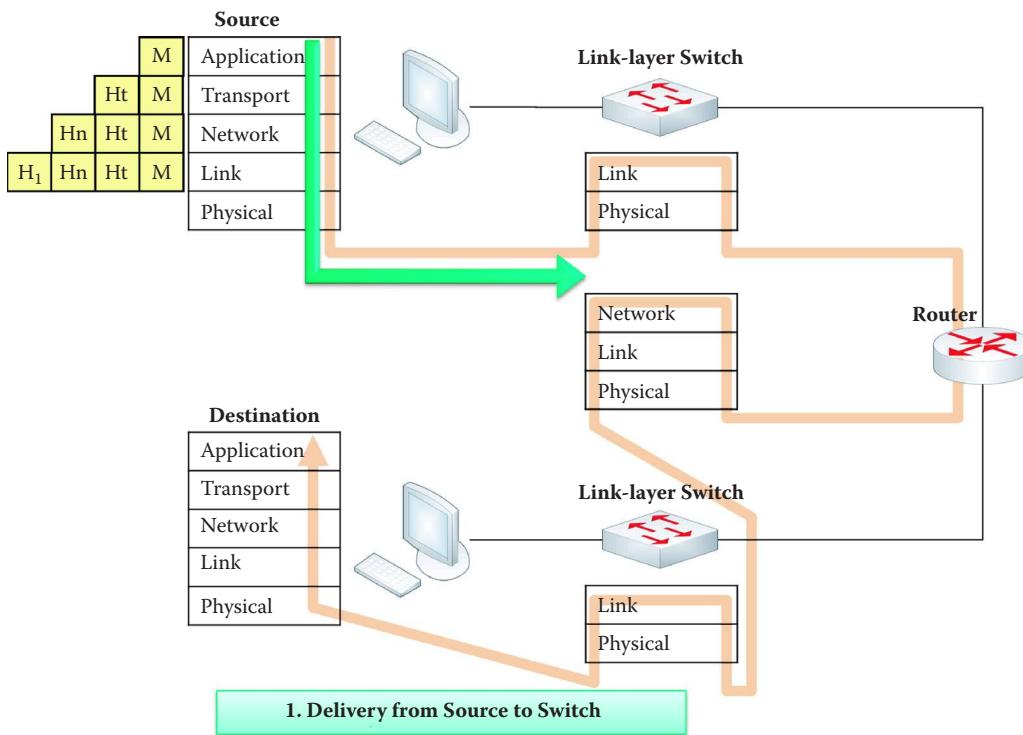


FIGURE I.32 Source to destination illustration—delivery from source to switch: The headers are added at each layer when the message is passed down the protocol stack. H_t is the transport layer header, H_n the network layer header and H_l the link layer header.

router interface. It is this physical layer that moves individual bits in a manner consistent with the actual transmission medium, such as copper wires. Clearly, what is happening is this: as the original message progresses down the stack each layer adds necessary information to the bits from the layer above.

Example I.7: The Operations Involved in Layer 2 Switch Forwarding

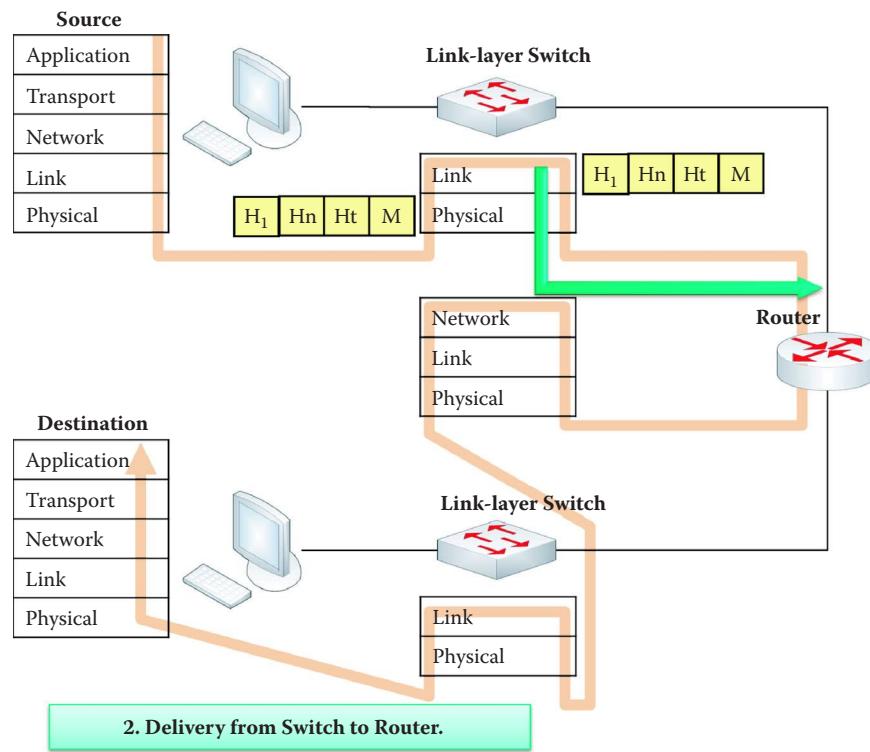
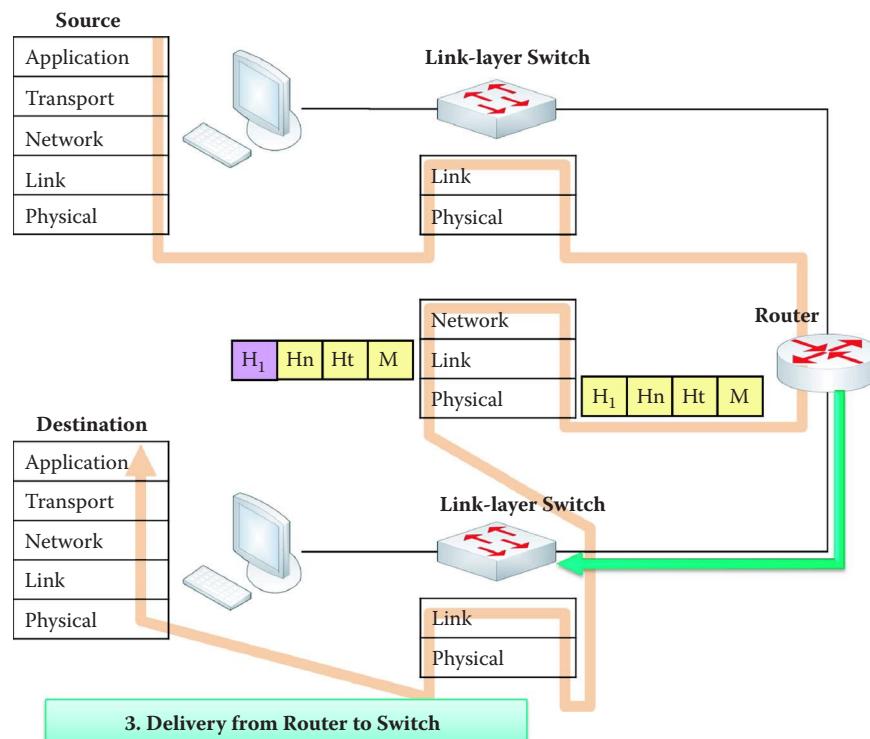
The link layer switch, shown in Figure I.33, is a device whose operation is confined to the bottom two layers of the protocol stack. This switch delivers the frame to the correct hardware output port based upon the destination MAC address in the header. The frame is forwarded to the router interface that has the destination MAC address.

Example I.8: The Operation of a Layer 3 Router

While the layer 2 switch's operation is based on the MAC address, the router is a layer 3 device, as indicated in Figure I.34. Thus, the router will route the datagram/packet based on the destination IP address, which has been supplied by the source host. Knowing the destination's IP address, the router must now use the proper destination MAC address for packing the link layer header. Therefore, the new destination MAC address is used by the next link-layer switch in order to forward the frame.

Example I.9: The Link-Layer Switch Functions in Delivering a Frame to the Destination Host

As indicated in Figure I.35, the link-layer switch delivers the frame from the router interface to the correct output port of the switch based on the destination MAC address, which is burned into the incoming interface of the destination host. The frame is then sent to this destination host.

**FIGURE I.33** Delivery from switch to router.**FIGURE I.34** Delivery from router to switch.

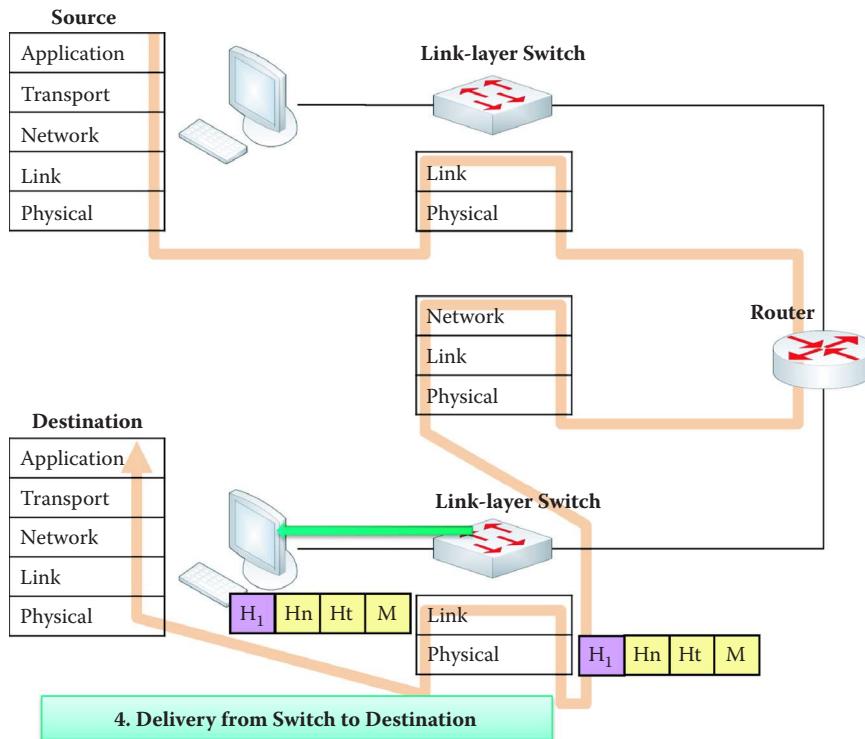


FIGURE I.35 Delivery from switch to destination.

Example I.10: The Operations of the Protocol Stack in Processing Frames at the Destination Host

Upon the frame's arrival at the destination host, as shown in Figure I.36, the frame progresses up the stack. The link layer takes the bits, strips off the header, containing the MAC addresses, and passes the packet/datagram up to the network layer. The network layer strips off the header containing the IP address, and passes the segment to the transport layer. The transport layer strips off its header, assembles the bytes, and passes the information to the proper port for the particular application, e.g., one port in a browser may be for Fox News and another for Amazon, if both ports are in use. Finally, the application layer, working in conjunction with the transport layer, reassembles the segments to form the message that was originally sent.

Example I.11: An Explanation of the Differences among Layer 2 and Layer 3 Operations

Having examined the progression of a message from source to destination through the various network elements, consider now some of the salient features of these elements. For example, the Layer 2 (Link-layer) switch cannot change the destination and source MAC address under any circumstances. However, it does know the port that is associated with the destination MAC address, and thus can process the packet and direct it toward the correct port. The layer 2 switch learns this information from the header that contains the source's MAC address. Thus, this learning process yields a switching table that is used to direct the packet. The source computer has to know the IP address of the first gateway, i.e., router, and employs the Address Resolution Protocol (ARP) to obtain the gateway's MAC address. The destination MAC address of the packet exiting the source host is the MAC address of the first router's interface, while the destination IP address is that of the terminal host.

In contrast to the layer 2 switch, routers and/or layer 3 switches understand both MAC and IP addresses. Routers work in concert with one another to generate routing tables. The routing table provides the router or layer 3 switch with the next hop's IP address. The router

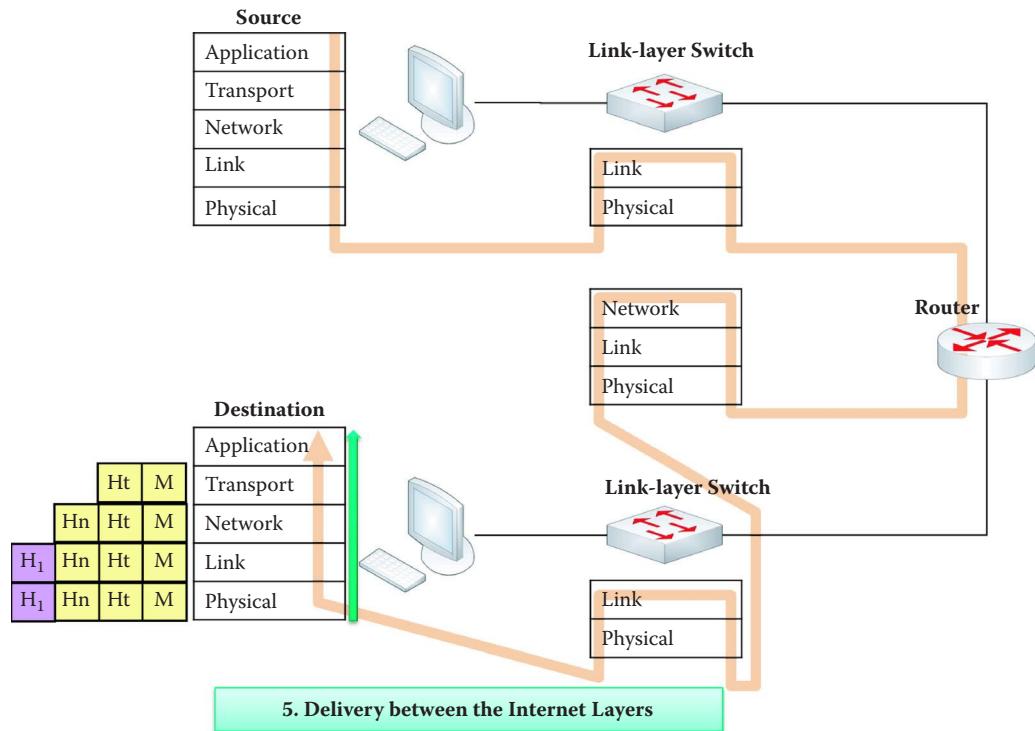


FIGURE I.36 Delivery between Internet layers at the destination host.

then uses the ARP to determine the MAC address of the terminal host. Once this destination MAC address is changed by the router, the layer 2 switch that lies between the router and the next host, can switch correctly. Therefore, the layer 2 switch learns from the source MAC address to derive the switching table, and the routing mechanism is learned from the routing table. The details of this process are found in Part 3 of this book.

I.7.5 A USER'S PERCEPTION OF PROTOCOLS

The manner in which a user employs the various protocols when accessing the web is outlined in the following example.

Example I.12: The Steps Involved in Connecting a Host to the Internet and Downloading a Webpage

The steps involved in using the Internet are outlined in Figure I.37. This figure specifically details the elements involved in the use of HTTP to access a web server. Although we have demonstrated the steps involved in using the Layer 2 and 3 protocols in the figures that began with Figure I.32 and ended with Figure I.36, there are a variety of protocols, and all communication and activities within the Internet are governed by them. For example, the Dynamic Host Configuration Protocol (DHCP) provides a client with an IP address, gateway IP address and DNS IP address. In general, protocols define the packet format, the sequence of packets sent and received among network entities, and the actions that take place based on the parameters contained within the fields of a received packet. The service (port) number is embedded in the TCP header, e.g., port 80 for HTTP. Sequence and acknowledgment numbers are also contained in the TCP header for tracking loss. Retransmission of a packet depends on the acknowledgment number obtained from the receiver. Clearly, it is important for all devices to use and understand the same language. That is why this *language* is specified as a standard that is set by the IETF, because syntax and semantics are critical in this environment.

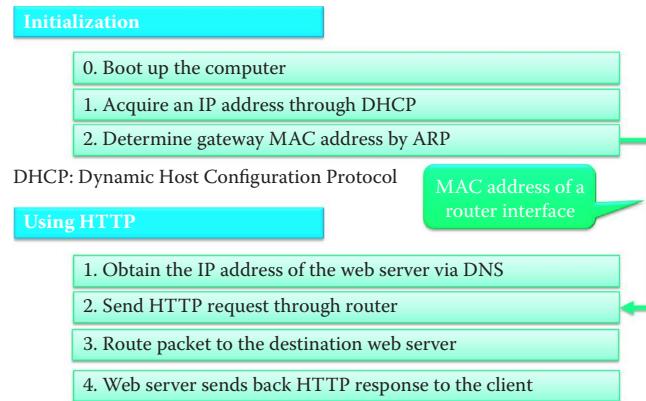


FIGURE I.37 The procedural steps for using the Internet.

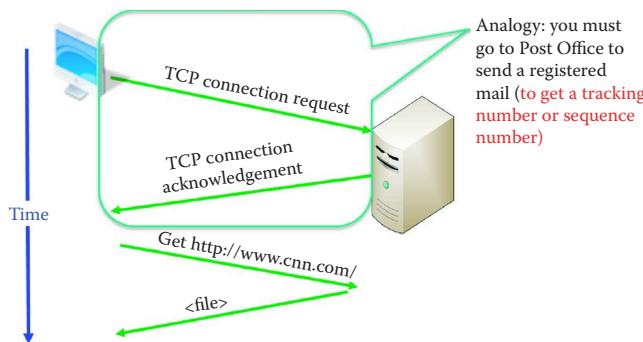


FIGURE I.38 The operation of the HTTP protocol.

As shown in Figure I.38, the HTTP protocol establishes a connection between client and server so that reliable delivery of information, e.g., the use of a packet sequence number for loss detection, can be established for the socket. Connection-oriented service derives its name from the establishment of a connection for reliable transport. The round-trip connection establishes parameters such as a sequence number and round-trip time (RTT) so that the sender will be able to retransmit a lost packet if no acknowledgment is received. In this HTTP protocol, the client makes a TCP connection request, the server sends back an acknowledgment, the client then requests the required data, which is then supplied by the server.

I.7.6 A COMPARISON OF THE CONNECTION-ORIENTED AND CONNECTIONLESS APPROACHES

Example I.13: The Overhead Involved in the Connection Oriented Approach (TCP) for Sending a File from a Host to the Server in Figure I.38

In using a connection-oriented approach, TCP requires a round trip for establishing a TCP connection prior to delivering a file. Suppose the file to be delivered is 4000 bytes in length and uses a link that has a 1.536 Mbps bandwidth and a 1ms propagation delay. Let us consider the percent overhead required to establish this connection and send the file from host A to host B. Neglecting other delays,

$$\text{The overhead} = \text{indirect cost/total cost.}$$

The total delay = round trip delay incurred in establishing a TCP connection + delay in sending the file = $2 * 1 \text{ ms} + 4000 * 8/(1536000) + 1 \text{ ms} = 2 + 20.83 \text{ ms} + 1 \text{ ms} = 23.83 \text{ ms}$

$$\text{Thus, the overhead} = 2 * 1 \text{ ms}/23.83 \text{ ms} = 8.39\%.$$

Example I.14: The Overhead Involved in the Connectionless Approach (UDP) for Sending a File from a Host to the Server

In using a connectionless approach, UDP does not require a round trip for establishing a TCP connection before delivering a file of 4000 bytes using a link that has a 1.536 Mbps bandwidth and a 1 ms propagation delay. Hence, there is no overhead associated with UDP.

Protocols, such as Ethernet 802.3 [6], IP, TCP and HTTP, perform a number of very important functions. For example, they govern the movement of packets from source to destination under the specifications of certain standards, take actions that are specified in the packets, manage packet flow and congestion for optimal performance and even recover lost packets, which require a connection oriented transport protocol (TCP). The protocols work in conjunction with one another to accomplish the specified task requested by the user. Applications, such as HTTP, invoke transport protocols, such as TCP; transport protocols invoke the IP protocol; and the IP protocol invokes Ethernet or something similar. In support of all of these functions are the Domain Name System (DNS) and other protocols, such as the Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP) and Internet Control Message Protocol (ICMP) that provide the glue that holds everything together. DNS and DHCP typically employ UDP since the information transmitted is very small and the connectionless approach (UDP) reduces overhead.

With the use of these protocols, the Internet becomes a distributed information sharing and delivery service. As such, the Internet supports distributed applications and services, such as a data sharing service involving the Web, email, games, e-commerce and file sharing, as well as a real-time service for the delivery of VoIP, video conferencing and IP TV. The transport services provided to applications are either a reliable data delivery service from source to destination that is characterized by more overhead, no tolerance for error or loss, but capable of tolerating delay and jitter, i.e., TCP, or a best effort, but unreliable, data delivery service that has less overhead, able to tolerate error and loss, but unable to tolerate jitter, i.e., UDP. The former transport service is good for data, such as email, and the latter transport service is good for voice and video.

I.8 PROVIDING THE BENEFITS OF CIRCUIT SWITCHING TO PACKET SWITCHING

In our earlier comparison of circuit switching and packet switching, it was indicated that while packet switching possessed a number of important and advantageous features, it was generally not suitable for voice and video. However, because it is useful in so many ways, we are naturally led to ask the question—isn't there some method that can be employed to make the packet switching-based Internet suitable for delivering voice and video?

When packet switching is employed, the data stream for each host is segmented into packets, and the destination IP address is contained in the packet header in the same way in which a standard letter would have the address written on the envelope. Each packet travels independently using the available resources provided by the routers. Packets may be lost or arrive out of order. It is the job of the transport layer at the destination to reassemble the received packets in the correct order.

In the real world there are typically finite resources, and all hosts must share them. For example there is only so much link bandwidth and router/switch buffer space. However, each packet uses the full link bandwidth during transmission and thus must compete for resources with other packets. Available resources are typically used on an as-needed basis. When the aggregated resource demand exceeds the amount available, congestion occurs. Packets are then placed in a queue and wait for the next available link, just as vehicles would do when a traffic jam turns a busy highway into a parking lot. Unlike the traffic analogy however, queue overflow can occur if packets overrun the available space in a router/switch and in this situation the excessive packets are dropped.

In order to maintain some Quality of Service (QoS), resource allocation and reservation is necessary. This is critical for voice and video and is typically organized so that all resources are fully utilized. Performance is optimized by strategically dividing resources among the competing

parties. These resources are link bandwidth, packet priorities in router and switch queues, the memory/buffer/queue in routers and any wireless spectrum needed.

Because both packet switching and circuit switching possess some distinct advantages, an obvious issue is the combination of the two. There are two approaches to this combination. The Telco approach employs ATM. In this case, a virtual circuit uses a sequence of 53-byte packets called cells that mimic the circuit-like connection, which involves connection setup and tear-down. The IP approach uses the Resource Reservation Protocol (RSVP). The RSVP is a Transport Layer protocol for reserving resources in order to achieve an integrated services Internet. The approach that is IP-based uses protocols based on IP for streaming video/audio over the Internet. These protocols are the Real-time Streaming Protocol (RTSP), the Real-time Transport Protocol (RTP) and the Real-time Transport Control Protocol (RTCP). RTSP permits the reservation of resources for a flow using RSVP and relies on RTP and RTCP for delivering audio/video datagrams. RTCP is used by RTP to ensure the QoS. An IP Multicast provides a means to send a single media stream to a group of recipients on the Internet. In contrast, Unicast sends one copy to each recipient causing excessive and unnecessary backbone traffic.

I.9 CYBERSECURITY

Although the targets for cyber attacks may vary widely, they are primarily focused on money, intellectual property and, of course, sabotage. Cybersecurity is a collection of defensive technologies (hardware/software), processes and practices designed to protect networks, computers, programs and information from attack, damage or unauthorized access in order to secure systems that are connected to the Internet. By definition, Cybersecurity protects against threats using defensive measures, including information assurance, computer systems, and applications hardening, malware protection, access control, information infrastructure protection, and network security.

I.9.1 ATTACKS AND MALWARE

Attacks on the Internet information infrastructure originate from the four corners of the world and can be absolutely devastating. The attacks on hosts are generated through malware and can easily gain unauthorized access to critical information. Another form of attack is the denial of service (DoS) attack in which legitimate users are denied access to resources. These DoS attacks will typically exhaust the server's memory and processing capacity and/or exhaust the link bandwidth. Imagine for a moment the impact of overwhelming the communications to a police headquarters in a large city.

Malware comes in five distinct categories/capabilities: (1) *Spyware*, (2) *Viruses*, (3) *Worms* (4) *Trojans* and (5) *Rootkits*. Spyware records keystrokes and other crucial activities and uploads this information to a collection site. A virus provides illegal access to a host's resources, infects it, e.g., through an email attachment, and may contain spyware, Trojans or worms. It is also capable of propagating to other hosts. A host can be infected through a worm by simply passively receiving an object that executes itself and then actively propagates to other hosts. Trojans that may be contained in spyware, a virus or a worm provide a backdoor for illegal access to a host. Rootkits are malware that is hidden in a host's file system and very difficult to detect. Currently, a single piece of malware may possess these 5 types of malware in order to expand its territory, control the infected hosts and steal information.

I.9.1.1 THE ZERO-DAY ATTACK AND MUTATION IN DELIVERY

The usefulness and importance of the Internet could hardly be overstated. However, these qualities are dependent upon the assurance that the information flow from source to destination is secure. And yet, we regularly hear stories that in fact the Internet is vulnerable to a variety of attacks, many of which can have devastating consequences. We are thus first led to ask "why is the Internet so vulnerable?" and "can we detect the malware as an initial step in reducing its effects?"

In addressing these questions we find that security improvements for hosts and the Internet must be approached at every juncture. Security must be incorporated at all protocol levels, the host Operating System (OS) must be hardened, and anti-malware capability must be installed in all hosts and routers. While it is believed that the host operating systems and the numerous applications present the weakest link in the Internet from a security standpoint, the vulnerabilities extend to router and switch firmware, firewalls and protocols. It is most unsettling to find that the security company, F-Secure, believes that the quantity of malware produced in 2007 was equivalent to that produced in the previous 20 years. To make matters worse, some of the malware mutates, i.e., changes form all by itself as it moves from one host to another. In addition, the zero-day attack, i.e., one that is brand new and has no signature, can be non-detectable, and therefore lethal. One must be aware that the life-cycle time of a piece of malware was reduced to two hours in 2009 [18] and this fact indicates that signature-based detection methods were no defense.

Malware is delivered in a variety of ways. It may be carried in an email or in the form of a worm that will self-propagate through the network. Websites are perhaps the worst sources of malware. The following list outlines some of the reasons that malware is such an enormous problem: it can mutate during propagation in a varying formation in order to defeat malware detectors; it can hide in a PC's BIOS where it cannot be detected; it can rewrite the first block of the hard disk or solid state drive so that detectors cannot be initialized; and it can upgrade itself to defeat or disable the newest defense measures delivered by software updates.

I.9.1.2 CRIMEWARE TOOLKITS AND TROJANS

Given the level of trouble that can be created with malware, it is reasonable to ask just how much crimeware actually exists? The answer is much too much. Why is there so much? The answer to this question is simply that it is cheap to get in and the business is very lucrative for profits or intellectual property. As a result, there are numerous versions of malware that are available for purchase. For example, the security firm, McAfee, has published an analysis of the "Zeus Crimeware Toolkit" [19]. An individual can purchase Zeus (\$4000/copy) or the SpyEye crimeware toolkit (for about \$500) [20]. For example, the ZeuS Trojan toolkit version, which is an attacker's package, allows criminals to make a customized web site in just a few clicks, and lure unsuspecting people to it. Then, their machines are infected with the malware, which may propagate to other hosts. Botnets (Zombies) can be established by an attacker for command and control or can be rented for profit. Symantec alone has detected that over 154,000 computers are infected with the Zeus Trojan and there existed 70,330 unique variants of the Zeus Trojan binary in 2009. Global tracking of ZeuS Command and Control servers (hosts) is performed by the ZeuS Tracker at <https://zeustracker.abuse.ch/>, while SpyEye Command and Control servers are globally tracked by the SpyEyeTracker at <https://spyeyetracker.abuse.ch/>. The totality of malware presents a clear danger for the legitimate user.

The ZeuS Trojan has the capability to capture passwords, even a one-time password. The security experts found that ZeuS is able to read PINs and transaction numbers (TANs) entered not only via keyboards, but also via mouse clicks [21]. RSA Security provided a service to verify a transaction using SMS in order to protect a one-time password against Zeus. According to a report on the S21sec blog, new versions of the ZeuS banking Trojan are now homing in on the SMS-TAN procedure, also known as mobile TAN or mTAN. In the SMS-TAN procedure, transaction numbers (TANs) for online transactions are sent to the customer's cell phone to authenticate that person for an online bank transfer that has been initiated, for instance, from a web browser. The use of the second communication channel for confirming the transaction is designed to make phishing and Trojan attacks impossible. After all, the transaction can only be hacked if users do not carefully check the data in the text message, if their cell phones get stolen, or the device is infected with a Trojan that passes on the text message to the phisher.

However, the developers of ZeuS have pursued the last strategy to get Trojans onto mobile devices for an attack requiring multiple stages. The most important step is still infecting a Windows PC. In this case, victims view a specially crafted web site that masquerades as a security update for the victim's cell phone. Victims are asked to enter their cell phone number so they can receive a link for the download in a text message. The PC infected with the Trojan then promptly sends a text message containing a link to what appears to be a new security certificate. Users

are then asked to download and install the certificate on their mobile phones, which requires an Internet connection on the phone. The downloaded file contains the mobile version of ZeuS, which then analyzes and forwards all incoming text messages. It also executes commands sent via SMS. S21sec says there is a version of the Trojan for Symbian (.sis) and BlackBerry (.jad). Criminals can then use the account access data stolen from the PC along with the TAN to make bank transactions from the account. On 10/19/2011, a variant of SpyEye was found to have the ability to infect a computer, steal the victim's logon credentials and change the phone number that the bank uses to confirm transactions [22].

Police in the U.K. have arrested 19 people on charges they used the Zeus Trojan to steal more than \$9.4 million from U.K. banks in September 2010. The bank software tracked the malware activity in the bank customers' computers and identified the attackers. With better security training, those hackers would have cleaned their trails in those computers, which would have made it harder for the police to trace them.

I.9.1.3 SOPHISTICATED MALWARE

Given the plethora of malware that exists and appears to be in a constant state of development, one is naturally led to ask the question: is it possible to escape an attack? Unfortunately, the answer to this question is no if you are being directly targeted by an entity that possesses the proper expertise and resources. A family of recently developed sophisticated malware is listed in Table I.3, and all shared a basic toolkit for malware development.

History would indicate that one of the world's most sophisticated malware is the Stuxnet worm [23] that is designed to attack the Siemens SimaticWinCC supervisory control and data acquisition (SCADA) system. These SCADA systems are installed in big facilities, like nuclear plants and utility companies, to manage operations. Step 7 is the Siemens software used to program and configure the German company's industrial control system hardware. Stuxnet works by infecting Windows machines using four zero-day vulnerabilities. One is used to spread the worm to a machine via a USB stick since the SCADA systems are isolated from the Internet. The second is a Windows printer-spoofer vulnerability used to propagate the malware from one infected machine to others on the network. The remaining two help the malware gain administrative privileges on infected machines to feed the system commands. Furthermore, the Step 7 propagation vector would insure that already-cleaned PCs would be re-infected if they later opened a malicious Step 7 project folder. Stuxnet searches for a way to reach the SCADA's programmable logic controller (PLC) and then takes control of the PLC and potentially alters the commands it sends through to the nuclear plants. It is capable of bypassing any other computers that are not Siemens SimaticWinCC machines. It is specifically designed for sabotage and reaches a level of sophistication that has not been seen before. The malware is digitally signed with legitimate certificates stolen from two certificate authorities in order to fake authenticity.

Flame is another unprecedented, sophisticated malware that relies on fake Microsoft certificates for Windows Update to infect fully patched Windows computers in addition to using zero-day attacks. Flame in an infiltrated computer acts as the man in the middle, intercepts a Windows Update request from a victim and infects it by installing bogus Windows Update software. The most detrimental capability of Flame is the feature it employs to forge certificates signed by Microsoft [24]. After infecting a Windows computer, Flame manipulates its microphones, cameras, and Bluetooth to collect intelligence in the immediate vicinity. The defense against this kind of innovative, advanced malware is not available yet and can only be patched once the malware is discovered.

TABLE I.3 A Cyber Espionage Malware Family's Main Features

Malware	Date of operation	Size	Special features
Stuxnet	June 2009	500 kilobytes	Sabotage program: sabotaging uranium centrifuges
DuQu	September 2011	300 kilobytes	Information gathering
Flame	March 2010	20 megabytes	A spyware program; Windows Update deception; Connect with Bluetooth devices in the area

I.9.2 DEFENSIVE MEASURES FOR CYBERSECURITY

Let us now consider the mechanisms that an enterprise can employ to defend itself against malware that is expanding in both scope and sophistication. In order to be active in the business community and use the Internet, defensive measures simply have to be used. Table I.4 lists the typical security devices/software, widely deployed by enterprises and described in the following sections.

I.9.2.1 THE FIREWALL, THE INTRUSION DETECTION SYSTEM (IDS) AND THE INTRUSION PREVENTION SYSTEM (IPS)

While it would appear that this malware is capable of destroying the Internet and everyone attached to it, the industry is not standing idly by watching everything this ubiquitous communication system has provided made useless. A tremendous industry has been established worldwide to address these problems. Three of the methods that are employed to protect systems are the *Firewall* [25], the *Intrusion Detection System (IDS)* and the *Intrusion Prevention System (IPS)* [26]. These elements are typically placed at critical entry and exit points to protect vital assets, such as a server farm, a financial database, or something else of significant value.

Host firewalls are used in a computer's OS/application to protect the host. Network firewalls are used to protect the entrance to a network and block packets based on the IP address and port number in the header (L3 to L4). In addition, a stateful inspection is performed in order to maintain a state transition table for a connection. Both IDS and IPS are used to monitor potentially malicious traffic by inspecting the entire packet (L2 to L5). IDS will let the packet pass, but sends an alert to the network administrator, while IPS will block a malicious packet and send a message to the network administrator.

A firewall operates in the manner shown in Figure I.39. Its purpose is to isolate an organization's internal network. As the arrows in the figure indicate, the firewall permits transmission from the organization to either the public Internet or the *Demilitarized Zone (DMZ)*, as well as transmission from the DMZ to the Internet. However, it blocks traffic into the organization from either the public Internet or the DMZ.

TABLE I.4 An Overview of Typical Security Devices/Software

Name	Security check	Action taken
Firewall	TCP/IP packet header inspection	Block
Intrusion Detection System (IDS)	TCP/IP packet header and content inspection	Alert
Intrusion Prevention System (IPS)	TCP/IP packet header and content inspection	Block and alert
VPN: SSL/TLS	Authentication, encryption and integrity	Communication protection
VPN: IPsec	Authentication, encryption and integrity	Communication protection
Network access control (NAC)	Host health inspection, authentication, encryption and integrity	Access control

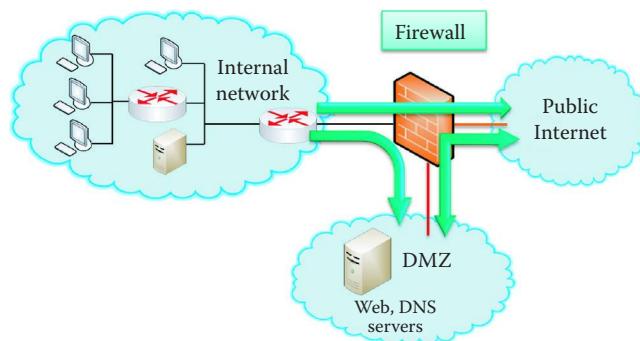


FIGURE I.39 Firewall protection for an organization.

As shown in Figure I.40, IDS/IPS is strategically placed at the entrance to an organization. From this vantage point it can detect a wide range of attacks. Attackers typically perform network mapping, in the form of reconnaissance using nmap, as well as port scans and TCP stack scans that can be detected/blocked by the IDS/IPS. It can also detect denial of service bandwidth-flooding attacks, worms and viruses, as well as both OS and application vulnerability attacks. The IDS/IPS can also be provided by software in a computer, which is usually integrated with anti-virus software. One must be cognizant of the fact that signature-based detection methods used in IDS/IPS and anti-virus software are ineffective against any zero-day or mutated malware. The IDS generates too many false positive alarms, which make it difficult for administrators to identify meaningful attacks. On the other end, the IPS only blocks the packets that are definitely malicious while other malicious packets pass through. It is the responsibility of every user to take precautionary measures, by employing the help of currently available defense products, when surfing the Internet.

Today's fully featured routers contain within them the firewall and IDS/IPS functions, which can be configured to perform the specified functions. It is for this reason that modern vendors typically claim that their routers perform the L2 to L7 switching functions.

I.9.2.2 VIRTUAL PRIVATE NETWORKS (VPN) AND ACCESS CONTROL

While it is clear that defensive measures must be applied at every possible location, the communication, which often carries sensitive information, must also be protected. There are several methods that can be employed with information transmission. Chief among them are *encryption*, *authentication* (credentials that state you are who you say you are coupled with integrity protection) and *authorization* (which verifies that you have permission to access the specific resources). For example, Secure Socket Layer/Transport Layer Security (SSL/TLS) [27] is used between the session and transport layers for such things as Internet shopping and web mail. The Internet Protocol Security (IPsec) [28] is used in the network layer for such things as a virtual private network (VPN), as shown in Figure I.41, and VPN is allowed to pass through a corporate firewall.

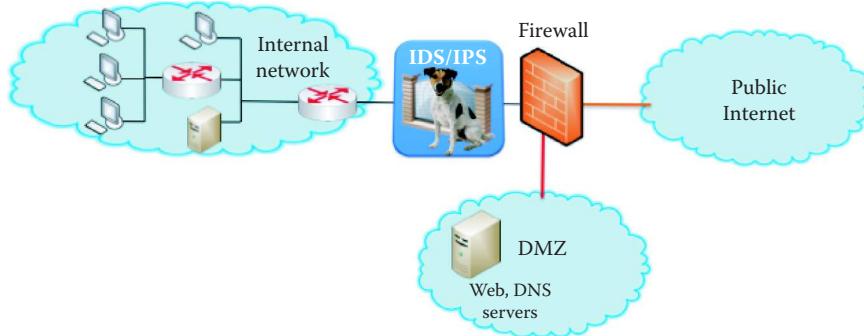


FIGURE I.40 Placement of the IDS/IPS protection system.

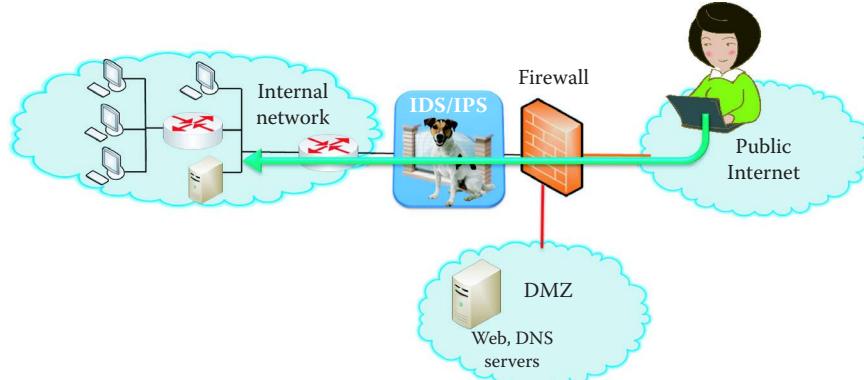


FIGURE I.41 A user can use VPN tunnel to securely pass through a firewall from the public Internet.

Organizational network access control (NAC) is agent-based NAC deployed at each host and central control server. Only healthy hosts that are certified by their agents can have network access, and security policy enforcement is a main feature of NAC in an enterprise network. 802.11i [8] is used in the data link layer for WiFi or 802.11 WLAN; organizational access control using Active Directory based on Kerberos is used for user access control, RADIUS/AAA protocol is employed for authentication and 802.1x [29] is placed in layer 2 for WiFi and LAN authentication.

Today's routers, including those used in the home, have IPsec or SSL/TLS VPN functions built right into the unit. Therefore, one can simply configure the router to perform the functions desired. The details involved in configuring VPNs will be discussed in Part 5 of this book.

I.9.2.3 INTEGRATED DEFENSE FOR AN ENTERPRISE NETWORK

The integrated defense for an enterprise network has the following formula:

$$\text{Integrated defense} = \text{endpoint security software} + \text{cloud} + \text{NAC} + \text{IDS/IPS} + \text{Firewall}$$

Endpoint security software contains an array of layered protection including

- Malware signatures
- Real-time code emulation
- Advanced heuristics
- A cloud-centric feedback loop from actual users, such as reputation services that blocks bad IP addresses, URLs, and files
- Application controls that are effective in decreasing the endpoint attack surface
- Tools provide kernel level, hypervisor level, or CPU level protection to protect against rootkits

The NAC uses centralized policy enforcement for endpoint security, that can be configured in accordance with the role of the user and associated devices and employed by the user for authorizing access. This is the most widely deployed integrated defense strategy in enterprise networks.

I.10 HISTORY OF THE INTERNET

I.10.1 THE DEVELOPMENT OF THE INTERNET

It is interesting to recount the development of the Internet. For almost five decades this ubiquitous information system has impacted, in a significant way, the lives of most people throughout the world. Its development is outlined in chronological order in Table I.5.

I.10.2 THE GLOBAL INFORMATION GRID (GIG) OF THE US DEPARTMENT OF DEFENSE (DOD)

The Global Information Grid (GIG) is a communications project of the United States Department of Defense. It is a secure, robust, optical terrestrial network that delivered very high-speed classified and unclassified Internet Protocol (IP) services to 87 key operating sites worldwide in 2005. Every site has an OC-192 (10 Gbps) pipe. The project is a physical manifestation of network-centric warfare (NCW). Because a robustly networked force improves information sharing, the quality of information and shared situational awareness is enhanced. This shared situational awareness enables collaboration and self-synchronization, enhances sustainability and speed of command, and in turn, has a dramatic effect on mission effectiveness [32].

This project provided nine functional GIG Enterprise Services (ES), i.e., core services, in 2004 and they are listed in Table I.6.

GIG also provides authorized users with

- A seamless, secure, and interconnected information environment
- Real-time and near real-time response of ES

TABLE I.5 The Important Developments in the History of the Internet

Year	Development
1961	Leonard Kleinrock (aka the Grandfather of the Internet) demonstrates the effectiveness of packet switching using queuing theory
1964	Packet switching is employed in military nets
1967	The Advanced Research Projects Agency conceives the ARPAnet
1969	The first ARPAnet node becomes operational. The four initial nodes are at UCLA, SRC, UCSB and UUtah
1970	The ALOHAnet, which is a satellite network, is developed in Hawaii
1972	The ARPAnet is demonstrated to the public and grows to 15 nodes. The Network Control Protocol (NCP) becomes the first host-host protocol, and the first email program is developed
1974	Vinton Cerf (aka the father of the Internet) and Robert Kahn's architecture for interconnecting networks becomes the foundation for the Internet Protocol. Its properties are minimalism, autonomy, best effort service, stateless routers and decentralized control
1976	Ethernet is developed at Xerox PARC, Intel and DEC
1977/78	Proprietary architectures, such as DECnet, SNA and XNA are developed, and ATM is developed for switching fixed length packets in hardware for virtual circuits
1979	ARPAnet grows to 200 nodes
1982	The email protocol, SMTP, is defined
1983	TCP/IP is deployed, and DNS is developed for name-to-IP address translation
1985	FTP protocol is defined
1988	TCP congestion control is developed, and new national networks, e.g., BITnet and NSFnet are developed, and 100,000 hosts are connected to form a confederation of networks
1991	NSF lifts restrictions on commercial use of NSFnet, and network access points are established to connect ISPs
Early 90's	ARPAnet is decommissioned, and the Web comes on-line with hypertext, HTML, HTTP, Mosaic and later Netscape
Late 90's, early 2000's	This period saw the development of the Web, instant messaging and P2P file sharing for music. Network security moved to the forefront. There were an estimated 50 million hosts and more than 100 million users. The backbone links were running at Gbps speeds and field tests of the Internet demonstrated decentralized control. One significant example of the Internet's value was the purchase order from Iraq to a company in Atlanta via email during the first Gulf war when the communication infrastructure was wiped out.
2008 - present	Approximately 1.7 billion users as of September 2009 [30]. The International Telecommunications Union (ITU) estimated two billion users by the end of 2010, and that is nearly a third of the world's total population currently estimated at about 6.9 billion [31]. Voice and video are delivered over IP. The P2P applications in use were BitTorrent (file sharing), Skype (VoIP), and PPLive (video). The social applications resulting from the Internet's development were huge and fostered such things as YouTube, Facebook, Twitter, various types of gaming and web 2.0. In addition, its implications on wireless and mobility proved to be enormous.

TABLE I.6 The Core Services Labeled as GIG Enterprise Services (ES)

Type	
Information sharing	Storage
Communication	Messaging
	Collaboration
Service	Discovery
	Mediation
	User assistant
	Application hosting
Security	Information assurance
Management	Enterprise service management

The GIG must permit both human users of the GIG, as well as automated services acting on behalf of GIG users, to access information and services from anywhere, based on need and capability. Information must be labeled and also cataloged using metadata, allowing users to search and retrieve the information required in order to provide them with the capability to fulfill their mission under a *smart-pull* and information management model. This requires the GIG to know where the information is posted and to recognize the user, regardless of location. While system access will be available regardless of location, access to information will be restricted based on the threat inherent at that location. An enforcement policy must be used to provide user privileges and access to the information, in addition to providing mechanisms, which ensure that the information can be trusted as coming from its claimed source. Thus, security is an embedded feature, designed into every system within the family of systems that comprise the GIG. All the policies are designed to ensure that an adversary is denied the capabilities inherent in the system for bona fide users.

I.11 CONCLUDING REMARKS

In summary, the key concepts that have been presented in this chapter are (a) the Internet architecture comprising the network edge, network core, and access networks, (b) Internet protocol layers and models, (c) the features and differences between packet-switching and circuit-switching, (d) packet loss, delay, congestion and throughput in packet-switching network, (e) the Layer 2 switch, layer 3 switch and router functions, and finally (f) security.

REFERENCES

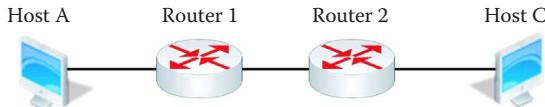
1. "Internet Engineering Task Force"; <http://www.ietf.org/rfc.html>.
2. "ICANN - Internet Corporation for Assigned Names and Numbers"; <http://www.icann.org/>.
3. J. Bingham and F. Van der Putten, *ANSI T1. 413 Issue 2: Network and Customer Installation Interfaces- Asymmetric Digital Subscriber Line (ADSL) Metallic Interface*, 1998.
4. "DOCSIS Specifications"; <http://www.cablelabs.com/cablemodem/specifications/index.html>.
5. ITU-T Rec., *G.984.1: Gigabit-capable passive optical networks (GPON): General characteristics*; <http://www.itu.int/rec/T-REC-G.984.1/en>.
6. *IEEE Std. 802.3-2008 IEEE Standard for Information technology-Specific requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CMSA/CD) Access Method and Physical Layer Specifications*, 2008; <http://standards.ieee.org/getieee802/portfolio.html>.
7. *IEEE P1901: Draft Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications*, 2010; <http://grouper.ieee.org/groups/1901/>.
8. *IEEE Std. 802.11-2007 IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 2007; <http://standards.ieee.org/getieee802/portfolio.html>.
9. *IEEE Std. 802.11n-2009 IEEE Standard for Information Technology— Telecommunications and Information Exchange Between Systems— Local and Metropolitan Area Networks— Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput*, 2009; <http://standards.ieee.org/getieee802/portfolio.html>.
10. *IEEE Std. 802.16-2009 IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems*, 2009; <http://standards.ieee.org/getieee802/portfolio.html>.
11. 3GPP specification: 25.306 V5.15.0 (2009-03) 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UE Radio Access capabilities (Release 5); <http://www.3gpp.org/ftp/Specs/html-info/25306.htm>.
12. 3GPP specification: 25.306 V7.10.0 (2009-09) 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UE Radio Access capabilities (Release 7); <http://www.3gpp.org/ftp/Specs/html-info/25306.htm>.
13. 3GPP2 Specifications: cdma2000 High Rate Packet Data Air Interface Specification (TIA-856 Rev.A), 2005; http://www.3gpp2.org/Public_html/specs/tsgc.cfm.
14. 3GPP2 Specifications: cdma2000 High Rate Packet Data Air Interface Specification (TIA-856 Rev.B), 2009; http://www.3gpp2.org/Public_html/specs/tsgc.cfm.
15. "Packet Clearing House (PCH) - Internet Exchange Directory," 2010; <https://prefix.pch.net/applications/ixpdir/>.

16. "Verizon Global Network"; <http://www.verizonbusiness.com/worldwide/about/network/maps/map.jpg>.
17. "The Internet2 Network"; <http://www.internet2.edu/network/>.
18. Blue Coat Systems, "Blue Coat Publishes Annual Web Security Report"; <http://www.bluecoat.com/news/pr/4372>.
19. C. Shan, "Zeus Crimeware Toolkit | Blog Central," 2010; <http://blogs.mcafee.com/mcafee-labs/zeus-crimeware-toolkit>.
20. P. Coogan, "SpyEye Bot versus Zeus Bot | Symantec Connect"; <http://www.symantec.com/connect/blogs/spyeye-bot-versus-zeus-bot>.
21. The H Security, "Banking trojan ZeuS homes in on SMS-TAN process - The H Security: News and Features," 2010; <http://www.h-online.com/security/news/item/Banking-trojan-ZeuS-homes-in-on-SMS-TAN-process-1097104.html>.
22. R. Lemos, "Banking Trojans Adapting To Cheat Out-of-Band Security - Dark Reading Oct 18, 2011," 2011; <http://www.darkreading.com/advanced-threats/167901091/security/client-security/231901086/banking-trojans-adapting-to-cheat-out-of-band-security.html>.
23. K. Zetter, "Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target | Threat Level | Wired.com"; <http://www.wired.com/threatlevel/2010/09/stuxnet/#ixzz10kctAGUH>.
24. Microsoft, "Microsoft Security Advisory (2718704) Unauthorized Digital Certificates Could Allow Spoofing," 2012; <http://technet.microsoft.com/en-us/security/advisory/2718704>.
25. NIST, *SP 800-41 Rev. 1: Guidelines on Firewalls and Firewall Policy*, 2009; <http://csrc.nist.gov/publications/PubsSPs.html>.
26. NIST, *SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, 2007; <http://csrc.nist.gov/publications/PubsSPs.html>.
27. A. Frier, P. Carlton, and P. Kocher, *The SSL 3.0 protocol*, 1996.
28. S. Kent and R. Atkinson, *RFC 2401: Security Architecture for the Internet Protocol*, 1998.
29. *IEEE Std. 802.1X-2004 IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control*, 2004; <http://standards.ieee.org/getieee802/portfolio.html>.
30. "World Internet Usage Statistics News and World Population Stats"; <http://www.internetworkworldstats.com/stats.htm>.
31. techspot.com, "Internet to exceed 2 billion users this year - TechSpot News," 2010; <http://www.techspot.com/news/40741-internet-to-exceed-2-billion-users-this-year.html>.
32. "Network Centric Warfare: Background and Oversight Issues for Congress. CRS Report for Congress - Storming Media"; <http://www.stormingmedia.us/50/5026/A502634.html>.

PROBLEMS

- I.1. If statistical multiplexing (SM) is used to provide Internet services, describe the ramifications of its use by an ISP when demand for bandwidth is high.
- I.2. Explain the difference between transmission delay and propagation delay.
- I.3. If a packet contains 100 bytes of headers (MAC, IP and TCP), 4 bytes of trailer for error detection, and 1000 bytes of payload, calculate the percent overhead (Indirect cost/ Total cost) spent in delivering the 1000 byte payload.
- I.4. If a packet contains 80 bytes of headers (MAC, IP and TCP), 4 bytes trailer for error detection, as well as 100 bytes of payload, calculate the overhead (%) involved in delivering the payload.
- I.5. A packet contains 60 bytes of headers (MAC, IP and UDP header), a 4 byte trailer for error detection, and 100 bytes of payload. Determine the overhead (%) involved in delivering this information.
- I.6. TCP's connection oriented approach requires a round trip for establishing a connection before delivering a file. If a file of 1000 bytes is sent over a link that has a 1.536 Mbps bandwidth and a 1 ms propagation delay, determine the overhead (%) involved in establishing a connection and sending the file from host A to host B. Neglect other delays.

- I.7. Given the network shown in Figure PI.7 with destination host C connected to Router 2, determine the delay involved in sending a packet from host A to host C if the queuing delay is 0 and the remaining parameters are as follows:



PI.7

Packet length = 7 Kbits
 Link rate R = 1 Mbps
 Packet processing time = 0.001 s
 Propagation speed s = 2×10^8 m/s
 Distance between routers d = 2×10^5 m
 Distance between router and host d = 0 m

- I.8. If a destination host C is connected to Router 2 as shown in the network in Figure PI.7, determine the delay involved in sending a packet from host A to host C given the following parameters and a router queuing delay of 5 ms:

Packet length = 7 Kbits
 Link rate R = 1 Mbps
 Packet processing time = 0.001 s
 Propagation speed s = 2×10^8 m/s
 Distance between routers d = 2×10^5 m
 Distance between router and host d = 0 m

- I.9. For the network shown in Figure PI.7, determine the delay involved in sending a packet from host A to host C given the following parameters:

Packet length = 10 Kbits
 Link rate R = 1 Mbps
 Packet processing time = 0.002 s
 Propagation speed s = 2×10^8 m/s
 Distance between routers d = 2×10^6 m
 Distance between router and host d = 0 m
 Queuing delay = 2 ms

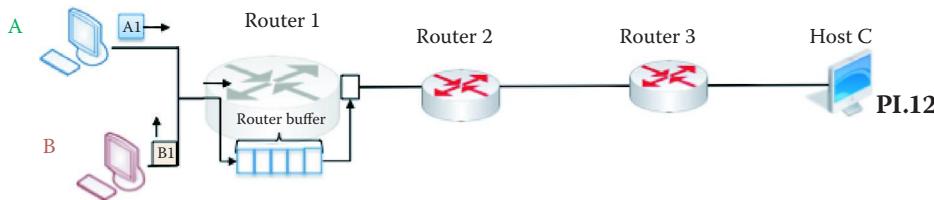
- I.10. If a destination host C is connected to Router 2 as shown in the network in Figure PI.7, determine the delay involved in sending a packet from host A to host C given the following parameters:

Packet length = 5 Kbits
 Link rate R = 2 Mbps
 Packet processing time = 100 μ s
 Propagation speed s = 2×10^8 m/s
 Distance between routers d = 5×10^4 m
 Queuing delay = 0.5 ms
 Distance between router and host d = 0 m

- I.11. Destination host C is connected to Router 2 in the network in Figure PI.7. Determine the delay involved in sending a packet from host A to host C given the following parameters:

Packet length = 3.1 Kbits
 Link rate R = 155 Mbps
 Packet processing time = 400 ns
 Propagation speed s = 2×10^8 m/s
 Distance between routers d = 5×10^3 m
 Queuing delay = 800 ns
 Distance between router and host d = 0 m

- I.12. Given the network shown in Figure PI.12, in which destination host C is connected to Router 3, determine the delay involved in sending a packet from host A to host C if the queuing delay is 0 and the remaining parameters are as follows:



Packet length = 7 Kbits

Link rate R = 1 Mbps

Packet processing time = 0.001 s

Propagation speed s = 2×10^8 m/s

Distance between routers d = 2×10^5 m

Distance between router and host d = 0 m

- I.13. If a destination host C is connected to Router 3 as shown in the network in Figure PI.12, determine the delay involved in sending a packet from host A to host C given the following parameters and a queuing delay of 5 ms:

Packet length = 7 Kbits

Link rate R = 1 Mbps

Packet processing time = 0.001 s

Propagation speed s = 2×10^8 m/s

Distance between routers d = 2×10^5 m

Distance between router and host d = 0 m

- I.14. For the network shown in Figure PI.12, determine the delay involved in sending a packet from host A to host C given the following parameters:

Packet length = 10 Kbits

Link rate R = 1 Mbps

Packet processing time = 0.002 s

Propagation speed s = 2×10^8 m/s

Distance between routers d = 2×10^6 m

Queuing delay = 2 ms

Distance between router and host d = 0 m

- I.15. For the network shown in Figure PI.12, determine the delay involved in sending a packet from host A to host C given the following parameters:

Packet length = 5 Kbits

Link rate R = 2 Mbps

Packet processing time = 100 us

Propagation speed s = 2×10^8 m/s

Distance between routers d = 5×10^4 m

Queuing delay = 0.5 ms

Distance between router and host d = 0 m

- I.16. For the network shown in Figure PI.12, determine the delay involved in sending a packet from host A to host C given the following parameters:

Packet length = 3.1 Kbits

Link rate R = 155 Mbps

Packet processing time = 400 ns

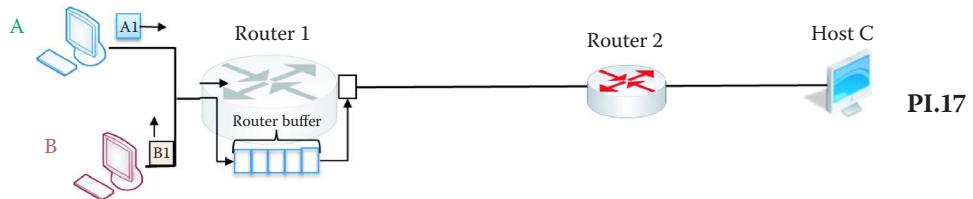
Propagation speed s = 2×10^8 m/s

Distance between routers d = 5×10^3 m

Queuing delay = 800 ns

Distance between router and host d = 0 m

- I.17. Given the network in Figure PI.17 and the following assumptions and parameters, determine the time at which Host C receives the packet B1:



Packet length $L = 2 \text{ Kbits}$

Link rate $R = 1 \text{ Mbps}$

Propagation speed $s = 2 \times 10^8 \text{ m/sec}$

Distance between routers $d = 2 \times 10^5 \text{ m}$

Propagation delay $= d/s = (2 \times 10^5 \text{ m})/(2 \times 10^8 \text{ m/sec}) = 0.001 \text{ s}$

Transmission delay $= L/R = (2 \text{ Kbits})/(1 \text{ Mbps}) = 0.002 \text{ s}$

Packet processing time $= 0.001 \text{ s}$

Distance between router and host $d = 0 \text{ m}$

A has 4 packets to send (A_1, A_2, A_3, A_4), B has 5 packets to send (B_1, B_2, B_3, B_4, B_5) and the packets are sent in the sequence $B_1, A_1, B_2, A_2, \dots$ etc.

Routers 1 and 2 have buffer space for 5 packets

A and B have infinite buffer space and their distances to the first router are assumed to be zero.

Assume UDP Transmission

- I.18. Given the data in Problem I.17, calculate the time at which the packet A_1 reaches Host C.

- I.19. Given the network in Figure PI.17 and the following assumptions and parameters, determine the time at which Host C receives the packet B1:

Packet length $L = 3 \text{ Kbits}$

Link rate $R = 1 \text{ Mbps}$

Propagation speed $s = 2 \times 10^8 \text{ m/sec}$

Distance between routers $d = 2 \times 10^5 \text{ m}$

Propagation delay $= d/s = (2 \times 10^5 \text{ m})/(2 \times 10^8 \text{ m/sec}) = 0.001 \text{ s}$

Transmission delay $= L/R = (3 \text{ Kbits})/(1 \text{ Mbps}) = 0.003 \text{ s}$

Packet processing time $= 0.001 \text{ s}$

Distance between router and host $d = 0 \text{ m}$

A has 4 packets to send (A_1, A_2, A_3, A_4), B has 5 packets to send (B_1, B_2, B_3, B_4, B_5) and the packets are sent in the sequence $B_1, A_1, B_2, A_2, \dots$ etc.

Routers 1 and 2 have buffer space for 5 packets

A and B have infinite buffer space and their distances to the first router are assumed to be zero.

Assume UDP Transmission

- I.20. Given the data in Problem I.19, determine the time at which packet A_1 arrives at Host C.

- I.21. Given the data in Problem I.19, determine the time at which packet B_2 arrives at Host C.

- I.22. Given the data in Problem I.19, determine the time at which packet A_2 arrives at Host C.

- I.23. Given the network in Figure PI.17 and the following assumptions and parameters, determine the time at which Host C receives the packet B1:

Packet length $L = 3 \text{ Kbits}$

Link rate $R = 1 \text{ Mbps}$

Propagation speed $s = 2 \times 10^8 \text{ m/sec}$

Distance between routers $d = 2 \times 10^5 \text{ m}$

Propagation delay = $d/s = (4 \times 10^5 \text{ m})/(2 \times 10^8 \text{ m/sec}) = 0.002 \text{ s}$

Transmission delay = $L/R = (2 \text{ Kbits})/(1 \text{ Mbps}) = 0.003 \text{ s}$

Packet processing time = 0.001 s

Distance between router and host $d = 0 \text{ m}$

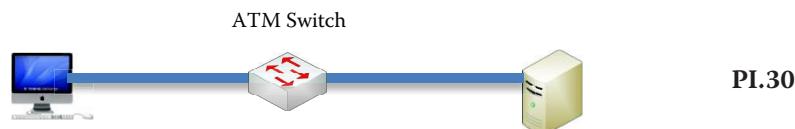
A has 4 packets to send (A1, A2, A3, A4), B has 5 packets to send (B1, B2, B3, B4, B5) and the packets are sent in the sequence B1, A1, B2, A2,—etc.

Routers 1 and 2 have buffer space for 5 packets

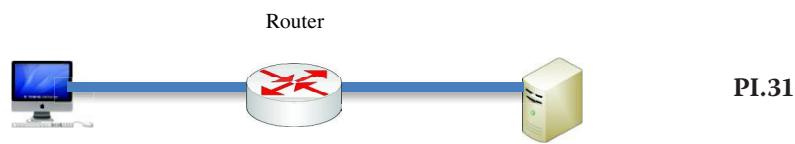
A and B have infinite buffer space and their distances to the first router are assumed to be zero.

Assume UDP Transmission

- I.24. Given the data in Problem I.23, determine the time at which packet A1 arrives at Host C.
- I.25. Given the data in Problem I.23, determine the time at which packet B2 arrives at Host C.
- I.26. Given the data in Problem I.23, determine the time at which packet A2 arrives at Host C.
- I.27. A house connected to the Internet uses a DSL modem with an average download rate 1.5 Mbps. If a 100 M-bit file is to be downloaded, what is the average time required?
- I.28. A house is connected to the Internet through a cable modem with an average downstream data rate of 948 Mbps to the neighborhood with 500 users. If a 100 M-bit file is to be downloaded, what is the average time required?
- I.29. A university is connected to the Internet via a 2.5 Gbps ATM circuit. The connection set-up time is 100ms. If a 100 M-bit file is to be downloaded, what is the shortest time required to download this file?
- I.30. A university is connected to the Internet via a 2.5 Gbps ATM circuit. The time needed to set up a connection is 100 ms in order to download a 100 M-bit file. If the server is connected as shown in Figure PI.30, and the propagation speed in the ATM circuit is $s = 2 \times 10^8 \text{ m/sec}$, what is the shortest time required to download this file?



- I.31. A university is connected to the Internet using a 2.5 Gbps IP network. The router needs 1ms to route a packet, each packet is 10000 bytes long and a 100 M-bit file must be downloaded. Assuming there is no congestion in the network, the server is connected as shown in Figure PI.31 and the propagation speed in the network is $s = 2 \times 10^8 \text{ m/sec}$, what is the shortest amount of time needed to download this file?



- I.32. Solve Problem I.30 if the distance between the server and host is 2 km.
- I.33. Solve Problem I.31 if the distance between the server and host is 2 km.
- I.34. Solve Problem I.32 if the ATM data rate is changed to 1.5 Mbps.
- I.35. Solve Problem I.33 if the link data rate is 1.5 Mbps.

- I.36. Solve Problem I.30 if the ATM data rate is 1.5 Mbps.
- I.37. Solve Problem I.31 if the link data rate is 1.5 Mbps.
- I.38. Compare the results obtained from Problem I.30 with those of Problem I.37, and determine if there is a dominant factor in each problem, and if so what it is.
- I.39. If statistical multiplexing (SM) is used to provide Internet services, describe the ramifications of its use by an ISP when demand for bandwidth is high.
- I.40. Explain the difference between transmission delay and propagation delay.
- I.41. If a packet contains 100 bytes of headers (MAC, IP and TCP), 4 bytes of trailer for error detection, and 1000 bytes of payload, calculate the percent overhead (Indirect cost/ Total cost) spent in delivering the 1000 byte payload.
- I.42. If a packet contains 80 bytes of headers (MAC, IP and TCP), 4 bytes trailer for error detection, as well as 100 bytes of payload, calculate the overhead (%) involved in delivering the payload.
- I.43. A packet contains 60 bytes of headers (MAC, IP and UDP header), a 4 byte trailer for error detection, and 100 bytes of payload. Determine the overhead (%) involved in delivering this information.
- I.44. TCP's connection oriented approach requires a round trip for establishing a connection before delivering a file. If a file of 1000 bytes is sent over a link that has a 1.536 Mbps bandwidth and a 1 ms propagation delay, determine the overhead (%) involved in establishing a connection and sending the file from host A to host B. Neglect other delays.
- I.45. The Internet backbone consists of a group of regional ISPs.
 - (a) True
 - (b) False
- I.46. Access networks are the links between ISPs.
 - (a) True
 - (b) False
- I.47. The standards that control the use of the Internet are listed in what are called
 - (a) RFPs
 - (b) RFCs
 - (c) RFIs
- I.48. Elements within the Internet core are typically interconnected with
 - (a) Wire
 - (b) Radio
 - (c) Fiber
 - (d) None of the above
- I.49. The standards body for IETF is ICANN.
 - (a) True
 - (b) False
- I.50. A LAN is connected to the hierarchical portion of the Internet via a
 - (a) Edge router
 - (b) Gateway
 - (c) All of the above
 - (d) None of the above

- I.51. The connection between a residence and an ISP can be of the form
(a) Cable modem
(b) DSL
(c) FITL
(d) All of the above
- I.52. The advantage of using a dialup connection to surf the Internet is that the phone can be used at the same time.
(a) True
(b) False
- I.53. The advertised speed of the digital subscriber line is 56 Kbps.
(a) True
(b) False
- I.54. The frequency range for an ordinary telephone is 0-4 KHz.
(a) True
(b) False
- I.55. The technology that uses fiber into a neighborhood and then coax to individual homes is
(a) DSL
(b) DSLAM
(c) HFC
(d) None of the above
- I.56. From the following, select the best technology for high speed communication:
(a) BPL
(b) FITL
(c) POTS
- I.57. In an Ethernet LAN, hosts are connected to an Ethernet switch and operate at which of the following speeds?
(a) 10 Mbps
(b) 100 Mbps
(c) 1 Gbps
(d) 10 Gbps
(e) All of the above
(f) None of the above
- I.58. Global ISPs are also known as Tier-1 ISPs.
(a) True
(b) False
- I.59. Tier-1 ISPs are interconnected at IXPs.
(a) True
(b) False
- I.60. Verizon and Level 3 Communications are examples of Tier-1 ISPs.
(a) True
(b) False
- I.61. The number of layers in the U.S. DoD protocol stack is
(a) 2
(b) 3
(c) 4
(d) 5
(e) 6

- I.62. The layer in the protocol stack that aggregates the media bits into, e.g., a frame is
- (a) Physical layer
 - (b) Network layer
 - (c) Data link layer
- I.63. The layer in the protocol stack that routes packets is the
- (a) Data link layer
 - (b) Network layer
 - (c) Transport layer
- I.64. TCP and UDP are handled by the following layer of the protocol stack
- (a) Data link layer
 - (b) Network layer
 - (c) Transport layer
- I.65. One or more protocols support each layer of the protocol stack.
- (a) True
 - (b) False
- I.66. Protocols are implemented only in software.
- (a) True
 - (b) False
- I.67. As a message at the host proceeds down the protocol stack, the destination IP address is added at the
- (a) Transport layer
 - (b) Network layer
 - (c) Data link layer
 - (d) None of the above
- I.68. The layer of the protocol stack at the source that is responsible for delivering packets to the transport layer at the destination is
- (a) Transport layer
 - (b) Network layer
 - (c) Data link layer
 - (d) None of the above
- I.69. The movement of bits in the physical transmission media is the responsibility of the
- (a) Transport layer
 - (b) Network layer
 - (c) Data link layer
 - (d) None of the above
- I.70. Routers operate at
- (a) Layer 2
 - (b) Layer 3
 - (c) None of the above
- I.71. In transmission from source to destination, the source has to know the IP address of the first gateway and uses which of the following to obtain the gateway's MAC address?
- (a) ARP
 - (b) TCP
 - (c) SMTP
 - (d) None of the above

- I.72. In contrast to a layer 2 switch, routers and layer 3 switches understand both MAC and IP addresses.
- (a) True
 - (b) False
- I.73. TCP is a best effort, unreliable data delivery service.
- (a) True
 - (b) False
- I.74. UDP is a good transport service for voice and video.
- (a) True
 - (b) False
- I.75. With circuit switching, packets may be lost, corrupted or delivered out of order.
- (a) True
 - (b) False
- I.76. When packet switching is used, the layer at the destination that is responsible for reassembling the packets in the correct order is the
- (a) Data link
 - (b) Network
 - (c) Transport
- I.77. In IP-based transmission, an IP unicast provides a mechanism for sending a single media stream to a group of recipients on the Internet.
- (a) True
 - (b) False
- I.78. Statistical multiplexing is an efficient method for packet switching.
- (a) True
 - (b) False
- I.79. Circuit switching is the best technique for bursty data while packet switching is best for voice and video.
- (a) True
 - (b) False
- I.80. Buffer overrun is a symptom of congestion that will trigger flow control.
- (a) True
 - (b) False
- I.81. When the speed of the incoming packets exceeds the link data rate which of the following may occur?
- (a) Transmission delay
 - (b) Queuing delay
 - (c) Packet loss
 - (d) All of the above
- I.82. One of the most devastating effects of malware is the fact that it can mutate.
- (a) True
 - (b) False

- I.83. Which of the following are categories of malware?
- (a) Trojans
 - (b) Spyware
 - (c) Viruses
 - (d) Worms
 - (e) All of the above
- I.84. Trojans that may contain other categories of malware can provide a backdoor for illegal access to a host.
- (a) True
 - (b) False
- I.85. Which of the following elements are placed at critical points within a system to protect vital assets?
- (a) Firewall
 - (b) IDS
 - (c) IPS
 - (d) All of the above
- I.86. Which of the following elements are used in a system to monitor traffic by inspecting the entire packet?
- (a) Firewall
 - (b) IDS
 - (c) IPS
 - (d) All of the above
- I.87. While a firewall will block traffic from the Internet to the internal network it does permit traffic originating in the DMZ to enter the internal network.
- (a) True
 - (b) False
- I.88. IDS/IPS is strategically located on the Internet side of the firewall in order to detect a wide range of attacks.
- (a) True
 - (b) False
- I.89. Encryption and authentication are protection mechanisms employed in the transmission media.
- (a) True
 - (b) False
- I.90. The approximate number of decades that the Internet has been in existence is
- (a) 3
 - (b) 4
 - (c) 5
 - (d) 6

1

Applications

References

An Introduction to Information Networks

16. "Verizon Global Network";
17. "The Internet2 Network";
[http://www.internet2.edu/network/.](http://www.internet2.edu/network/)
18. Blue Coat Systems, "Blue Coat Publishes Annual Web Security Report"; [http://www.bluecoat.com/news/pr/4372.](http://www.bluecoat.com/news/pr/4372)
19. C. Shan, "Zeus Crimeware Toolkit | Blog Central," 2010;
[http://blogs.mcafee.com/mcafee-labs/zeuscrimeware-toolkit.](http://blogs.mcafee.com/mcafee-labs/zeuscrimeware-toolkit)
20. P. Coogan, "SpyEye Bot versus Zeus Bot | Symantec Connect"; [http://www.symantec.com/connect/blogs/spyeye-bot-versus-zeus-bot.](http://www.symantec.com/connect/blogs/spyeye-bot-versus-zeus-bot)
21. The H Security, "Banking trojan ZeuS homes in on SMS-TAN process - The H Security: News and Features," 2010;
22. R. Lemos, "Banking Trojans Adapting To Cheat Out-of-Band Security - Dark Reading Oct 18, 2011," 2011;
23. K. Zetter, "Blockbuster Worm Aimed for Infrastructure, But No Proof Iran Nukes Were Target | Threat Level | Wired.com";
24. Microsoft, "Microsoft Security Advisory (2718704) Unauthorized Digital Certificates Could Allow Spoofing," 2012;
25. NIST, SP 800-41 Rev. 1: Guidelines on Firewalls and Firewall Policy, 2009;
[http://csrc.nist.gov/publications/PubsSPs.html.](http://csrc.nist.gov/publications/PubsSPs.html)
26. NIST, SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, 2007;
[http://csrc.nist.gov/publications/PubsSPs.html.](http://csrc.nist.gov/publications/PubsSPs.html)
27. A. Frier, P. Karlton, and P. Kocher, The SSL 3.0 protocol, 1996.
28. S. Kent and R. Atkinson, RFC 2401: Security Architecture for the Internet Protocol, 1998.
29. IEEE Std. 802.1X-2004 IEEE Standard for Local and

Metropolitan Area Networks- Port-Based Network Access Control, 2004;
<http://standards.ieee.org/getieee802/portfolio.html>.

30. "World Internet Usage Statistics News and World Population Stats"; <http://www.internetworkworldstats.com/stats.htm>.
31. techspot.com, "Internet to exceed 2 billion users this year - TechSpot News," 2010; <http://www.techspot.com/news/1155/internet-to-exceed-2-billion-users-this-year.html>.

32. "Network Centric Warfare: Background and Oversight Issues for Congress. CRS Report for Congress - Storming Media"; <http://www.stormingmedia.us/50/5026/A502634.html>.

PROBLEMS

I.1. If statistical multiplexing (SM) is used to provide Internet services, describe the ramifications of its use by an ISP when demand for bandwidth is high.

I.2. Explain the difference between transmission delay and propagation delay.

I.3. If a packet contains 100 bytes of headers (MAC, IP and TCP), 4 bytes of trailer for error detection, and 1000 bytes of payload, calculate the percent overhead (Indirect cost/ Total cost) spent in delivering the 1000 byte payload.

I.4. If a packet contains 80 bytes of headers (MAC, IP and TCP), 4 bytes trailer for error detection, as well as 100 bytes of payload, calculate the overhead (%) involved in delivering the payload.

I.5. A packet contains 60 bytes of headers (MAC, IP and UDP header), a 4 byte trailer for error detection, and 100 bytes of payload. Determine the overhead (%) involved in delivering this information.

I.6. TCP's connection oriented approach requires a round trip for establishing a connection before delivering a file. If a file of 1000 bytes is sent over a link that has a 1.536 Mbps bandwidth and a 1 ms propagation delay, determine the overhead (%) involved in establishing a connection and sending the file from host A to host B. Neglect other delays. I.7. Given the network shown in Figure PI.7 with destination host C connected to Router 2, determine the delay involved in sending a packet from host A to host C if the queuing delay is 0 and the remaining

parameters are as follows: Host A Host C Router 1 Router 2
PI.7 Packet length = 7 Kbits Link rate R = 1 Mbps Packet
processing time = 0.001 s Propagation speed s = 2×10^{-8}
m/s Distance between routers d = 2×10^{-5} m Distance
between router and host d = 0 m I.8. If a destination host
C is connected to Router 2 as shown in the network in
Figure PI.7, determine the delay involved in sending a
packet from host A to host C given the following parameters
and a router queuing delay of 5 ms: Packet length = 7 Kbits
Link rate R = 1 Mbps Packet processing time = 0.001 s
Propagation speed s = 2×10^{-8} m/s Distance between
routers d = 2×10^{-5} m Distance between router and host d
= 0 m I.9. For the network shown in Figure PI.7, determine
the delay involved in sending a packet from host A to host
C given the following parameters: Packet length = 10 Kbits
Link rate R = 1 Mbps Packet processing time = 0.002 s
Propagation speed s = 2×10^{-8} m/s Distance between
routers d = 2×10^{-6} m Distance between router and host d
= 0 m Queuing delay = 2 ms I.10. If a destination host C
is connected to Router 2 as shown in the network in Figure
PI.7, determine the delay involved in sending a packet
from host A to host C given the following parameters:
Packet length = 5 Kbits Link rate R = 2 Mbps Packet
processing time = 100 μ s Propagation speed s = 2×10^{-8}
m/s Distance between routers d = 5×10^{-4} m Queuing delay
= 0.5 ms Distance between router and host d = 0 m I.11.
Destination host C is connected to Router 2 in the network
in Figure PI.7. Determine the delay involved in sending a
packet from host A to host C given the following
parameters: Packet length = 3.1 Kbits Link rate R = 155
Mbps Packet processing time = 400 ns Propagation speed s =
 2×10^{-8} m/s Distance between routers d = 5×10^{-3} m
Queuing delay = 800 ns Distance between router and host d =
0 m

I.12. Given the network shown in Figure PI.12, in which
destination host C is connected to Router 3, determine the
delay involved in sending a packet from host A to host C if
the queuing delay is 0 and the remaining parameters are as
follows: Router 1 A1 B1 B A Router buffer Router 2 Router 3
Host C PI.12 Packet length = 7 Kbits Link rate R = 1 Mbps
Packet processing time = 0.001 s Propagation speed s = $2 \times$
 10^{-8} m/s Distance between routers d = 2×10^{-5} m Distance
between router and host d = 0 m

I.13. If a destination host C is connected to Router 3 as
shown in the network in Figure PI.12, determine the delay
involved in sending a packet from host A to host C given
the following parameters and a queuing delay of 5 ms:
Packet length = 7 Kbits Link rate R = 1 Mbps Packet

processing time = 0.001 s Propagation speed s = 2×10^8 m/s Distance between routers d = 2×10^5 m Distance between router and host d = 0 m

I.14. For the network shown in Figure PI.12, determine the delay involved in sending a packet from host A to host C given the following parameters: Packet length = 10 Kbits Link rate R = 1 Mbps Packet processing time = 0.002 s Propagation speed s = 2×10^8 m/s Distance between routers d = 2×10^6 m Queuing delay = 2 ms Distance between router and host d = 0 m

I.15. For the network shown in Figure PI.12, determine the delay involved in sending a packet from host A to host C given the following parameters: Packet length = 5 Kbits Link rate R = 2 Mbps Packet processing time = 100 us Propagation speed s = 2×10^8 m/s Distance between routers d = 5×10^4 m Queuing delay = 0.5 ms Distance between router and host d = 0 m

I.16. For the network shown in Figure PI.12, determine the delay involved in sending a packet from host A to host C given the following parameters: Packet length = 3.1 Kbits Link rate R = 155 Mbps Packet processing time = 400 ns Propagation speed s = 2×10^8 m/s Distance between routers d = 5×10^3 m Queuing delay = 800 ns Distance between router and host d = 0 m

I.17. Given the network in Figure PI.17 and the following assumptions and parameters, determine the time at which Host C receives the packet B1:
Router 1 A1 B1 B A Router buffer Router 2 Host C PI.17
Packet length L = 2 Kbits Link rate R = 1 Mbps Propagation speed s = 2×10^8 m/sec Distance between routers d = 2×10^5 m Propagation delay = $d/s = (2 \times 10^5 \text{ m})/(2 \times 10^8 \text{ m/sec}) = 0.001 \text{ s}$ Transmission delay = $L/R = (2 \text{ Kbits})/(1 \text{ Mbps}) = 0.002 \text{ s}$ Packet processing time = 0.001 s Distance between router and host d = 0 m A has 4 packets to send (A1, A2, A3, A4), B has 5 packets to send (B1, B2, B3, B4, B5) and the packets are sent in the sequence B1, A1, B2, A2, etc. Routers 1 and 2 have buffer space for 5 packets A and B have infinite buffer space and their distances to the first router are assumed to be zero. Assume UDP

I.18. Given the data in Problem I.17, calculate the time at which the packet A1 reaches Host C.

I.19. Given the network in Figure PI.17 and the following assumptions and parameters, determine the time at which Host C receives the packet B1: Packet length L = 3 Kbits Link rate R = 1 Mbps Propagation speed s = 2×10^8 m/sec Distance between routers d = 2×10^5 m Propagation delay = $d/s = (2 \times 10^5 \text{ m})/(2 \times 10^8 \text{ m/sec}) = 0.001 \text{ s}$ Transmission delay = $L/R = (2 \text{ Kbits})/(1 \text{ Mbps}) = 0.003 \text{ s}$

Packet processing time = 0.001 s Distance between router and host d = 0 m A has 4 packets to send (A1, A2, A3, A4), B has 5 packets to send (B1, B2, B3, B4, B5) and the packets are sent in the sequence B1, A1, B2, A2,-etc. Routers 1 and 2 have buffer space for 5 packets A and B have infinite buffer space and their distances to the first router are assumed to be zero. Assume UDP Transmission

I.20. Given the data in Problem I.19, determine the time at which packet A1 arrives at Host C. I.21. Given the data in Problem I.19, determine the time at which packet B2 arrives at Host C. I.22. Given the data in Problem I.19, determine the time at which packet A2 arrives at Host C. I.23. Given the network in Figure PI.17 and the following assumptions and parameters, determine the time at which Host C receives the packet B1. Packet length L = 3 Kbits Link rate R = 1 Mbps Propagation speed s = 2×10^8 m/sec Distance between routers d = 2×10^5 m Propagation delay = $d/s = (4 \times 10^5 \text{ m})/(2 \times 10^8 \text{ m/sec}) = 0.002 \text{ s}$ Transmission delay = $L/R = (2 \text{ Kbits})/(1 \text{ Mbps}) = 0.003 \text{ s}$ Packet processing time = 0.001 s Distance between router and host d = 0 m A has 4 packets to send (A1, A2, A3, A4), B has 5 packets to send (B1, B2, B3, B4, B5) and the packets are sent in the sequence B1, A1, B2, A2,-etc. Routers 1 and 2 have buffer space for 5 packets A and B have infinite buffer space and their distances to the first router are assumed to be zero. Assume UDP Transmission

I.24. Given the data in Problem I.23, determine the time at which packet A1 arrives at Host C.

I.25. Given the data in Problem I.23, determine the time at which packet B2 arrives at Host C.

I.26. Given the data in Problem I.23, determine the time at which packet A2 arrives at Host C.

I.27. A house connected to the Internet uses a DSL modem with an average download rate 1.5 Mbps. If a 100 M-bit file is to be downloaded, what is the average time required?

I.28. A house is connected to the Internet through a cable modem with an average downstream data rate of 948 Mbps to the neighborhood with 500 users. If a 100 M-bit file is to be downloaded, what is the average time required?

I.29. A university is connected to the Internet via a 2.5 Gbps ATM circuit. The connection set-up time is 100ms. If a 100 M-bit file is to be downloaded, what is the shortest time required to download this file?

I.30. A university is connected to the Internet via a 2.5 Gbps ATM circuit. The time needed to set up a connection is 100 ms in order to download a 100 M-bit file. If the server is connected as shown in Figure PI.30, and the propagation speed in the ATM circuit is $s = 2 \times 10^8$ m/sec, what is the shortest time required to download this file? ATM Switch PI.30

I.31. A university is connected to the Internet using a 2.5 Gbps IP network. The router needs 1ms to route a packet, each packet is 10000 bytes long and a 100 M-bit file must be downloaded. Assuming there is no congestion in the network, the server is connected as shown in Figure PI.31 and the propagation speed in the network is $s = 2 \times 10^8$ m/sec, what is the shortest amount of time needed to download this file? Router PI.31

I.32. Solve Problem I.30 if the distance between the server and host is 2 km.

I.33. Solve Problem I.31 if the distance between the server and host is 2 km.

I.34. Solve Problem I.32 if the ATM data rate is changed to 1.5 Mbps.

I.35. Solve Problem I.33 if the link data rate is 1.5 Mbps.

I.36. Solve Problem I.30 if the ATM data rate is 1.5 Mbps.

I.37. Solve Problem I.31 if the link data rate is 1.5 Mbps.

I.38. Compare the results obtained from Problem I.30 with those of Problem I.37, and determine if there is a dominant factor in each problem, and if so what it is.

I.39. If statistical multiplexing (SM) is used to provide Internet services, describe the ramifications of its use by an ISP when demand for bandwidth is high. I.40. Explain the difference between transmission delay and propagation delay. I.41. If a packet contains 100 bytes of headers (MAC, IP and TCP), 4 bytes of trailer for error detection, and 1000 bytes of payload, calculate the percent overhead (Indirect cost/ Total cost) spent in delivering the 1000 byte payload. I.42. If a packet contains 80 bytes of headers (MAC, IP and TCP), 4 bytes trailer for error detection, as well as 100 bytes of payload, calculate the overhead (%) involved in delivering the payload. I.43. A packet contains 60 bytes of headers (MAC, IP and UDP header), a 4 byte trailer for error detection, and 100 bytes of payload. Determine the overhead (%) involved in delivering this information. I.44. TCP's connection oriented approach requires a round trip for establishing a

connection before delivering a file. If a file of 1000 bytes is sent over a link that has a 1.536 Mbps bandwidth and a 1 ms propagation delay, determine the overhead (%) involved in establishing a connection and sending the file from host A to host B. Neglect other delays. I.45. The Internet backbone consists of a group of regional ISPs.

(a) True (b) False I.46. Access networks are the links between ISPs. (a) True (b) False I.47. The standards that control the use of the Internet are listed in what are called (a) RFPs (b) RFCs (c) RFIs I.48. Elements within the Internet core are typically interconnected with (a) Wire (b) Radio (c) Fiber (d) None of the above I.49. The standards body for IETF is ICANN. (a) True (b) False I.50. A LAN is connected to the hierarchical portion of the Internet via a (a) Edge router (b) Gateway (c) All of the above (d) None of the above

I.51. The connection between a residence and an ISP can be of the form

- (a) Cable modem
- (b) DSL
- (c) FITL
- (d) All of the above

I.52. The advantage of using a dialup connection to surf the Internet is that the phone can be used at the same time.

- (a) True
- (b) False

I.53. The advertised speed of the digital subscriber line is 56 Kbps.

- (a) True
- (b) False

I.54. The frequency range for an ordinary telephone is 0-4 KHz.

- (a) True
- (b) False

I.55. The technology that uses fiber into a neighborhood and then coax to individual homes is

- (a) DSL
- (b) DSLAM
- (c) HFC
- (d) None of the above

I.56. From the following, select the best technology for high speed communication:

- (a) BPL
- (b) FITL
- (c) POTS

I.57. In an Ethernet LAN, hosts are connected to an Ethernet switch and operate at which of the following speeds?

- (a) 10 Mbps
- (b) 100 Mbps
- (c) 1 Gbps
- (d) 10 Gbps
- (e) All of the above
- (f) None of the above

I.58. Global ISPs are also known as Tier-1 ISPs.

- (a) True
- (b) False

I.59. Tier-1 ISPs are interconnected at IXPs.

- (a) True
- (b) False

I.60. Verizon and Level 3 Communications are examples of Tier-1 ISPs.

(a) True

(b) False

I.61. The number of layers in the U.S. DoD protocol stack is

(a) 2

(b) 3

(c) 4

(d) 5

(e) 6 I.62. The layer in the protocol stack that aggregates the media bits into, e.g., a frame is (a) Physical layer (b) Network layer (c) Data link layer

I.63. The layer in the protocol stack that routes packets is the (a) Data link layer (b) Network layer (c) Transport layer I.64. TCP and UDP are handled by the following layer of the protocol stack (a) Data link layer

(b) Network layer (c) Transport layer I.65. One or more protocols support each layer of the protocol stack. (a) True (b) False I.66. Protocols are implemented only in software. (a) True (b) False I.67. As a message at the host proceeds down the protocol stack, the destination IP address is added at the (a) Transport layer (b) Network layer (c) Data link layer (d) None of the above I.68.

The layer of the protocol stack at the source that is responsible for delivering packets to the transport layer at the destination is (a) Transport layer (b) Network layer (c) Data link layer (d) None of the above I.69.

The movement of bits in the physical transmission media is the responsibility of the (a) Transport layer (b) Network layer (c) Data link layer (d) None of the above I.70.

Routers operate at (a) Layer 2 (b) Layer 3 (c) None of the above I.71. In transmission from source to

destination, the source has to know the IP address of the first gateway and uses which of the following to obtain the gateway's MAC address? (a) ARP (b) TCP (c) SMTP (d)

None of the above

I.72. In contrast to a layer 2 switch, routers and layer 3 switches understand both MAC and IP addresses.

(a) True

(b) False

I.73. TCP is a best effort, unreliable data delivery service.

- (a) True
- (b) False

I.74. UDP is a good transport service for voice and video.

- (a) True
- (b) False

I.75. With circuit switching, packets may be lost, corrupted or delivered out of order.

- (a) True
- (b) False

I.76. When packet switching is used, the layer at the destination that is responsible for reassembling the packets in the correct order is the

- (a) Data link
- (b) Network
- (c) Transport

I.77. In IP-based transmission, an IP unicast provides a mechanism for sending a single media stream to a group of recipients on the Internet.

- (a) True
- (b) False

I.78. Statistical multiplexing is an efficient method for packet switching.

- (a) True
- (b) False

I.79. Circuit switching is the best technique for bursty data while packet switching is best for voice and video.

- (a) True

(b) False

I.80. Buffer overrun is a symptom of congestion that will trigger flow control.

(a) True

(b) False

I.81. When the speed of the incoming packets exceeds the link data rate which of the following may occur?

(a) Transmission delay

(b) Queuing delay

(c) Packet loss

(d) All of the above

I.82. One of the most devastating effects of malware is the fact that it can mutate.

(a) True

(b) False I.83. Which of the following are categories of malware? (a) Trojans (b) Spyware (c) Viruses (d) Worms

(e) All of the above I.84. Trojans that may contain other categories of malware can provide a backdoor for illegal access to a host. (a) True (b) False I.85. Which of the following elements are placed at critical points within a system to protect vital assets? (a) Firewall (b) IDS (c)

IPS (d) All of the above I.86. Which of the following

elements are used in a system to monitor traffic by inspecting the entire packet? (a) Firewall (b) IDS (c)

IPS (d) All of the above I.87. While a firewall will

block traffic from the Internet to the internal network it does permit traffic originating in the DMZ to enter the internal network. (a) True (b) False I.88. IDS/IPS is strategically located on the Internet side of the firewall in order to detect a wide range of attacks. (a) True (b)

False I.89. Encryption and authentication are protection mechanisms employed in the transmission media. (a) True

(b) False I.90. The approximate number of decades that the Internet has been in existence is (a) 3 (b) 4 (c) 5 (d)

6 Applications 1

1 Chapter 1 - The Application Layer

1. "RFC-Editor Webpage"; <http://www.rfc-editor.org/>.
 2. T. Berners-Lee, R. Fielding, and H. Frystyk, RFC 1945: Hypertext Transfer Protocol-HTTP/1.0, 1996.
 3. R. Fielding, J. Gettys, J. Mogul, H. Frystyk, and T. Berners-Lee, RFC 2068: Hypertext Transfer Protocol-HTTP/1.1, 1997.
 4. R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, RFC 2616: Hypertext transfer protocol-HTTP/1.1, 1999.
 5. T. Berners-Lee, R. Fielding, and L. Masinter, "RFC 2396: Uniform resource identifiers (URI): Generic syntax," Status: Draft Standard, 1998.
 6. E. Wilde and M. Duerst, RFC 5147: URI Fragment Identifiers for the text/plain Media Type, 2008.
 7. T. Berners-Lee, L. Masinter, and M. McCahill, RFC 1738: Uniform resource locators (URL), 1994.
 8. Y. Cheng, A. Jain, S. Radhakrishnan, and J. Chu, IETF Draft: Tcp fast open, 2011; <http://tools.ietf.org/html/draft-cheng-tcpm-fastopen-01>.
 9. J. Postel and J. Reynolds, RFC 959: File transfer protocol, 1985.
 10. P. Oppenheimer, "FTP Protocol Analysis"; <http://www.troubleshootingnetworks.com/ftpinfo.html>.
 11. J. Klensin, RFC 2821: Simple Mail Transfer Protocol (SMTP), 2001.
 12. D.H. Crocker, RFC 822: Standard for the Format of ARPA Internet Text Messages, 1982.
 13. N. Freed and N. Borenstein, RFC 2045: Multipurpose Internet Mail Extensions, 1996.
 14. N. Freed and N. Borenstein, RFC 2046: Multipurpose Internet Mail Extensions (MIME) part two: Media types, 1996.
 15. J. Myers and M. Rose, RFC 1939: Post office protocol-Version 3, 1996.
 16. M. Crispin, RFC 1730: Internet Message Access Protocol-Version 4, 1994.
 17. M. CRISPIN, RFC 3501: Interact Message Access Protocol-Version 4rev1, 2003.
 18. "Messaging Application Programming Interface (MAPI)"; [http://msdn.microsoft.com/en-us/library/aa142548\(EXCHG.65\).aspx](http://msdn.microsoft.com/en-us/library/aa142548(EXCHG.65).aspx).
 19. XAPIA: X.400 Application Programming Interface Standards, 1995; <http://www.auditmypc.com/acronym/XAPIA.asp>.
 20. ITU-T Rec., X.400: Message handling system and service overview, 1996.
- CHAPTER 1 PROBLEMS
- 1.1. Compare the transport layer ports used by the following protocols: FTP, SFTP, SMTP, IMAP4 and POP3 as well as those used by the Microsoft Exchange Server.
 - 1.2. List and compare the similarities and differences that exist among SMTP, IMAP4, POP3, Microsoft Messaging clients and web mail for email client support.
 - 1.3. Compare the TCP ports used by active and passive FTP.
 - 1.4. Assume the following: (1) the propagation delay between browser and server is 100 ms,

(2) the transmission rate of the link is 10 Mbps, (3) a web page, base HTML file 100 Kbytes in length, contains two images of 1000 KBytes each. Compute the total delay when a browser downloads this web page given the use of non-persistent HTTP with Parallel TCP Connections and neglecting all other delays.

1.5. Given the same conditions stated in Problem 4, compute the total delay encountered when the browser downloads the web page if persistent HTTP with pipelining is used.

1.6. Given the same conditions stated in Problem 4, compute the total delay encountered when the browser downloads the web page if persistent HTTP with non-pipelining is used.

1.7. Given the same conditions stated in Problem 4, assume the browser relies on a proxy for web surfing. If the propagation delay is 10 microseconds between the browser and proxy, the proxy uses If-modified-since and the page is up-to-date, compute the total delay for a browser in downloading the web page when persistent HTTP with pipelining is used.

1.8. A browser is used to download a homepage that contains 10 images. The base file size is 100 Kbits and each image file is 100 Kbits. Assume that the link bandwidth is 10 Mbps, the distance between the client and server is 2000 Km and there is no queuing or processing delay. If persistent HTTP is used, determine the time required by the client to download the page.

1.9. A browser is used to download a homepage that contains 10 images. The base file size is 100 Kbits and each image file is 100 Kbits. Assume that the link bandwidth is 10 Mbps, the distance between the client and server is 200 m and there is no queuing or processing delay. If persistent HTTP is used, determine the time required by the client to download the page..

1.10. A browser is used to download a homepage that contains 10 images. The base file size is 100 Kbits and each image file is 100 Kbits. Assume that the link bandwidth is 1 Gbps, the distance between the client and server is 2000 Km and there is no queuing or processing delay. If persistent HTTP is used, determine the time required by the client to download the page.

1.11. A browser is used to download a homepage that contains 10 images. The base file size is 100 Kbits and each image file is 100 Kbits. Assume that the link bandwidth is 1 Gbps, the distance between the client and server is 200 m and there is no queuing or processing delay. If persistent HTTP is used, determine the time required by the client to download the page.

1.12. A browser is used to download a homepage that contains 10 images. The base file size is 100 Kbits and each image file is 100 Kbits. Assume that the link bandwidth is 10 Mbps, the distance between the client and server is 2000 Km and there is no queuing or processing delay. If non-persistent HTTP with serial TCP connections is used, determine the time required by the client to download the page.

1.13. A browser is used to download a homepage that contains 10 images. The base file size is 100 Kbits and each image file is 100 Kbits. Assume that the link bandwidth is 10 Mbps, the distance between the client and server is 200 m and there is no queuing or processing delay. If non-persistent HTTP with serial TCP connections is used, determine the time required by the client to download the page.

1.14. A browser is used to download a homepage that contains 10 images. The base file size is 100 Kbits and each image file is 100 Kbits. Assume that the link bandwidth is 1 Gbps, the distance between the client and server is 2000 Km and there is no queuing or processing delay. If non-persistent HTTP with serial TCP connections is used, determine the time required by the client to download the page.

1.15. A browser is used to download a homepage that contains 10 images. The base file size is 100 Kbits and each image file is 100 Kbits. Assume that the link bandwidth is 1 Gbps, the distance between the client and server is 200 m and there is no queuing or processing delay. If non-persistent HTTP with serial TCP connections is used, determine the time required by the client to download the page.

1.16. A browser is used to download a homepage that contains 10 images. The base file size is 100 Kbits and each image file is 100 Kbits. Assume that the link bandwidth is 10 Mbps, the distance between the client and server is 2000 Km and there is no queuing or processing delay. If non-persistent HTTP with parallel TCP connections is used, determine the time required by the client to download the page.

1.17. A browser is used to download a homepage that contains 10 images. The base file size is 100 Kbits and each image file is 100 Kbits. Assume that the link bandwidth is 10 Mbps, the distance between the client and server is 200 m and there is no queuing or processing

delay. If non-persistent HTTP with parallel TCP connections is used, determine the time required by the client to download the page. 1.18. A browser is used to download a homepage that contains 10 images. The base file size is 100 Kbytes and each image file is 100 Kbytes. Assume that the link bandwidth is 1 Gbps, the distance between the client and server is 2000 Km and there is no queuing or processing delay. If non-persistent HTTP with parallel TCP connections is used, determine the time required by the client to download the page. 1.19. A browser is used to download a homepage that contains 10 images. The base file size is 100 Kbytes and each image file is 100 Kbytes. Assume that the link bandwidth is 1 Gbps, the distance between the client and server is 200 m and there is no queuing or processing delay. If non-persistent HTTP with parallel TCP connections is used, determine the time required by the client to download the page. 1.20. A browser is used to download a homepage that contains 10 images. The base file size is 100 Kbytes and each image file is 100 Kbytes. Assume that the link bandwidth is 10 Mbps, the distance between the client and server is 2000 Km. There is an average delay of 100 ms for queuing and processing when sending the packet out to the Internet. When a response is sent back to the client, the processing delay is 0.001 ms and the queuing delay is 0. If persistent HTTP is used, determine the time required by the client to download the page.

1.21. A browser is used to download a homepage that contains 10 images. The base file size is 100 Kbytes and each image file is 100 Kbytes. Assume that the link bandwidth is 10 Mbps, the distance between the client and server is 2000 Km. There is an average delay of 100 ms for queuing and processing when sending out a request. When a response is sent back to the client, the processing delay is 0.001 ms and the queuing delay is 0. To improve the performance, a proxy server is installed. Assume the local cached homepage has no delay (but the transmission delay should be included) and the hit rate for the cached page is 0.5. If persistent HTTP is used, determine the time required by the client to download the page. 1.22. Based on the data contained in Problem 1.21, determine of the range of hit rate that makes the proxy cost effective. Consider the two cases in which the local link bandwidth is 10 Mbps and 1 Gbps. 1.23. Compare the transport layer ports used by the following protocols: FTP, SFTP, SMTP, IMAP4 and POP3 as well as those used by the Microsoft Exchange Server. 1.24. List and compare the similarities and differences that exist among SMTP, IMAP4, POP3, Microsoft Messaging clients and web mail for email client support. 1.25. Compare the TCP ports used by the active and passive FTP. 1.26. Assume the following: (1) the

propagation delay between client and server is 100 ms, (2) the transmission rate of the link is 10 Mbps, (3) a web page, base HTML file 100 Kbytes in length, contains two images of 1000 KBytes each. Compute the total delay when a browser downloads this web page given the use of non-persistent HTTP with parallel TCP Connections and neglecting all other delays. 1.27. Given the same conditions stated in Problem 1.26, compute the total delay encountered when the browser downloads the web page if persistent HTTP with pipelining is used. 1.28. Given the same conditions stated in Problem 1.26, compute the total delay encountered when the browser downloads the web page if persistent HTTP with non-pipelining is used.

1.29. Given the same conditions stated in Problem 1.26, assume the browser relies on a proxy for web surfing. If the propagation delay is 10 microseconds between the client and proxy, the proxy uses If-modified-since and the page is up-to-date, compute the total delay for a browser in downloading the web page when persistent HTTP with pipelining is used.

1.30. Application software is written for

- (a) Global ISPs
- (b) Regional ISPs
- (c) Root Domain Servers
- (d) All of the above
- (e) None of the above

1.31. A computer operates as both a client and server in a

- (a) Client-server architecture
- (b) P2P architecture
- (c) All of the above
- (d) None of the above

1.32. The Gnutella software runs on a

- (a) Client-server architecture
- (b) P2P architecture

(c) All of the above

(d) None of the above

1.33. In the client-server, P2P and hybrid architectures that support network applications, the inter-process communications are supported by

(a) The Global ISPs

(b) The Regional ISPs

(c) The computer operating systems

(d) All of the above

(e) None of the above

1.34. The application layer interface within a host is called the

(a) Application programming interface

(b) Socket

(c) All of the above

(d) None of the above

1.35. In the Internet, a host is identified by an IP address, the length of which is

(a) 16 bits

(b) 32 bits

(c) 64 bits

(d) All of the above

1.36. A process running on a host has a specific identifier. This identifier consists of

(a) An IP address

(b) A port number

(c) All of the above

(d) None of the above

1.37. If a FTP connection message is to be sent to a FTP server, the destination port number to be used is

- (a) 21
- (b) 25
- (c) 80
- (d) None of the above 1.38. A connection-oriented service in which the socket contains both the source and destination's IP address and port number is (a) TCP (b) UDP (c) All of the above (d) None of the above 1.39. The application layer protocol defines (a) The types of messages (b) Message syntax (c) Message semantics (d) All of the above (e) None of the above 1.40. Which of the following Application layer protocols are defined by RFCs? (a) HTTP (b) SMTP (c) Skype (d) All of the above (e) None of the above 1.41. TCP/IP networks employ which of the following protocols? (a) HTTP (b) SMTP (c) TCP (d) UDP (e) All of the above (f) None of the above 1.42. Flow control is a protocol service provided by (a) TCP (b) UDP (c) All of the above (d) None of the above 1.43. Which of the following applications will effectively run on UDP? (a) Email (b) File Transfer (c) Multimedia (d) VoIP (e) Web 1.44. Objects on a web page are addressable by a (a) URI (b) URL (c) All of the above (d) None of the above 1.45. The Web's application layer protocol is (a) TCP (b) UDP (c) FTP (d) HTTP (e) All of the above (f) None of the above

1.46. In a client/server connection using HTTP over TCP, if multiple objects are sent over the same TCP connection, then the connection is classified as

- (a) Stateless
- (b) Persistent
- (c) Non-persistent
- (d) None of the above

1.47. The default destination port number used in a TCP connection to a HTTP server is

- (a) 21
- (b) 25

(c) 80

(d) None of the above

1.48. Multiple objects can be retrieved from a web page in the shortest interval if the HTTP connection is

(a) Persistent

(b) Non-persistent

(c) Neither (a) nor (b)

1.49. Which of the following alternatives is the fastest HTTP connection?

(a) Persistent with pipelining

(b) Persistent without pipelining

(c) (a) and (b) have the same speed

1.50. The “methods” used in a HTTP request are

(a) GET

(b) POST

(c) URL

(d) All of the above

1.51. A Cookie will not be sent by the browser to the server if

(a) An expiration date has been set and passed

(b) The browser deletes the Cookie in response to a request by the user

(c) All of the above

(d) None of the above

1.52. Cookies can be used to

(a) Identify a user

(b) Obtain a considerable amount of data about a user

(c) All of the above

(d) None of the above

1.53. A web proxy server

(a) Is a client and server at the same time

(b) Reduces the access link bandwidth

(c) Is essentially a web cache

(d) All of the above

(e) None of the above

1.54. The Wide Area Application Service (WAAS) was developed as a joint effort among which of the following entities?

(a) Cisco

(b) DoD

(c) Intel

(d) Microsoft 1.55. If the proxy does not have the most up-to-date version of an object, HTTP will use the following method to obtain it: (a) The GET method (b) The POST method (c) The Conditional GET method (d) The Conditional POST method 1.56. In a FTP process, the client contacts the server on which port number in order to establish a connection? (a) 21 (b) 25 (c) 80 (d) Any of the above (e) None of the above 1.57. In a FTP process for transferring a file (a) A single TCP connection is used (b) Two parallel TCP connections are used (c) Both (a) and (b) (d) Neither (a) nor (b) 1.58. In a FTP process, maintaining state refers to (a) Holding a connection open (b) Maintaining two parallel connections (c) Keeping track of all aspects of a client's operations on the file structure (d) All of the above (e) None of the above 1.59. Control information in a FTP process is said to be out-of-band because (a) It is resident on the same connection with the data but in a different band (b) A separate connection is used for control purposes (c) It is unavailable to the server (d) None of the above 1.60.

With either active or passive FTP, the TCP control connection employs port number (a) 20 (b) 21 (c) 22 (d) A number greater than 1024 (e) None of the above 1.61.

The direct transfer of Internet mail employs TCP and uses port number (a) 20 (b) 21 (c) 22 (d) None of the above

1.62. The principal protocol for sending Internet mail is

(a) ASCII (b) MIME (c) SMTP (d) JPEG (e) None of the above

1.63. Which of the following are mail access protocols?

(a) FTP

(b) HTTP

(c) IMAP

(d) POP3

(e) None of the above

1.64. A mail access protocol that carries state information is

(a) POP3

(b) IMAP

(c) POP3 and IMAP

(d) Neither POP3 nor IMAP

2 Chapter 2 - DNS and Active Directory

9. R. Braden, RFC 1123: Requirements for Internet Hosts-Application and Support, 1989.
10. Zytrax.com, “Chapter 8 - Resource Records”; <http://www.zytrax.com/books/dns/ch8/>.
11. zytrax, “Chapter 6 DNS Sample Configurations,” 2012; <http://www.zytrax.com/books/dns/ch6/>.
12. M. Andrews, RFC 2308: Negative caching of DNS queries (DNS NCACHE), March 1998, 1998.
13. R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, RFC 4033: DNS security introduction and requirements, 2004.
14. R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, RFC 4034: Resource records for the DNS security extensions, 2005.
15. R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, RFC 4035: Protocol modifications for the DNS security extensions, 2005.
16. K. Zeilenga and others, RFC 4510: Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, 2006.
17. C. Neuman, T. Yu, S. Hartman, and K. Raeburn, RFC 4120: The Kerberos Network Authentication Service (V5), 2005.
18. A. Gulbrandsen, P. Vixie, and L. Esibov, RFC 2782: A DNS RR for specifying the location of services (DNS SRV), 2000.
19. A. Gulbrandsen and P. Vixie, RFC 2052: A DNS RR for specifying the location of services (DNS SRV), 1996.
20. Microsoft, “SRV Resource Records”; <http://technet.microsoft.com/en-us/library/cc961719.aspx>.

CHAPTER 2 PROBLEMS

2.1. Create a zone file for the domain, wareagle.com. This zone contains

- (a) DNS servers: ns1.wareagle.com, ns2.wareagle.com and ns3.wareagle.com

(b) A web server: www.wareagle.com or wareagle.com

(c) An email server: mail.wareagle.com

(d) A FTP server: ftp.ns.wareagle.com

2.2. In order to provide the required information for the zone file in Problem 2.1, the administrator must provide a number of RRs to ICANN. Describe the RRs and the place where they will be inserted.

2.3. Use the nslookup command to discover the canonical name of the email servers for mit.edu

2.4. Use the whois service to discover the public information for apple.com.

2.5. Create the RRs required for a client host in order to obtain the IP address of the Microsoft Active Directory server. The server's type A RR is: dc.wareagle.com A 131.204.79.100

2.6. Assume that company x has two web servers, w1.x.com (IP address 131.204.1.5), and w2.x.com (IP address 131.204.3.5). The company wants them both to have the alias name www.x.com when the company's web site is accessed. Create the necessary RR's in the RR format so that the two web servers can serve in the role of www.x.com.

2.7. Assume that company x has two mail servers, m1.x.com (IP address 131.204.1.6), and m2.x.com (IP address 131.204.1.8). This company wants its employees to have an email address of the form Joe.Smith@x.com. Create the necessary RRs in the RR format so that the two mail servers can share the load.

2.8. Given the data in problems 2.1 and 2.7, assume that company x is using an ISP y to host the external DNS services. Identify the place in which to put RRs so that the general public can access www.x.com and send email to Joe.Smith@x.com. Show the RRs as well as their locations.

2.9. Assume company x now decides to host its own external DNS service locally, and to use ns1.x.com (IP address 131.204.1.2), and ns2.x.com (IP address 131.204.1.3) as its primary and secondary authoritative name servers, respectively. In this case, show the RR's and their locations.

2.10. Assume z is a small company, and it too uses y as its ISP for hosting external DNS services. z.com has only one server that serves as www. z.com, a mail

server, and a FTP server. The server's name is sole.z.com and its IP address is 131.204.10.3. Identify all the necessary RR's and their locations. 2.11. Use nslookup to discover the names of your favorite company's name server, mail server and web servers and the corresponding IP addresses. List them in a table. 2.12. Because of its importance, the DNS service is centralized. (a) True (b) False 2.13. In the DNS structure, the servers that sit at the top of the hierarchical structure are the ___ name server. (a) Authoritative (b) Root (c) Top-level domain (d) None of the above 2.14. The servers responsible for the name service of .com .edu, etc. are (a) Authoritative servers (b) Root name servers (c) Top-level domain servers 2.15. Every organization with hosts connected to the Internet has the following type of server: (a) Authoritative (b) Root name (c) Top-level domain 2.16. The following are types of DNS queries: (a) Unidirectional (b) Bidirectional (c) Iterative (d) Recursive (e) None of the above 2.17. ICANN maintains the IP addresses for the authoritative DNS servers. (a) True (b) False 2.18. A DNS resolver is a process within a host that maps from a name to an IP address. (a) True (b) False 2.19. BIND is the most commonly used DNS implementation in the Internet. (a) True (b) False

2.20. In order to mitigate risk, DNS servers are sometimes deployed in full replication.

(a) True

(b) False

2.21. DNS uses TCP on port 80 for lookups and transfers.

(a) True

(b) False

2.22. The type of server that provides name resolution for computers in the same domain is

(a) Recursive

(b) DNS cache

(c) Caching-only name

(d) All of the above

(e) None of the above

2.23. The format for the RR is a 4-tuple.

(a) True

(b) False

2.24. DNS messages are typically

(a) Query

(b) Reply

(c) All of the above

(d) None of the above

2.25. The DNS message header consumes

(a) 8 bytes

(b) 16 bytes

(c) 32 bytes

(d) None of the above

2.26. The DNS provides which of the following services?

(a) Host name-to-IP address translation

(b) Host aliasing

(c) Mail service load sharing

(d) Load balance

(e) All of the above

(f) None of the above

2.27. Company x must put its NS RR at the ___ name server.

(a) Authoritative

(b) Root name

(c) Top-level domain

2.28. Company x must put its MX RR at the ___ name server.

- (a) Authoritative
- (b) Root name
- (c) Top-level domain

2.29. Company x must locate its name server's IP address at the ___ name server.

- (a) Authoritative
- (b) Root name

(c) Top-level domain 2.30. To enable a mail server's services, ___ RR's are necessary. (a) 1 (b) 2 (c) 3 (d) None of the above 2.31. Type ___ RR allows a client computer to locate a PDC and be authenticated by it. (a) A (b) NS (c) SRV (d) MX 2.32. A host name-to-IP address could be classified as an rDNS. (a) True (b) False 2.33. rDNS can be used as an anti-spam technique. (a) True (b) False 2.34. AD is a distributed database that operates in the DNS hierarchy. (a) True (b) False 2.35. Kerberos is the industry standard for directory access. (a) True (b) False 2.36. In a hierarchical network, only the primary domain controller maintains a copy of the AD through replication and synchronization. (a) True (b) False 2.37. A forest may contain multiple AD trees. (a) True (b) False 2.38. Which of the following objects can be an AD OBJECT? (a) Application (b) Service (c) User (d) All of the above (e) None of the above 2.39. The AD schema describes (a) AD attributes (b) AD classes (c) Rules for creating and manipulating classes and attributes (d) All of the above 2.40. An Object Identifier (OID) is guaranteed to be unique across all networks worldwide. (a) True (b) False

2.41. In an AD network, bridgehead servers handle inter-site information exchange.

- (a) True
- (b) False

2.42. OD is a service provided by Mac OS that is similar to AD.

- (a) True
- (b) False

3 Chapter 3 - XML-Based Web Services

1. W3C, “Standards - W3C”; <http://www.w3.org/standards/>.
2. W3Schools, “XML Tutorial”; <http://www.w3schools.com/xml/>.
3. W3Schools, “AJAX Tutorial”;
<http://www.w3schools.com/ajax/default.asp>.
4. “W3C Recommendation: SOAP Version 1.2 Specification Assertions and Test Collection (Second Edition),” 2007; <http://www.w3.org/TR/soap12-testcollection/>.
5. “W3C Recommendation: Web Services Description Language (WSDL) Version 2.0 Part 0: Primer,” 2007; <http://www.w3.org/TR/wsdl120-primer/>.
6. “OASIS Standards and Other Approved Work”; <http://www.oasis-open.org/specs/index.php#uddiv3.0.2>.
7. W3Schools, “JavaScript Tutorial”; <http://www.w3schools.com/js/default.asp>.
8. W3Schools, “VBScript Tutorial”; <http://www.w3schools.com/vbscript/default.asp>.
9. W3Schools, “HTML Tutorial”; <http://www.w3schools.com/html/default.asp>.
10. W3Schools, “PHP Tutorial”; <http://www.w3schools.com/php/default.asp>.
11. W3Schools, “ASP Tutorial”; <http://www.w3schools.com/asp/default.asp>.
12. W3Schools, “PHP \$_GET Function”; http://www.w3schools.com/php/php_get.asp.
13. W3Schools, “CSS Tutorial”; <http://www.w3schools.com/css/default.asp>.
14. W3Schools, “AJAX Create an XMLHttpRequest Object”; [http://www.w3schools.com/ajax/default.asp](#).
15. W3C, “W3C Recommendation: Extensible Markup Language (XML) 1.0 (Fifth Edition),” 2008; <http://www.w3.org/TR/2008/REC-xml-20081126/>.
16. “XML Editors”; <http://www.xml.com/pub/pt/3>.
17. M. Mealling and R. Denenberg, RFC 3305: Report from the

Joint W3C/IETF URI Planning Interest Group: Uniform Resource Identifiers (URIs), 2002.

18. "W3C XML Schema Tools";
<http://www.w3.org/XML/Schemas#Tools>.

19. "W3C Document Object Model (DOM)";
<http://xml.coverpages.org/dom.html>.

20. W3C, "Document Object Model (DOM) Specifications";
<http://www.w3.org/DOM/DOMTR>.

21. W3Schools, "PHP XML DOM";
http://www.w3schools.com/php/php_xml_dom.asp.

22. W3Schools, "PHP Example AJAX and XML";
http://www.w3schools.com/php/php_ajax_xml.asp.

CHAPTER 3 PROBLEMS

3.1. Describe the major deployments of AJAX-based applications in the Internet.

3.2. Describe the "Back" button malfunction that may occur in an AJAX-based web page and the means to correct it.

3.3. To solidify an understanding of the iframe concept in Problem 3.2, write a simple iFrame html using the techniques in http://www.w3schools.com/html/html_iframe.asp. Show the iFrame in an html page by screen capturing the web page in a browser.

3.4. Show the use of a URL Fragment ID for the attribute tag in Problem 3.3.

3.5. Describe the bookmark malfunction that can occur in an AJAX-based web page and the means to correct it.

3.6. Describe the relative number of requests generated by a user when using an AJAXbased web page and the impact of these requests on both the web and backend database servers.

3.7. XML provides the foundation for storing and exchanging data across different operating systems.

(a) True (b) False

3.8. AJAX is the foundation for Web 2.0.

(a) True (b) False

3.9. In client/server web

applications, XML is a format for data transport.

(a) True (b) False

3.10. PHP is the Post Hypertext Processor script

language for the server side

(a) True (b) False

3.11. When a server-side PHP script is used to receive

information from a client-side HTML using the GET command,

the information being passed can be encrypted.

(a) True (b) False

(b) False 3.12. Interaction between a client's HTML and server's PHP using the POST command does not permit the information being passed to be encrypted. (a) True (b) False 3.13. The response time of HTTP can be increased through the use of AJAX. (a) True (b) False 3.14. The XMLHttpRequest Object is supported by all major browsers. (a) True (b) False 3.15. XML is a good replacement for HTML. (a) True (b) False 3.16. When using XML, data transport is independent of platform. (a) True (b) False 3.17. The XML schema language is used for XML schema definition. (a) True (b) False 3.18. An XML file can be validated against a XSD file. (a) True (b) False

3.19. There is no standard way to access and manipulate XML documents.

(a) True

(b) False

3.20. W3C DOM is separated into the following number of parts

(a) 2

(b) 3

(c) 4

(d) None of the above

3.21. XML DOM defines a standard set of objects for any structured document.

(a) True

(b) False

3.22. The W3C recommended DOM standard provides for the following number of levels of specifications:

(a) 2

(b) 3

(c) 4

(d) None of the above

3.23. The Node object is the primary data type for the

entire DOM.

(a) True

(b) False

3.24. The `nodeValue` ___ the value of a node, depending on its type.

(a) sets

(b) returns

(c) All of the above

(d) None of the above

3.25. Each node in a `NodeList` object has ___ properties of an item.

(a) Length

(b) Type

(c) All of the above

(d) None of the above

3.26. ___ is used by AJAX on the client side as an indication of a successful response capture from the server.

(a) `xmlHttp.readyState`

(b) `xmlHttp.responseText`

(c) `document.getElementById`

(d) All of the above

(e) None of the above

4 Chapter 4 - Socket Programming

1. J.M. Winett, RFC 147: the definition of a socket, 1971.
2. W. Stevens, M. Thomas, E. Nordmark, and T. Jinmei, RFC 3542: Advanced Sockets API for IPv6, May, 2003.
3. "What Is a Socket? (The Java™ Tutorials > Custom Networking > All About Sockets)"; <http://java.sun.com/docs/books/tutorial/networking/sockets/definition.html>.
4. "Uses of Class java.net.ServerSocket (Java 2 Platform SE 5.0)"; <http://java.sun.com/j2se/1.5.0/docs/api/java/net/class-use/ServerSocket.html>.
5. "IOException (Java 2 Platform SE 5.0)";
6. "System (Java 2 Platform SE v1.4.2)";
7. "Socket (Java 2 Platform SE v1.4.2)";
8. "PrintWriter (Java 2 Platform SE v1.4.2)";

FIGURE 4.21 Running EchoClient_v3.java in theIPv6 mode. 9. "InputStreamReader (Java Platform SE 6)"; <http://java.sun.com/javase/6/docs/api/java/io/InputStreamReader.html>. 10. "Uses of Class java.io.BufferedReader (Java 2 Platform SE 5.0)"; <http://java.sun.com/j2se/1.5.0/docs/api/java/io/class-use/BufferedReader.html>. 11. "Integer (Java 2 Platform SE 5.0)";

4.14. TCP packets are limited to 64 kilobytes for datagrams.

- (a) True
- (b) False

4.15. Socket programming is recommended for web-based applications.

- (a) True
- (b) False

4.16. A socket provides an API between the application process and the end-to-end transport protocol.

- (a) True

(b) False

4.17. A connection must be established between client and server to exchange messages with TCP.

(a) True

(b) False

4.18. In establishing a TCP socket between a client and server, the source port number assigned to the client will be less than 1024.

(a) True

(b) False

4.19. A TCP socket is clearly identified as a

(a) 2-tuple

(b) 4-tuple

(c) 6-tuple

4.20. A fundamental difference between TCP and UDP is that TCP is connection-oriented, while UDP is connectionless.

(a) True

(b) False

4.21. A UDP socket is identified as a

(a) 2-tuple

(b) 4-tuple

(c) 6-tuple

4.22. A client's IP address and port number are explicitly specified in the UDP socket.

(a) True

(b) False

4.23. The ___ must be specified in the Java code for a socket.

- (a) Server IP address
- (b) Server port number
- (c) Client IP address
- (d) Client port number
- (e) All of the above

4.24. The ___ server socket can simultaneously handle multiple clients.

- (a) Single thread
 - (b) Multiple thread
 - (c) TCP
 - (d) UDP
 - (e) All of the above
- 4.25. The ___ class is used for a UDP socket in Java. (a) ServerSocket (b) DatagramSocket (c) All of the above (d) None of the above
- 4.26. The ___ method is used by a TCP socket in order to receive data in Java. (a) GetInputStream (b) Receive (c) All of the above (d) None of the above
- 4.27. The ___ method is used by a UDP socket to send data in Java. (a) GetOutputStream (b) Send (c) All of the above (d) None of the above

5 Chapter 5 - Peer-to-Peer (P2P) Networks and Applications

5.5. Describe the use of protocols by Bonjour for service discovery in a single subnet and multiple subnets.

5.6. When comparing a client/server network with a P2P network with bidirectional links, which network has a speed advantage and why?

- (a) Client/server network
- (b) P2P network
- (c) Neither network has a speed advantage over the other

5.7. The BitTorrent with trackers architecture is an example of a

- (a) Purely decentralized P2P architecture
- (b) Partially decentralized P2P architecture
- (c) Hybrid decentralized P2P architecture
- (d) None of the above

5.8. The Gnutella architecture is an example of a

- (a) Purely decentralized P2P architecture
- (b) Partially decentralized P2P architecture
- (c) Hybrid decentralized architecture
- (d) None of the above

5.9. The P2P architecture in which there is a central server that maintains file directories and facilitates file exchanges among peers is the

- (a) Purely decentralized
- (b) Partially decentralized
- (c) Hybrid decentralized

5.10. Napster is a good example of the following P2P architecture:

- (a) Purely decentralized
- (b) Partially decentralized
- (c) Hybrid decentralized

5.11. The following architecture is an example of a P2P network with no central servers:

- (a) BitTorrent with trackers
- (b) Gnutella
- (c) Napster

5.12. The root structure of a Gnutella network is formed by

- (a) Leaf nodes
- (b) Ultra nodes
- (c) (a) and (b)
- (d) None of the above

5.13. In a Gnutella network, a client that wishes to download a file from a source might employ a

- (a) Push request
- (b) Push proxy
- (c) (a) and (b)
- (d) None of the above

5.14. The most efficient protocol for sending a push request to a push proxy is

- (a) TCP
 - (b) FTP
 - (c) UDP
- 5.15. A torrent is a
(a) File index
(b) File distribution center
(c) Small file containing the information of file locations and trackers
(d) File header
- 5.16. In a BitTorrent network, a group of peers interconnected to share a torrent is called a
(a) Tracker group
(b) Leaf nodes
(c) Swarm
(d) Ultra peer set
- 5.17. Which of the following are examples of client software used

by eDonkey? (a) eMule (b) iMule (c) Morpheus (d) All of the above (e) (a) and (b) 5.18. Skype (a) Is a VoIP application (b) Uses a centralized server for a client-to-client voice connection (c) Uses a centralized server for IP address lookup (d) All of the above 5.19. The length of the session key employed in the establishment of a new Skype session is (a) 64 bits (b) 128 bits (c) 256 bits (d) None of the above 5.20. The type of encryption used in a Skype session is (a) Advanced Encryption Standard (b) Diffie-Hellman (c) RSA (d) None of the above 5.21. In a Skype session, a supernode (a) Resides behind a firewall (b) Resides behind a NAT (c) (a) and (b) (d) None of the above 5.22. Users access Internet Relay Chat networks via (a) Client/server (b) P2P (c) None of the above 5.23. Structured P2P uses a ___ for searching data. (a) Keyword (b) DHT (c) All of the above (d) None of the above 5.24. Napster must use the central server to find popular content. (a) True
(b) False

5.25. Skype also uses the private/public signing key pair for authentication.

(a) True

(b) False

5.26. DHT uses (put(key, value)) to save an object, where the key is

(a) The encryption key

(b) The identifier of value

(c) All of the above

(d) None of the above

5.27. DHT uses (value = get(key)) to retrieve an object, where value is

(a) The encryption key value

(b) The identifier of value

(c) The object data

(d) All of the above

(e) None of the above Link and Physical Layers 2

6 Chapter 6 - The Data Link Layer and Physical Layer

6. IEEE Std. 802.15.1-2005 IEEE Standard for Information technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements. Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks, 2005; <http://standards.ieee.org/getieee802/portfolio.html>.
7. IEEE Std. 802.5-1998 (ISO/IEC 8802-5:1998) IEEE Standard for Information technology– Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements–Part 5: Token Ring Access Method and Physical Layer Specification, 1998; <http://standards.ieee.org/getieee802/portfolio.html>.
8. IEEE Std. 802.2-1998 (ISO/IEC 8802-2:1998), IEEE Standard for Information technology– Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements–Part 2: Logical Link Control, 1998; <http://standards.ieee.org/getieee802/portfolio.html>.
9. IEEE Std. 802.1D-2004 IEEE Standard for Local and Metropolitan Area Networks–Media access control (MAC) Bridges (Incorporates IEEE 802.1t-2001 and IEEE 802.1w), 2004; <http://standards.ieee.org/getieee802/portfolio.html>.
10. “Review: 5 power-line devices that take you online where Ethernet or Wi-Fi can’t”; http://www.computerworld.com/s/article/9127759/Review_5_power_line_devices_that_take_you_online_where_Ethernet_or_Wi-Fi_can_t?source=NLT_AM.
11. IEEE P1901: Draft Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications, 2010; <http://grouper.ieee.org/groups/1901/>.
12. D. Perkins, RFC 1547: Requirements for an Internet Standard Point-to-Point Protocol, 1993.
13. Telecommunications Systems Management, “A Look at LLC”; http://campus.murraystate.edu/tsm/tsmdb/db32/ep2_LLC.doc.
14. Cisco, “Understanding Rapid Spanning Tree Protocol (802.1w),” Cisco; http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cf.shtml.

15. J. Touch and R. Perlman, RFC 5556: Transparent interconnection of lots of links (TRILL), May, 2009.
16. R. Perlman, D. Eastlake, D. Dutt, S. Gai, and A. Ghanwani, RFC 6325: RBridges: Base Protocol Specification, 2011.
17. D. Eastlake, Banerjee, D. Dutt, R. Perlman, and A. Ghanwani, RFC 6326: Transparent Interconnection of Lots of Links (TRILL) Use of IS-IS, 2011.
18. D. Eastlake, R. Perlman, A. Ghanwani, D. Dutt, and V. Manral, RFC 6327: Routing Bridges (RBridges): Adjacency, 2011.
19. IEEE, IEEE Std. 802.1aq Shortest Path Bridging, 2011.
20. N. Farrington, E. Rubow, and A. Vahdat, “Data center switch architecture in the age of merchant silicon,” Power (W), vol. 200, pp. 11-500.
21. “IEEE 802.11 WEP Integrity Check Vulnerability”;

CHAPTER 6 PROBLEMS

- 6.1. Using a tabular format, describe the LLC functions performed by NetBIOS/NetBEUI.
- 6.2. Compare the LLC functions performed by L2 NetBIOS/NetBEUI with those performed by L4 TCP.
- 6.3. Calculate the channel capacity when the sampling frequency is 100 MHz, and the S/N = 3 dB.
- 6.4. Calculate the sampling frequency when the channel capacity is 1 Gbps, and the S/N = 3 dB.
- 6.5. Describe the differences between Channel Partitioning and Random Access MAC protocols including the advantages and disadvantages of each.
- 6.6. List the available parallel paths from S1 to S2 in the following network configuration. Root port Root port Root port Root port Root port A S1 CB D F E S2 P6.6
- 6.7. Based on the findings in Problem 6.6, separate the paths into groups so that each group has the same number of hops.
- 6.8. Fill in the blanks for the source and destination IP addresses, as well as the source and destination MAC addresses, for a frame traveling from Station A to Station B in the network shown in Figure for Problem 6.8.
- Station A Station B

00-50-12-FB-76-C9 131.204.1.2 Subnet 1 R Src MAC Dest MAC
Src IP Dest IP Payload Src MAC Dest MAC Src IP Dest IP
Payload 00-10-41-16-FE-24 131.204.1.3 131.204.1.1
00-50-12-FB-70-11 P6.8 6.9. Three stations A, B and C are lined up in that order and the stations are 200 m apart. Station A begins sending data to Station C at $t = 0$ and Station C starts sending data to Station B at $t = 0.5 \mu s$. The speed = 200 m/ μs , the Rate = 1 Gbps, and the Packet size = 4000 bits. Draw the spatial and temporal diagram for this scenario. Do Stations A and C detect any collision? Will the stations receive the data correctly? 6.10. Three stations A, B and C are lined up in that order and the stations are 200 m apart. Station A starts sending data to Station C at $t = 0$ and Station C begins sending data to Station B at $t = 0.5 \mu s$. The Speed = 200 m/ μs , the Rate = 1 Gbps, and the Packet size = 1000 bits. Draw the spatial and temporal diagram for this scenario. Discuss the collision detections at Stations A and C. Will the stations receive the data correctly?

6.11. Compute the CRC-6 code for the data 1100111011 using 1101101 as the divisor, and determine the form of the data that would be sent using this code.

6.12. Given the network in Problem 6.12, draw a series of diagrams to show how the MAC address of Station B is obtained by Station A using the ARP. Clearly label the IP and MAC addresses for each frame. Station A 131.204.1.2 Station B 131.204.1.3 LAN (wired or wireless)
00-50-12-FB-76-C9 00-10-6F-72-B8-5E 00-10-82-3D-7F-A2
00-10-41-16-FE-24 Src MAC Dest MAC Src IP Dest IP Payload
Src MAC Dest MAC Src IP Dest IP Payload P6.12

6.13. Repeat Problem 6.8 for a frame traveling from Station B to Station A.

6.14. Repeat Problem 6.8 for a frame traveling from the router to Station B.

6.15. Repeat Problem 6.8 for a frame traveling from the router to Station A.

6.16. Repeat Problem 6.9 if stations A and C are both transmitting at $t = 0$, the speed is 200 m/ μs , the rate is 1 Gbps and the packet size is 1000 bits. Do any stations detect a collision, and if so, when?

6.17. Repeat Problem 6.9 if stations A and C are both transmitting at $t = 0$, the speed is 200 m/ μs , the rate is 1 Gbps and the packet size is 3000 bits. Do any stations

detect a collision, and if so, when?

6.18. Repeat Problem 6.9 if stations A and B are transmitting at $t = 0$, the speed is 200 m/ μ s, the rate is 1 Gbps, and the packet size is 3000 bits. Do any stations detect a collision, and if so, when?

6.19. Repeat Problem 6.9 if station A starts transmitting at $t = 0$ and station B starts transmitting at $t = 1$ microsecond. The speed is 200 m/ μ s, the rate is 1 Gbps and the packet size is 3000 bits. Do any stations detect a collision, and if so, when?

6.20. Repeat Problem 6.9 if station A begins transmitting at $t = 0$ and station C begins transmitting at $t = 1$ microsecond. The speed is 200 m/ μ s, the rate is 1 Gbps and the packet size is 500 bits.

6.21. Repeat Problem 6.9 if stations A and C are transmitting at $t = 0$. The speed is 200 m/s, the rate is 1 Gbps and the packet size is 500 bits. Do any stations detect a collision, and if so, when?

6.22. Compute the CRC-3 code for the 8-bit data 11010101 using the divisor 1001 and determine the data that will be sent using this code. 6.23. The 8-bit data 1 0 1 1 1 0 0 1 is to be coded with a CRC-3 code with the divisor 1 0 0 1. Determine the 3-bit code and the form of the data to be sent. 6.24. The 8-bit data 10011111 is to be coded with a CRC-3 code with the divisor 1100. Determine the 3-bit code and the data to be sent. 6.25. Determine the CRC-6 code for the data 1011011101 using the divisor 1010100, and the form of the data when the code is applied. 6.26. Determine the CRC-6 code for the data 1111001111 using the divisor 1001001 and the form of the data when the code is applied. 6.27. A source wishes to send the bit stream 10110101 to a receiver. If a bit is to be added to the end of this data to achieve even parity, what is the bit? 6.28. If a source wishes to provide the destination with the capability to determine if a single error has occurred in the sequence 11100101 during transmission by using a parity bit to establish odd parity, what bit should be chosen? 6.29. Source and destination have agreed that the transmission between them will be conducted with even parity. The following string was received 100100111. Is the transmission error-free? 6.30. The following sequence is received 10011101. The transmission was to be achieved with odd parity. Does the data appear to be correct or not? 6.31. Source and destination agree that they will use a CRC code with the generator $g = 1011$. The data received at the

destination is 11010110111. Determine if the data received is correct. 6.32. Source and destination have agreed to use a CRC code with the generator $g = 1011$. The data received at the destination is 11010110101. Determine if this data is error free. 6.33. Source and destination agree to use a CRC code with the generator $g = 1011$. If the data bits to be encoded are 11100111, determine the remainder that must be employed. 6.34. Source and destination agree to use the CRC code with the generator $g = 1011$. If the bit stream received at the destination is 11100111111, determine if this data has been received correctly. 6.35. Source and destination agree to use the CRC code with generator $g = 1011$. The bit stream received at the destination is 11000111111. Was this bit stream received correctly? 6.36. A signal has frequency components in the range from 0 to 150 KHz. This signal is to be digitized and forwarded to a receiver via a transmission facility. What is the minimum sampling rate that must be applied to ensure that the signal is accurately represented by the digitized values? 6.37. A signal that contains frequencies in the band from 0 to 100 KHz is to be digitized for transmission. If the number of bits used to represent each sample is 32, determine the minimum sampling rate and the bit rate of transmission. 6.38. Data that has frequencies that range from very low frequencies to high frequencies of about 500 KHz must be transmitted from point A to point B. The signal is to be digitized and the number of bits used to represent each of the samples is 64. What is the minimum rate at which the data must be sampled, and what is the resulting bit rate on the transmission facility?

6.39. A digitized signal at the destination end of a transmission facility is received at a speed of 32 Mbps. Assuming the minimum sampling rate was used to digitize the signal and that 64 bits were used for each sample, determine the highest frequency contained in the signal.

6.40. A signal that has been digitized on the sending end of a transmission facility is received at a bit rate of 16 Mbps. It is known that the signal was sampled at the Nyquist rate, and that 64 bits were used to represent each sample. Given this data, determine the highest frequency contained in the signal.

6.41. At the sending end, the checksum for a UDP segment is computed as follows: the 16-bit words within the segment are added and any overflows are wrapped around. Then the one's complement is generated by changing all 0's to 1's and all 1's to 0's. The result is the checksum. At the

receiving end, all the words are added including the checksum. The result should be a string of 1's. If the addition produces a 0 anywhere in the result, then an error in transmission has occurred. For simplicity, assume that there are four 16-bit words: W1: 0100101101001100 W2: 0101010101010010 W3: 1001101001010010 W4: 1000101100110100

- (a) Determine the 1's complement of the four words.
- (b) Is it possible that a 2-bit error could go undetected?

6.42. Given the following two words W1 = 10010100 W2 = 01011010 Determine the 1's complement of the two words.

6.43. Given the words W1 = 10011100 W2 = 01001001

- (a) Determine the 1's complement of the two words.
- (b) Show that the 1's complement will not change if there is an error in the 8 th bit of each word.

6.44. The link layer encapsulates the datagram received from the network layer into a frame.

- (a) True
- (b) False

6.45. The link layer is incapable of detecting an error in a received frame.

- (a) True
- (b) False

6.46. One of the services provided by the link layer is flow control.

- (a) True
- (b) False

6.47. The link layer supports which of the following operations.

- (a) Half-duplex
- (b) Full-duplex
- (c) All of the above

(d) None of the above 6.48. The IEEE 802 standard was developed in cooperation with (a) IETF (b) ITU (c) ISO
(d) All of the above 6.49. The standard commonly known as WiFi is (a) 802.3 (b) 802.5 (c) 802.11 (d) 802.15
6.50. The link layer contains the following sublayers (a) LLC (b) LLP (c) MAC (d) MAP (e) None of the above
6.51. Part of the link layer is implemented in a NIC. (a) True (b) False 6.52. A NIC can be in the form of a (a) PCMCIA card (b) PCI card (c) USB adapter (d) All of the above 6.53. A NIC provides the interface between the PC and the network. (a) True (b) False 6.54. Links connecting two nodes can be classified as (a) Point-to-point (b) Broadcast (c) All of the above (d) None of the above 6.55. Which of the following are data link protocols? (a) HDLC (b) PPP (c) All of the above (d) None of the above 6.56. The PPP employs CRC. (a) True (b) False 6.57. The MAC protocol is designed to alleviate the collision problem that naturally results from multiple hosts using a single shared channel. (a) True (b) False

6.58. Which of the following are classes of MAC protocols?

- (a) Channel partitioning
- (b) Random access
- (c) Token ring
- (d) All of the above
- (e) None of the above

6.59. TDMA and FDMA are MAC protocols used with

- (a) Channel partitioning
- (b) Random access
- (c) Token ring
- (d) All of the above
- (e) None of the above

6.60. CSMA, CSMA/CD and CSMA/CA are MAC protocols used with

- (a) Channel partitioning
- (b) Random access

- (c) Token ring
- (d) All of the above

6.61. CSMA/CD differs from CSMA in that the node that is transmitting is also listening

- (a) True
- (b) False

6.62. Channel partitioning MAC protocols are efficient at low load.

- (a) True
- (b) False

6.63. Random access MAC protocols are inefficient at low load.

- (a) True
- (b) False

6.64. The token employed with token ring is essentially a small packet.

- (a) True
- (b) False

6.65. The token ring MAC protocol

- (a) Is known as 802.5
- (b) More efficient than shared Ethernet
- (c) Decentralized in nature
- (d) All of the above
- (e) None of the above

6.66. The different classifications for every station in a token ring network are

- (a) AM

- (b) PM
- (c) SM
- (d) All of the above

6.67. One of the advantages of the token ring MAC protocol is the lack of collisions.

- (a) True
- (b) False 6.68. If a node within the token ring fails, the MAU can provide a bypass circuit. (a) True (b) False 6.69. The importance of the token ring technology has declined as a result of advances in Ethernet technology. (a) True (b) False 6.70. MAC addresses are 32 bits in length while IP addresses are 48 bits in length. (a) True (b) False 6.71. As a general rule, the MAC address for a LAN is burned into the NIC's ROM. (a) True (b) False 6.72. In a LAN with multiple adapters, if an adapter wants to broadcast to all other adapters it uses a string of 0's represented in hexadecimal as the destination MAC address. (a) True (b) False 6.73. The ARP performs the IP-to-MAC address translation. (a) True (b) False 6.74. Entries in the ARP table remain there until they are updated. (a) True (b) False 6.75. As networks increase in size, loops can be prevented with the use of (a) ARP (b) STP (c) RSTP (d) All of the above (e) None of the above 6.76. MAC protocols employ CRC to detect errors. (a) True (b) False 6.77. The physical topology of a token ring LAN is a_. (a) STAR (b) BUS (c) Ring (d) All of the above (e) None of the above 6.78. CRC-32 in Ethernet is implemented in __. (a) NIC hardware (b) OS software (c) NIC driver (d) All of the above (e) None of the above

6.79. ___ token(s) is/are available for capture by token ring nodes.

- (a) 0
- (b) 1
- (c) 2
- (d) All of the above
- (e) None of the above

6.80. A node that receives a frame can detect collisions from multiple frames.

(a) True

(b) False

6.81. As it relates to the Ethernet frame structure, DIX stands for Digital Internet eXchange.

(a) True

(b) False

6.82. Ethernet DIX V2.0 is both connectionless and unreliable.

(a) True

(b) False

6.83. An Ethernet frame contains a trailer for error detection.

(a) True

(b) False

6.84. SNAP provides ___ service to Ethernet for transporting an IP datagram.

(a) Connectionless

(b) Connection-oriented

(c) Connectionless and ACKed

(d) All of the above

(e) None of the above

6.85. LLC provides ___ service to Ethernet for transporting an IP datagram.

(a) Connectionless

(b) Connection-oriented

(c) Connectionless and ACKed

(d) All of the above

(e) None of the above

6.86. LLC2 provides ___ service to Ethernet for transporting an IP datagram.

(a) Connectionless

(b) Connection-oriented

(c) Connectionless and ACKed

(d) All of the above

(e) None of the above

6.87. LLC2 uses ___ to detect frame loss and handle frame retransmission.

(a) Sequence number

(b) DSAP

(c) DSNAP

(d) All of the above

(e) None of the above

6.88. The minimum header size of an Ethernet header is ___ bytes without preamble.

(a) 12

(b) 14

(c) 16

(d) 18

(e) None of the above

7 Chapter 7 - The Ethernet and Switches

1. IEEE Std. 802.3-2008 IEEE Standard for Information technology-Specific requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 2008; <http://standards.ieee.org/getieee802/portfolio.html>.
2. IEEE Std. 802.1D-2004 IEEE Standard for Local and Metropolitan Area Networks—Media access control (MAC) Bridges (Incorporates IEEE 802.1t-2001 and IEEE 802.1w), 2004; <http://standards.ieee.org/getieee802/portfolio.html>.
3. TIA-568-C.0 Generic Telecommunications Cabling For Customer Premises, 2009; http://global.ihs.com/doc_detail.cfm?currency_code=USD&customer_id=2125492B3B0A&shopping_cart_id=2827483F2F494034415A2D28230A&rid=TIA&country_code=US&lang_code=ENGL&input_doc_number=&input_doc_title=&item_s_key=00519378&item_key_date=910613&origin=DSSC.
4. TIA-568-C.1: Commercial Building Telecommunications Cabling Standards - Part 1 General Requirements; http://global.ihs.com/doc_detail.cfm?currency_code=USD&customer_id=2125492B3B0A&shopping_cart_id=2827483F2F494034415A2D28230A&rid=TIA&country_code=US&lang_code=ENGL&input_doc_number=&input_doc_title=&item_s_key=00339844&item_key_date=900931&origin=DSSC.
5. TIA-568-C.2 Balanced Twisted-Pair Telecommunications Cabling And Components Standards; http://global.ihs.com/doc_detail.cfm?currency_code=USD&customer_id=2125492B3B0A&shopping_cart_id=2827483F2F494034415A2D28230A&rid=TIA&country_code=US&lang_code=ENGL&input_doc_number=&input_doc_title=&item_s_key=00339844&item_key_date=900931&origin=DSSC.
6. TIA-568-C.3 Optical Fiber Cabling Components Standard; http://global.ihs.com/doc_detail.cfm?currency_code=USD&customer_id=2125492B3B0A&shopping_cart_id=2827483F2F494034415A2D28230A&rid=TIA&country_code=US&lang_code=ENGL&input_doc_number=&input_doc_title=&item_s_key=00339844&item_key_date=900931&origin=DSSC.
7. “Kasolo the ‘digital Strategist’”; <http://www.kasolo.org/>.

8. IEEE Std. 802.3ba-2010 IEEE Standard for Information technology-Specific requirements - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 4: Media Access Control Parameters, Physical Layers and Management Parameters for 40 Gb/s and 100 Gb/s Operation, 2010; <http://standards.ieee.org/getieee802/portfolio.html>.

9. W. Bux, W.E. Denzel, T. Engbersen, A. Herkersdorf, and R.P. Luijten, "Technologies and building blocks for fast packet forwarding," Communications Magazine, IEEE, vol. 39, 2001, pp. 70-77.

10. N. McKeown, "A fast switched backplane for a gigabit switched router," Business Communications Review, vol. 27, 1997, pp. 1020-1030.
11. J. Van Lunteren and T. Engbersen, "Fast and scalable packet classification," Selected Areas in Communications, IEEE Journal on, vol. 21, 2003, pp. 560-571.
12. Cisco, "The Cisco QuantumFlow Processor: Cisco's Next Generation Network Processor [Cisco ASR 1000 Series Aggregation Services Routers] - Cisco Systems";

CHAPTER 7 PROBLEMS

7.1. Describe the reason why the L2/L3 packet forwarding in a switch is usually implemented in an ASIC while the routing table generation is implemented using software in a CPU.

7.2. For a 100 Gbps interface that has $100,000 \times 1$ Mbps flows, estimate the buffer size based on RFC 3439 and the small buffer model when RTT = 250 msec.

7.3. For a 100 Gbps interface that has $100,000 \times 1$ Mbps flows, estimate the buffer size based on RFC 3439 and the small buffer model when RTT = 500 msec.

7.4. For a 100 Gbps interface that has $10,000 \times 10$ Mbps flows, estimate the buffer size based on RFC 3439 and the small buffer model when RTT = 500 msec.

7.5. In the network in Problem 7.5, when station A sends a frame to station D for the first time, the self-learning process creates entries in the switch tables. Provide a listing of the step-by-step development of the switch tables in S 1 , S 2 , and S 3 until D receives the frame.
A B C D E F S 2 S 3 G H I S 1 S 4 P7.5

7.6. Given the activities outlined in Problem 7.5, the

self-learning process will create entries in the switch tables when D responds with a frame to A for the first time. Show the step-by-step development of the switch tables in S 1 , S 2 , and S 3 until A receives the frame.

7.7. A 1000BASE-T cable of length 100 meters is used for communication. Show that with a minimum frame size of 512 bytes the sender is able to detect a collision during transmission of a frame.

7.8. In the network in Problem 7.8, when Station A sends a frame to Station B for the first time, the self-learning process creates entries in the switch tables. Provide a listing of the step-by-step development of the switch tables in S 1 , and S 2 until B receives the frame.

Station A Station B S 1 R S 2 131.204.1.1 00-50-12-FB-70-11
00-50-12-FB-76-C9 131.204.1.2 00-10-41-16-FE-24

131.204.10.3 131.204.10.1 00-50-12-FB-70-12 Subnet 1 Src
MAC Src IP Dest IP PayloadDest MAC Src MAC Src IP Dest IP
PayloadDest MAC Subnet 2 P7.8 7.9. Based upon the activities outlined in Problem 7.8, when Station B responds with a frame to Station A for the first time, the self-learning process creates entries in the switch tables. Provide a listing of the step-by-step development of the switch tables in S 1 and S 2 until A receives the frame.

7.10. Outline the exponential backoff procedure when a station has experienced 3 collisions in the process of sending out a frame. Select a random number in order to obtain the corresponding waiting time for each collision.

7.11. A 10BASE-T cable of length 50 meters is used for communication. The frame size is 200 bytes. Given these parameters, can the sender detect a collision during transmission of a frame?

7.12. A 1BASE-T cable of length 250 meters is used for communication. The frame size is 100 bytes. Given these parameters, can the sender detect a collision during transmission of a frame?

7.13. A 1BASE-T cable of length 500 meters is used for communication. The frame size is 20 bytes. Given these parameters, can the sender detect a collision during transmission of a frame?

7.14. A 100BASE-TX cable of length 400 meters is used for communication. The frame size is 128 bytes. Given these parameters, can the sender detect a collision during transmission of a frame?

7.15. A 100BASE-TX cable of length 200 meters is used for communication. The frame size is 16 bytes. Given these parameters, can the sender detect a collision during transmission of a frame?

7.16. A 100BASE-T4 cable of length 200 meters is used for communication. The frame size is 64 bytes. Given these parameters, can the sender detect a collision during transmission of a frame?

7.17. The primary topologies used

with Ethernet are (a) Bus (b) Star (c) Ring (d) All of the above 7.18. The exponential backoff used in the algorithm for Ethernet CSMA/CD is a procedure that produces a random waiting period. (a) True (b) False 7.19. The efficiency of CSMA/CD is only about ten percent when there are a few computers in the LAN. (a) True (b) False 7.20. The transmission delay between sender and receiver places restrictions on the Ethernet frame size. (a) True (b) False

7.21. The cables employed for Ethernet transmission are rated using four factors: data rate, maximum length, maximum number of segments and the number of stations per segment.

(a) True

(b) False

7.22. Connections to CAT X cables are typically done using a standard RJ-45 connector.

(a) True

(b) False

7.23. When cabling an Ethernet connection, the items to consider are

(a) Type of cable

(b) Straight-through connection

(c) Cross-over connection

(d) All of the above

7.24. Straight-through cable connections are used for

(a) Switch to hub

(b) Switch to router

(c) Switch to switch

(d) All of the above

(e) None of the above

7.25. Crossover cable connections are used for

- (a) Switch to hub
- (b) Switch to router
- (c) Switch to switch
- (d) All of the above
- (e) None of the above

7.26. The approximate number of fibers contained in a modern fiber optic cable is

- (a) 10
- (b) 100
- (c) 1000
- (d) 10,000

7.27. 10G Ethernet is the technology typically employed in backbones and data centers.

- (a) True
- (b) False

7.28. 10G Ethernet supports CSMA/CD.

- (a) True
- (b) False

7.29. 10GBASE-T provides 10 Gbps connections over both conventional unshielded and shielded twisted pair cables.

- (a) True
- (b) False

7.30. A LAN bridge for connecting two or more LANs uses a bridging table to forward frames from source to destination.

- (a) True
 - (b) False
- 7.31. A switch is nothing more than a bridge with a hardware switching fabric.
- (a) True
 - (b) False

7.32. Hubs are more capable than switches and take an active role in handling frames. (a) True (b) False 7.33. All shared medium LANs operate in a half-duplex mode. (a) True (b) False 7.34. The switch table, created and maintained by a learning process, contains which of the following information? (a) MAC address of a host (b) Interface to reach the host (c) TTL (d) All of the above 7.35. A layer 3 switch uses routing tables and a destination MAC address to forward packets. (a) True (b) False 7.36. A layer 2 switch forwards packets using a switching table and IP address. (a) True (b) False 7.37. The common types of switch fabric are (a) Banyan multistage (b) Crossbar (c) Exchange (d) Interconnect 7.38. For $n \times n$ switching, the Banyan multistage switch is best for small values of n (n is the number of hosts). (a) True (b) False 7.39. A crossbar switch is characterized by high cost and high performance. (a) True (b) False 7.40. In a comparison among a hub, layer 2 switch and layer 3 switch, the MAC layer switching feature is capable with (a) Hub and layer 2 switch (b) Hub and layer 3 switch (c) Layer 2 switch and layer 3 switch 7.41. The Cisco Supervisor Engine 720 employs a crossbar switch. (a) True (b) False 7.42. The Cisco Supervisor Engine 720 uses (a) A switch processor (b) A route processor (c) All of the above (d) None of the above

7.43. A bus structure is used for central forwarding in the Cisco Supervisor Engine 720.

- (a) True
- (b) False

7.44. Which of the following are used in a device-based switch management system?

- (a) SNMP
- (b) RMON
- (c) All of the above
- (d) None of the above

7.45. CEE and DCE are designed as an enhanced Ethernet for transporting SANs traffic.

- (a) True
- (b) False

7.46. IEEE 802.3 standards provide ___ Gbps as the highest data rate Ethernet.

- (a) 1
- (b) 10
- (c) 40
- (d) 100
- (e) None of the above

8 Chapter 8 - Virtual LAN, Class of Service, and Multilayer Networks

1. IEEE Std. 802.1Q-2005 IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Revision, 2005;
<http://standards.ieee.org/getieee802/portfolio.html>.
2. IEEE Std. 802.1Q-2005/Cor1-2008 IEEE Standard for Local and metropolitan area networks—Virtual Bridged Local Area Networks Corrigendum 1: Corrections to the Multiple Registration Protocol, 2008;
<http://standards.ieee.org/getieee802/portfolio.html>.
3. IEEE Std. 802.1ak-2007 IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks Amendment 7: Multiple Registration Protocol, 2007;
<http://standards.ieee.org/getieee802/portfolio.html>.
Subscriber networks: Company A and B Aggregation Networks using Aggregation Router (AR) Core Network using Core Router (CR) WDM Optical Networks (WAN) A B A's data centers Data Centers Access Networks

FIGURE 8.25 A MLN provides two sets of CapabilityPlanes for Companies A and B.

4. Cisco, “Cisco Nexus 5000 Series Architecture: The Building Blocks of the Unified Fabric [Cisco Nexus 5000 Series Switches] - Cisco Systems”;
http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9670/white_paper_c11-462176.html.
5. K.Y. Siu and R. Jain, “A brief overview of ATM: protocol layers, LAN emulation, and traffic management,” ACM SIGCOMM Computer Communication Review, vol. 25, 1995, pp. 6-20.
6. M.A. Rahman, Guide to ATM systems and technology, Artech House on Demand, 1998.
7. M. Laubach and J. Halpern, RFC 2225: Classical IP and ARP over ATM, 1998.
8. D. Grossman and J. Heinanen, RFC 2684: Multiprotocol Encapsulation over ATM Adaptation Layer 5, 1999.
9. ITU-T Rec., ITU-T I.363.5: B-ISDN ATM Adaptation Layer Specification: Type 5 AAL - Series I: Integrated Services Digital Network Overall Network Aspects and Functions—Protocol Layer Requirements, 1996.
10. M. Laubach, RFC 1577: Classical IP and ARP over ATM, 1994.
11. Microsoft Technet, “ATM Addresses”;
<http://technet.microsoft.com/en-us/library/cc976977.aspx>.
12. A. McKenzie, RFC 941: Addendum to the network service definition covering network layer addressing, 1985;
<http://tools.ietf.org/html/rfc941>.
13. ITU-T Rec., E.164: The international public telecommunication numbering plan, 2005; <http://www.itu.int/rec/T-REC-E.164-200502-I/en>.
14. E. Rosen, A. Viswanathan, and R. Callon, RFC 3031: Multiprotocol Label

Switching Architecture, 2001. 15. D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, and G. Swallow, RFC 3209: RSVP-TE: Extensions to RSVP for LSP Tunnels, 2001. 16. A. Farrel, A. Ayyangar, and J. Vasseur, RFC 5151: Inter-Domain MPLS and GMPLS Traffic Engineering- Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions, 2008.

17. T. Lehman, Xi Yang, N. Ghani, Feng Gu, Chin Guok, I. Monga, and B. Tierney, "Multilayer networks: an architecture framework," IEEE Communications Magazine, vol. 49, May. 2011, pp. 122-130.

CHAPTER 8 PROBLEMS

8.1. Given the network shown in Figure P 8.1, assume a frame is traveling from Station A to Station B. The switches have been configured with fixed ports assigned to VLANs and GVRP/VTP has established the VLAN ports for both S1 and S2. Assume that the switches S1 and S2 are just being turned on. Determine the frame header and tag information and

(a) Show the frame that Station A sends to S1. (b) Show how S1 processes the frame and delivers it. Also show the switch table. (c) Show how S2 processes the frame and delivers it. Also show the switch table.

VLAN 1 VLAN 1 VLAN 1 VLAN 2 VLAN 3 VLAN 2 VLAN 2 VLAN 3 VLAN 3 VLAN 3 Station A Station B S1 S2 Backbone VLAN trunk P8.1

8.2. Given the information provided in Problem 8.1, determine the response frame traveling from Station B to Station A. The switches have been configured with fixed ports assigned to VLANs and GVRP/VTP has established the VLAN ports for both S1 and S2. Determine the frame header and tag information and

(a) Show the frame that Station B sends to S2. (b) Show how S2 processes the frame and delivers it. Also show the switch table. (c) Show how S1 processes the frame and delivers it. Also show the switch table.

8.3. Given the network in Figure P8.3, assume a frame is traveling from Station A to Station C. The switches have been configured with fixed ports assigned to VLANs and GVRP/VTP has established the VLAN ports for both S1 and S2. Assume that the switches S1 and S2 are just being turned on. Determine the frame header and tag information and

- (a) Show the frame that Station A sends to S1.
- (b) Show how S1 processes the frame and delivers it. Also show the switch table.
- (c) Show how S2 processes the frame and delivers it. Also show the switch table.
- VLAN 1 VLAN 1 VLAN 1 VLAN 2 VLAN 3 VLAN 2 VLAN 2 VLAN 3 VLAN 3 Station A Station D Station F Station G Station H Station C Station B Station E S1 S2 Backbone VLAN trunk P8.3

8.4. Given the information provided in Problem 8.3, determine the response frame traveling from Station C to Station A. The switches have been configured with fixed ports assigned to VLANs and GVRP/VTP has established the VLAN ports for both S1 and S2. Determine the frame header and tag information and

- (a) Show the frame that Station C sends to S2.
- (b) Show how S2 processes the frame and delivers it. Also show the switch table.
- (c) Show how S1 processes the frame and delivers it. Also show the switch table.

8.5. Given the network shown in Figure P8.3, assume a frame is traveling from Station D to Station E. The switches have been configured with fixed ports assigned to VLANs and GVRP/VTP has established the VLAN ports for both S1 and S2. Assume that the switches S1 and S2 are just being turned on. Determine the frame header and tag information and

- (a) Show the frame that Station D sends to S1.
- (b) Show how S1 processes the frame and delivers it. Also show the switch table.
- (c) Show how S2 processes the frame and delivers it. Also show the switch table.

8.6. Given the information provided in Problem 8.5, determine the response frame traveling from Station E to Station D. The switches have been configured with fixed ports assigned to VLANs and GVRP/VTP has established the VLAN ports for both S1 and S2. Determine the frame header and tag information and

- (a) Show the frame that Station E sends to S2.
- (b) Show how S2 processes the frame and delivers it. Also show the switch table.
- (c) Show how S1 processes the frame and delivers it. Also show the switch table.

8.7. Given the network shown in Figure P8.3, assume a frame is traveling from Station F to Station H. The switches have been configured with fixed ports assigned to VLANs and GVRP/VTP has established the VLAN ports for both S1 and

S2. Assume that the switches S1 and S2 are just being turned on. Determine the frame header and tag information and

- (a) Show the frame that Station F sends to S1.
- (b) Show how S1 processes the frame and delivers it. Also show the switch table.
- (c) Show how S2 processes the frame and delivers it. Also show the switch table. 8.8. Given the information provided in Problem 8.7, determine the response frame traveling from Station H to Station F. The switches have been configured with fixed ports assigned to VLANs and GVRP/VTP has established the VLAN ports for both S1 and S2. Determine the frame header and tag information and (a) Show the frame that Station H sends to S2. (b) Show how S2 processes the frame and delivers it. Also show the switch table. (c) Show how S1 processes the frame and delivers it. Also show the switch table. 8.9. Given the network shown in Figure P8.3, assume a frame is traveling from Station G to Station H. The switches have been configured with fixed ports assigned to VLANs and GVRP/VTP has established the VLAN ports for both S1 and S2. Assume that the switches S1 and S2 are just being turned on. Determine the frame header and tag information and (a) Show the frame that Station G sends to S1. (b) Show how S1 processes the frame and delivers it. Also show the switch table. (c) Show how S2 processes the frame and delivers it. Also show the switch table. 8.10. Given the information provided in Problem 8.9, determine the response frame traveling from Station H to Station G. The switches have been configured with fixed ports assigned to VLANs and GVRP/VTP has established the VLAN ports for both S1 and S2. Determine the frame header and tag information and. (a) Show the frame that Station H sends to S2. (b) Show how S2 processes the frame and delivers it. Also show the switch table. (c) Show how S1 processes the frame and delivers it. Also show the switch table. 8.11. Design a network that connects two buildings using Layer 2 switches with VLAN capabilities. Three VLANs will be established: one for faculty, one for staff and one for students. Each building has one switch and each switch has ports 1-8 for faculty, 9-16 for staff and 17-24 for students. Draw a network diagram for this configuration and list the VLAN membership ports established by GVRP/VTP. 8.12. Design a network that connects two buildings using Layer 2 switches with VLAN capabilities. Establish two networks: one for engineering and one for manufacturing. Each building has one switch and each switch has ports 1-8 for engineering

and 9-16 for manufacturing. Draw a network diagram for this configuration and list the VLAN membership ports established by GVRP/VTP. 8.13. Design a network that connects two buildings using Layer 2 switches with VLAN capabilities. Establish two networks: one for management and one for marketing. Each building has one switch and each switch has ports 1-16 for management and 17-24 for marketing. Draw a network diagram for this configuration and list the VLAN membership ports established by GVRP/VTP.

8.14. Assume that a switch is using Weighted Round Robin and the weights for the queues are set as follows: (a) Q4 weight: 0.5 (b) Q3 weight: 0.25 (c) Q2 weight: 0.125 (d) Q1 weight: 0.125 At t = 0, port 1's Q4 has 3 packets, Q3 has 2 packets, Q2 has 4 packets, and Q1 has 3 packets. Every packet has 10,000 bits. The output link has a rate of 100 Mbps. Show the packet delivery from each queue as a function of time by allocating packets in blocks of four time slots.

8.15. Assume that a switch is using Weighted Round Robin and the weights for the queues are set as follows:

(a) Q3 weight: 0.5

(b) Q2 weight: 0.25

(c) Q1 weight: 0.25 At t = 0, port 1's Q3 has 4 packets, Q2 has 3 packets and Q1 has 1 packet. Every packet has 10,000 bits. The output link has a rate of 100 Mbps. Show the packet delivery from each queue as a function of time by allocating packets in blocks of four time slots.

8.16. Assume that a switch is using Weighted Round Robin and the weights for the queues are set as follows:

(a) Q3 weight: 0.6

(b) Q2 weight: 0.3

(c) Q1 weight: 0.1 At t = 0, port 1's Q3 has 2 packets, Q2 has 3 packets and Q1 has 3 packets. Every packet has 10,000 bits. The output link has a rate of 100 Mbps. Show the packet delivery from each queue as a function of time by allocating packets in blocks of four time slots.

8.17. Assume that a switch is using Weighted Round Robin and the weights for the queues are set as follows:

(a) Q4 weight: 0.6

(b) Q3 weight: 0.2

(c) Q2 weight: 0.1

(d) Q1 weight: 0.1 At $t = 0$, port 1's Q4 has 2 packets, Q3 has 4 packets, Q2 has 1 packet and Q1 has 1 packet. Every packet has 10,000 bits. The output link has a rate of 100 Mbps. Show the packet delivery from each queue as a function of time by allocating packets in blocks of four time slots.

8.18. Assume that a switch is using Weighted Round Robin and the weights for the queues are set as follows:

(a) Q4 weight: 0.4

(b) Q3 weight: 0.3

(c) Q2 weight: 0.2

(d) Q1 weight: 0.1 At $t = 0$, port 1's Q4 has 1 packet, Q3 has 3 packets, Q2 has 2 packets and Q1 has 2 packets. Every packet has 10,000 bits. The output link has a rate of 100 Mbps. Show the packet delivery from each queue as a function of time by allocating packets in blocks of four time slots.

8.19. Assume that a switch is using Weighted Round Robin and the weights for the queues are set as follows:

(a) Q4 weight: 0.5

(b) Q3 weight: 0.2

(c) Q2 weight: 0.2

(d) Q1 weight: 0.1 At $t = 0$, port 1's Q4 has 2 packets, Q3 has 2 packets, Q2 has 2 packets and Q1 has 2 packets. Every packet has 10,000 bits. The output link has a rate of 100 Mbps. Show the packet delivery from each queue as a function of time by allocating packets in blocks of four time slots.

8.20. Illustrate the ATM ARP operation in the following network by
(a) Designating an ATM ARP server
(b) Showing how Interface 1 obtains the ATM address of interface 2 in a step-by-step manner
Link IP AAL ATM PHY
ATM PHY ATM PHY PHY Link IP AAL ATM PHY I n t e r f a c e 2
I n t e r f a c e 1 PHY P8.20
8.21. A VLAN is a logical group of stations in the same physical location/building.
(a) True (b) False
8.22. In a multiple VLAN network, the Layer 2 switches communicate with one another via a VLAN

trunk. (a) True (b) False 8.23. The manager of a multiple VLAN network establishes the guidelines for the filtering and forwarding decisions made for each frame by the VLAN switches. (a) True (b) False 8.24. Switch ports in a VLAN network are said to run in which of the following modes? (a) Forwarding (b) Broadcast (c) All of the above (d) None of the above 8.25. When traffic is multiplexed over the same physical link to support multiple VLANs the mode of operation is called (a) Access (b) Broadcast (c) Trunk (d) None of the above 8.26. Tags are employed in multiple VLANs in order to identify the frames received with a particular VLAN. (a) True (b) False

8.27. When the ISL protocol is employed, only routers with 10 Mbps or faster Ethernet ports can do VLAN trunking.

(a) True

(b) False

8.28. When the GARP is being employed, each switch involved in a VLAN reconfiguration must be manually configured.

(a) True

(b) False

8.29. Which of the following protocols is most efficient in a VLAN configuration?

(a) GVRP

(b) MVRP

8.30. Frame tagging in a VLAN can be categorized as either implicit or explicit.

(a) True

(b) False

8.31. If a packet belongs to a specific VLAN based upon MAC address, protocol or switch receiving port, the tagging is termed

(a) Explicit

(b) Implicit

8.32. 802.1Q frame tagging functions at

(a) Layer 2

(b) Layer 3

8.33. A Layer 3 switch or router must be employed to support inter-VLAN communication.

(a) True

(b) False

8.34. In accordance with IEEE 802.1Q, the TPID in the tagging frame consists of

(a) 1 byte

(b) 2 bytes

(c) 3 bytes

(d) 4 bytes

8.35. The TCI format employed in the tagging frame consists of

(a) VID

(b) CFI

(c) User priority

(d) All of the above

(e) None of the above

8.36. In general, the number of VLAN configuration options is

(a) 1

(b) 2

(c) 3

(d) 4

8.37. From a quality of service perspective, the most flexible traffic is

(a) Voice

(b) Video

(c) Data 8.38. The different scheduling methods specified in 802.1p are (a) Strict priority (b) Weighted round robin (c) A combination of (a) and (b) (d) All of the above 8.39. The maximum number of classes of service for 802.1p-compliant devices is (a) 2 (b) 4 (c) 8 (d) 16 8.40. The 802.1p priority class given for best effort is (a) 0 (b) 2 (c) 4 (d) 8 8.41. Priority classification in 802.1p is an egress function of a frame. (a) True (b) False 8.42. If the priority classification option is 802.1p and the packet retains its incoming user priority value, then the mode of operation is (a) Fixed (b) Transparent (c) None of the above 8.43. The two most popular CoS queuing methods employed in switches are FIFO and LIFO. (a) True (b) False 8.44. ATM uses circuit switching with small packets 53 bytes long, called cells. (a) True (b) False 8.45. Cell switching in ATM is performed at the ATM layer that is analogous to the Internet transport layer. (a) True (b) False 8.46. The primary function of ATM is the interconnection of Internet backbone routers. (a) True (b) False 8.47. The AAL2 ATM service class is a constant bit rate service for circuit emulation. (a) True (b) False 8.48. The AAL5 ATM Service class is a VBR service for MPEG video. (a) True (b) False

8.49. The service provided by the ATM layer is analogous to that provided by the IP network layer.

(a) True

(b) False

8.50. The number of bits used for the header in an ATM cell is

(a) 8

(b) 24

(c) 40

(d) None of the above

8.51. The field in the ATM cell header that consumes the smallest number of bits is the

(a) VCI

- (b) PT
- (c) CLP
- (d) HEC
- (e) None of the above

8.52. The field in the ATM cell header that provides the cyclic redundancy check for the cell header is

- (a) VCI
- (b) PT
- (c) CLP
- (d) HEC
- (e) None of the above

8.53. The ATM physical layer consists of how many sublayers?

- (a) 1
- (b) 2
- (c) 3
- (d) 4

8.54. The ATM sublayer that is dependent upon the actual physical medium being used is the

- (a) TC
- (b) PMD
- (c) None of the above

8.55. The ATM sublayer that must guarantee proper bit timing reconstruction at the receiver is the

- (a) TC
- (b) PMD
- (c) None of the above

8.56. Classical IP over ATM is a mechanism that maps IP addresses to ATM addresses using an ATM ARP server.

- (a) True
- (b) False

8.57. The number of bytes used for an ATM address is

- (a) 8
- (b) 16
- (c) 20

8.58. The number of ATM network prefix addressing schemes is
(a) 2 (b) 3 (c) 4

9 Chapter 9 - Wireless and Mobile Networks

12. IEEE Std. 802.3at-2009: Data Terminal Equipment (DTE) power via the Media Dependent Interface (MDI) enhancements, 2009; <http://standards.ieee.org/getieee802/portfolio.html>.
13. "IEEE 802.15 Working Group for Wireless Personal Area Networks (WPANs)"; <http://www.ieee802.org/15/>.
14. IEEE Std. 802.15.1-2005 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements. Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks, 2005; <http://standards.ieee.org/getieee802/portfolio.html>.
15. IEEE Std. 802.15.2-2003 IEEE Recommended Practice for Telecommunications and Information exchange between systems – Local and metropolitan area networks Specific Requirements - Part 15.2: Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Band; <http://standards.ieee.org/getieee802/portfolio.html>.
16. IEEE Std. 802.15.3-2003 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPAN); <http://standards.ieee.org/getieee802/portfolio.html>.
17. IEEE Std. 802.15.3b-2005 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15.3b: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs) Amendment 1 : MAC Sublayer, 2005; <http://standards.ieee.org/getieee802/portfolio.html>.
18. IEEE Std. 802.15.3c-2009 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements— Part 15.3c: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area

Networks (WPANs): Amendment 2: Millimeter-wave-based Alternative Physical Layer Extension, 2005;
<http://standards.ieee.org/getieee802/portfolio.html>.

19. IEEE Std. 802.15.4-2006 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), 2006;
<http://standards.ieee.org/getieee802/portfolio.html>.

20. IEEE Std. 802.15.4a-2007 IEEE Standard for PART 15.4: Wireless MAC and PHY Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs): Amendment 1: Add Alternate PHY, 2007;
<http://standards.ieee.org/getieee802/portfolio.html>.

21. IEEE Std. 802.15.5-2009 IEEE Standard for Recommended Practice for Information technology— Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 15.5: Mesh Topology Capability in Wireless Personal Area Networks (WPANS), 2009;
<http://standards.ieee.org/getieee802/portfolio.html>.

22. Bluetooth.com, “Bluetooth Specification Version 2.0 + EDR,” 2004; <http://www.bluetooth.com/English/Technology/Building/Pages/Specification.aspx>.

23. Bluetooth.com, “Bluetooth Specification Version 2.1 + EDR,” 2007; <http://www.bluetooth.com/English/Technology/Building/Pages/Specification.aspx>.

24. Bluetooth.com, “Bluetooth Core Specification Addendum 1,” 2008; <http://www.bluetooth.com/English/Technology/Building/Pages/Specification.aspx>.

25. Bluetooth.com, “Bluetooth Specification Version 3.0 + HS,” 2009; <http://www.bluetooth.com/English/Technology/Building/Pages/Specification.aspx>.

26. Bluetooth.com, “Bluetooth Specification Version 4.0,” 2010; <http://www.bluetooth.com/English/Technology/Building/Pages/Specification.aspx>.

27. B. Treister, “Adaptive Frequency Hopping: A Non-collaborative Coexistence Mechanism,” 2001;

28. [usb.org](http://www.bluetooth.com/English/Technology/Building/Pages/Specification.aspx), “Wireless Universal Serial Bus Specification Revision 1.0,” 2005; <http://www.bluetooth.com/English/Technology/Building/Pages/Specification.aspx>.
29. IEEE Std. 802.15.4-2003 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), 2006; <http://standards.ieee.org/getieee802/portfolio.html>.
30. IEEE Std. 802.15.4c-2009 IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and IEEE Standard for Information technology- Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANS) Amendment 2: Alternative Physical Layer Extension to support one or more of the Chinese 314-316 MHz, 430-434 MHz, and 779-787 MHz band, 2009; <http://standards.ieee.org/getieee802/portfolio.html>. 31. IEEE Std. 802.15.4d-2009 IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANS) Amendment 3: Alternative Physical Layer Extension to support the Japanese 950 MHz bands, 2009; <http://standards.ieee.org/getieee802/portfolio.html>. 32. IEEE Std. 802.16-2009 IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems, 2009; <http://standards.ieee.org/getieee802/portfolio.html>. 33. IEEE Std. 802.16.2-2004 IEEE Recommended Practice for Local and metropolitan area networks— Coexistence of Fixed Broadband Wireless Access Systems, 2004; <http://standards.ieee.org/getieee802/portfolio.html>. 34. S. Ahmadi, “An overview of next-generation mobile WiMAX technology,” IEEE Communications Magazine, vol. 47, 2009, pp. 84-98. 35. “Digital AMPS: IS-136 Wikipedia, the free encyclopedia”; http://en.wikipedia.org/wiki/Digital_AMPS.
36. J. Scourias, Overview of GSM: The Global System for Mobile Communications, 1996; <http://www.shoshin.uwaterloo.ca/pub/papers/Ps/TR-9>. 37. C. Lin and J. Shieh, IS-95 North American Standard - A CDMA Based Digital

Cellular System; <http://www.ctr.columbia.edu/~cylin/pub/cdma.ps>. 38. 3GPP2 Specifications: cdma2000 High Rate Packet Data Air Interface Specification (TIA-856 Rev.A), 2005; http://www.3gpp2.org/Public_html/specs/tsgc.cfm. 39. 3GPP2 Specifications: cdma2000 High Rate Packet Data Air Interface Specification (TIA-856 Rev.B), 2009; http://www.3gpp2.org/Public_html/specs/tsgc.cfm. 40. Agilent, 3GPP Long Term Evolution: System Overview, Product Development, and Test Challenges;

9.3. A station, transmitting over a medium, employs exponential back-off. The parameters that govern the exponential back-off are CWE = 32, CW min = 31 and CW max = 1023. When CW > CW max , retransmission is aborted. Assuming the slot time is 15 ns and the frame is sent after the third retransmission of the frame, determine the delay due to the error recovery time.

9.4. A station, transmitting over a medium, employs exponential back-off. The parameters that govern the exponential back-off are CWE = 32, CW min = 31 and CW max = 1023. When CW > CW max , retransmission is aborted. Assuming the slot time is 8 ns and the frame is sent after the fourth retransmission of the frame, determine the delay due to the error recovery time.

9.5. A station, transmitting over a medium, employs exponential back-off. The parameters that govern the exponential back-off are CWE = 32, CW min = 31 and CW max = 1023. When CW > CW max , retransmission is aborted. Assuming the slot time is 4 ns and the frame is sent after the fifth retransmission of the frame, determine the delay due to the error recovery time.

9.6. In an attempt to deliver video more efficiently, a station employs exponential backoff using the following parameters and conditions. The exponential back-off window uses a CWE = 16 CW min = 15, CW max = 31, and when CW > CW max , retransmission is aborted. Assuming the slot time is 18 ns and the frame is sent after the first retransmission of the frame, determine the delay due to the error recovery time.

9.7. In an attempt to deliver video more efficiently, a station employs exponential back-off using the following parameters and conditions. The exponential back-off window uses a CWE = 16 CW min = 15, CW max = 31, and when CW > CW max , retransmission is aborted. Assuming the slot time is 10 ns and the frame is sent after the second

retransmission of the frame, determine the delay due to the error recovery time.

9.8. In an attempt to deliver video more efficiently, a station employs exponential back-off using the following parameters and conditions. The exponential back-off window uses a CWE = 16 CW min = 15, CW max = 31, and when CW > CW max , retransmission is aborted. Assuming the slot time is 15 ns and the frame is sent after the third retransmission of the frame, determine the delay due to the error recovery time.

9.9. In an attempt to deliver video more efficiently, a station employs exponential back-off using the following parameters and conditions. The exponential back-off window uses a CWE = 8, CW min = 7, CW max = 15, and when CW > CW max , retransmission is aborted. Assuming the slot time is 6 ns and the frame is sent after the first retransmission of the frame, determine the delay due to the error recovery time.

9.10. In an attempt to deliver video more efficiently, a station employs exponential back-off using the following parameters and conditions. The exponential back-off window uses a CWE = 8, CW min = 7, CW max = 15, and when CW > CW max , retransmission is aborted. Assuming the slot time is 2 ns and the frame is sent after the second retransmission of the frame, determine the delay due to the error recovery time.

9.11. In an attempt to deliver video more efficiently, a station employs exponential back-off using the following parameters and conditions. The exponential back-off window uses a CWE = 8, CW min = 7, CW max = 15, and when CW > CW max , retransmission is aborted. Assuming the slot time is 12 ns and the frame is sent after the third retransmission of the frame, determine the delay due to the error recovery time. 9.12. Can 802.11 now support VoIP and Video conferencing as well as a 3G cellular network and WiMax? 9.13. With reference to Example 9.13, determine the highest data rate that a master node, M, can deliver to a slave node S 1 ? Assume there are only 2 active nodes and the maximum data rate for all slots is 1 Mbps. 9.14. Given the mode of operation described in Example 9.13 with three active nodes, M, S 1 and S 2 , and a maximum data rate for all slots of 2 Mbps, determine the highest data rate that a master node, M, can deliver to S 1 . 9.15. Given the mode of operation described in Example 9.13 with three active nodes, M, S 1 and S 2 , and a maximum data rate for all slots of 0.5 Mbps, determine the highest data rate

that a master node, M, can deliver to S 2 . 9.16. Given the mode of operation described in Example 9.13 with three active nodes, M, S 1 and S 2 , and a maximum data rate for all slots of 0.5 Mbps, determine the highest data rate that node S 1 can deliver to S 2 . 9.17. Given the mode of operation described in Example 9.13 with three active nodes, M, S 1 and S 2 , and a maximum data rate for all slots of 4 Mbps, determine the highest data rate that node S 1 can deliver to S 2 . 9.18. Given the mode of operation described in Example 9.13 with four active nodes, M, S 1 , S 2 , and S 3 and a maximum data rate for all slots of 3 Mbps, determine the highest data rate that node M can deliver to S 3 . 9.19. Given the mode of operation described in Example 9.13 with four active nodes, M, S 1 , S 2 , and S 3 and a maximum data rate for all slots of 6 Mbps, determine the highest data rate that node S 1 can deliver to S 3 . 9.20. Given the mode of operation described in Example 9.13 with four active nodes, M, S 1 , S 2 , and S 3 and a maximum data rate for all slots of 6 Mbps, determine the highest data rate that node S 2 can deliver to S 1 . 9.21. Consider the mode of operation described in Example 9.14 with three active nodes, M, S 1 and S 2 . In order to provide a higher data rate, the master sends a 3-slot frame to S 1 and a 1-slot frame to S 2 . If the maximum data rate for all slots is 1 Mbps, what is the maximum frame rate for master to S 1 transmission? 9.22. Consider the mode of operation described in Example 9.14 with three active nodes, M, S 1 and S 2 . In order to provide a higher data rate, the master sends a 5-slot frame to S 1 and a 1-slot frame to S 2 . If the maximum data rate for all slots is 1 Mbps, what is the maximum frame rate for master to S 1 transmission? 9.23. Consider the mode of operation described in Example 9.14 with three active nodes, M, S 1 and S 2 . In order to provide a higher data rate, the master sends a 5-slot frame to S 1 and a 3-slot frame to S 2 . If the maximum data rate for all slots is 1 Mbps, (a) what is the maximum frame rate for master to S 1 transmission and (b) what is the maximum frame rate for master to S 2 transmission?

9.24. Determine the values for address 1 to address 4 in the 802.11 frame which is sent from source to destination, shown in Figure P9.24(a) for the network in Figure P9.24(b), given the following data. Node MAC address A 111111111111 B 222222222222 C 333333333333 AP1 444444444444
AP2 555555555555 D 666666666666

Frame

control Address 1 Duration Payload CRC Address 2 Address 3

Address 4 Seq control 2 62 0 - 2312 4 (bytes) 6 6 62 P9.24a
A AP1 AP2 B P9.24b

9.25. Repeat Problem 9.24 for the network shown in Figure
P9.25. A AP1 AP2 B P9.25

9.26. Repeat Problem 9.24 for the network shown in Figure
P9.26. A AP1 B P9.26

9.27. Repeat Problem 9.24 for the network shown in Figure
P9.27 A AP1 B P9.27

9.28. Repeat Problem 9.24 for the network shown in Figure
P9.28. A AP1 B P9.28 9.29. Repeat Problem 9.24 for the
network shown in Figure P9.29. A AP1 B P9.29 9.30. Repeat
Problem 9.24 for the network shown in Figure P9.30(a). One
802.11 frame and one 802.3 frame are used for sending from
source to destination. The Ethernet frame format is shown
in Figure P9.30(b). Specify all addresses in those two
frames. A AP1 B C D P9.30a 8 bytes 2 bytes Preamble Type 4
bytes FCS Src. MAC add Dest. MAC add 46 to 1500 bytes
Payload P9.30b 9.31. Repeat Problem 9.30 for the network
shown in Figure P9.31. A AP1 B C D P9.31 9.32. Repeat
Problem 9.30 for the network shown in Figure P9.32. A AP1
AP2 B C D P9.32 9.33. Repeat Problem 9.30 for the network
shown in Figure P9.33. A AP1 AP2 B C D P9.33

9.34. 802.11n covers technology for operation in the

- (a) Short range
- (b) Mid range
- (c) Long range

9.35. Which of the following technologies are classified as
3G?

- (a) GPRS
- (b) GSM
- (c) HSDPA
- (d) W-CDMA

9.36. In a wireless mesh infrastructure mode of operation,
routing is performed by

- (a) A central server

- (b) Mobile stations
- (c) Network access points

9.37. The ad hoc mode of operation is characterized by which of the following?

- (a) Nodes organize themselves into networks
- (b) Routing is performed by the stations
- (c) No access points
- (d) All of the above
- (e) None of the above

9.38. The Independent Basic Service Set (IBSS) is characterized by which of the following?

- (a) The mode of operation is ad hoc
- (b) The structure consists of wireless hosts and base stations
- (c) The cell diameter is determined by the coverage distance between two stations

9.39. A standalone WLAN without an access point is a part of

- (a) A BSS
- (b) An IBSS
- (c) All of the above
- (d) None of the above

9.40. Within an Extended Service Set (ESS), a ___ is used to bridge wired LANs.

- (a) Portal
- (b) Switch
- (c) None of the above

9.41. Which of the following is/are used by a BSS within an ESS to forward traffic?

- (a) A destination MAC address
- (b) A bridge learning table
- (c) An Association table
- (d) All of the above
- (e) None of the above

9.42. CSMA/CD is an effective technology in

- (a) Wired LANs
- (b) Wireless LANs
- (c) All of the above
- (d) None of the above

9.43. The wireless standard that can be employed in both the ISM and UNII bands is

- (a) 802.11a
 - (b) 802.11b
 - (c) 802.11g
 - (d) 802.11n
- 9.44. Which of the following standards can be employed in the MIMO mode? (a) 802.11a (b) 802.11b (c) 802.11g (d) 802.11n
- 9.45. The standard that employs only DSSS as the carrier technique in the physical layer is (a) 802.11a (b) 802.11b (c) 802.11g (d) 802.11n
- 9.46. The frequency spectrum for 802.11b is divided into 11 channels. The three channels that do not overlap are (a) 1, 5 and 10 (b) 1, 6 and 11 (c) 2, 6 and 10 (d) 3, 7 and 11
- 9.47. Space time coding is employed with which of the following? (a) 802.11a (b) 802.11b (c) 802.11g (d) 802.11n
- 9.48. Multiple antennas are employed in the following mode: (a) MIMO (b) SISO (c) All of the above (d) None
- 9.49. Which of the following are benefits associated with beam forming/diversity in MIMO systems?
- (a) Mitigation of fading effects
 - (b) Reduction in spectral nulls
 - (c) Reduction in co-channel inter-cell interference
 - (d) All of the above
- 9.50. The MIMO system employs which of the following? (a) Space time coding (b) Space division multiplexing (c) Time division multiplexing (d) All of the above
- 9.51. Which of the following is/are

critical issue(s) in a CSMA/CA environment? (a) Collision detection is difficult in free space radio (b) The station transmitting cannot hear other signals (c) There is a hidden node problem (d) All of the above (e) None of the above 9.52. Which of the following collision avoidance functions is used for asynchronous data service and employs virtual collision detection? (a) The distributed coordinated function (b) The point coordinated function (c) All of the above (d) None of the above

9.53. When a frame is sent from the sending station to the receiving station, the two time intervals when there are no signals associated with (1) sending and (2) receiving are

- (a) 1-DIFS, 2-SIFS
- (b) 1-SIFS, 2-DIFS
- (c) Either (a) or (b)

9.54. If a collision occurs in a CSMA/CA broadcast, error detection must be handled by the

- (a) Application layer
- (b) Data link layer
- (c) Transport layer
- (d) Network Layer

9.55. Virtual carrier sensing is performed at the

- (a) PHY layer
- (b) MAC layer
- (c) All of the above
- (d) None of the above

9.56. Error recovery for a unicast frame is the responsibility of

- (a) The station that initiates transmission
- (b) The station that is to receive a transmission
- (c) All stations on the network

(d) None of the above

9.57. When a PCF supported by an AP is used to control the transmission medium, the contention-free repetition interval consists of two periods: a contention-free period and a contention period. DCF is used in which period?

(a) Contention-free

(b) Contention

(c) All of the above

(d) None of the above

9.58. Which of the following are MAC frame types?

(a) Application

(b) Management

(c) Control

(d) Data

(e) All of the above

9.59. A station on the network can remain asleep and will wake up when it is sent a

(a) Probe signal

(b) Re-association request

(c) Beacon frame

(d) All of the above

(e) None of the above

9.60. The FCC of the U.S. has approved the following number of channels for 802.11a:

(a) 3

(b) 11

(c) 23

(d) 36

9.61. G.729 is an ITU-T standard used primarily for

- (a) PCM for voice
- (b) VoIP
- (c) All of the above

(d) None of the above 9.62. When power over Ethernet is implemented, it employs a nominal voltage of (a) 12 V (b)

36 V (c) 48 V (d) 64 V 9.63. Which of the following

characteristics describes WPAN? (a) Evolved from Bluetooth
(b) Is a short range technology (c) Employs a master

controller to mediate communication within WPAN (d)

Employs a beacon used for synchronization of all devices

(e) All of the above (f) None of the above 9.64. The

basic unit of networking in Bluetooth is called a (a) LAN

(b) Piconet (c) Scatternet (d) None of the above 9.65. A

slave within a piconet can exist in which of the following states? (a) Parked (b) Standby (c) Connection (d) All

of the above (e) None of the above 9.66. The number of

slaves within a piconet that can be active at any given time is (a) 2 (b) 7 (c) 256 (d) Any number 9.67.

Piconet channel access can be characterized as (a)

FH-CSMA/CD (b) FH-TDMA (c) FH-TDD-TDMA (d) FH-TDD-CSMA

9.68. Devices on a piconet hop from one channel to another using a (a) Round-robin sequence (b) Pseudorandom

sequence (c) Hierarchical sequence 9.69. The time slot

employed by devices on a piconet is ___ long. (a) 225

microseconds (b) 425 microseconds (c) 625 microseconds

(d) 825 microseconds 9.70. Each device on a piconet has

(a) a 32-bit IEEE MAC address (b) a 48-bit IEEE MAC

address (c) a 64-bit IEEE MAC address (d) None of the

above

9.71. With co-located piconets, a device may serve as a master in one and a slave in another.

- (a) True
- (b) False

9.72. The number of bands employed by UWB is

- (a) 1
- (b) 2

- (c) 4
- (d) 16
- (e) None of the above

9.73. ZigBee is a WPAN that operates in the ISM radio bands.

- (a) True
- (b) False

9.74. ZigBee can operate in the following configuration(s):

- (a) Single cluster
- (b) Mesh network of clusters
- (c) All of the above
- (d) None of the above

9.75. WiMAX is a viable alternative to cable and DSL.

- (a) True
- (b) False

9.76. A typical WiMAX network consists of base stations, stationary stations and/or mobile stations and an Access Service Network (ASN) Gateway.

- (a) True
- (b) False

9.77. WiMAX employs the following in the physical layer:

- (a) FDD
- (b) TDD
- (c) All of the above
- (d) None of the above

9.78. The techniques used in cellular networks for sharing radio spectrum are

- (a) FDMA/TDMA

- (b) FDMA and CDMA
- (c) TDMA and CDMA
- (d) FDMA/TDMA and CDMA

9.79. The Universal Mobile Telecommunications Service (UMTS) is

- (a) 2G technology
- (b) 2.5 G technology
- (c) 3G technology
- (d) None of the above

9.80. The RNC within a UTRAN controls the channel coding, rate adaptation, synchronization and power control.

- (a) True
- (b) False 9.81. CDMA-2000 is (a) 2G technology (b) 2.5G technology (c) 3G technology (d) None of the above 9.82. Mobility and roaming in a cellular network are handled by the (a) Core network (b) Home location register (c) Visitor location register (d) All of the above (e) None of the above 9.83. The authentication in CDMA2000 is handled by the ___ server. (a) AAA (b) BSC (c) PSDN (d) All of the above (e) None of the above 9.84. An 802.11 MAC frame header contains ___ MAC address fields. (a) 2 (b) 3 (c) 4 (d) All of the above (e) None of the above 9.85. An 802.11 MAC frame header contains a sequence number field for error recovery. (a) True (b) False 9.86. An 802.11 MAC frame header contains a ___ byte RTS/CTS field for VCS. (a) 1 (b) 2 (c) 3 (d) 4 (e) All of the above (f) None of the above 9.87. When an ESS contains a wired 802.3 LAN and an 802.11 AP as shown in Figure 9.24, an 802.11 station is communicating with a server in an 802.3 LAN. The MAC frame header must specify ___ MAC address fields in the MAC header. (a) 2 (b) 3 (c) 4 (d) All of the above (e) None of the above 9.88. When an ESS contains a WDS as shown in Figure 9.26, an 802.11 station is communicating with a server in an 802.3 LAN. The MAC frame header must specify ___ MAC address fields in the MAC header. (a) 2 (b) 3 (c) 4 (d) All of the above (e) None of the above Network Layer 3

10 Chapter 10 - The Network Layer

1. J. Heinanen, RFC 1483: Multiprotocol Encapsulation over ATM Adaptation Layer 5, 1993.
2. D.C. Plummer, RFC 826: Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48-bit Ethernet address for transmission on Ethernet hardware, 1982.
3. J. Postel, RFC 791: Internet protocol, 1981.
4. K. Nichols, S. Blake, F. Baker, and D. Black, RFC 2474: Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, 1998.
5. "Keith Henson 127.0.0.1 court deposit church scientology - Google Search," Happy Hacker; <http://www.google.com/search?q =>
6. V. Fuller, T. Li, J. Yu, and K. Varadhan, RFC 1519: Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy, 1993.
7. "IPv4 Address Space Registry;"
<http://www.iana.org/assignments/ipv4-address-space/>.
8. R. Droms, RFC 2131: Dynamic Host Configuration Protocol, 1997.
9. R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6), 2003.
10. "Internet Multicast Addresses;"
<http://www.iana.org/assignments/multicast-addresses/>.
11. W. Fenner, RFC 2236: Internet Group Management Protocol, Version 2, 1997.
12. B. Fenner, H. He, B. Haberman, and H. Sandick, RFC 4605: Internet Group Management Protocol (IGMP) Multicast Listener Discovery (MLD)-Based Multicast Forwarding, 2006.
13. Cisco Systems, "Internetworking Technology Handbook;"
14. B. Fenner and others, RFC 2362: Protocol Independent Multicast-Sparse Mode (PIM SM): Protocol Specification, 2003.

15. A. Adams, J. Nicholas, and W. Siadak, RFC 3973: Protocol Independent Multicast-Dense Mode (PIM-DM): Protocol Specification (Revised).
16. B. Fenner, M. Handley, and H.K.I. Holbrook, RFC 4601: Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised) 2006, RFC 4601, 2006.
- Correspondent Home network Home agent (HA) Foreign agent (FA) Internet Tunnel Visited network:
- FIGURE 10.56 The routing procedure for a mobile node in a visited network.
17. C. Diot, L. Giuliano, G. Shepherd, R. Rockell, D. Meyer, J. Meylor, and B. Haberman, RFC 3569: An Overview of Source-Specific Multicast (SSM), RFC 3569, 2003.
18. M. Handley, I. Kouvelas, T. Speakman, and L. Vicisano, RFC 5015: Bidirectional Protocol Independent Multicast (BIDIR-PIM), 2007.
19. E. Rosen, A. Viswanathan, and R. Callon, RFC 3031: Multiprotocol Label Switching Architecture, 2001.
20. D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, and G. Swallow, RFC 3209: RSVP-TE: Extensions to RSVP for LSP Tunnels, 2001.
21. A. Farrel, A. Ayyangar, and J. Vasseur, RFC 5151: Inter-Domain MPLS and GMPLS Traffic Engineering- Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions, 2008.
22. P. Srisuresh and M. Holdrege, RFC 2663: IP network address translator (NAT) terminology and considerations, RFC 2663, August 1999, 1999.
23. P. Srisuresh and K. Egevang, RFC 3022: Traditional IP network address translator, 2001.
24. J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy, RFC 3489: STUN-Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), Mar. 2003, 2003.
25. F. Audet and C. Jennings, RFC 4787: Network Address Translation NAT Behavioral Requirements for Unicast UDP, January, 2007.
26. S. Guha, K. Biswas, B. Ford, S. Sivakumar, and P. Srisuresh, RFC 5382: NAT Behavioral Requirements for TCP, 2008.
27. G. Huston, "Anatomy: A Look Inside Network Address Translators - The Internet Protocol Journal - Volume 7, Number 3 - Cisco Systems," The Internet Protocol Journal, vol. 7, 2004;

CHAPTER 10 PROBLEMS

- 10.1. Use the “arp-a” command to illustrate the arp cache for your personal computer.
- 10.2. Fill in the blanks for the source and destination IP addresses as well as the source and destination MAC addresses for a frame traveling from Station A to Station B in the network in Figure P10.2. Station A 131.204.1.1

00-50-12-FB-70-11 00-50-12-FB-76-CP 131.204.1.2
00-10-41-16-FE-24 131.204.10.3 R S 2 S 2 131.204.10.1
00-50-12-FB-70-12 Subnet 1 Src MAC Src IPDest MAC Dest IP
Payload

Src MAC Src IPDest MAC Dest IP Payload Subnet 2 Station B
P10.2

10.3. Fill in the blanks for the source and destination IP addresses as well as the source and destination MAC addresses for a frame traveling from Station A to Station B in the network in Figure P10.3. Station A 131.204.1.1

00-50-12-FB-70-11 131.204.2.2 00-50-12-FB-70-14
00-50-12-FB-76-C9 131.204.1.2 00-10-41-16-FE-2 4
131.204.10.3 R1 R2 S 2 S 2 131.204.10.1 00-50-12-FB-70-15
131.204.2.1 00-50-12-FB-70-12 Subnet 1 Src MAC Src IPDest
MAC Dest IP Payload Src MAC Src IPDest MAC Dest IP Payload

Src MAC Src IPDest MAC Dest IP Payload Subnet 2 Station B

P10.3 10.4. Fill in the blanks for the source and destination IP addresses as well as the source and destination MAC addresses for a frame traveling from Station A to Station B in the network in Figure P10.4.
Station A 131.204.1.1 00-50-12-FB-70-11 131.204.2.2
00-50-12-FB-70-14 00-50-12-FB-70-15 00-50-12-FB-76-C9
131.204.1.2 00-10-41-16-FE-24 131.204.10.3 R1 R2 R3 S 1 S 2
S 3 131.204.10.1 131.204.2.1 00-50-12-FB-70-12 Subnet 1 Src
MAC Src IPDest MAC Dest IP Payload Src MAC Src IPDest MAC
Dest IP Payload Src MAC Src IPDest MAC Dest IP Payload
Subnet 2 Station B P10.400 10.5. Assuming all switches are layer 2 switches, determine the number of subnets present in the network in Figure P10.5. 131.204.1.2 131.204.1.4
131.204.1.1 131.204.2.1 131.204.2.4 131.204.2.2 131.204.3.5
131.204.3.2 131.204.3.1 P10.5 10.6. Assuming all switches are layer 2 switches, assign IP addresses and subnet masks to the router interfaces that do not have IP addresses in the network in Problem 10.5.

10.7. Assuming all switches are layer 2 switches, determine the number subnets in the network in Figure P10.7.

131.204.1.2 131.204.1.4 131.204.1.1 131.204.2.1 131.204.2.4
131.204.2.2 131.204.3.5 131.204.3.2 131.204.3.1 131.204.4.1
131.204.4.4 131.204.4.2 P10.7

10.8. Assuming all switches are layer 2 switches, assign IP addresses and subnet masks to the router interfaces that do not have IP addresses in Problem 10.7.

10.9. Determine the IP address and subnet mask for the new subnet formed by combining the following two subnets in

Problem 10.7: 131.204.2.0/24 and 131.204.3.0/24. In addition, assign the gateway IP address for the new subnet. (Assume all switches are Layer 2 switches.)

10.10. An external host sends a HTTP request to a web server behind the NAT router shown in Figure P10.10. A fixed mapping is used to open a port for the remote HTTP request. Determine the NAPT table inside the NAT router and list the step-by-step development of the NAPT table for both an incoming HTTP request and an outgoing HTTP response. 131.204.2.3 69.1.1.7 Internet 10.1.1.1 NAT router 10.1.1.2 P10.10

10.11. Network layer protocols are built into every host and router.

(a) True

(b) False

10.12. Which of the following functions are performed by the network layer?

(a) Encapsulating

(b) Forwarding

(c) Routing

(d) All of the above

(e) None of the above

10.13. Which of the following types of service is performed by the network layer?

(a) Connectionless

(b) Connection-oriented

(c) All of the above

(d) None of the above 10.14. Virtual circuits provide a reserved link from source interface to destination interface. (a) True (b) False 10.15. Packets belonging to a specific VC carry with it the destination IP address.

(a) True (b) False 10.16. Within a VC, the VCI can be changed on each link/hop. (a) True (b) False 10.17. In a connectionless datagram network, no call setup is required at the network layer. (a) True (b) False 10.18. One

characteristic of a connectionless datagram network is that the packets arrive at the destination in order. (a) True
(b) False 10.19. A router forwarding table specifies the router interface for a given destination IP address range.
(a) True (b) False 10.20. Datagram networks are ideal for audio and video services. (a) True (b) False 10.21. The length of the IPv4 datagram is (a) 4 bytes (b) 8 bytes
(c) 16 bytes (d) None of the above 10.22. An incoming datagram that will be protected by IPsec using a router must employ fragmentation. (a) True (b) False 10.23. The type of service field in the IP header dictates the operation of the router in satisfying a specified QoS. (a) True (b) False 10.24. Marking traffic for a certain priority which corresponds to a specific QoS is done by (a) Originating equipment (b) VLAN switch (c) Router (d) All of the above (e) None of the above 10.25. With IPv4, a relationship is established between the DSCP and the IPP values. (a) True (b) False

10.26. Which of the following are scheduling methods?

- (a) FIFO
- (b) WFQ
- (c) LLC
- (d) All of the above

10.27. The default queuing method used on WAN interfaces with a speed of E1 or less is

- (a) FIFO
- (b) WFQ
- (c) LLC

10.28. The IP address is a 32-byte identifier for a host or router interface.

- (a) True
- (b) False

10.29. Each network interface has one IP address and one MAC address.

- (a) True

(b) False

10.30. In a network composed of an interconnection of subnets, the host portion of the IP address is the high order bits.

(a) True

(b) False

10.31. CIDR

(a) Eliminates the class limitation resulting from the network ID

(b) Is the representation used for configuring routers and firewalls

(c) All of the above

(d) None of the above

10.32. The information needed to map from IP address to MAC address within each host is saved in the ARP cache.

(a) True

(b) False

10.33. The following information is required in order for an individual to obtain the IP address of his or her own PC:

(a) Subnet mask

(b) Gateway IP address

(c) None of the above

10.34. When a host joins a network, it can dynamically obtain its IP address from the network DHCP server.

(a) True

(b) False

10.35. Unicast is a more efficient use of network resources than multicast when broadcasting a video stream.

(a) True

(b) False

10.36. When a receiving host joins an IP multicast group, the primary protocol used to construct the multicast distribution tree is

(a) EIGRP

(b) IGMP

(c) PIM

(d) None of the above 10.37. PIM-SM, DM and SSM are all different forms of (a) EIGRP (b) IGMP (c) PIM (d) None of the above 10.38. MPLS works for (a) Circuit-based clients (b) Packet switching clients (c) All of the above (d) None of the above 10.39. MPLS carries the following types of traffic: (a) ATM (b) Ethernet frames (c) SONET (d) All of the above (e) None of the above 10.40. MPLS uses a LSR and LER. (a) True (b) False 10.41. When using MPLS, the LSR performs the translation between MPLS packets and IP packets. (a) True (b) False 10.42. The LER examines incoming packets and forwards them based upon their label instructions. (a) True (b) False 10.43. One of the functions of the MPLS is the sorting of traffic into forward equivalence classes. (a) True (b) False 10.44. In general, a private network uses a single IP address to connect to the Internet. (a) True (b) False 10.45. The one-to-one mapping between the source IP address/port number and the destination IP address/port number is provided by the NAPT translation table. (a) True (b) False 10.46. The number of bits employed in the NAPT port number field is (a) 4 (b) 8 (c) 16 (d) None of the above

10.47. One possible solution to the problem of connecting to a server within a private network is to statically configure the NAPT router to always forward incoming connection requests at a given port to a specific server.

(a) True

(b) False

10.48. The vehicle employed by hosts and routers to trigger diagnostics when an IP packet encounters problems is an ICMP packet.

(a) True

(b) False

10.49. The traceroute diagnostic technique employs a series of TCP packets that are sent to a destination using a destination port that is not in use.

(a) True

(b) False

10.50. To minimize security risks in hosts and routers, the ICMP response should be turned off.

(a) True

(b) False

10.51. When a local address is obtained using the DHCP in a visited network it is called a

(a) Foreign agent care-of address

(b) Co-located care-of address

10.52. A ___ router forwards datagrams based on the destination IP prefix.

(a) Unicast

(b) Multicast

(c) All of the above

(d) None of the above

10.53. A ___ router forwards datagrams based on both source and destination IP prefixes.

(a) Unicast

(b) Multicast

(c) All of the above

(d) None of the above

10.54. A mobile device discovers the home agent using a ___ datagram in a visited network.

- (a) Unicast ICMP
- (b) Multicast ICMP
- (c) DHCP
- (d) All of the above
- (e) None of the above

10.55. A traceroute command sends ___ datagrams to routers and the destination host.

- (a) UDP
 - (b) ICMP
 - (c) All of the above
 - (d) None of the above
- 10.56. A ___ NAPT router relies on an external relay server to permit the entry of incoming datagrams. (a) IGD-enabled (b) STUN-enabled (c) All of the above (d) None of the above
- 10.57. A ___ NAPT router relies on the discovery of services for port mapping. (a) IGD-enabled (b) STUN-enabled (c) All of the above (d) None of the above
- 10.58. A STUN agent discovers the type of NAPT router using ___ packets. (a) TCP (b) UDP (c) All of the above (d) None of the above
- 10.59. A multiprotocol label switching (MPLS) provides ___ service for the datagrams delivered from connected Ethernet networks. (a) Connectionless (b) Connection-oriented (c) All of the above (d) None of the above
- 10.60. A DHCP server uses a ___ datagram to deliver a DHCP offer to a DHCP client. (a) Unicast (b) Broadcast (c) All of the above (d) None of the above
- 10.61. The PM-SM uses a ___ tree to distribute information about active sources. (a) Source (b) Shared (c) All of the above (d) None of the above
- 10.62. The ___ client performs the binding request. (a) STUN (b) ICE (c) TURN (d) All of the above (e) None of the above
- 10.63. The ___ uses the STUN and TURN as tools to gather candidates. (a) STUN (b) ICE (c) TURN (d) All of the above (e) None of the above

10.64. The ICE uses the ___ to test connectivity between peers.

- (a) STUN
- (b) ICE

- (c) TURN
- (d) All of the above
- (e) None of the above

10.65. The TURN server visualizes packets from the client as though they had come from the client's ___ transport address.

- (a) Host
- (b) Server-reflexive
- (c) Relayed
- (d) All of the above
- (e) None of the above

10.66. The ICE server establishes a connection between two peers that are behind NATs.

- (a) True
- (b) False

11 Chapter 11 - IPv6

1. "Free Pool of IPv4 Address Space Depleted | The Number Resource Organization"; <http://www.nro.net/news/ipv4-free-pool-depleted>.
2. S. Wexler, "IPv6 Momentum Takes Huge Swing - Network Computing," 2011;
3. "IPv6 e-learning"; <http://www.6diss.org/e-learning/>.
4. S. Deering and R. Hinden, RFC 2460: Internet Protocol, 1998.
5. D. Borman, RFC 2147: TCP and UDP over IPv6 Jumbograms, 1997.
6. D. Borman, S. Deering, and R. Hinden, RFC 2675: IPv6 Jumbograms, 1999.
7. A. Conta and S. Deering, "RFC 2463: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification," 1998.
8. B. Fenner, H. He, B. Haberman, and H. Sandick, RFC 4605: Internet Group Management Protocol (IGMP) Multicast Listener Discovery (MLD)-Based Multicast Forwarding, 2006.
9. S. Deering, B. Fenner, and B. Haberman, RFC 2710: Multicast Listener Discovery (MLD) for IPv6, 1999, 1999.
10. R. Vida and L. Costa, RFC 3810: Multicast Listener Discovery Version 2 (MLDv2) for IPv6, 2004.
11. R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6), 2003.
12. T. Narten and R. Draves, RFC 3041: Privacy Extensions for Stateless Address Autoconfiguration in IPv6, 2001.
13. R. Hinden and B. Haberman, RFC 4193: Unique Local IPv6 Unicast Addresses, 2005.
14. R. Hinden and S. Deering, RFC 2373: IP version 6 addressing architecture, 1998.
15. "IPv6 Multicast Address Space Registry"; <http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xml>.

16. R. Hinden and S. Deering, RFC 4291: IP Version 6 Addressing Architecture, 2006.
17. C. Huitema and B. Carpenter, RFC 3879: Deprecating Site Local Addresses, 2004.
18. G. Huston, A. Lord, and P. Smith, RFC 3849: IPv6 Address Prefix Reserved for Documentation, 2004.
19. S. Miyakawa, "IPv4 to IPv6 Transformation Schemes," IEICE TRANSACTIONS on Communications, vol. 93, 2010, pp. 1078-1084.
20. E. Nordmark and R. Gilligan, RFC 4213: Basic transition mechanisms for IPv6 hosts and routers, 2005.
21. Cisco Systems, "Cisco Carrier-Grade IPv6 (CGv6) Solution Delivering on the future of the Internet";
22. J. Yamaguchi, Y. Shirasaki, S. Miyakawa, A. Nakagawa, and H. Ashida, "NAT444 addressing models: draft-shirasaki-nat444-isp-shared-addr-04.txt";
23. S. Guha, K. Biswas, B. Ford, S. Sivakumar, and P. Srisuresh, RFC 5382: NAT Behavioral Requirements for TCP, 2008.
24. F. Audet and C. Jennings, RFC 4787: Network Address Translation NAT Behavioral Requirements for Unicast UDP, January, 2007.
25. B.F.S.S.. Srisuresh, B. Ford, S. Sivakumar, and S. Guha, RFC 5508: Nat behavioral requirements for icmp, RFC 5508 (Best Current Practice), 2009.
26. S. Jiang, D. Guo, and B. Carpenter, "An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition: draft-jiang-incremental-cgn-00.txt," 2009; <http://tools.ietf.org/html/draft-jiang-incremental-cgn-00>.
27. Cisco Systems, "How Can Service Providers Face IPv4 Address Exhaustion? IPv6. - Cisco Systems";
28. G. Tsirtsis and P. Srisuresh, RFC 2766: Network address translation-protocol translation, February, 2000.
29. C. Aoun and E. Davies, RFC 4966: Reasons to Move the Network Address Translator-Protocol Translator (NAT-PT) to Historic Status, 2007.

30. D. Wing, D. Ward, and A. Durand, "A Comparison of Proposals to Replace NAT-PT: draft-wing-nat-ptreplacement-comparison-02.txt," 2008;
31. X. Li, C. Bao, M. Chen, H. Zhang, and J. Wu, "draft-xli-behave-ivi-02 - The CERNET IVI Translation Design and Deployment for the IPv4/IPv6 Coexistence and Transition"; <http://tools.ietf.org/html/draft-xli-behave-ivi-02>.
32. C. Diot, L. Giuliano, G. Shepherd, R. Rockell, D. Meyer, J. Meylor, and B. Haberman, RFC 3569: An Overview of Source-Specific Multicast (SSM), RFC 3569, 2003.
33. A. Durand, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion, draft-ietf-softwiredual-stack-lite-05," 2010;

11.6. Describe the source IP and destination IP addresses for packets A, B, and C shown in the network in Figure P11.6.

P11.6. C B 6to4 site 1 6to4 site 2 6to4 router X 6to4
router Y IPv4 IPv4 IPv6 IPv6 131.204.2.3 131.204.2.2

IID = 7 A B IID = 23 A P11.6

11.7. Describe the source IP and destination IP addresses for packets A, B, and C shown in the network in Figure P11.7.

P11.7. C B 6to4 site 1 6to4 site 2 6to4 router X 6to4
router Y IPv4 IPv4 IPv6 IPv6 131.204.2.3 131.204.2.2

IID = 7 A B IID = 23 A P11.7

11.8. Describe the new broadcast methods included in IPv6.

11.9. Describe the use of an IPv6 anycast address.

11.10 Describe the advantage of IPv6 rapid deployment on IPv4 infrastructures (6rd).

11.11. The header length for an IPv6 datagram is

- (a) 16 bytes
- (b) 32 bytes
- (c) 64 bytes
- (d) None of the above

11.12. The maximum non-jumbo payload in an IPv6 packet is

- (a) 32 bytes
- (b) 64 bytes
- (c) 128 bytes
- (d) None of the above

11.13. Which of the following types of addresses are used by IPv6?

- (a) Anycast
- (b) Multicast
- (c) Unicast
- (d) All of the above
- (e) None of the above

11.14. The scope of unicast addresses falls into which of the following categories?

- (a) Link local
 - (b) Site local
 - (c) Global
 - (d) All of the above
 - (e) None of the above
- 11.15. An anycast address is assigned to more than one interface. (a) True (b) False
- 11.16. Anycast addresses are (a) Assigned only to routers
(b) Used only as destination addresses (c) All of the above (d) None of the above
- 11.17. The techniques used for routing with co-existent IPv4 and IPv6 routers are (a) Dual stack (b) Tunneling (c) All of the above (d) None of the above
- 11.18. In the IPv6-to-IPv4 (6To4) tunneling process, the encapsulation/decapsulation takes place entering/leaving the (a) IPv4 domain (b) IPv6 domain (c) None of the above
- 11.19. 6To4 relay routers permit networks using IPv6-to-IPv4 addresses to exchange traffic with hosts using native IPv6 addresses. (a) True (b) False
- 11.20. Teredo tunneling grants IPv6 connectivity to nodes located behind a NAT. (a) True (b) False
- 11.21. IPv4 hosts located behind a NAT have a global IPv4 address. (a) True (b) False
- 11.22. Teredo servers and relays are

assigned global IPv4 addresses. (a) True (b) False
11.23. Teredo technology is supported by Windows (a) XP
(b) 7/Vista (c) Server 2003 (d) Server 2008 (e) All of
the above (f) None of the above 11.24. Teredo servers and
relays listen for Teredo traffic on (a) TCP port number
3454 (b) UDP port number 5434 (c) TCP port number 3544
(d) UDP port number 3544 (e) None of the above

11.25. After a Teredo tunnel is established, traffic is
routed between Teredo hosts and native IPv6 hosts by the

- (a) Teredo server
- (b) Teredo relay
- (c) All of the above
- (d) None of the above

11.26. The length of the Teredo address is

- (a) 32 bits
- (b) 64 bits
- (c) 128 bits
- (d) 264 bits

11.27. In addition to the IPv6 payload, the Teredo data
packet contains an

- (a) IPv4 header
- (b) IPv6 header
- (c) UDP header
- (d) All of the above
- (e) None of the above

11.28. As a security measure, Windows turns off the echo
response to a ping.

- (a) True
- (b) False

11.29. The NAT444 scheme uses ___ NAT translations when the

datagrams leave an ISP's network.

- (a) 1
- (b) 2
- (c) 3
- (d) All of the above
- (e) None of the above

11.30. The CGN must support the translation between IPv4 and ___ packets.

- (a) IPv4
- (b) IPv6
- (c) All of the above
- (d) None of the above

11.31. The Stateful AFT (aka NAT64) can allow ___ clients to connect to IPv4-only servers.

- (a) IPv4-only
- (b) IPv4 and IPv6
- (c) IPv6-only
- (d) All of the above
- (e) None of the above

11.32. The ___ AFT is only required to translate IP addresses in IP headers.

- (a) Stateful
 - (b) IVI
 - (c) All of the above
 - (d) None of the above
- 11.33. The dual-stack lite (DS-Lite) uses ___ for bridging IPv4 to IPv6. (a) Tunneling (b) NAT
(c) All of the above (d) None of the above
- 11.34. To deploy the Dual-stack lite (DS-Lite), the ISP uses the ___ network. (a) IPv4 (b) IPv6 (c) All of the above (d)

None of the above 11.35. The 6rd uses the standard 6To4 prefix 2002::/16 as the IPv6 address prefix for IPv6 hosts. (a) True (b) False 11.36. To deploy the 6rd, the ISP uses the ___ network. (a) IPv4 (b) IPv6 (c) All of the above (d) None of the above 11.37. The 6rd CPEs support ___ on the customer-site side. (a) IPv4 (b) IPv6 (c) All of the above (d) None of the above 11.38. In the use of Teredo, the client is allowed to be behind a ___ NAT. (a) Full-cone (b) Restricted-cone (c) Symmetric (d) All of the above (e) None of the above 11.39. In order to use Teredo, the client ___ a Teredo server. (a) Is configured to use (b) Discovers (c) All of the above (d) None of the above 11.40. In order to use Teredo to send a datagram to an IPv6 network, the client ___ a Teredo relay. (a) Is configured to use (b) Discovers (c) All of the above (d) None of the above

12 Chapter 12 - Routing and Interior Gateways

1. C. Hedrick, RFC 1058: Routing information protocol, 1988.
 2. J. Moy, RFC 2328: OSPF version 2, 1998.
 3. Y. Rekhter, T. Li, and S. Hares, RFC 4271: a Border Gateway Protocol 4 (BGP-4), 2006.
 4. Q. Vohra and E. Chen, RFC 4893: BGP Support for Four-octet AS Number Space, 2007.
 5. J. Moy, RFC 1247: OSPF version 2 (1991), 1991.
 6. D. Knuth, "A generalization of Dijkstra's algorithm," Information Processing Letters, vol. 6, 1977, pp. 1-5.
 7. G. Malkin, RFC 2453: routing information protocol version 2, 1998.
 8. J. Moy, RFC 1245: OSPF protocol analysis, 1991.
 9. G. Malkin and R. Minnear, RFC 2080: RIPng for IPv6, 1997.
 10. R. Coltun, D. Ferguson, and J. Moy, RFC 2740: OSPF for IPv6, 1999.
 11. C. Steigner, H. Dickel, and T. Keupen, "RIP-MTI: A New Way to Cope with Routing Loops," Proceedings of the Seventh International Conference on Networking, 2008, pp. 626-632.
- CHAPTER 12 PROBLEMS
- 12.1. Given the network in Figure P12.1, manually create routing tables for Routers 1 and 2. Show both the MAC and IP headers for propagating a frame from Station A to Station B. In addition, illustrate the manner in which the router forwards the datagram. (Assume all switches are Layer 2 switches.)
- | | | | | | |
|-------------|-------------|-------------|-------------|-------------|-------------|
| Station A | Station B | Station C | Station D | Router 1 | 131.204.1.1 |
| 131.204.2.1 | 131.204.3.1 | 131.204.2.4 | 131.204.2.2 | 131.204.3.5 | |
| 131.204.3.2 | 131.204.1.2 | 131.204.1.4 | Router 2 | P12.1 | 12.2. |
- In the networks shown in Figure P12.2, assume Stations A and B belong to VLAN 1 and Stations C and D belong to VLAN 2. Manually create routing tables for Routers 1 and 2, as well as the necessary Layer 2 switching tables for the involved switches. Show the MAC header, the 802.11q tag, and the IP header for the frame propagating from Station A to Station B. In addition, illustrate the manner in which the router and switch forward the datagram.
- | | | | | | |
|-------------|-------------|-------------|-------------|-------------|-------------|
| Station A | Station B | Station C | Station D | Router 1 | 131.204.1.4 |
| 131.204.2.2 | 131.204.3.5 | 131.204.3.2 | 131.204.1.2 | 131.204.2.4 | |

VLAN 1: 131.204.1.0/24 VLAN 1: 131.204.2.0/24 Router 2
P12.2

12.3. Assume Stations A and B belong to VLAN 1 and Stations C and D belong to VLAN 2 as shown in Problem 12.1.

Manually create routing tables for Routers 1 and 2, as well as the necessary Layer 2 switching tables for the involved switches. Show the MAC header, the 802.11q tag, and the IP header for the frame propagating from Station A to Station C. In addition, indicate the manner in which the router and switch forward the datagram.

12.4. Given the network in Figure P12.4, illustrate the development of the OSPF routing table for router W in a step-by-step manner. W X Y Z U V 6 7 3 5 2 2 4 1 1 3 P12.4

12.5. Given the network in Figure P12.5, illustrate the development of the OSPF routing table for router W in a step-by-step manner. W X Y T Z U V 6 7 3 5 2 2 2 4 2 4 1 3 3 P12.5

12.6. Given the network in Figure P12.6, illustrate the development of OSPF routing table for router W in a step-by-step manner. 2 2 2 2 3 3 4 6 9 5 2 7 8 6 S V X W Z

Y T U 1 1 1 P12.6 12.7. Illustrate the step-by-step development of the RIP routing tables for the network

shown in Figure P12.7. 6 7 4 4 2 3 5 V X Y W Z P12.7 12.8.

Illustrate the step-by-step development of the RIP routing tables for the network shown in Figure P12.8. 6 4 4 3 2 6

5 3 2 Y Z X W U V P12.8 12.9. Routing tables are generated

(a) Statically (b) Dynamically (c) All of the above (d)

None of the above 12.10. Routing tables are maintained by

(a) Periodic updates (b) Triggered updates in response to link changes (c) All of the above (d) None of the above

12.11. The knowledge base for routing algorithms is either global or decentralized. (a) True (b) False 12.12. Which of the following are common interior gateway protocols (IGPs)? (a) RIP (b) OSPF (c) IGRP (d) All of the above

(e) None of the above

12.13. BGP is a common exterior gateway protocol.

(a) True

(b) False

12.14. The OSPF configuration differs from the RIP configuration as a result of its use of a wildcard mask instead of a subnet mask in the defining network statement.

(a) True

(b) False

12.15. Route computation in OSPF is performed using Dijkstra's algorithm.

(a) True

(b) False

12.16. With OSPF, advertisements carried in OSPF messages employ both TCP and UDP.

(a) True

(b) False

12.17. Link-state advertisements employed in a hierarchical OSPF structure are performed in the hierarchical structure as a whole, global topology.

(a) True

(b) False

12.18. Which of the following are types of routers used in conjunction with OSPF?

(a) AS border

(b) Area border

(c) Backbone

(d) All of the above

(e) None of the above

12.19. When OSPF is in use, a LSA is sent to exchange LSDB and may contain one or more LSUs.

(a) True

(b) False

12.20. When using OSPF, the SPF algorithm calculates best paths to all destinations using the LSDB producing a routing table.

(a) True

(b) False

12.21. One commonality factor between OSPF and RIP is that they both permit multiple same-cost paths.

(a) True

(b) False

12.22. Fundamental to the use of Dijkstra's algorithm for link state routing in OSPF is the fact that each router knows the least cost path from itself to all other nodes.

(a) True

(b) False

12.23. When Dijkstra's algorithm is employed with OSPF all routers in the network simultaneously develop their shortest path tree and forwarding table.

(a) True

(b) False 12.24. In order to enhance security, both OSPF and all versions of RIP employ message authentication and VLSM. (a) True (b) False 12.25. In general, OSPF is more efficient than RIP in that it does not need a header for the transport layer. (a) True (b) False 12.26. The

distance vector algorithm employed in RIP is based upon the Bellman-Ford equation. (a) True (b) False 12.27. Unlike OSPF, RIP has global information and a router's knowledge is not limited to the local area. (a) True (b) False

12.28. The distance vectors used in RIP contain both magnitude and direction. (a) True (b) False 12.29. Once the RIP initialization process is complete, each node propagates its distance table to its immediately adjacent neighbors. (a) True (b) False 12.30. Once set, the distance vector tables employed in RIP need not be updated.

(a) True (b) False 12.31. In the computation of distance vectors in RIP, the poison reverse is effective in some cases in preventing what is called the ping-pong effect.

(a) True (b) False 12.32. Once the ping-pong effect begins, the updating process used to determine the shortest paths will not reach equilibrium. (a) True (b) False

12.33. Split horizon is a rule designed to prevent the establishment of a ping-pong loop. (a) True (b) False

12.34. The maximum hop limit imposed by RIP is (a) 7 (b) 15 (c) 50 12.35. Poison reverse is effective in

preventing the count to infinity in the 3-node case. (a) True (b) False

12.36. OSPF is a local operation while RIP is global in nature.

(a) True

(b) False

12.37. OSPF converges faster than RIP.

(a) True

(b) False

12.38. Given an n -node network with no hierarchical areas, the total memory requirements are on the order of ____.

(a) n for RIP

(b) n^2 for OSPF

(c) All of the above

(d) None of the above

12.39. Which of the following techniques is capable of solving the 3-node routing loop problem?

(a) Split horizon with poison reverse

(b) Split horizon

(c) Timeout

(d) All of the above

(e) None of the above

12.40. A single router interface can connect to ____ VLAN(s).

(a) Zero

(b) One

(c) One or multiple

(d) All of the above

(e) None of the above

13 Chapter 13 - Border Gateway Routing

1. Q. Vohra and E. Chen, RFC 4893: BGP Support for Four-octet AS Number Space, 2007.
2. Y. Rekhter and T. Li, RFC 1771: A Border Gateway Protocol 4 (BGP-4), 1995.
3. K. Lougheed and Y. Rekhter, RFC 1105: Border Gateway Protocol (BGP), 1989.
4. D. Mills, RFC 904: Exterior gateway protocol formal specification, 1984.
5. K. Lougheed and Y. Rekhter, RFC 1163 : Border Gateway Protocol (BGP), 1990; <http://tools.ietf.org/html/rfc1163>.
6. K. Lougheed and Y. Rekhter, RFC 1267: Border Gateway Protocol 3, 1991.
7. V. Fuller, T. Li, J. Yu, and K. Varadhan, RFC 1519: Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy, 1993.
8. Y. Rekhter and P. Gross, RFC 1772: Application of the Border Gateway Protocol in the Internet, March 1995, 1995.
9. M. Caesar and J. Rexford, "BGP routing policies in ISP networks," IEEE network, vol. 19, 2005, pp. 5-11.
10. Cisco Systems, "Cisco IOS IP Routing: BGP Configuration Guide, Release 12.2SR"; www.cisco.com/en/
11. K. Butler, T. Farley, P. McDaniel, and J. Rexford, "A survey of BGP security issues and solutions," Proceedings of the IEEE, vol. 98, 2010, pp. 100-122.
12. D. Turk, RFC 3882: Configuring BGP to block Denial-of-Service attacks, 2004.
13. T. Greene, "2010's biggest security SNAFUs";
14. M. Brown, "Pakistan Hijacks YouTube: A Closer Look," 2008; http://www.circleid.com/posts/82258_pakistan_hijacks_youtube_closer_look.
15. T. Bates, R. Chandra, and D. Katz, RFC 4760: Multiprotocol Extensions for BGP-4, 2007.
16. M. Yannuzzi, X. Masip-Bruin, and O. Bonaventure, "Open

issues in interdomain routing: a survey," IEEE network, vol. 19, 2005, pp. 49-56.

CHAPTER 13 PROBLEMS

13.1. With reference to Figure 13.15 and Example 13.7, determine the next hop and destination AS routing table information for router A in Figure P13.1.

AS 1 204.70.0.0/15 AS 6112
131.204.0.0/16 AS 209 204.171.0.0/16 205.171.2.4
205.171.2.3 205.171.1.3.3 205.171.3.2 205.171.3.133
205.171.3.132 205.171.2.6 205.171.2.5 205.171.2.1
205.171.2.2 G C F B E A AS 5 192.67.95.0/24 AS 6
140.222.0.0/16 P13.1

13.2. With reference to Figure 13.15 and Example 13.7, determine the next hop and destination AS routing table information for router B in Figure P13.1.

13.3. With reference to Figure 13.15 and Example 13.7, determine the next hop and destination AS routing table information for router C in Figure P13.1.

13.4. With reference to Figure 13.15 and Example 13.7, determine the next hop and destination AS routing table information for router E in Figure P13.1.

13.5. With reference to Figure 13.15 and Example 13.7, determine the next hop and destination AS routing table information for router F in Figure P13.1.

13.6. With reference to Figure 13.15 and Example 13.7, determine the next hop and destination AS routing table information for router G in Figure P13.1.

13.7. Given the network in Figure P13.1, determine the AS Path in an advertisement to AS 1.

13.8. Given the network in Figure P13.1, determine the AS Path in an advertisement to AS 5.

13.9. Given the network in Figure P13.1, determine the AS Path in an advertisement to AS 6.

13.10. Given the network in Figure P13.1, determine the AS Path in an advertisement to AS 209 Router B.

13.11. Given the network in Figure P13.1, determine the AS Path in an advertisement to AS 209 Router C.

13.12. Determine the forwarding table for router R1 in the network shown in Figure P13.12.

R5 R1 R2 AS 9122 AS 6112
131.210.0.0/16 205.171.0.0/16 131.204.0.0/16 AS 209
192.168.2.0/30 192.168.3.0/30 192.168.3.1 192.168.2.1
205.171.4.1 205.171.4.0/30 205.171.3.133 205.171.3.132/30
R3 R4 P13.12

13.13. Determine the forwarding table for router R2 in the network shown in Figure P13.12.

13.14. Determine the forwarding table for router R3 in the network shown in Figure P13.12.

13.15. Determine the forwarding table for router R4 in the network shown in Figure P13.12.

13.16. Determine the forwarding table for router R5 in the

network shown in Figure P13.12.

13.17. Show the step-by-step procedure for obtaining a BGP routing table for Router C in Figure P13.17 from the advertisements. A B C 1.1.1.0/24 1.1.8.0/24 1.1.9.0/24
1.1.0.0 /24 1.1.4.0/23 1.1.6.0/23 D E P13.17

13.18. Routers within a given AS can run different intra-AS protocols.

(a) True

(b) False

13.19. The administration in charge of intra-AS routing must be concerned with global policy decisions.

(a) True

(b) False

13.20. The internal topology of neighboring autonomous systems is shared to facilitate interaction.

(a) True

(b) False

13.21. The number of bits currently used to assign a number to each AS is

(a) 16 bits

(b) 32 bits

(c) 64 bits

13.22. The type of AS that maintains an Internet connection even if one of the AS to which it is connected experiences a complete failure is

(a) Multi-homed

(b) Stub

(c) Transit 13.23. An ISP always functions as a (a)
Multi-homed AS (b) Stub AS (c) Transit AS 13.24. The de
facto standard for inter-AS routing is (a) BGP (b) IXP
(c) POP 13.25. The most economical routing mechanism used
with BGP is (a) Link state (b) Distance vector (c) All

of the above (d) None of the above 13.26. CIDR reduces the number of routes in a BGP router. (a) True (b) False 13.27. BGP sessions between two ASs are established on TCP port number (a) 159 (b) 169 (c) 179 (d) None of the above 13.28. A BGP message format for a route update contains the following: (a) Open plus update (b) Keep alive plus notification (c) Prefix plus attribute values (d) None of the above 13.29. Border routers at the edge of an AS act upon a received route advertisement based upon (a) Updates (b) Notifications (c) Import policies (d) None of the above 13.30. Routers within an AS will learn multiple routes to a destination. (a) True (b) False 13.31. A trace route can be used to discover BGP connections. (a) True (b) False 13.32. When a route advertisement crosses an AS boundary, the next hop attribute is changed to the IP address of the destination AS. (a) True (b) False 13.33. ASs propagate their advertisements in a manner that facilitates routing loop detection. (a) True (b) False

13.34. For an advertisement propagation from AS 1 to AS 2 to AS 3, AS 1 provides its IP address, the next hop and the AS_Path, which in this case is

- (a) AS 1
- (b) AS1 and AS 2
- (c) AS 1, AS 2 and AS 3

13.35. The best route from one AS to another is decided by border routers using the prevailing BGP policy.

- (a) True
- (b) False

13.36. Different prefixes are required when propagating to an AS via multiple routes.

- (a) True
- (b) False

13.37. The BGP policy for path decisions is available in

- (a) RIP
- (b) OSPF

(c) All of the above

(d) None of the above

13.38. BGP policies are applied to

(a) Filter routes

(b) Adjust route attributes

(c) All of the above

(d) None of the above

13.39. If the same prefix propagates to an AS via multiple routes, it is the responsibility of the border gateway router to select the best route.

(a) True

(b) False

13.40. When attributes are employed to select routes, the highest priority is given to

(a) Shortest AS path

(b) Local preference

(c) Lowest MED

(d) None of the above

13.41. When an AS is dual-homed, the forwarding table of that AS is configured by

(a) Intra-AS routing algorithms

(b) Inter-AS routing algorithms

(c) All of the above

(d) None of the above

13.42. In a multi-homed AS, the egress traffic is routed based upon the ___ attribute decided by the local AS administration.

(a) Inbound traffic

(b) Outbound traffic

(d) None of the above

13.43. In route advertisement, MED should be considered prior to any consideration of IGP distance.

(a) True

(b) False 13.44. The problem with MED is that it does not provide routing information all the way back to the ingress router of that AS. (a) True (b) False 13.45. The advertisement propagated from AS to AS may contain the following information (a) Prefix (b) Next hop (c) AS path (d) MED (e) All of the above (f) None of the above

13.46. BGP export policies are typically applied to block paths that are security risks. (a) True (b) False 13.47.

BGP cannot detect a routing loop in a route advertisement.

(a) True (b) False 13.48. BGP is vulnerable to (a) DoS attacks (b) Route injection attacks (c) Policy

misconfiguration (d) Policy conflict with neighboring ASs (e) All of the above (f) None of the above 13.49. For an advertisement propagation from AS 1 to AS 2 to AS 3 to AS

4, AS 1 provides its IP address and the next hop. What is the AS_Path received by AS 4? (a) AS1 (b) AS1 AS2 (c)

AS1 AS2 AS3 (d) AS3 AS2 AS1 (e) AS4 AS3 AS2 AS1 (f) None of the above 13.50. The BGP protocol's import and export policy are specified in the RFC. (a) True (b) False

13.51. Every AS's BGP router has the knowledge of the global network topology of every AS. (a) True (b) False

13.52. When an AS wants to prevent its network from sending packets through an adversary AS, this AS should use its

___ policy to block the routes. (a) Import (b) Export

(c) All of the above (d) None of the above Transport Layer
4

14 Chapter 14 - The Transport Layer

CHAPTER 14 PROBLEMS

14.1. The following HTTP response and request data corresponds to the sequence of events outlined in Figure P14.1: $S_1 = 1000$, $A_1 = 2000$, $L_1 = 100$ and $L_2 = 1500$. Determine the quantities X , Y , Z , S_2 , A_2 , S_3 , A_3 and L_3 .
Client Browser sends in http request Google web server Google ACKs the receipt of http request Google sends http response Client ACKs receipt of http response Seq = S_1 , ACK = A_1 , datalength = L_1 Seq = X , ACK = Y , datalength = Z Seq = S_2 , ACK = A_2 , datalength = L_2 Seq = S_3 , ACK = A_3 , datalength = L_3

Time P14.1

14.2. The following HTTP response and request data corresponds to the sequence of events outlined in Figure P14.1: $S_1 = 1000$, $A_1 = 3000$, $L_1 = 200$ and $L_2 = 1500$. Determine the quantities X , Y , Z , S_2 , A_2 , S_3 , A_3 and L_3 .

14.3. The following HTTP response and request data corresponds to the sequence of events outlined in Figure P14.1: $S_1 = 1500$, $A_1 = 3500$, $L_1 = 300$ and $L_2 = 1400$. Determine the quantities X , Y , Z , S_2 , A_2 , S_3 , A_3 and L_3 .

14.4. The following HTTP response and request data corresponds to the sequence of events outlined in Figure P14.1: $S_1 = 1100$, $A_1 = 2500$, $L_1 = 200$ and $L_2 = 1300$. Determine the quantities X , Y , Z , S_2 , A_2 , S_3 , A_3 and L_3 .

14.5. The following HTTP response and request data corresponds to the sequence of events outlined in Figure P14.1: $S_1 = 1300$, $A_1 = 2300$, $L_1 = 100$ and $L_2 = 1200$. Determine the quantities X , Y , Z , S_2 , A_2 , S_3 , A_3 and L_3 .

14.6. Given the simple acknowledgment scheme shown in Figure P14.6, and the following data: $L = 10,000$ bits, $R = 1$ Gbps, and $RTT = 0.07$ s, determine the link utilization. Sender $t = 0$ $t = L/R$ RTT Time ACK $t = RTT + L/R$ Receiver
P14.6 14.7. Given the simple acknowledgment scheme shown in Figure P14.6, and the following data: $L = 100,000$ bits, $R = 1$ Gbps, and $RTT = 0.05$ s, determine the link utilization. 14.8. Given the simple acknowledgment scheme shown in Figure P14.6, and the following data: $L = 1$ Mbit, $R = 10$ Gbps, and $RTT = 0.06$ s, determine the link utilization. 14.9. Given the simple acknowledgment scheme shown in Figure P14.6, and the following data: $L = 1$ Mbit,

R = 1 Gbps, and RTT = 0.08 s, determine the link utilization. 14.10. Given the simple acknowledgment scheme shown in Figure P14.6, and the following data: L = 10 Mbit, R = 1 Gbps, and RTT = 0.05 s, determine the link utilization. 14.11. If a sender sends N packets to a receiver in a pipelined fashion, as outlined in Figure P14.11, and the parameters are L = 10,000 bits, R = 1 Gbps, RTT = 0.07 s, the transmission delay D TR = L/R and N = 2, determine the link utilization. Sender t = 0 RTT N packets Receiver P14.11 14.12. If a sender sends N packets to a receiver in a pipelined fashion, as outlined in Figure P14.11, and the parameters are L = 1,000,000 bits, R = 1 Gbps, RTT = 0.06 s, the transmission delay D TR = L/R and N = 2, determine the link utilization. 14.13. If a sender sends N packets to a receiver in a pipelined fashion, as outlined in Figure P14.11, and the parameters are L = 1 Mbit, R = 10 Gbps, RTT = 0.08 s, the transmission delay D TR = L/R and N = 3, determine the link utilization. 14.14. If a sender sends N packets to a receiver in a pipelined fashion, as outlined in Figure P14.11, and the parameters are L = 10 Mbits, R = 10 Gbps, RTT = 0.075 s, the transmission delay D TR = L/R and N = 2, determine the link utilization. 14.15. If a sender sends N packets to a receiver in a pipelined fashion, as outlined in Figure P14.11, and the parameters are L = 10 Mbits, R = 1 Gbps, RTT = 0.075 s, the transmission delay D TR = L/R and N = 3, determine the link utilization. 14.16. Given the data in Problem 14.11, determine the minimum window size at the receiver. 14.17. Given the data in Problem 14.12, find the minimum window size at the receiver. 14.18. Given the data in Problem 14.13, determine the minimum window size at the receiver.

14.19. Given the information in Problem 14.14, determine the minimum window size at the receiver.

14.20. Given the information in Problem 14.15, determine the minimum window size at the receiver.

14.21. Since the effective bandwidth, B, is limited by the available window size at the receiver, determine this effective bandwidth if N = 2, MSS = 1500 bytes and RTT = 1 ms.

14.22. The receiver's window size limits the effective bandwidth B. Given that N = 100, MSS = 4000 bytes and a RTT = 10 ms, determine the value of B.

14.23. Since the effective bandwidth, B, is limited by the available window size at the receiver, determine this

effective bandwidth if $N = 1000$, $MSS = 18000$ bytes and $RTT = 50$ ms.

14.24. The receiver's window size limits the effective bandwidth B . Given that $N = 12,000$, $MSS = 20,000$ bytes and a $RTT = 100$ ms, determine the value of B .

14.25. Since the effective bandwidth, B , is limited by the available window size at the receiver, determine this effective bandwidth if $N = 100,000$, $MSS = 80,000$ bytes and $RTT = 400$ ms.

14.26. The receiver's window size limits the effective bandwidth B . Given that $N = 500,000$, $MSS = 60,000$ bytes and a $RTT = 800$ ms, determine the value of B .

14.27. Consider the communication between sender and receiver, outlined in Figure P14.27, where the various variables involved in a round trip time measurement are displayed. If the clock number that the sender receives for the Block 0 ACK is $X = 100$, the clock number that the sender sends for Block 0 is $Y = 200$, the clock number the sender receives for Block 1 is $Z = 210$ and the clock number that the receiver receives for Block 1 is $M = 110$, determine the following: (a) the quantities I , J , U and V , and (b) the RTTM derived by the sender when both sender and receiver have a 10 ms clock. Sender $Tsecr = X$ $T1 = Y$ $T2 = Z <ACK$, $Tsval = U$, $Tsecr = V> <Block 1$, $Tsval = I$, $Tsecr = J>$ Receiver $T3 = M$ P14.27

14.28. Given the data in Problem 14.27, determine the RTTM derived by the receiver.

14.29. Consider the communication between sender and receiver, outlined in Figure P14.27, where the various variables involved in a round trip time measurement are displayed. If the clock number that the sender receives for the Block 0 ACK is $X = 200$, the clock number that the sender sends for Block 0 is $Y = 400$, the clock number the sender receives for Block 1 is $Z = 410$ and the clock number that the receiver receives for Block 1 is $M = 210$, determine the following: (a) the quantities I , J , U and V , and (b) the RTTM derived by the sender when both sender and receiver have a 20 ms clock.

14.30. Given the data in Problem 14.29, determine the RTTM derived by the receiver.

14.31. Consider the communication between sender and receiver, outlined in Figure P14.27, where the various

variables involved in a round trip time measurement are displayed. If the clock number that the sender receives for the Block 0 ACK is $X = 150$, the clock number that the sender sends for Block 0 is $Y = 300$, the clock number the sender receives for Block 1 is $Z = 330$ and the clock number that the receiver receives for Block 1 is $M = 170$, determine the following: (a) the quantities I, J, U and V, and (b) the RTTM derived by the sender when both sender and receiver have a 30 ms clock. 14.32. Given the data in Problem 14.31, determine the RTTM derived by the receiver.

14.33. Consider the communication between sender and receiver, outlined in Figure P14.27, where the various variables involved in a round trip time measurement are displayed. If the clock number that the sender receives for the Block 0 ACK is $X = 120$, the clock number that the sender sends for Block 0 is $Y = 240$, the clock number the sender receives for Block 1 is $Z = 280$ and the clock number that the receiver receives for Block 1 is $M = 180$, determine the following: (a) the quantities I, J, U and V, and (b) the RTTM derived by the sender when the sender has a 25 ms clock and receiver has a 30 ms clock. 14.34. Given the data in Problem 14.33, determine the RTTM derived by the receiver. 14.35. Consider the communication between sender and receiver, outlined in Figure P14.27, where the various variables involved in a round trip time measurement are displayed. If the clock number that the sender receives for the Block 0 ACK is $X = 180$, the clock number that the sender sends for Block 0 is $Y = 360$, the clock number the sender receives for Block 1 is $Z = 400$ and the clock number that the receiver receives for Block 1 is $M = 220$, determine the following: (a) the quantities I, J, U and V, and (b) the RTTM derived by the sender when the sender has a 10 ms clock and receiver has a 20 ms clock.

14.36. Given the data in Problem 14.35, determine the RTTM derived by the receiver. 14.37. If the maximum effective bandwidth at which TCP is able to transmit over a particular path is 1.5 Mbps, determine the wraparound time for the sequence number of the TCP. 14.38. If the maximum effective bandwidth at which TCP is able to transmit over a particular path is 10 Mbps, determine the wraparound time for the sequence number of the TCP. 14.39. If the maximum effective bandwidth at which TCP is able to transmit over a particular path is 45 Mbps, determine the wraparound time for the sequence number of the TCP. 14.40. If the maximum effective bandwidth at which TCP is able to transmit over a particular path is 100 Mbps, determine the wraparound time for the sequence number of the TCP. 14.41. If the maximum effective bandwidth at which TCP is able to transmit over a particular path is 1 Gbps, determine the wraparound time for the sequence number of the TCP. 14.42. If the maximum

effective bandwidth at which TCP is able to transmit over a particular path is 10 Gbps, determine the wraparound time for the sequence number of the TCP. 14.43. If the maximum effective bandwidth at which TCP is able to transmit over a particular path is 40 Gbps, determine the wraparound time for the sequence number of the TCP.

14.44. If the maximum effective bandwidth at which TCP is able to transmit over a particular path is 100 Gbps, determine the wraparound time for the sequence number of the TCP.

14.45. If the maximum effective bandwidth at which TCP is able to transmit over a particular path is 1 Gbps and PAWS is employed, determine the wraparound time for the sequence number of the TCP.

14.46. If the maximum effective bandwidth at which TCP is able to transmit over a particular path is 10 Gbps and PAWS is employed, determine the wraparound time for the sequence number of the TCP.

14.47. If the maximum effective bandwidth at which TCP is able to transmit over a particular path is 40 Gbps and PAWS is employed, determine the wraparound time for the sequence number of the TCP.

14.48. If the maximum effective bandwidth at which TCP is able to transmit over a particular path is 100 Gbps and PAWS is employed, determine the wraparound time for the sequence number of the TCP.

14.49. The sending host uses transport protocols to break application layer messages into segments and pass them to the link layer.

(a) True

(b) False

14.50. The transport protocol employed is application dependent.

(a) True

(b) False

14.51. The transport protocol used for the delivery of voice and video is

- (a) SCTP
- (b) TCP
- (c) UDP
- (d) None of the above

14.52. Which of the following transport protocols provide(s) reliable delivery?

- (a) SCTP
- (b) TCP
- (c) UDP
- (d) All of the above

14.53. The protocol that is labeled as a best effort connectionless protocol is

- (a) SCTP
- (b) TCP
- (c) UDP

14.54. Each transport layer segment in an IP datagram in the client/server model contains the source and destination port numbers.

- (a) True
- (b) False

14.55. A UDP socket is identified by the destination IP address.

- (a) True
 - (b) False
- 14.56. A TCP socket is identified by the destination IP address and port number. (a) True (b) False
- 14.57. Handshaking is required when the UDP is employed. (a) True (b) False
- 14.58. The length in bytes of the UDP header is (a) 4 (b) 8 (c) 16
- 14.59. IPsec uses UDP as the transport protocol. (a) True (b) False
- 14.60. When UDP is employed, the sending and receiving order of the packets is the same. (a) True (b) False
- 14.61. When UDP is employed, the network layer uses a

checksum to provide payload error detection. (a) True
(b) False 14.62. The reliable transport of messages is the responsibility of the (a) Transport layer (b) Network layer (c) Data link layer (d) None of the above 14.63. The exchange of sequence numbers between the client and server can be used as a mechanism for detecting packet loss. (a) True (b) False 14.64. An ACK is sent from receiver to sender in response to a received packet. (a) True (b) False 14.65. The use of a pipeline protocol has no impact on link utilization. (a) True (b) False 14.66. The reception of an ACK in the pipelined TCP protocol is the trigger for sending the next packet. (a) True (b) False 14.67. Flow control will use the receiver's buffer size to determine the number of packets the sender will send in the first burst. (a) True (b) False

14.68. In a pipelined transmission, an ACK is sent from sender to receiver between each packet.

(a) True

(b) False

14.69. When a sliding window is used in pipelined transmission, the size of the available window is constantly adjusted by the receiver.

(a) True

(b) False

14.70. TCP is a connectionless service that uses handshaking to establish a socket prior to data exchange.

(a) True

(b) False

14.71. TCP employs an ACK to detect corrupted data at the receiver.

(a) True

(b) False

14.72. In a pipelined TCP transmission, sequence numbers and RTT are used to detect loss/ errors and provide the information for reordering data that has been received out of sequence.

(a) True

(b) False

14.73. The length of a TCP packet header without any option is

(a) 8 bytes

(b) 16 bytes

(c) 32 bytes

(d) None of the above

14.74. When SACK is employed the receiver is able to acknowledge isolated blocks of packets that were received correctly, rather than the sequence number of the last packet received successfully.

(a) True

(b) False

14.75. The receiving host will assume a packet is genuine based upon the fact that the packet arrives at the destination with the correct source and destination IP addresses and port numbers.

(a) True

(b) False

14.76. An ACK is the first byte number, within the receiver's sliding window, following the received data segment and serves as an index for the next data segment.

(a) True

(b) False

14.77. The selection of the ISN carries with it security ramifications.

(a) True

(b) False

14.78. Segments may arrive at the destination out of order due to

- (a) Load balancing
- (b) BGP route changes
- (c) All of the above

(d) None of the above 14.79. The length of the sequence number proposed by the IETF's PAWS scheme to protect against wrapped sequence numbers is (a) 32 bits (b) 64 bits (c) 128 bits 14.80. The 3-way handshake between client and server consists of a SYN, SYN ACK and ACK packets. (a) True (b) False 14.81. Prior to the 3-way handshake between client and server, the two must agree on an ISN for performing handshake. (a) True (b) False 14.82. A socket is established by the information passed back and forth in the 3-way handshake. (a) True (b) False 14.83. In general, the number of bytes in an Ethernet payload that are consumed by both of the TCP and IP headers is (a) 16 (b) 32 (c) 64 (d) None of the above 14.84. When a TCP connection is torn down, the first half close is initiated by the (a) Client (b) Server (c) None of the above 14.85. The ACK number is a self-clocking mechanism which the sender uses to push data to the receiver. (a) True (b) False 14.86. SCTP is unable to handle data transfers in which multiple independent message sequences may not need to be in order. (a) True (b) False 14.87. SCTP is capable of (a) Multi-homing (b) Multi-streaming (c) All of the above (d) None of the above 14.88. One of the benefits of multi-streaming is that messages within the same stream need not be in order. (a) True (b) False

14.89. The SCTP mechanism that permits graceful shutdown in which each endpoint has confirmation that the data has been received by the remote endpoint prior to completion of shutdown is

- (a) 2-way
- (b) 3-way
- (c) 4-way
- (d) None of the above

14.90. The sequence of message units in a SCTP packet is called

- (a) Bits

- (b) Bytes
- (c) Chunks
- (d) None of the above

14.91. The checksum used by SCTP is

- (a) 16 bits
- (b) 32 bits
- (c) 64 bits

14.92. The receiver of a SCTP packet validates the sender with a

- (a) ACK
- (b) Chunk flag
- (c) Verification tag
- (d) None of the above

14.93. If the U-bit contained in the payload data format for a SCTP chunk is set to 0, the data is

- (a) Ordered
- (b) Unordered
- (c) There is no ordering information

14.94. The fragment bits contained within a SCTP chunk's data format are labeled as

- (a) A bits
- (b) B bits
- (c) D bits
- (d) E bits
- (e) All of the above

14.95. The SCTP association establishment sequence that begins with INIT and concludes with COOKIE-ACK requires

how many messages?

- (a) 2
- (b) 3
- (c) 4
- (d) 6
- (e) None of the above

14.96. The SCTP shutdown procedure is a n-message sequence where n is

- (a) 1
- (b) 2
- (c) 3

(d) 4 14.97. If a node has multiple interfaces with multiple IP addresses, a special packet can be used to determine if one of these alternate paths can be used in the event that the primary path fails or becomes congested. This special packet is named (a) Cookie (b) Echo (c) Heartbeat (d) None of the above 14.98. One application in which SCTP is not viable is telephony signaling. (a) True (b) False

15 Chapter 15 - Packet Loss Recovery

8. S. Floyd, T. Henderson, and others, RFC 3782: The NewReno Modification to TCP's Fast Recovery Algorithm, 2004.
9. N. Dukkipati, T. Refice, Y. Cheng, J. Chu, T. Herbert, A. Agarwal, A. Jain, and N. Sutin, "An argument for increasing TCP's initial congestion window," ACM SIGCOMM Computer Communication Review, vol. 40, 2010, pp. 26-33.
10. P. Karn and C. Partridge, "Improving round-trip time estimates in reliable transport protocols," ACM SIGCOMM Computer Communication Review, vol. 25, 1995, pp. 66-74.
11. J. Nagle, RFC 896: Congestion Control in IP/TCP Internetworks, 1984.
12. S. Floyd, J. Mahdavi, M. Mathis, and M. Podolsky, RFC 2883: An Extension to the Selective Acknowledgment (SACK) Option for TCP, 2000.
13. E. Blanton, M. Allman, K. Fall, and L. Wang, RFC 3517: A conservative selective acknowledgment (SACK)-based loss recovery algorithm for TCP, 2003.

CHAPTER 15 PROBLEMS

15.1. Figure P15.1 illustrates the process involved in the creation of a duplicate ACK together with the various parameters that define the data packets and sequence numbers. Given the following parameters: A = 2000, B = 1000, C = 3000, D = 1000, F = 4000, G = 1000, determine the remaining quantities E, H, I, J, U, V, X and Y. Last byte received (LastByteRcvd) = Y X Bytes are missing = V bytes Next byte expected (NextByteExpected) = U Last byte read by receiving process (LastByteRead) Receiving process Duplicate ACK Receiver Sender Time Seq = 2000 time out Retransmission Seq = 1000 time out Seq = A, Bytes data Seq = I, Bytes data ACK = E ACK = H Seq = F, Bytes data Seq = C, Bytes data P15.1

15.2. Repeat Problem 15.1 if A = 1500, B = 1000, C = 2500, D = 500, F = 4000 and G = 500.

15.3. Repeat Problem 15.1 if A = 1600, B = 800, C = 2400, D = 600, F = 4000 and G = 600.

15.4. Repeat Problem 15.1 if A = 1200, B = 600, C = 1800, D

= 300, F = 3000 and G = 300.

15.5. Repeat Problem 15.1 if A = 1500, B = 400, C = 1900, D = 200, F = 3400 and G = 200. 15.6. In the data transmission sequence shown in Figure P15.6, A = 2000, B = 1000, C = 3000, D = 1000, E = 4000, F = 1000, G = 5000, H = 1000, I = 6000, and J = 1000. If the packet Seq = E is lost and the TCP SACK option is being employed, determine the ACK and SACK produced by the Receiver for each received packet. Receiver Sender Time out Seq = A, B bytes Data Seq = C, D bytes Data Seq = E, F bytes Data Seq = G, H bytes of Data Seq = I, J bytes of Data Seq = K, L bytes of Data P15.6 15.7. Repeat Problem 15.6 given the following data: A = 200, B = 100, C = 300, D = 100, E = 400, F = 100, G = 500, H = 100, I = 600, J = 100 and the lost packet is Seq = G. 15.8. Repeat Problem 15.6 given the following data: A = 100, B = 100, C = 200, D = 100, E = 300, F = 100, G = 400, H = 100, I = 500, J = 100 and the lost packet is Seq = C. 15.9. Repeat Problem 15.6 given the following data: A = 1000, B = 1000, C = 2000, D = 1000, E = 3000, F = 1000, G = 4000, H = 1000, I = 5000, J = 1000 and the lost packets are Seq = C and Seq = G. 15.10. Repeat Problem 15.6 given the following data: A = 100, B = 100, C = 200, D = 100, E = 300, F = 100, G = 400, H = 100, I = 500, J = 100 and the lost packets are Seq = C and Seq = E. 15.11. The detection of both packet loss and errors with TCP is based upon (a) ACK number (b) RTT (c) All of the above (d) None of the above 15.12. The process by which the receiver explicitly lists the segments in a stream that are acknowledged is (a) Cumulative acknowledgment (b) Selective acknowledgement (c) All of the above (d) None of the above 15.13. Packet retransmission with TCP is coupled with (a) Flow control (b) Congestion control (c) All of the above (d) None of the above

15.14. TCP Tahoe, TCP Reno and TCP Vegas are schemes for

- (a) Flow control
- (b) Congestion control
- (c) Packet transmission

15.15. RTT is typically longer than TCP timeout.

- (a) True
- (b) False

15.16. RTO is based upon

- (a) Karn's algorithm
- (b) Jacobson's algorithm
- (c) All of the above
- (d) None of the above

15.17. Jacobson's algorithm specifies the approach for sampling segments in RTO.

- (a) True
- (b) False

15.18. A duplicate ACK results from a lost ACK.

- (a) True
- (b) False

15.19. The size of the sender's sliding window is determined by RevWindow.

- (a) True
- (b) False

15.20. The size of the sender's sliding window is typically very small.

- (a) True
- (b) False

15.21. A duplicate ACK may result from ____ .

- (a) ACK loss
- (b) Data packet loss
- (c) Packet delay
- (d) All of the above

15.22. The sender's sliding window size is a TCP header parameter.

(a) True

(b) False

15.23. The receiver's sliding window contains slots for the following types of data:

- (a) Data received and read by the application layer
- (b) Data gap not yet received
- (c) Data received, but not yet read by the application layer
- (d) (b) and (c)
- (e) All of the above

15.24. If a data segment arrives that does not fit within the sliding window

- (a) It is stored in a buffer awaiting space
- (b) It is discarded
- (c) None of the above 15.25. The delayed ACKs are used by TCP to
 - (a) Increase the sliding window's buffer size
 - (b) Reduce the number of packets in the transmission media
 - (c) None of the above15.26. An ACK is sent for every TCP segment received on a connection. (a) True (b) False 15.27. Lost segments can be detected by duplicate ACKs.
 - (a) True
 - (b) False15.28. In each segment of the TCP header the receiver specifies in the receive window field
 - (a) The amount of data it can buffer for a particular connection
 - (b) The total size of the buffer
 - (c) The size of the window
 - (d) None of the above15.29. The silly window syndrome is characterized by which of the following?
 - (a) The host is unable to process the incoming data fast enough
 - (b) Window size becomes smaller
 - (c) Data transmission becomes extremely inefficient
 - (d) All of the above
 - (e) None of the above15.30. A Telnet session is a good example of high overhead transmission in which the data is small in comparison to the TCP header. (a) True (b) False 15.31. A proposed method for reducing the overhead when sending TCP packets is known as
 - (a) Jacob's algorithm
 - (b) Nagle's algorithm
 - (c) None of the above15.32. Silly windows can be avoided by increasing the receiver's window size which is dependent upon
 - (a) The receiver's buffer size
 - (b) The maximum segment size
 - (c) All of the above
 - (d) None of the above15.33. A

SACK-permitted option can be sent on any packet. (a) True
(b) False 15.34. A SACK-permitted option is enabled by
every OS by default without any negotiation. (a) True (b)
False 15.35. ___ is the choice for handling multiple TCP
segment losses. (a) SACK (b) CACK (c) All of the above
(d) None of the above

16 Chapter 16 - TCP Congestion Control

1. R.T. Braden, RFC 1122: Requirements for Internet Hosts-Communication Layers, October, 1989.
2. M. Allman, V. Paxson, and W. Stevens, RFC 2581: TCP Congestion Control, 1999.
3. M. Duke, R. Braden, W. Eddy, and E. Blanton, RFC 4614: A Roadmap for Transmission Control Protocol (TCP) Specification Documents, 2006.
4. V. Jacobson, "Congestion avoidance and control," ACM SIGCOMM Computer Communication Review, vol. 25, 1995, p. 187.
5. V. Jacobson, "Modified TCP Congestion Avoidance Algorithm";
<ftp://ftp.isi.edu/end2end/end2endinterest-1990.mail>.
6. R.S. Prasad, C. Dovrolis, and M. Thottan, "Router buffer sizing revisited: the role of the output/input capacity ratio," Proceedings of the 2007 ACM CoNEXT conference, 2007, pp. 1-12.
7. N. Beheshti, Y. Ganjali, M. Ghobadi, N. McKeown, and G. Salmon, "Experimental study of router buffer sizing," Proceedings of the 8th ACM SIGCOMM conference on Internet measurement, 2008, pp. 197-210.
8. G. Appenzeller, I. Keslassy, and N. McKeown, "Sizing router buffers," Proceedings of the 2004 conference on applications, technologies, architectures, and protocols for computer communications, 2004, pp. 281-292.
9. J. Sommers, P. Barford, A. Greenberg, and W. Willinger, "An SLA perspective on the router buffer sizing problem," ACM SIGMETRICS Performance Evaluation Review, vol. 35, 2008, pp. 40-51.
10. A. Vishwanath, V. Sivaraman, and M. Thottan, "Perspectives on router buffer sizing: Recent results and open problems," ACM SIGCOMM Computer Communication Review, vol. 39, 2009, pp. 34-39.
11. K. Ramakrishnan, S. Floyd, and D. Black, RFC 3168: The Addition of Explicit Congestion Notification (ECN) to IP, 2001.
12. L. Martini, J. Jayakumar, M. Bocci, N. El-Aawar, J.

Brayley, and G. Koleyni, RFC 4717: Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks, 2006; <http://www.faqs.org/rfcs/rfc4717.html>.

13. J. Hadi Salim and U. Ahmed, RFC 2884: Performance Evaluation of Explicit Congestion Notification (ECN) in IP Networks, 2000.

14. W. Stevens, RFC 2001: TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms, 1997.

15. S. Floyd and T. Henderson, RFC 2582: The NewReno Modification to TCP's Fast Recovery Algorithm, 1999.

16. S. Floyd, T. Henderson, and others, RFC 3782: The NewReno Modification to TCP's Fast Recovery Algorithm, 2004.

17. E. Blanton, M. Allman, K. Fall, and L. Wang, RFC 3517: A conservative selective acknowledgment (SACK)-based loss recovery algorithm for TCP, 2003.

18. S. Floyd, RFC 3649: HighSpeed TCP for Large Congestion Windows, 2003.

19. M. Sridharan, K. Tan, D. Bansal, and D. Thaler, "IETF Draft: Compound TCP: A new TCP congestion control for high-speed and long distance networks," Downloaded from the Internet Sep, vol. 5, 2007.

20. I. Rhee, L. Xu, and S. Ha, IETF Draft: CUBIC for fast long-distance networks, 2007.

21. M. Allman, S. Floyd, and C. Partridge, RFC 3390: Increasing TCP's Initial Window, 2002. 22. N. Dukkipati, T. Refice, Y. Cheng, J. Chu, T. Herbert, A. Agarwal, A. Jain, and N. Sutin, "An argument for increasing TCP's initial congestion window," ACM SIGCOMM Computer Communication Review, vol. 40, 2010, pp. 26-33. 23. K. Fall and S. Floyd, "Simulation-based comparisons of Tahoe, Reno and SACK TCP," ACM SIGCOMM Computer Communication Review, vol. 26, 1996, p. 21. 24. CHEETAH Software, "Welcome to the CHEETAH Home Page"; <http://www.ece.virginia.edu/cheetah/software/software.html>. 25. M. Allman, H. Balakrishnan, and S. Floyd, RFC 3042: Enhancing TCP's Loss Recovery Using Limited Transmit, 2001. 26. M. Nabeshima, "Performance Evaluation of MuTCP in High-Speed Wide Area Networks," IEICE Transactions on Communications, 2005, pp. 392-396.

27. E. de Souza and D. Agarwal, "A HighSpeed TCP study: Characteristics and deployment issues," LBL Technique report, vol. LBNL-53215. 28. S. Floyd, RFC 3742: Limited slow-start for TCP with large congestion windows, 2004.
29. D. Leith and R. Shorten, "H-TCP protocol for high-speed long distance networks," Proc. PFLDnet, 2004. 30. S. Tella, "Performance of Competing High Speed TCP Flows with Background Traffic," 2008; <http://www.cs.odu.edu/~mw/eigle/Main/Students>. 31. Y. Iwanaga, K. Kumazoe, D. Cavendish, M. Tsuru, and Y. Oie, "High-Speed TCP Performance Characterization under Various Operating Systems," The Fifth International Conference on Mobile Computing and Ubiquitous Networking, 2010. 32. Y. Iwanaga, "TCP Performance across various Operating System"; <http://infonet.cse.kyutech.ac.jp/~yoichi/HSTCP/>. 33. P. Yang, W. Luo, L. Xu, J. Deogun, and Y. Lu, "TCP congestion avoidance algorithm identification," Distributed Computing Systems (ICDCS), 2011 31st International Conference on, 2011, pp. 310-321. 34. L.S. Brakmo and L.L. Peterson, "TCP Vegas: End to end congestion avoidance on a global Internet," Selected Areas in Communications, IEEE Journal on, vol. 13, 2002, pp. 1465-1480. 35. D. Hayes and G. Armitage, "Revisiting TCP Congestion Control Using Delay Gradients," NETWORKING 2011, Lecture Notes in Computer Science, vol. 6641, 2011, pp. 328-341. 36. K.T.. Song, M. Sridharan, and C.Y. Ho, "CTCP: Improving TCP-Friendliness Over Low-Buffered Network Links." 37. J. Davies, "The Cable Guy: TCP Receive Window Auto-Tuning"; <http://technet.microsoft.com/en-us/magazine/2007.01.cableguy.aspx>. 38. M. Scharf, S. Floyd, and P. Sarolahti, IETF Draft: Avoiding interactions of Quick-Start TCP and flow control, IETF Internet Draft, work in progress, 2007. 39. S. Floyd, M. Allman, A. Jain, and P. Sarolahti, RFC 4782: Quick-Start for TCP and IP, RFC 4782, January, 2007. 40. "Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2 - Congestion Avoidance Overview [Cisco IOS Software Releases 12.2 Mainline] - Cisco Systems"; http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfconav_ps1835_TSD_Products_Configuration_Guide_Chapter.html.
41. B. Braden, D. Clark, J. Crowcroft, B. Davie, S. Deering, D. Estrin, S. Floyd, V. Jacobson, G. Minshall, C. Partridge, and others, RFC 2309: Recommendations on queue management and congestion avoidance in the internet, 1998.
42. K. Chan, J. Babiarz, and F. Baker, RFC 5127: Aggregation of DiffServ Service Classes, 2007. 43. R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, RFC 2205: Resource ReSerVation Protocol (RSVP) Version 1 Functional Specification, 1997. 44. T. FERRARI, "Throughput comparison of TCP streams with TWO points of

- congestion"; <http://www.cnaf.infn.it/~ferrari/tfnngn/tcp/ecn/testWan/testC-tcp-RR/>. 45. M. Alizadeh, A. Greenberg, D.A. Maltz, J. Padhye, P. Patel, B. Prabhakar, S. Sengupta, and M. Sridharan, "Data center tcp (dctcp)," Proceedings of the ACM SIGCOMM 2010 conference on SIGCOMM, 2010, pp. 63-74. 46. M. Alizadeh, A. Javanmard, and B. Prabhakar, "Analysis of DCTCP: stability, convergence, and fairness," Proceedings of the ACM SIGMETRICS joint international conference on Measurement and modeling of computer systems, 2011, pp. 73-84. 47. S. Floyd and J. Kempf, RFC 3714: IAB Concerns Regarding Congestion Control for Voice Traffic in the Internet, 2004. 48. S. Floyd, RFC 2914: Congestion Control Principles, 2000. 49. S. Floyd and M. Allman, RFC 5290: Comments on the Usefulness of Simple Best-Effort Traffic, 2003; <http://tools.ietf.org/html/rfc5290>. 50. S. Ha, I. Rhee, and L. Xu, "CUBIC: A new TCP-friendly high-speed TCP variant," ACM SIGOPS Operating Systems Review, vol. 42, 2008, pp. 64-74.
51. K. Munir, M. Welzl, and D. Damjanovic, "Linux beats windows!-or the worrying evolution of TCP in common operating systems," PFLDnet Workshop, 2007.
52. I. Abdeljaouad, H. Rachidi, S. Fernandes, and A. Karmouch, "Performance analysis of modern TCP variants: A comparison of Cubic, Compound and New Reno," Communications (QBSC), 2010 25th Biennial Symposium on, pp. 80-83.
53. L.A. Dalton and C. Isen, "A study on high speed TCP protocols," Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE, 2004, pp. 851-855 Vol.2.
54. S. Ha, Y. Kim, L. Le, I. Rhee, and L. Xu, "A step toward realistic performance evaluation of high-speed TCP variants," Fourth International Workshop on Protocols for Fast Long-Distance Networks (PFLDNet06), 2006.
55. D. Miras, M. Bateman, and S. Bhatti, "Fairness of High-Speed TCP Stacks," Advanced Information Networking and Applications, 2008. AINA 2008. 22nd International Conference on, 2008, pp. 84-92.
56. N. Spring, D. Wetherall, and D. Ely, RFC 3540: Robust explicit congestion notification (ECN) signaling with nonces, 2003.

CHAPTER 16 PROBLEMS

- 16.1. Compare the differences between TCP NewReno in RFC 3782 and Limited Transmit in RFC 3042 in terms of their

application scenarios.

16.2. Explain why TCP NewReno cannot be scaled to gigabit networks.

16.3. Explain how to reduce the large transient queue size present during slow-start in order to reduce the chance of congestion in gigabit networks.

16.4. Under the assumption that when the 3rd duplicate ACK is received, the Fast Retransmit is performed by TCP, and the Fast Recovery operates with CWND = 96 MSS and RevWindow = 128, determine the new ssthresh and CWND using RFC 2001.

16.5. Under the assumption that when the 3rd duplicate ACK is received, the Fast Retransmit is performed by TCP, and the Fast Recovery operates with CWND = 256 MSS and RevWindow = 128, determine the new ssthresh and CWND using RFC 2001.

16.6. Under the assumption that when the 3rd duplicate ACK is received, the Fast Retransmit is performed by TCP, and the Fast Recovery operates with CWND = 96 MSS and FlightSize = 128 * MSS, determine the new ssthresh and CWND using RFC 2581.

16.7. Under the assumption that when the 3rd duplicate ACK is received, the Fast Retransmit is performed by TCP, and the Fast Recovery operates with CWND = 256 MSS and FlightSize = 320 * MSS, determine the new ssthresh and CWND using RFC 2581.

16.8. Assume that TCP NewReno performs the Fast Recovery with CWND = 256 MSS and FlightSize = 320 * MSS, and when the full ACK is received, the CWND = 170 MSS and FlightSize = 200 * MSS. Given this information, determine the new ssthresh and CWND = min(ssthresh, FlightSize + MSS) using NewReno in RFC 3782.

16.9. Assume that the TCP NewReno conducts the Fast Recovery as the CWND = 256 MSS and FlightSize = 320 * MSS, and when the full ACK is received, the CWND = 170 MSS and FlightSize = 100 * MSS. Given this information, determine the new ssthresh and CWND using NewReno in RFC 3782.

16.10. When $w = 84035$ or $CWND = 84035 * MSS = 122691100$ bytes, then $a(w) = 71$ and $b(w) = 0.1$ according to RFC 3649. Find the rate of increase for w per RTT and the rate of decrease for w per RTT.

16.11. When $w = 84035$ or

CWND = 84035 * MSS = 122,691,100 bytes, find the rate of increase for w per RTT and the rate of decrease for w per RTT using TCP Reno in slow start. 16.12. Assume that you are a network administrator for a company that uses leased lines (WAN) to connect multiple sites. Which ACK protocol should you choose to use for the client computers and servers for the best congestion control in WAN? 16.13. TCP flow control advertises RevWindow by the receiver to prevent buffer overflow. (a) True (b) False 16.14. With TCP flow control, the buffer at the receiver consists of two parts, one of which is the data read by the application layer. (a) True (b) False 16.15. By its very nature, flow control and congestion control are one in the same. (a) True (b) False 16.16. Which of the following represent an approach to congestion control? (a) Network-assisted (b) End-to-end (c) All of the above (d) None of the above 16.17. The two approaches to congestion control are separate and never employed together. (a) True (b) False 16.18. ATM congestion control is solely for ABR. (a) True (b) False 16.19. ATM congestion control provides ABR with the capability to fully utilize available ATM resources. (a) True (b) False 16.20. The ER is indicated by a two-byte ER field in the ABR data cell. (a) True (b) False 16.21. Timeouts and three duplicate ACKs are events that will prompt TCP end-to-end congestion control. (a) True (b) False 16.22. In TCP end-to-end congestion control, the CWND used by the sender is governed by which of the following mechanisms? (a) AIMD (b) Conservative after timeout events (c) Slow start (d) All of the above (e) None of the above

16.23. In TCP end-to-end congestion control, MSS negotiation is a process used to determine the minimum payload size.

- (a) True
- (b) False

16.24. The exponential rate employed in Slow Start continues until the first indication of a loss event occurs.

- (a) True
- (b) False

16.25. The receiver's advertised window size is a fundamental parameter in the achievement of TCP flow control.

(a) True

(b) False

16.26. An effective parameter that comes into play when congestion occurs is CWND.

(a) True

(b) False

16.27. Only a lost or delayed segment in TCP results in a duplicate ACK.

(a) True

(b) False

16.28. In the AIMD operation, additive increase is accomplished by doubling MSS every RTT until a loss occurs.

(a) True

(b) False

16.29. In the AIMD operation, multiplicative decrease is accomplished by cutting CWND in half after a loss.

(a) True

(b) False

16.30. With the use of Jacobson's algorithm, TCP Tahoe is more efficient than TCP Reno.

(a) True

(b) False

16.31. The number of steps employed in the fast recovery phase of TCP Reno is

(a) 2

(b) 3

(c) 4

16.32. In the TCP Reno fast recovery phase, CWND can be used in place of FlightSize.

(a) True

(b) False

16.33. TCP NewReno, defined by RFC 3782, is the most widely used TCP congestion control implementation.

(a) True

(b) False

16.34. TCP Reno enters the congestion avoidance state when a full ACK is received.

(a) True

(b) False 16.35. The TCP packet format contains a number of items. One of the items is ToS. (a) True (b) False

16.36. Successful completion of the ECN 3-way handshake between two hosts ensures that they are capable of participating as ECN endpoints. (a) True (b) False

16.37. WRED works in conjunction with IP-precedence to provide higher priority packets with preferential traffic handling. (a) True (b) False 16.38. Marking traffic for levels of priority is performed only by the originating equipment. (a) True (b) False 16.39. When a transmitting interface becomes congested or full and traffic is placed in a queue, the traffic that is given highest priority to be transmitted is video instead of voice. (a) True (b)

False 16.40. For TCP connections with large congestion windows, the use of limited slow-start represents a viable enhancement to HSTCP. (a) True (b) False 16.41. WRED is designed to ___ lower priority packets at the onset of congestion. (a) Mark (b) Discard (c) All of the above (d) None of the above 16.42. The HSTCP performs better than TCP Reno when the data rate of the link is low. (a) True (b) False Cybersecurity 5

17 Chapter 17 - Cybersecurity Overview

1. Nsslabs.com, "Vulnerability-based protection and Operation Aurora," 2010; <http://nsslabs.com/anti-malware>.
2. NIST, SP 800-53 Rev. 3: Recommended Security Controls for Federal Information Systems and Organizations, 2010; <http://csrc.nist.gov/publications/PubsSPs.html>.
3. M. Fossi, D. Turner, E. Johnson, T. Mark, J. Blackbird, S. Entwise, Graveland, D. McKinney, J. Mulcahy, and C. Rueest, Symantec Global Internet Security Threat Report-Trends for 2009, Technical Report XV, Symantec Corporation, 2010.
4. "PandaLabs Annual Malware Report 2009"; <http://www.pandasecurity.com/homeusers/security-info/tools/reports/>.
5. McAfee @ Labs, "McAfee Threats Report: Third Quarter 2010," 2010; http://www.mcafee.com/us/local_content/reports/q32010_threats_report_en.pdf.
6. M. Fossi, T. Mark, D. Turner, D. Mazurek, G. Egan, T. Adams, D. McKinney, K. Haley, J. Blackbird, P. Wood, E. Johnson, and M. Low, Symantec Internet Security Threat Report-Trends for 2010, Technical Report XVI, Symantec Corporation, 2011.
7. D. Turner, M. Fossi, E. Johnson, T. Mark, J. Blackbird, S. Entwise, M.K. Low, D. McKinney, and C. Rueest, Symantec Global Internet Security Threat Report-Trends for 2008, Technical Report XIV, Symantec Corporation, 2009.
8. Trend Micro, "Trend Micro 2008 Annual Threat Roundup and 2009 Forecast"; <http://us.trendmicro.com/us/threats/enterprise/security-library/threat-reports/>.
9. "MessageLabs Intelligence: 2008 Annual Security Report"; <http://www.message-labs.com/resources/mlireports>.
10. "MessageLabs Intelligence: 2009 Annual Security Report"; <http://www.message-labs.com/resources/mlireports>.
11. Blue Coat Systems, "Blue Coat Publishes Annual Web Security Report"; <http://www.bluecoat.com/news/pr/4372>.
12. "Cisco 2009 Annual Security Report - Cisco Systems"; http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html.

13. "Microsoft Security Intelligence Report - SIR Volume 8 (July 2009 through December 2009)"; <http://www.microsoft.com/security/portal/Threat/SIR.aspx>.
14. IBM Security Solutions, X-Force 2009 Trend and Risk Report: Annual Review of 2009; <http://www-935.ibm.com/services/us/iss/xforce/trendreports/>.
15. P. Porras, H. Saidi, and V. Yegneswaran, "An Analysis of Conficker's Logic and Rendezvous Points"; <http://mtc.sri.com/Conficker/>.
16. "US Air Force phishing test transforms into a problem"; <http://www.networkworld.com/news/2010/043010-us-air-force-phishing-test.html>.
17. S.P. Correll, "U.S. Treasury Website Hacked Using Exploit Kit | PandaLabs Blog," 2010;
47. F. Leder, B. Steinbock, and P. Martini, "Classification and Detection of Metamorphic Malware using Value Set Analysis";
48. J. Newsome, B. Karp, and D. Song, "Polygraph: Automatically generating signatures for polymorphic worms," Proceedings of the IEEE Symposium on Security and Privacy, 2005, pp. 226-241.
49. A.E. Stepan, "Defeating polymorphism: Beyond emulation," Proceedings of the Virus Bulletin International Conference, 2005.
50. "Dark Paranoid | ESET Threat Encyclopedia"; <http://www.eset.com/threat-center/encyclopedia/threats/darkparanoid>.
51. M. Stamp and W. Wong, "Hunting for metamorphic engines," Journal in Computer Virology, vol. 2, 2006.
52. P. Ször and P. Ferrie, "Hunting for metamorphic," VIRUS, vol. 123, 2001.
53. M. Christodorescu and S. Jha, "Static analysis of executables to detect malicious patterns," Proceedings of the 12th conference on USENIX Security Symposium-Volume 12, 2003, p. 12.
54. M. Schiffman, "A Brief History of Malware Obfuscation: Part 1 of 2 - Security"; <http://blogs.cisco.com/>

55. P. Szor, "Symantec Security Response - W32.Bolzano";
<http://service1.symantec.com/sarc/sarc.nsf/html/W32.Bolzano.html>.
56. "Virus Construction Tools - Overwriting Virus Construction Toolkit (VX heavens)"; <http://vx.netlux.org/vx.php?id=t000>.
57. "Virus Construction Tools - Next Generation Virus Construction Kit (VX heavens)"; <http://vx.netlux.org/vx.php?id=tn02>.
58. "Virus Construction Tools - G2 Virus Generator (VX heavens)"; <http://vx.netlux.org/vx.php?id=tg00>.
59. "Virus Construction Tools - Phalcon/Skism Mass-Produced Code Generator (VX heavens)"; <http://vx.netlux.org/vx.php?id=tp00>.
60. "An Analysis of Simile";
<http://www.securityfocus.com/infocus/1671>.
61. P. Szor, The art of computer virus research and defense, Addison-Wesley Professional, 2005.
62. G. Tenebro, "W32.Waledac Threat Analysis," 2009;
<http://www.google.com/url?sa=t&source=web&ct=res&cd=2&ved=0CA0QFjAB&url=http%3A%2F%2Fwww.symantec.com%2Fcontent%2Fen%2F>
63. Bkis - Internet Security, "Metamorphic virus - challenges to antivirus software"; http://www.bkis.com/top_news/23/01/2010/17/755/.
64. D. Spinellis, "Reliable identification of bounded-length viruses is NP-complete," IEEE Transactions on Information Theory, vol. 49, 2003, pp. 280-284.
65. G. Jacob, H. Debar, and E. Filiol, "Behavioral detection of malware: from a survey towards an established taxonomy," Journal in computer Virology, vol. 4, 2008, pp. 251-266.
66. Y. Ye, D. Wang, T. Li, D. Ye, and Q. Jiang, "An intelligent PE-malware detection system based on association mining," Journal in Computer Virology, vol. 4, 2008, pp. 323-334.
67. J. Xue, C. Hu, K. Wang, R. Ma, and J. Zou, "Metamorphic

malware detection technology based on aggregating emerging patterns," Proceedings of the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, 2009, pp. 1293-1296.

68. M. Christodorescu, S. Jha, J. Kinder, S. Katzenbeisser, and H. Veith, "Software transformations to improve malware detection," Journal in Computer Virology, vol. 3, 2007, pp. 253-265.

69. M.D. Preda, M. Christodorescu, S. Jha, and S. Debray, "A semantics-based approach to malware detection," ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 30, 2008, p. 25.

70. S. Treadwell and M. Zhou, "A heuristic approach for detection of obfuscated malware," Proceedings of the 2009 IEEE international conference on Intelligence and security informatics, 2009, pp. 291-299.

71. J.R. Crandall, Z. Su, S.F. Wu, and F.T. Chong, "On deriving unknown vulnerabilities from zero-day polymorphic and metamorphic worm exploits," Proceedings of the 12th ACM conference on Computer and communications security, 2005, p. 248.

72. P. Vinod, V. Laxmi, M.S. Gaur, G.P. Kumar, and Y.S. Chundawat, "Static CFG analyzer for metamorphic Malware code," Proceedings of the 2nd international conference on Security of information and networks, 2009, pp. 225-228.

73. J.M. Borello, É. Filiol, and L. Mé, "Are current antivirus programs able to detect complex metamorphic malware? An empirical evaluation."

74. Consumer Reports, "U.S. consumers lose more than \$7 billion on on-line threats";

75. Trend Micro, "Trend Micro Threat Roundup and Forecast-1H 2008"; <http://us.trendmicro.com/us/threats/enterprise/security-library/threat-reports/>.

76. V. Martinez, PandaLabs Report: Mpack uncovered, 00, 2007. 77. Trend Micro, "Trend Micro 2009's Most Persistent Malware Threats";

17.9. Describe how to assess and mitigate the risks associated with deploying enterprise patch management tools.

17.10. Describe how to consistently measure the effectiveness of the patch and vulnerability management program and apply corrective actions as necessary.

17.11. Describe how to ensure the availability objective for security in information systems.

17.12. Describe the important types of cyber incidents in information systems.

17.13. Describe techniques that can be applied to reduce the frequency of cyber incidents.

17.14. The security property that indicates that only the receiver or sender is able to understand the contents of a message is called

- (a) Authentication
- (b) Confidentiality
- (c) Integrity

17.15. The assurance that information is not altered by elements along the communication path is known as

- (a) Authentication
- (b) Accountability
- (c) Integrity
- (d) Confidentiality

17.16. Eavesdropping and packet sniffing are considered to be attacks on

- (a) Authentication
- (b) Confidentiality
- (c) Integrity

17.17. Identity theft and password cracking are considered to be attacks on

- (a) Authentication
- (b) Confidentiality

(c) Integrity

17.18. Attacks that disrupt or block availability are known as

(a) DNS attacks

(b) DDoS attacks

(c) None of the above

17.19. A heap spray is an example of a specially crafted code that is injected at a predetermined location in the memory of a target to gain privileged rights in order to access a host or data.

(a) True

(b) False

17.20. The heap spray technique is not effective against browsers.

(a) True

(b) False

17.21. SSL is vulnerable to a man-in-the-middle attack.

(a) True

(b) False 17.22. The average lifespan of a malware continues to increase. (a) True (b) False 17.23.

Vulnerabilities in software are the primary cause of the threats and security issues that come with social media.

(a) True (b) False 17.24. Worms are more common in home computers and Trojans are more common in the enterprise environment. (a) True (b) False 17.25. Which of the following are propagation mechanisms for worms? (a) P2P

(b) Email (c) File sharing (d) Buffer overflow (e) All of the above (f) None of the above 17.26. The method used by the Conficker worm to ensure that other groups could not upload codes to their infected computers was encryption and authentication. (a) True (b) False 17.27. The Conficker worm is considered to be a polymorphic virus. (a) True

(b) False 17.28. Conficker is unusual in that it is worm as well as a rootkit. (a) True (b) False 17.29. The latest advances in malware possess which of the following characteristics? (a) The malware can propagate itself (b) The malware can defend itself (c) The malware can update

itself (d) All of the above (e) None of the above 17.30. When an identity thief tricks an individual into divulging personal information, the attack is called (a) Worm (b) Phishing (c) Trojan horse 17.31. When an individual is under a personal phishing attack, the attack is called (a) Smishing (b) Spear phishing (c) Vishing (d) None of the above 17.32. The phrase coined to represent voice and phishing scams is “vishing.” (a) True (b) False

17.33. Which of the following are considered to be types of phishing toolkits?

- (a) Domain-based
- (b) Replacement-based
- (c) All of the above

17.34. The term “backdoor” is used to represent a secret entry point into a program that provides illegal access.

- (a) True
- (b) False

17.35. The Trojan that becomes an integral part of the web browser using HTML injection is the

- (a) Sinowal/Mebroot/Torpig
- (b) Limbo
- (c) Zeus

17.36. The Trojan that infects a PC’s master boot record in the first sector of the hard drive is the

- (a) Sinowal/Mebroot/Torpig
- (b) Limbo
- (c) Zeus

17.37. A group of computers that are configured to operate upon a given set of instructions are known as a botnet.

- (a) True
- (b) False

17.38. A public protocol for real-time Internet text messaging is

- (a) RTITM
- (b) IRC
- (c) C&C
- (d) None of the above

17.39. A move to IRC Bot C&C communication frameworks is making botnets more difficult to detect and disable.

- (a) True
- (b) False

17.40. The Rock Phish Toolkit employs the fast-flux technology.

- (a) True
- (b) False

17.41. Botmasters that use Conficker have their own federation known as Confickerworkinggroup.org.

- (a) True
- (b) False

17.42. The Conficker.C, .D and .E worms use P2P and HTTP-based networking.

- (a) True
- (b) False

17.43. Zbot is another name for the Zeus Trojan.

- (a) True
 - (b) False
- 17.44. Although the Zeus Trojan is a menace in many ways, its primary function is that of stealing online credentials.
- (a) True
 - (b) False
- 17.45. The first major botnet to exploit a PDF's launch feature was
- (a) Sinowal/Mebroot/Torpig
 - (b) Limbo
 - (c) Zeus
 - (d) None of the above
- 17.46. The most popular location for hiding rootkit files on Windows machines is in the.exe files.

(a) True (b) False 17.47. Rootkits log in with a ____ .
(a) Stolen password (b) Dictionary attack (c) All of the above (d) None of the above 17.48. The typical infection path employed by a rootkit is (a) The web (b) Clickjacking (c) All of the above (d) None of the above
17.49. The different types of rootkits include the following (a) User-mode (b) Robust-mode (c) Reliable-mode (d) Kernel-mode (e) (a) and (d) (f) (b) and (c) 17.50. The rootkit that installs itself on the first sector of the user's hard drive and then modifies other sectors is the ____ mode. (a) Sniffer (b) MBR (c) None of the above 17.51. Modification of the Windows OS kernel is the most popular mechanism by which a rootkit becomes active and starts hiding on a computer. (a) True (b) False 17.52. Once a hacker installs a MBR rootkit on a machine, the hacker has complete control of the machine.
(a) True (b) False 17.53. A computer virus carries with it the recipe for its replication. (a) True (b) False

17.54. Trojan horses, viruses and rootkits are examples of malicious programs that

- (a) Propagate independently
- (b) Require a host program
- (c) None of the above

17.55. Worms and Zombies are examples of malicious programs that

- (a) Propagate independently
- (b) Require a host program
- (c) None of the above

17.56. Malware propagation mechanisms include

- (a) SQL injection
- (b) Buffer overflow
- (c) All of the above
- (d) None of the above

17.57. When malware is hidden within a program or command, it is typically known as a

- (a) Phisher
- (b) Trojan horse
- (c) None of the above

17.58. A typical Trojan mechanism is to substitute a phishing site for the original site that the program addresses.

- (a) True
- (b) False

17.59. Zombies are normally controlled by Botnets.

- (a) True
- (b) False

17.60. The fast flux switching mechanism combines the following:

- (a) Distributed command and control
- (b) P2P networking
- (c) Proxy redirection
- (d) Web-based load balancing
- (e) All of the above
- (f) (a) and (d)
- (g) (b) and (c)
- (h) None of the above

17.61. Mutation is commonly employed in macro and script malware.

- (a) True
- (b) False

17.62. Executable packing is not a viable approach in preventing reverse engineering.

- (a) True

(b) False

17.63. UPX is a free, open-source executable packer.

(a) True

(b) False

17.64. A RVA is used to specify many of the fields in PE files.

(a) True

(b) False 17.65. A common approach used in metamorphic malware is the insertion of junk instructions. (a) True
(b) False 17.66. The Conficker worm is metamorphic. (a) True
(b) False 17.67. In order to hinder binary detection, the Conficker.C uses (a) Code obfuscation
(b) Encryption (c) Packing (d) All of the above (e) None of the above 17.68. The use of a decryptor facilitates the detection of (a) Metamorphic malware (b) Polymorphic malware (c) All of the above 17.69. Code emulation is a technique for decrypting (a) Metamorphic malware (b) Polymorphic malware 17.70. The heuristic-based methods used to detect polymorphic malware may be either static or dynamic. (a) True (b) False 17.71. An algorithm that automatically generates signatures for polymorphic worms is known as Polyplot. (a) True (b) False 17.72. Dynamic Translation is a procedure proposed by Microsoft to speed up the decryption of metamorphic malware. (a) True (b) False 17.73. Metamorphic malware can automatically recode itself each time it propagates to a new host. (a) True
(b) False 17.74. It is easier to detect a polymorphic virus than an encrypted virus. (a) True (b) False 17.75. Bad metamorphic software is capable of avoiding malware signature detection. (a) True (b) False 17.76. The compiler is the mechanism used to mutate the body of the virus by metamorphism. (a) True (b) False

17.77. Both polymorphic and metamorphic malware can be created using a number of toolkits.

(a) True

(b) False

17.78. There are no examples of a virus that is both polymorphic and metamorphic.

(a) True

(b) False

17.79. W32.Evol was the first malware that used a 32-bit polymorphic engine.

(a) True

(b) False

17.80. As a general rule, the more packers employed with malware, the more difficult it is to analyze and detect it.

(a) True

(b) False

17.81. In spite of the use of encryption, a Trojan is available that is capable of eavesdropping on conversations made with Skype.

(a) True

(b) False

17.82. Syntactic analysis is no longer an effective tool against metamorphic malware.

(a) True

(b) False

17.83. The mutated replication of a known malware can be detected by most of the antimalware products.

(a) True

(b) False

17.84. The modern cyber criminals that employ malware are focused primarily on profits.

(a) True

(b) False

17.85. The most sought-after malware for sale in the underground economy is that used to obtain the following

information:

- (a) Bank account credentials
- (b) Credit card information
- (c) Email accounts

17.86. Although phishing activity impacts a number of sectors including retail, insurance, etc., the largest sector by far is the financial sector.

- (a) True
- (b) False

17.87. The tools used for automated web-based attacks include:

- (a) Icepack
- (b) Hotpack
- (c) Firepack
- (d) (a) and (b)
- (e) (a) and (c)
- (f) None of the above 17.88. Mpack is a automated system for web-based attacks. (a) True (b) False 17.89. From a browser perspective, malicious PDFs and Active X vulnerabilities have overshadowed core browser vulnerabilities. (a) True (b) False 17.90. Vulnerabilities that are not known prior to exploitation and have no known patch are called zero-day vulnerabilities. (a) True (b) False 17.91. Buffer overflows are a serious security issue of some software. (a) True (b) False 17.92. Kerberos is an excellent method for (a) Confidentiality (b) Authentication (c) Integrity (d) None of the above 17.93. A set of policies used to protect the information infrastructure can be employed by NAC. (a) True (b) False 17.94. An enterprise network that employs a firewall and IDS/IPS does permit a VPN through the firewall. (a) True (b) False 17.95. Web/transport layer security can be provided by SSL/TLS. (a) True (b) False 17.96. The deep packet inspection provided by Secure Content (SC) filtering employs which of the following? (a) Anti-malware (b) Anti-spam (c) URL filtering (d) Packet content filtering (e) All of the

above 17.97. The guidelines for a penetration test that evaluates the security of an enterprise network and hosts have been published by the U.S. Government. (a) True (b) False 17.98. One of the popular tools for penetration testing is Wireshark that provides a technique for scanning open services and vulnerabilities. (a) True (b) False

17.99. Signature-based techniques will detect zero-day attacks.

(a) True

(b) False

17.100. The Einstein program is a worldwide program for sharing intelligence about cyber attacks.

(a) True

(b) False

17.101. Intrusion detection systems can be classified as

(a) Signature-based

(b) Behavior-based

(c) All of the above

(d) None of the above

17.102. The protection mechanism that involves encryption for confidentiality and hash for authentication is

(a) Public key crypto

(b) Symmetric key crypto

(c) All of the above

(d) None of the above

17.103. IDS/IPS plays a significant role in perimeter protection.

(a) True

(b) False

18 Chapter 18 - Firewalls

1. R. Oppliger, "Internet security: firewalls and beyond," 1997.
2. Y.D. Lin, H.Y. Wei, S.T. Yu, and others, "Building an Integrated Security Gateway: Mechanisms, Performance Evaluations, Implementations, AND Research Issues," Nation Chiao Tung University, IEEE Communication Surveys, 2002.
3. "Ubiq-Freedom: 3 steps to Free UTM based Internet Security"; <https://free-utm.com/web/guest/;jsessionid=AAF5EB6319D6BBBB2973CDA1CF4A4D2AC>.
4. Imperva, "Web Application Firewall"; <http://www.imperva.com/products/web-application-firewall.html>.
5. H. Kitamura, A. Jinzaki, and S. Kobayashi, RFC 3089: A SOCKS-based IPv6/IPv4 gateway mechanism, 2001.
6. NIST, SP 800-41 Rev. 1: Guidelines on Firewalls and Firewall Policy, 2009; <http://csrc.nist.gov/publications/PubsSPs.html>.
7. Cisco Systems, "Configuring IP Access Lists"; http://www.cisco.com/en/US/products/sw/secumgrsw/ps1018/products_tech_note09186a00800_a5b9a.shtml.
8. R. Zalenski, "Firewall technologies," IEEE potentials, vol. 21, 2002, pp. 24-29.
9. M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, and L. Jones, RFC 1928: SOCKS protocol version 5, 1996.
10. M. Leech, RFC 1929: Username/password authentication for SOCKS V5, 1996.
11. N. Ayuso and others, "Demystifying Cluster-Based Fault-Tolerant Firewalls," IEEE Internet Computing, vol. 13, 2009, pp. 31-38.
12. T. Li, B. Cole, P. Morton, and D. Li, RFC 2281: Cisco Hot Standby Router Protocol (HSRP), 1998.
13. R. Hinden, RFC 3768: Virtual Router Redundancy Protocol, 2004.
14. "List of TCP and UDP port numbers - Wikipedia, the free encyclopedia"; <http://en.wikipedia.org/wiki/>

List_of_TCP_and_UDP_port_numbers.

15. J. Postel and J.K. Reynolds, RFC 1700: Assigned Numbers, 1994.
16. "SANS: Intrusion Detection FAQ: I am seeing odd ICMP traffic, what could this mean?"; <http://www.sans.org/security-resources/idfaq/traffic.php>.
17. Palo Alto Networks, "Single Pass Parallel Processing (SP3) Architecture"; <http://www.paloaltonetworks.com/technology/platform.html>.
18. Savant, "Application Whitelisting Prevents Spyware, Trojans, Malware, Bots"; <http://www.savantprotection.com/solutions.html>.
19. Bit9, "Secure Endpoints with Bit9"; <http://www.bit9.com/solutions/security/index.php>.
20. Playbook, "Flint is firewall checkup"; <http://runplaybook.com/p/11>.

CHAPTER 18 PROBLEMS

- 18.1. Describe the manner in which an organization develops a firewall policy that defines how their firewalls should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the organization's information security policies.
- 18.2. Identify all deployment requirements that should be considered when determining the locations and features of firewalls.
- 18.3. Describe the important practices required in maintaining the effectiveness of a firewall.
- 18.4. Use a network diagram to illustrate the manner in which to use a HTTP proxy to protect outbound HTTP requests from internal hosts.
- 18.5. Describe the manner in which to inspect packets at a border firewall for VPNs.
- 18.6. Describe the manner in which to use a personal firewall to protect a computer based on location and applications.
- 18.7. Describe the limitations of firewall inspection.
- 18.8. Describe the types of traffic an organization must block using a network layer header to protect its internal routers and network performance.
- 18.9. Write a packet filtering rule to allow the mail delivered from outside of 131.204.0.0/16 to the mail server 131.204.128.3. interface Ethernet 0/1 ip address 131.204.1.1 255.255.255.0 ip access-group 101 in access-list 101 permit tcp _____ host

_____ 18.10. Write a packet filtering rule to allow users of 131.204.0.0/16 to use IMAP from outside to read emails in the inboxes of mail server 131.204.128.3.
interface Ethernet 0/1 ip address 131.204.1.1 255.255.255.0
ip access-group 101 in access-list 101 permit tcp _____
host _____ 18.11. Write a packet filtering rule to allow the hosts in 131.204.0.0/16, i.e., the internal network, to use a mail agent to deliver the mail to mail server 131.204.128.3. interface Ethernet 0/1 ip address 131.204.1.1 255.255.255.0 ip access-group 101 in access-list 101 permit tcp _____ host _____
18.12. Write a packet filtering rule that will block the hosts in 131.204.0.0/16, i.e., the internal network, with the exception of mail server 131.204.128.3, from delivering the mail to outside mail servers. interface Ethernet 0/1 ip address 131.204.1.1 255.255.255.0 ip access-group 101 out access-list 101 permit tcp _____ any _____
access-list 101 deny tcp _____ any _____
18.13. Firewalls block traffic between the internal network and the (a) Internet (b) DMZ (c) All of the above
18.14. VPN traffic is allowed through the firewall. (a) True (b) False

18.15. A firewall passes or blocks traffic based upon

- (a) IP address
- (b) Port number
- (c) All of the above
- (d) None of the above

18.16. A firewall is typically located at only one position in an organization.

- (a) True
- (b) False

18.17. Packet filtering firewalls provide

- (a) Stateless inspection
- (b) Stateful inspection
- (c) All of the above
- (d) None of the above

18.18. A proxy gateway operates at only the application level.

(a) True

(b) False

18.19. Stateless packet filtering is performed on a per-packet basis.

(a) True

(b) False

18.20. In stateless packet filtering, the context of the packet is examined.

(a) True

(b) False

18.21. Packet filters are effective in preventing application-specific attacks, such as SQL injection.

(a) True

(b) False

18.22. The TCP port numbers greater than 1024 are used for servers with TCP connections in a stateless packet filtering environment.

(a) True

(b) False

18.23. In a stateful filtering environment, filters can be bypassed with VPN using IP tunneling.

(a) True

(b) False

18.24. SOCKS is a ____ .

(a) Application-level gateway

(b) Circuit-level gateway

(c) Internet protocol

(d) None of the above

18.25. SOCKS performs at the ___ layer of the OSI model and below.

(a) Application

(b) Presentation

(c) Session

(d) Transport

(e) Network 18.26. It is easy to track the state of ___ in a stateful packet filter. (a) TCP (b) UDP (c) ICMP (d) All of the above 18.27. Firewalls do not always provide protection against the following attacks: (a) Buffer overflows (b) SQL injection (c) DoS (d) All of the above

(e) None of the above 18.28. The Windows 7/Vista firewall supports filtering only for incoming traffic. (a) True (b) False 18.29. The Windows 7/Vista firewall has the following profiles: (a) Public network (b) Private network (c) Domain network (d) (a) and (b) (e) All of the above (f) None of the above 18.30. Egress filtering is an effective tool in preventing leaks from a network to the Internet. (a) True (b) False 18.31. NATs are effective devices in preventing leaks of internal network IP addresses to the Internet. (a) True (b) False

18.32. Egress filtering must ensure that outbound traffic to the Internet has a legal IP address. (a) True (b) False 18.33. An effective tool used by an attacker to move their toolkit onto the system is (a) TFTP (b) FTP (c) ICMP (d) All of the above 18.34. Tool(s) that can be used by an attacker to reveal critical information about the infrastructure is (are) (a) SNMP (b) TFTP (c) SYSLOG (d) All of the above (e) None of the above

18.35. Echo-reply packets received in response to echo-request packets indicate that someone is ___ .

(a) Using the Whois service

(b) Using a ping utility

(c) Surveying the network

(d) None of the above

18.36. An attacker can be prevented from learning a network

by blocking ICMP host unreachables at the firewall.

(a) True

(b) False

18.37. Filtering outbound time-exceeded-in-transit errors is an effective tool in preventing reconnaissance.

(a) True

(b) False

18.38. A reasonable approach to security for home networks involves

(a) Closing all incoming ports

(b) Open only outbound ports 53, 80 and 443

(c) All of the above

18.39. If SMTP and IMAP are used in a home network, then outbound ports 25 and 143 must be open.

(a) True

(b) False

18.40. A typical firewall has the following interfaces:

(a) Outside

(b) Inside

(c) DMZ

(d) All of the above

18.41. The security rules for protecting a small or home office that provides HTTP and HTTPS services include:

(a) Allow all outgoing packets

(b) Deny all incoming packets with the exception of HTTP and HTTPS

(c) All of the above

(d) None of the above

18.42. The ___ firewall can block malicious packets that contain JavaScripts.

- (a) Application-level gateway
- (b) Circuit-level gateway
- (c) Packet filter
- (d) None of the above

18.43. The ___ firewall requires the most computation.

- (a) Application-level gateway
- (b) Circuit-level gateway
- (c) Packet filter

(d) None of the above 18.44. The ___ firewall must have a module for each application protocol. For example, a FTP module is needed for protecting a FTP server. (a)

Application-level gateway (b) Circuit-level gateway (c)

Packet filter (d) None of the above 18.45. The ___

firewall can support all applications based on TCP, UDP and ICMP. (a) Application-level gateway (b) Circuit-level

gateway (c) Packet filter (d) None of the above 18.46.

The ___ firewall can provide optimal security and performance. (a) Application-level gateway (b)

Circuit-level gateway (c) Packet filter (d) Hybrid

firewall (e) None of the above 18.47. The ___ firewall

can provide uninterruptable operation even when a hardware failure occurs. (a) Application-level gateway (b)

primary-backup (c) Circuit-level gateway (d) Packet

filter (e) None of the above 18.48. The ___

representation is used by a firewall to represent a subnet.

(a) IP addresses (b) MAC addresses (c) Subnet mask (d)

CIDR (e) None of the above

19 Chapter 19 - Intrusion Detection/Prevention System

9. "Cisco Adaptive Wireless Intrusion Prevention Service Configuration Guide, Release 5.2 - wIPS Policy Alarm Encyclopedia [Cisco Adaptive Wireless IPS Software] - Cisco Systems"; <http://www.cisco.com/>
10. G. Fengmin, "Deciphering Detection Techniques: Part II Anomaly-Based Intrusion Detection," White Paper, McAfee Security, 2009.
11. "Defeating DDOS Attacks [Cisco Traffic Anomaly Detectors] - Cisco Systems"; <http://www.cisco.com>.
12. "Cisco Traffic Anomaly Detector Web-Based Manager Configuration Guide (Software Version 6.1) - Activating Anomaly Detection [Cisco Traffic Anomaly Detectors] - Cisco Systems"; <https://www.cisco.com>.
13. TippingPoint,
"TippingPoint_Intrusion_Prevention_System_(IPS)";
<http://www.google.com/url?sa=t&source=web&ct=res&cd=1&ved=0CBIQFjAA&url=http%3A%2F%2Fwww.tippingpoint.com%>
14. Cisco, "Cisco ACE 4700 Series Appliance Security Configuration Guide - Configuring TCP/IP Normalization and IP Reassembly Parameters";
15. Sourcefire, "Sourcefire Cybersecurity";
<http://www.sourcefire.com/.>
16. "Bro Intrusion Detection System - Bro Overview";
<http://www.bro-ids.org/.>
17. D. Cid, J. Rossi, D. Parriott, and M. Starks, "OSSEC Architecture," 2010; <http://www.ossec.net/main/ossec-architecture/.>
18. C. Manikopoulos and S. Papavassiliou, "Network intrusion and fault detection: a statistical anomaly approach," IEEE Communications Magazine, vol. 40, 2002, pp. 76-82.
19. "Developments of the Honeyd Virtual Honeypot";
<http://www.honeyd.org/.>
20. C. Kreibich and J. Crowcroft, "Honeycomb: creating intrusion detection signatures using honeypots," SIGCOMM

Comput. Commun. Rev., vol. 34, 2004, pp. 51-56.

21. P. Li, M. Salour, and X. Su, "A survey of Internet worm detection and containment," Communications Surveys & Tutorials, IEEE, vol. 10, 2008.
22. "code.mwcollect.org"; <http://code.mwcollect.org/>.
23. "Nepenthes - finest collection"; <http://nepenthes.carnivore.it/>.
24. "honeytrap | Get honeytrap at SourceForge.net"; <http://sourceforge.net/projects/honeytrap/>.
25. T. Liston, "LaBrea-Intro History"; <http://labrea.sourceforge.net/Intro-History.html>.
26. H.A. Kim and B. Karp, "Autograph: Toward automated, distributed worm signature detection," Proceedings of the 13th USENIX Security Symposium, 2004, pp. 271-286.
27. J. Newsome, B. Karp, and D. Song, "Polygraph: Automatically generating signatures for polymorphic worms," Proceedings of the IEEE Symposium on Security and Privacy, 2005, pp. 226-241.
28. J. Aussibal and L. Gallon, "A New Distributed IDS Based on CVSS Framework," IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008. SITIS'08, 2008, pp. 701-707.
29. B. Feinstein and G. Matthews, RFC 4767: The Intrusion Detection Exchange Protocol (IDXP), 2007.
30. H. Debar, D. Curry, and B. Feinstein, RFC 4765: The Intrusion Detection Message Exchange Format (IDMEF), 2007.
31. C. Lonvick, RFC 3164: The BSD syslog Protocol, 2001.
32. Mitre, "CEE Architecture Overview Specification v1.0α"; <http://cee.mitre.org/docs/overview.html>.
33. J. Bianco, "EZ Snort Rules: Find the Truffles, Leave the Dirt"; <http://www.vorant.com/downloads.html>.
34. "res Protocol";
35. "Kiwi Enterprises - Kiwi Log Viewer Overview"; <http://www.kiwisyslog.com/kiwi-log-viewer-overview/>.

36. "NSMWiki"; http://nsmwiki.org/Main_Page.
37. "SANS: Intrusion Detection FAQ: Build Securely Snort with Sguil Sensor Step-by-Step Powered by Slackware Linux";
<http://www.sans.org/security-resources/idfaq/slackware.php>.
38. B. Caswell, "Writing Snort Rules A quick guide";
39. "SANS Internet Storm Center; Cooperative Network Security Community - Internet Security"; <http://isc.sans.org/>.
40. "What is EINSTEIN? - Definition from Whatis.com";
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1309040,00.html. CHAPTER 19 PROBLEMS 19.1. Describe and compare the key functions of IDS and IPS. 19.2. Describe how to appropriately secure all IDS/IPS components in order to protect the IDS/IPS targeted by attackers. 19.3. Describe the limitations of IDS/IPS. 19.4. Describe the advantages and disadvantages of signature-based detection. 19.5. Describe the advantages and disadvantages of anomaly-based detection. 19.6. Describe the advantages and disadvantages of stateful protocol analysis. 19.7. Describe how to use multiple types of IDS/IPS technologies to achieve more comprehensive and accurate detection and prevention of malicious activity. 19.8. Describe the advantage of using a single management console for integrating multiple types of IDS/IPS technologies or multiple products of the same IDS/IPS technology type. 19.9. Describe how to define the requirements that IDS/IPS products should meet prior to evaluating them. 19.10. Describe how to assess the IDS/IPS products' characteristics and capabilities when evaluating them. 19.11. The IDS/IPS system is positioned in front of the firewall to provide a first line of defense. (a) True (b) False 19.12. VPN is permitted to pass through the firewall. (a) True (b) False 19.13. The IDS provides ___ detection. (a) In-band (b) Out-of-band (c) None of the above 19.14. The IPS provides ___ filtering. (a) In-band (b) Out-of-band (c) None of the above 19.15. IPS cannot have false negative alerts. (a) True (b) False 19.16. Anomaly-based detection mechanisms are very useful with both IDS and IPS. (a) True (b) False
19.17. The advantage of a host-based IDS/IPS system is that a single system can protect many hosts.
(a) True

(b) False

19.18. The best protection against all types of intrusions is perhaps a combination of network and host-specific IPS systems.

(a) True

(b) False

19.19. IDS/IPS systems can be effective against attacks by legitimate as well as non-legitimate users/insiders.

(a) True

(b) False

19.20. The general classifications for approaches to intrusion detection are

(a) Anomaly-based

(b) Signature-based

(c) Behavior-based

(d) All of the above

19.21. Signature-based detection schemes can be classified as (1) statistical-based, (2) knowledge-based and (3) machine learning-based.

(a) True

(b) False

19.22. In the anomaly detection process, threshold detection uses thresholds that are userdependent in examining the frequency of the occurrence of events.

(a) True

(b) False

19.23. One advantage of the statistical approach to anomaly detection is the lack of a requirement for prior knowledge about the normal activity of the target system.

(a) True

(b) False

19.24. A key advantage of knowledge/expert-based detection is the low false alarm rate.

(a) True

(b) False

19.25. Machine learning is essentially the same as statistical-based methods since it discovers the characteristics for building a model of behaviors.

(a) True

(b) False

19.26. The training techniques employed in machine learning for anomaly detection are classified as either supervised or unsupervised.

(a) True

(b) False

19.27. Bayesian networks, neural networks and genetic algorithms are three of the machine learning methods for generating IDS/IPS rules.

(a) True

(b) False 19.28. Signature-based detection is an effective means of detecting zero-day and mutated attacks. (a) True

(b) False 19.29. A behavioral-only detection system is the most effective technique when there are a large number of hosts. (a) True (b) False 19.30. False positives are a problem with ___ detection. (a) Signature-based (b)

Anomaly-based (c) None of the above 19.31. False

negatives are a problem with ___ detection. (a)

Signature-based (b) Anomaly-based (c) None of the above

19.32. Signature-based detection cannot detect zero-day

attacks. (a) True (b) False 19.33. Most anti-virus, anti-spyware and firewall products provide an integrated solution consisting of both behavior- and signature-based

intrusion detection. (a) True (b) False 19.34. The

self-learning invoked by an administrator when activating

anomaly detection in IDS/IPS that is characterized by an

analysis of zone traffic and the simultaneous initiation of

threshold tuning of the learning process is called (a)

Detect (b) Detect and learn (c) Threshold initiation (d)

All of the above (e) None of the above 19.35. The mode of operation used by an administrator to detect traffic anomalies in a zone without any review can be classified as (a) Automatic detection (b) Interactive detection (c) Manual detection (d) All of the above 19.36. NIDS/NIPS is capable of detecting and/or blocking malware, Trojans, botnets and the like. (a) True (b) False 19.37. NIDS/NIPS may not detect encrypted traffic that contains malware. (a) True (b) False 19.38. Snort uses a combination of signature- and anomaly-based inspection. (a) True (b) False

19.39. HIDS/HIPS is effective in protecting a host from an encrypted data stream.

(a) True

(b) False

19.40. A TPM on the motherboard and external to the CPU can be used to protect the integrity of the database used by HIDS/HIPS.

(a) True

(b) False

19.41. The only problem with Honeypots is they are designed to attract both legitimate and non-legitimate users.

(a) True

(b) False

19.42. Honeypots are a viable supplement to IDS/IPS.

(a) True

(b) False

19.43. Autograph, which is capable of automatically generating signatures for TCP worms, consists of the following module(s):

(a) Flow monitor

(b) Payload-based optimizer

(c) Repeater

(d) All of the above

(e) None of the above

19.44. In an attempt to match the worm, Autograph relies on a single contiguous substring of the worm's payload of sufficient length and the assumption that this substring will remain invariant on every worm connection.

(a) True

(b) False

19.45. Polygraph was proposed to address some of the inherent problems associated with Autograph.

(a) True

(b) False

19.46. Polygraph uses ___ to match patterns in the payload of a packet.

(a) A single contiguous substring

(b) Tokens

(c) None of the above

19.47. The IDXP is designed for sharing logs in distributed IDS.

(a) True

(b) False

19.48. Automated intrusion detection systems can use IDMEF to report alerts about suspicious events.

(a) True

(b) False

19.49. IDWG is part of IETF.

(a) True

(b) False 19.50. Which of the following are protocols for sharing IDS alerts? (a) RDEP (b) Syslog protocol (c) IDXP (d) All of the above (e) None of the above 19.51.

In a distributed IDS, the NAC serves as the central manager and correlates HIDS and NIDS for constantly monitoring and blocking malicious activity. (a) True (b) False 19.52.

Snort is a proprietary IDS/IPS technology developed by Martin Roesch and currently under development by SourceFire. (a) True (b) False 19.53. IPS policy settings typically list a severity index corresponding to different types of attacks. If the severity index is 1, this is an indication of the need for immediate attention. (a) True (b) False 19.54. Vuze and LimeWire both use Java in one manner or another. (a) True (b) False 19.55. The free P2P file sharing client for the Java platform which uses the Gnutella network to locate and share files is (a) Azureus (b) Vuze (c) LimeWire (d) None of the above 19.56. LimeWire Alive is the attack name for the attack that is blocked by configuring IPS. (a) True (b) False 19.57. Attacks can at least be detected because they are outside the bounds of normal activity. (a) True (b) False 19.58. The SANS Internet Storm Center maintains data on ports that are experiencing malicious attacks. (a) True (b) False 19.59. Although the ISC collects a large amount of data from intrusion detection log entries, this data is not readily available. (a) True (b) False 19.60. The U.S. Federal Government employs a program by the name of Einstein at the gateways of their networks to filter packets and report anomalies. (a) True (b) False

20 Chapter 20 - Hash and Authentication

4. X. Wang, Y.L. Yin, and H. Yu, "Finding Collisions in the Full SHA-1, Advances in Cryptology," proceedings of CRYPTO 2005, Lecture Notes in Computer Science, vol. 3621, 2005, pp. 17-36.
5. NIST, SP 800-107: Recommendation for Applications Using Approved Hash Algorithms, 2009; <http://csrc.nist.gov/publications/PubsSPs.html>.
6. S. Gueron, S. Johnson, and J. Walker, "SHA-512/256"; <http://eprint.iacr.org/2010/548.pdf>.
7. NIST, FIPS 180-4: Secure hash standard (SHS), <http://csrc.nist.gov/publications/PubsFIPS.html>, 2011.
8. X. Wang, X. Lai, D. Feng, H. Chen, and X. Yu, "Cryptanalysis of the Hash Functions MD4 and RIPEMD, EUROCRYPT 2005," Springer LNCS, vol. 3494, 2005, p. 118.
9. X. Wang and H. Yu, "How to Break MD5 and Other Hash Functions," EUROCRYPT 2005, LNCS 3494, 2005.
10. D. Molnar, M. Stevens, A. Lenstra, B. de Weger, A. Sotirov, J. Appelbaum, and D.A. Osvik, "MD5 Considered Harmful Today: Creating a Rogue CA Certificate," 25th Chaos Communication Congress, Berlin, Germany, 2008.
11. M. Stevens, A. Lenstra, and B. de Weger, "Chosen-prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities," Eurocrypt 2007.
12. H. Yu, G. Wang, G. Zhang, and X. Wang, "The second-preimage attack on MD4," Lecture notes in computer science, vol. 3810, 2005, p. 1.
13. X. Wang, H. Yu, and Y.L. Yin, "Efficient Collision Search Attacks on SHA-0," Advances in CryptologyCRYPTO 2005, Lecture Notes in Computer Science, vol. 3621, pp. 1-16.
14. M. Stevens, Attacks on Hash Functions and Applications, Centrum Wiskunde & Informatica, 2012;
15. Microsoft, "Microsoft Security Advisory (2718704) Unauthorized Digital Certificates Could Allow Spoofing," 2012;
16. NIST, FIPS 198-1: The Keyed-Hash Message Authentication

Code (HMAC), 2008.

17. H. Krawczyk, M. Bellare, and R. Canetti, RFC 2104: HMAC: Keyed-hashing for message authentication, 1997.

18. NIST, SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, 2007;
<http://csrc.nist.gov/publications/PubsSPs.html>.

19. NIST, SP 800-56B: Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, 2009;
<http://csrc.nist.gov/publications/PubsSPs.html>.

20. NIST, SP 800-108: Recommendation for Key Derivation Using Pseudorandom Functions, 2009; <http://csrc.nist.gov/publications/PubsSPs.html>.

21. NIST, SP 800-90: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, 2007; <http://csrc.nist.gov/publications/PubsSPs.html>.

22. NIST, SP 800-118: Guide to Enterprise Password Management, 2009; <http://csrc.nist.gov/publications/PubsSPs.html>.

23. NIST, FIPS 190: Guideline for the Use of Advanced Authentication Technology Alternatives, 1994.

24. NIST, SP 800-77: Guide to IPsec VPNs, 2005;
<http://csrc.nist.gov/publications/PubsSPs.html>.

25. “Jasypt: Java simplified encryption - Encrypting passwords”;
<http://www.jasypt.org/encrypting-passwords.html>.

26. L. Howard, RFC 2307: An Approach for Using LDAP as a Network Information Service, 1998.

27. R. Lemos, “Cracking Windows passwords in seconds,” CNET News; http://news.cnet.com/21001009_3-5053063.html.

28. T. Ptacek, “Enough With The Rainbow Tables: What You Need To Know About Secure Password Schemes,” Matasano Security LLC;

29. “MDCrack Homepage”; <http://c3rb3r.openwall.net/mdcrack/>.

30. G. Duchemin, “MDCrack”;

- <http://www.securityfocus.com/tools/4242>.
31. B. Byfield, "Password's Progress," Linux Journal; <http://www.linuxjournal.com/article/4846>.
 32. B. Kaliski, RFC 2898: PKCS# 5: Password-Based Cryptography Specification Version 2.0, 2000.
 33. NIST, FIPS 81: DES Modes of Operation, 1980.
 34. NIST, FIPS 46-3: Data Encryption Standard (DES); specifies the use of Triple DES, 1999.
 35. NIST, FIPS 171: Key Management Using ANSI X9.17, 1972.
 36. IEEE P1363.2: Password-Based Public-Key Cryptography, 2010; <http://grouper.ieee.org/groups/1901/>.
 37. NIST, SP 800-63 Rev. 1: DRAFT Electronic Authentication Guideline, 2008; <http://csrc.nist.gov/publications/PubsSPs.html>.
 38. NIST, FIPS 140-2: Security Requirements for Cryptographic Modules, 2001; <http://csrc.nist.gov/publications/fips/fips1401.htm>.
 39. ANSI, X9.31-1998: Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry (rDSA), 1998.
 40. C. Neuman, T. Yu, S. Hartman, and K. Raeburn, RFC 4120: The Kerberos Network Authentication Service (V5), 2005.
 41. L. Zhu and S. Hartman, RFC 4121: The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2, 2005.
 42. L. Lamport, "Password authentication with insecure communication," Communications of the ACM, vol. 24, 1981, pp. 770-772.
 43. N. Haller, RFC 1760: The S/KEY One-Time Password System, RFC, IETF, February 1995, <ftp://ftp.isi.edu/in-notes/rfc1760.txt>.
 44. D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen, RFC 4226: HOTP: An HMAC-based one time password algorithm, 2005.
 45. J. Initiative for Open AuTHentication (OATH), OATH Reference Architecture Version 2.0, 2007.
 46. J. Initiative for Open AuTHentication (OATH), IETF Draft: OCRA - OATH Challenge/Response Algorithms Specification, 2010.
 47. J. Initiative for Open AuTHentication (OATH), IETF Draft: TOTP - Time-based One-time Password Algorithm, 2010.
 48. J. Linn and M. Nyström, IETF Draft: OTP Methods for TLS, 2006.
 49. RSA Laboratories, OTP-PKCS #11: PKCS #11 mechanisms for

One-Time Password tokens, 2005; <http://www.rsa.com/rsalabs/node.asp?id=2818>. 50. M. Nystroem, RFC 4793: The EAP protected one-time password protocol (EAP-POTP), 2007. 51. G. Richards, IETF Draft: OTP-Kerberos: Using OTPs in Kerberos pre-authentication, 2010. 52. "Final: OpenID Authentication 2.0 - Final"; http://openid.net/specs/openid-authentication-2_0.html. 53. "OAuth Spec"; <http://oauth.net/documentation/spec/>.

CHAPTER 20 PROBLEMS

20.1. Compare the advantages and disadvantages of Intel IPT versus the SecureID token by creating a table that lists various compromises and the steps taken by each to address them.

20.2. Given a password that is 15 characters long where each character can be one of the 52 upper- and lower-case letters, 10 digits or 32 punctuation symbols and assuming each hash requires 1 ns, compute the total time consumed in a brute force attack.

20.3. Given the data in Problem 20.2, compute the size of the hard disk needed to house a rainbow table if each hash is 512 bits in length.

20.4. Using the information in Problem 20.2 and assuming that each password has a 16 byte salt and each hash requires 1 ns, compute the total time needed for a brute force attack.

20.5. Given the data in Problem 20.2 and the fact that each password has a 16 byte salt, determine the size of the hard disk that is needed to house a rainbow table assuming each hash is 512 bits in length.

20.6. In addition to the data in Problem 20.2, assume that each password has a 16 byte salt and is hashed a random number of times r , i.e., $\text{hash} = H^r(\text{password})$, $r \in [1, 16]$. Furthermore, assume that each hash requires 1 ns. Given these conditions, compute the total time required for a brute force attack.

20.7. In the event that a token with some physical manifestation, cell phone or one-time password device, is stolen by an attacker, specify the proper threat mitigation strategy.

20.8. If an attacker connects to a Verifier online and attempts to guess a valid token authenticator, outline the proper threat mitigation strategy.

20.9. In phishing or pharming attacks, the token secret or authenticator, e.g., password, is captured by fooling the Subscriber into thinking the Attacker is a Verifier or Relying Party. What is the proper threat mitigation strategy for this scenario?

20.10. Determine the manner in which to protect a user who uses the OAuth open-standard protocol if they wish to publish their information on Facebook using their Google account password.

20.11. If the security strength of K (key) is 128 bits and SHA-256 is used, the security strength of the HMAC

algorithm is ___ bits.

20.12. If the security strength of K is 256 bits and SHA-1 is used, the security strength of the HMAC algorithm is ___ bits.

20.13. If the security strength of K is 256 bits and SHA-256 is used, the security strength of the HMAC algorithm is ___ bits.

20.14. If the desired security strength of the HMAC algorithm is 256 bits and SHA-512/256 is used, determine the security strength of K.

20.15. If the desired security strength of the HMAC algorithm is 256 bits and SHA-512/224 is used, determine the security strength of K.

20.16. If the desired security strength of the HMAC algorithm is 512 bits and SHA-512/256 is used, determine the security strength of K.

20.17. If the desired security strength of the KDF algorithm is 128 bits and SHA-1 is used, determine the security strength of K.

20.18. If the desired security strength of the KDF algorithm is 256 bits and SHA-256 is used, determine the security strength of K.

20.19. Based upon the specifications outlined in NIST Special Publication 800-108, draw a block diagram that constructs a KDF as a PRNG using HMAC as the building block.

20.20. In terms of security, the term confidentiality refers to protection against message tampering.

(a) True

(b) False

20.21. Encryption is employed to guarantee confidentiality and integrity.

(a) True

(b) False

20.22. The strategic use of a hash function can enhance

security.

(a) True

(b) False

20.23. The prevention of message tampering while it is in transit can be achieved through the use of

(a) Authentication

(b) Integrity

(c) All of the above

(d) None of the above

20.24. Any bit in a message digest resulting from a hash should be a 1 only half of the time.

(a) True

(b) False 20.25. If a hash function exhibits the property that $\text{hash}(x) = \text{hash}(y)$ for two different inputs x and y , then a collision is said to exist. (a) True (b) False

20.26. If a hash function produces a full-length hash value of 512 bits, then the collision resistance is approximately (a) 1024 bits (b) 512 bits (c) 256 bits (d) 128 bits (e) None of the above 20.27. A message digest can be inverted to obtain the original message. (a)

True (b) False 20.28. If the approximate preimage resistance produced by a hash function is 512 bits, then the length of the hash value is (a) 1024 bits (b) 512 bits (c) 256 bits (d) 128 bits (e) None of the above

20.29. SHA-512 is a viable hash algorithm. (a) True (b) False

20.30. One Initialization Vector is used for both SHA-256 and SHA-512. (a) True (b) False 20.31. The message authentication code HMAC uses (a) Cryptographic key (b) Hash function (c) All of the above (d) None of the above 20.32. An important feature of HMAC is the fact that hashing is faster than encryption in software. (a)

True (b) False 20.33. HMAC employs multiple hashes. (a) True (b) False 20.34. The key used in HMAC must be (a) A random bit string obtained using an approved generator (b) Generated using an approved key establishment method (c) All of the above (d) None of the above

20.35. The security strength of the HMAC algorithm can be expressed as $\text{Min}(\text{security strength of } K, L)$, where K is the key and L is the length of the key.

(a) True

(b) False

20.36. Password-only authentication can be implemented entirely in software.

(a) True

(b) False

20.37. A dictionary attack is a trial and error approach to password guessing.

(a) True

(b) False

20.38. The only methods used to capture a password can be classified as either hardware, e.g., a Trojan horse or software, e.g., spyware.

(a) True

(b) False

20.39. Storing a hash of the password rather than the password is an effective technique in password protection.

(a) True

(b) False

20.40. A dictionary attack is typically a viable approach to password cracking because humans normally use passwords that are not truly random.

(a) True

(b) False

20.41. A message authentication scheme consists of a

(a) MAC generation operation

(b) MAC verification operation

(c) All of the above

(d) None of the above

20.42. Computer-generated passwords are not popular because

(a) They are hard to remember

(b) May be written down somewhere to facilitate their use

(c) All of the above

20.43. The IEEE plays a significant role in the development of cryptographic standards.

(a) True

(b) False

20.44. Kerberos serves as the foundation for authentication in a domain and is used by

(a) Active directory

(b) UNIX

(c) Linux

(d) All of the above

20.45. A one-time password uses ___ to ensure it can only be used once, as specified in RFC 2289.

(a) A shared key

(b) Multiple hashes

(c) A timestamp

(d) All of the above 20.46. A HOTP one-time password uses ___ to ensure it can only be used once, as specified in

RFC 2289. (a) A shared key (b) One counter (c) A timestamp (d) All of the above 20.47. A TOTP one-time

password uses ___ to ensure it can only be used once, as specified in RFC 2289. (a) A shared key (b) One counter

(c) A timestamp (d) All of the above 20.48. Multiple

factor authentication uses ___ to ensure it can only be used once, as specified in RFC 2289. (a) A password (b) A token

(c) A pin (d) All of the above 20.49. A one-time

password uses ___ to implement the algorithm. (a) Hardware (b) Software (c) All of the above (d) None of the above

21 Chapter 21 - Symmetric Key Ciphers and Wireless LAN Security

1. NIST, FIPS 46-3: Data Encryption Standard (DES); specifies the use of Triple DES, 1999.
2. ANSI, ANSI X9.17: Financial Institution Key Management (Wholesale), 1995.
3. ISO 9798-3: Security techniques-Entity authentication-Part 3: Mechanisms using digital signature techniques, 1998.
4. D. Coppersmith, D.B. Johnson, and S.M. Matyas, "A proposed mode for triple-DES encryption," IBM Journal of Research and Development, vol. 40, 1996, pp. 253-262.
5. NIST, SP 800-67 1.1: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, 2008; <http://csrc.nist.gov/publications/PubsSPs.html>.
6. NIST, FIPS 197: Advanced encryption standard (AES), 2001.
7. NIST, SP 800-38A: Recommendation for Block Cipher Modes of Operation - Methods and Techniques, 2001; <http://csrc.nist.gov/publications/PubsSPs.html>.
8. NIST, FIPS 81: DES Modes of Operation, 1980.
9. ANSI X9.52:1998 Triple Data Encryption Algorithm Modes of Operation, 1998; <http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.52%3A1998>.
10. "Block cipher modes of operation - Wikipedia, the free encyclopedia"; http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation.
11. I. Mantin and A. Shamir, "A practical attack on broadcast RC4," FSE 2001, Lecture Notes in Computer Science, 2001, pp. 152-164.
12. S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," Selected Areas in Cryptography 2001, Lecture Notes in Computer Science, 2001, pp. 1-24.
13. I. Mironov, "(Not So) Random Shuffles of RC4," Proc. of CRYPTO'02, 2002, pp. 304-319.
14. A. Klein, "Attacks on the RC4 stream cipher," Designs,

Codes and Cryptography, vol. 48, 2008, pp. 269-286.

15. E. Tews, R.P. Weinmann, and A. Pyshkin, "Breaking 104 bit WEP in less than 60 seconds," WISA, Lecture Notes in Computer Science, vol. 4867, 2007, pp. 188-202. 16.
"aircrack-ptw";
<http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/>.
17. J. Schaad and R. Housley, RFC 3394: advanced encryption standard (AES) key wrap algorithm, 2002. 18. E. Tews and M. Beck, "Practical attacks against WEP and WPA," Proceedings of the second ACM conference on Wireless network security, Zurich, Switzerland: ACM, 2009, pp. 79-86; <http://portal.acm.org/citation.cfm?id=1514274.1514286>. 19. "Aircrack-ng";
<http://www.aircrack-ng.org/>. 20. T. Ohigashi and M. Morii, "A Practical Message Falsification Attack on WPA," IEICE Information System Researcher's Conference, 2009. 21. D. Whiting, R. Housley, and N. Ferguson, RFC 3610: Counter with CBC-MAC, 2003. 22. R. Housley, RFC 4309: Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP), 2005. 23. NIST, SP 800-38C: Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, 2007;
<http://csrc.nist.gov/publications/PubsSPs.html>. 24. IEEE Std. 802.11-2007 IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007;
<http://standards.ieee.org/getieee802/portfolio.html>. 25. NIST, FIPS 140-2: Security Requirements for Cryptographic Modules, 2001;
<http://csrc.nist.gov/publications/fips/fips1401.htm>. 26. NIST, FIPS 140-3: Draft Security Requirements for Cryptographic Modules, 2009; <http://csrc.nist.gov/publications/fips/fips1401.htm>. 27. NIST, "Cryptographic Module Validation Program (CMVP)";
<http://csrc.nist.gov/groups/STM/cmvp/>. 28. "Official CC/CEM versions - The Common Criteria Portal";
<http://www.commoncriteriaportal.org/thecc.html>. 29. "NESSIE: New European Schemes for Signatures, Integrity, and Encryption"; <https://www.cosic.esat.kuleuven.be/nessie/>. 30. "Side Channel Cryptanalysis of Product Ciphers";
<http://www.schneier.com/paper-side-channel.html>. 31. M.A. Hasan, "Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz curve cryptosystems," IEEE Transactions on Computers, 2001, pp. 1071-1083. 32.

- D.A. Osvik, A. Shamir, and E. Tromer, "Cache attacks and countermeasures: the case of AES," Proceedings of RSA Conference Cryptographers Track 2006, Lecture Notes in Computer Science, vol. 3860, 2006, pp. 1-20. 33. S.
- Vaudenay, "Security Flaws Induced by CBC Padding—Applications to SSL, IPSEC, WTLS...," Advances in Cryptology—EUROCRYPT 2002, 2002, pp. 534-545; <http://www.springerlink.com/index/u95c49b6hacfeghe.pdf>.
34. K. Paterson and A. Yau, "Padding oracle attacks on the ISO CBC mode encryption standard," Topics in Cryptology—CT-RSA 2004, 2004, pp. 1995-1995. 35. A. Yau, K. Paterson, and C. Mitchell, "Padding oracle attacks on CBC-mode encryption with secret and random IVs," Fast Software Encryption, 2005, pp. 11-43; <http://www.springerlink.com/index/5pq1814upk91yaha.pdf>.
36. R. Bardou, R. Focardi, Y. Kawamoto, G. Steel, J.K. Tsai, and others, "Efficient Padding Oracle Attacks on Cryptographic Hardware," 2012; <http://hal.inria.fr/hal-00691958/>.
- CHAPTER 21 PROBLEMS
- 21.1. Compare the AES-CBC and AES-counter mode using a table that illustrates their similarities and differences, including the IV. 21.2. List the important features of an IV and the methods used to generate them for both the AES-CBC and AES-counter mode. 21.3. Lists the differences and similarities for the IV and counter used in WPA2 and RFC 4309. 21.4. Describe the procedure for deriving a fresh pairwise key for WPA2 when it is deployed in a home wireless network. 21.5. Prepare a table that lists the advantages and disadvantages of AES-CBC-MAC versus HMAC.
- 21.6. When AES-128 is used in CBC mode, determine the size of the IV.
- 21.7. When 3DES is used in CBC mode using a 112-bit key, determine the size of the IV.
- 21.8. When 3DES is used in CBC mode using a 168-bit key, determine the size of the IV.
- 21.9. When AES-256 is used in CBC mode, determine the size of the IV.
- 21.10. When AES-128 in CBC mode is used to encrypt a file containing 4015 bytes, determine the padding required for this file.
- 21.11. When AES-128 in CBC mode is used to encrypt a file containing 4014 bytes, determine the padding required for this file.

21.12. When AES-256 in CBC mode is used to encrypt a file containing 4013 bytes, determine the padding required for this file.

21.13. When 3DES in CBC mode is employed with a 112-bit key to encrypt a file containing 4013 bytes, determine the padding required for this file.

21.14. When 3DES in CBC mode is used with a 168-bit key to encrypt a file containing 4012 bytes, determine the padding required for this file.

21.15. When AES counter mode is used, as shown in Figure 21.24, determine the counter values A_i , $i = 0, 1, 2, \dots$ using the Hex format.

21.16. When CCMP is used, as illustrated in Figure 21.26, to protect an 802.11 frame containing a 1280-byte payload, determine the value x for A_i , $i = 0, 1, 2, \dots, x$, where x is the number of AES blocks. The 1280-byte payload does not contain the 802.11 header, ICV and FCS.

21.17. When CCMP is used, as shown in Figure 21.26, to protect an 802.11 frame containing a 1408-byte payload, determine the value x for A_i , $i = 0, 1, 2, \dots, x$, where x is the number of AES blocks. The 1408-byte payload does not contain the 802.11 header, ICV and FCS.

21.18. Determine the maximum frame length imposed by a particular CCMP field in WPA2.

21.19. Describe the security strength of CCMP and its capability in defending anti-replay attacks.

21.20. Discuss the security that is obtained through the use of a pre-share secret key (PSK) for WPA2 and its feasibility in an enterprise network.

21.21. The two types of symmetric key ciphers that are used to ensure integrity are block ciphers and stream ciphers.

(a) True

(b) False

21.22. When using block ciphers the two parties share a secret key.

(a) True

(b) False

21.23. The advanced encryption standard (AES) is a

(a) Block cipher

(b) Stream cipher

(c) None of the above 21.24. Triple DES, operating in the ___ mode, is secure. (a) AES (b) ECB (c) CBC (d) All of the above 21.25. RC4 is a ___. (a) Block cipher (b) Stream cipher (c) None of the above 21.26. A block cipher operates on one block of plaintext, which is 64 bits for AES and 128 bits for DES. (a) True (b) False 21.27. In a block cipher operation, the plaintext occupies the first set of ciphertext bits. (a) True (b) False 21.28. Triple DES was a useful technique but is no longer secure. (a) True (b) False 21.29. The Feistel function is a structure of crypto operations employed with (a) AES (b) DES (c) None of the above (d) All of the above 21.30. Triple DES is an effective tool for use with (a) IPsec (b) PGP (c) S/MIME (d) All of the above (e) None of the above 21.31. The input for AES is a 64-bit plaintext block that is arranged as an array. (a) True (b) False 21.32. The number of times AES employs a shuffle, shift and mix operation on the plaintext input is dependent upon the key size. (a) True (b) False 21.33. Cipher key used in AES is a synonym for round key. (a) True (b) False 21.34. In the electronic code book mode of operation for symmetric key block cipher algorithms the plaintext is split into blocks and each block is XORed with the result obtained from encrypting the previous blocks. (a) True (b) False

21.35. The number of modes of operation for Triple DES is

(a) 3

(b) 5

(c) 7

(d) 9

(e) None of the above

21.36. The various modes of operation for Triple DES are based upon

(a) ECB

- (b) CBC
- (c) CFB
- (d) OFB
- (e) All of the above

21.37. ECB is primarily used to send very small quantities of data since in large quantities of data, repetitions may occur.

- (a) True
- (b) False

21.38. An initialization vector is used in conjunction with the plaintext in the encryption processes of the following modes:

- (a) CBC
- (b) CFB
- (c) OFB
- (d) All of the above
- (e) None of the above

21.39. The initialization vector is used in the initial step of the decryption process for CBC.

- (a) True
- (b) False

21.40. When an initialization vector is used as an input in the encryption process, it must always be a secret.

- (a) True
- (b) False

21.41. In the CBC encryption process the initialization vector must be unpredictable by an attacker.

- (a) True
- (b) False

21.42. When used in communication applications, block ciphers have an inherent advantage.

- (a) True
- (b) False

21.43. An advantage of stream ciphers is the ability to reuse the stream key.

- (a) True
- (b) False

21.44. RC4 is a byte-oriented stream cipher with a fixed key length of 128 bits.

- (a) True
- (b) False

21.45. A stream cipher is created from a block cipher in the AES counter mode encryption algorithm.

- (a) True
 - (b) False
- 21.46. CTR is an excellent encryption process for use with bursty high speed links. (a) True (b) False
- 21.47. The four levels of security specified by the joint effort between NIST and CSE specify in detail the level required for specific applications. (a) True (b) False
- 21.48. Measurements made to support a side channel attack include (a) Acoustic radiation (b) Electromagnetic radiation (c) Power consumption (d) All of the above (e) None of the above
- 21.49. A power analysis used to support a side channel attack is especially useful with devices that rely on an external source of power. (a) True (b) False
- 21.50. DPA is a procedure in which a small portion of a cryptographic key is guessed and then this guess is checked against measurements to see if there is any correlation. (a) True (b) False
- 21.51. Fixing the response time of the server to different messages provides at least some protection from network attacks. (a) True (b) False
- 21.52. Timing attacks are typically very successful against symmetric key algorithms. (a) True (b) False
- 21.53. An effective defense against side channel attacks involves changing keys frequently and ensuring that protocols never use a key often enough that an attacker is able to collect data from its use. (a) True

(b) False 21.54. The European standards for side channel attacks are based primarily upon a timing analysis. (a) True (b) False 21.55. The number of levels of CMVP security specified by the US Federal Information Processing Standards is (a) 3 (b) 4 (c) 5 (d) None of the above 21.56. Level 1 in the FIPS 140-2 standards is the highest level of security in the standard. (a) True (b) False

21.57. NESSIE provides recommendations for both block and stream ciphers.

(a) True

(b) False

21.58. DES has a ___-bit key.

(a) 56

(b) 64

(c) 128

(d) 256

(e) None of the above

21.59. Triple DES has a ___-bit key.

(a) 56

(b) 64

(c) 112

(d) 168

(e) None of the above

21.60. Counter mode ciphers allow pre-computed keystreams in order to improve performance.

(c) True

(d) False

22 Chapter 22 - Public Key Cryptography, Infrastructure and Certificates

1. NIST, SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, 2007;
<http://csrc.nist.gov/publications/PubsSPs.html>.
2. NIST, SP 800-56B: Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, 2009;
<http://csrc.nist.gov/publications/PubsSPs.html>.
3. E. Rescorla, RFC 2631: Diffie-Hellman key agreement method, 1999.
4. NIST, FIPS 186-3: Digital Signature Standard (DSS),
<http://csrc.nist.gov/publications/PubsFIPS.html>, 2009.
5. D. Harkins and D. Carrel, "RFC 2409: The Internet Key Exchange (IKE)," 1998.
6. C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen, RFC 5996: Internet key exchange (ikev2) protocol, 2010.
7. T. Kivinen and M. Kojo, RFC 3526: More Modular Exponential (MODP) Diffie-Hellman Groups for Internet Key Exchange (IKE), 2003.
8. D. Eastlake, RFC 2539: Storage of Diffie-Hellman Keys in the Domain Name System (DNS), RFC 2539, March 1999, 1999.
9. C. Kaufman, RFC 4306: Internet key exchange (ikev2) protocol, 2005.
10. NIST, SP 800-57: Recommendation for Key Management, 2009; <http://csrc.nist.gov/publications/PubsSPs.html>.
11. NIST, SP 800-77: Guide to IPsec VPNs, 2005;
<http://csrc.nist.gov/publications/PubsSPs.html>.
12. RSA, PKCS # 1: RSA Encryption Standard, 2002.

TABLE 22.21 A Comparative Analysis of S/MIME and OpenPGP

Features S/MIME v3 OpenPGP

Message format CMS (cryptographic message syntax RFC 3370)
Radix-64, RFC4880

Certificate format Binary, based on X.509v3 Supports X.509 plus original format

Symmetric encryption

algorithm TripleDES (DES EDE3 CBC), AES-128, AES-192, AES-256 TripleDES (DES EDE3)/AES/IDEA/CAST/Blowfish/Twofish

Signature algorithm DSS or RSA RSA or DSS

Hash algorithm MD5, SHA-1, SHA-256, SHA-384, SHA-512 MD5, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, RIPEMD160,

MIME encapsulation of

signed data Choice of multipart/signed or CMS format
Multipart/signed with ASCII armor (puts specific headers around the Radix-64 encoded data)

MIME encapsulation of

encrypted data Application/pkcs7-mime Multipart/encrypted
13. H.L. Garner, "The Residue Number System," IRE Transactions on Electronic Computers, vol. EC-8, Jun. 1959, pp. 140-147. 14. A.K. Lenstra et al., "Ron was wrong, Whit is right," 2012; <http://eprint.iacr.org/2012/064.pdf>. 15. ANSI, X9.31-1998: Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry (rDSA), 1998. 16. ANSI, X9.62: The elliptic curve digital signature algorithm (ECDSA), 2005. 17. RSA, PKCS #13: Elliptic Curve Cryptography Standard, 1998. 18. RSA Laboratories, "The RSA Challenge Numbers"; <http://www.rsa.com/rsalabs/node.asp?id = 2093>. 19. NIST, Recommended elliptic curves for federal government use, 1999; http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTR_eCur.pdf. 20. Certicom, "ECC Tutorial"; <http://www.certicom.com/index.php/ecc-tutorial>. 21. M. Massierer, "ECC Notebook: An Interactive Introduction to Elliptic Curve Cryptography"; <http://sagenb.org/home/pub/1126/>. 22. D. Fu and J. Solinas, RFC 4753: ECP Groups for IKE and IKEv2, 2007. 23. M. Lepinski and S. Kent, RFC 5114: Additional Diffie-Hellman Groups for Use with IETF Standards, Jan, 2008. 24. D. Fu and J. Solinas, RFC 5903: Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2, 2010. 25. D. McGrew, K. Igoe, and M. Salter, RFC 6090: Fundamental Elliptic Curve Cryptography Algorithms, 2011. 26. NSA, Suite B Implementer's Guide to FIPS 186-3. (ECDSA), 2010; <http://csrc.nist.gov/publications/PubsSPs.html>. 27. M. Qu, SEC 2: Recommended Elliptic

Curve Domain Parameters, 1999. 28. D. Brown, IETF Draft: Additional ECC Groups For IKE and IKEv2, 2006. 29. "The Case for Elliptic Curve Cryptography - NSA/CSS"; http://www.nsa.gov/business/programs/elliptic_curve.shtml. 30. "The Certicom ECC Challenge"; <http://www.certicom.com/index.php/the-certicom-ecc-challenge>. 31. ITU-T Rec., X.509: Information Technology - Open Systems Interconnection - The Directory: publickey and attribute certificate frameworks, 1996. 32. R. Housley, W. Polk, W. Ford, and D. Solo, RFC 3280: Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile, RFC 3280, April 2002, 2002. 33. M. Cooper, Y. Dzambasow, P. Hesse, S. Joseph, and R. Nicholas, RFC 4158: Internet X.509 Public Key Infrastructure: Certification Path Building, RFC 4158, September 2005. 34. D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, RFC 5280: Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile, Obsoletes RFC 3280, 2008. 35. "RSA Laboratories - Section Index"; <http://www.rsa.com/rsalabs/node.asp?id = 2153>. 36. "RSA Laboratories - Public-Key Cryptography Standards (PKCS)"; <http://www.rsa.com/rsalabs/node.asp?id = 2124>. 37. "NSA Suite B Cryptography - NSA/CSS"; http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml. 38. E. Allman, J. Callas, M. Delany, M. Libbey, J. Fenton, and M. Thomas, RFC 4869: Suite B Cryptographic Suites for IPsec, 2007. 39. NIST, SP 800-78-2: DRAFT Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV), 2009; <http://csrc.nist.gov/publications/PubsSPs.html>. 40. ANSI, X9.42: Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, 2003. 41. ANSI, X9.63: Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2001. 42. NIST, FIPS 196: Entity Authentication Using Public Key Cryptography, 1997. 43. P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems," Advances in Cryptology-Crypto'96, Lecture Notes in Computer Science, vol. 1109, 1996, pp. 104-113. 44. A. Pellegrini, V. Bertacco, and T. Austin, "Fault-Based Attack of RSA Authentication," Design Automation and Test in Europe (DATE), 2010. 45. A. Sotirov, "Creating a rogue CA certificate"; <http://www.phreedom.org/research/rogue-ca/>. 46. D. Molnar, M. Stevens, A. Lenstra, B. de Wever, A. Sotirov, J. Appelbaum, and D.A. Osvik, "MD5 Considered Harmful Today: Creating a Rogue CA Certificate," 25th Chaos Communication Congress, Berlin, Germany, 2008. 47.

- Sotirov, "MD5 considered harmful today";
<http://www.win.tue.nl/hashclash/rogue-ca/>. 48. Microsoft, "Microsoft Security Advisory (2718704) Unauthorized Digital Certificates Could Allow Spoofing," 2012; <http://technet.microsoft.com/en-us/security/advisory/2718704>.
49. D. Bleichenbacher, "Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS# 1," Advances in Cryptology- CRYPTO'98, 1998, pp. 1-12;
<http://www.springerlink.com/index/j5758n240017h867.pdf>.
50. R. Bardou, R. Focardi, Y. Kawamoto, G. Steel, J.K. Tsai, and others, "Efficient Padding Oracle Attacks on Cryptographic Hardware," 2012;
<http://hal.inria.fr/hal-00691958/>.
51. J. Callas, L. Donnerhacke, H. Finney, and R. Thayer, "RFC 2440: OpenPGP message format," 1998.
52. J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, RFC 4880: OpenPGP Message Format, November, 2007.
53. B. Ramsdell, RFC 3850: Secure/multipurpose Internet mail extensions (S/MIME) version 3.1 certificate handling, July, 2004.
54. B. Ramsdell, RFC 3851: Secure/multipurpose Internet mail extensions (S/MIME) version 3.1 message specification, 2004.
55. J. Galvin, S. Murphy, S. Crocker, and N. Freed, RFC 1847: Security Multiparts for MIME: Multipart, 1995.
56. M. Elkins, D. Del Tarto, R. Levien, and T. Roessler, RFC 3156: Mime security with openPGP, 2001.
57. M. Elkins, RFC 2015: MIME Security with Pretty Good Privacy, October, 1996.
58. B. Kaliski, RFC 2315: PKCS # 7: Cryptographic Message Syntax Version 1.5, 1998.
59. D. Steedman, Abstract syntax notation one (ASN. 1): the tutorial and reference, Technology Appraisals, 1990.
60. R. Housley, RFC 3852: Cryptographic message syntax (CMS), 2004.
61. R. Housley, RFC 3370: Cryptographic Message Syntax (CMS) Algorithms. The Internet Society, 2002.

CHAPTER 22 PROBLEMS

22.1. Compare the key pair used in the RSA signature with DSA by creating a table that outlines the properties of each, including the way in which they are generated and employed.

22.2. Prepare a table that describes the differences and similarities that exist between ECDH and ECIES.

22.3. Prepare a table that compares the differences and similarities that exist between RSA encryption and ECIES encryption by describing such factors as speed of computation, key wrapping and key sizes, etc.

22.4. Using a table, compare the differences and similarities that exist between public keybased unilateral and mutual authentication protocols by including such things as the verification steps.

22.5. Compare the differences and similarities that exist between PGP encryption and ECIES encryption by using a table that lists the properties of each and such things as the steps employed in encryption/decryption.

22.6. Complete the following table with a yes or no answer to outline the differences and similarities that exist between the PKI in support of DH, ECDH, RSA signature, ECDSA and ECIES. DH ECDH RSA ECDSA ECIES Key agreement
Encryption key derivation Encryption Signature Signature
verify Supported by CA's 22.7. Lists the differences and similarities that exist between a simple power analysis (SPA) and a differential power analysis (DPA). 22.8.

Using Table 22.12, which contains the NIST recommended key sizes of the same security strength for both FFC and ECC, determine the length of p and the length of the private key x when using the D-H protocol for establishing a fresh, shared key ($g^{xy} \bmod p$) for AES-128. 22.9. Using Table 22.12, which contains the NIST recommended key sizes of the same security strength for both FFC and ECC, determine the length of p and the length of the private key x when using the D-H protocol for establishing a fresh, shared key ($g^{xy} \bmod p$) for 3DES. 22.10. Using Table 22.12, which contains the NIST recommended key sizes of the same security strength for both FFC and ECC, determine the length of p and the length of the private key x when using the D-H protocol for establishing a fresh, shared key ($g^{xy} \bmod p$)

$xy \bmod p$) for AES-256. 22.11. Using Table 22.12, which contains the NIST recommended key sizes of the same security strength for both FFC and ECC, determine the length of modulus when using the RSA protocol for encrypting a fresh, shared secret for AES-256. 22.12.

Using Table 22.12, which contains the NIST recommended key sizes of the same security strength for both FFC and ECC, determine the length of modulus when using the RSA protocol for encrypting a fresh, shared secret for AES-128.

22.13. Using Table 22.12, which contains the NIST recommended key sizes of the same security strength for both FFC and ECC, determine the length of modulus when using the RSA protocol for encrypting a fresh, shared secret for 3DES. 22.14. Using Table 22.12, which contains the NIST recommended key sizes of the same security strength for both FFC and ECC, determine the curve over prime fields that should be employed when using the ECDH protocol for establishing a fresh, shared key for AES-128.

22.15. Using Table 22.12, which contains the NIST recommended key sizes of the same security strength for both FFC and ECC, determine the curve over prime fields that should be employed when using the ECDH protocol for establishing a fresh, shared key for AES-256. 22.16.

Using Table 22.12, which contains the NIST recommended key sizes of the same security strength for both FFC and ECC, determine the curve over binary fields that should be employed when using the ECDH protocol for establishing a fresh, shared key for AES-128. 22.17. Using Table 22.12, determine the curve over binary fields that should be employed when using the ECDH protocol for establishing a fresh, shared key for AES-256. 22.18. Using Table 22.1 and Table 22.12, determine the required hash algorithm and the length of the RSA modulus that should be employed when using the RSA signature for verifying a client certificate in the SSL protocol in order to establish a fresh, shared key for AES-256. 22.19. Using Table 22.1 and Table 22.12, determine the required hash algorithm and the length of the RSA modulus that should be employed when using the RSA signature for verifying a client certificate in the SSL protocol in order to establish a fresh, shared key for AES-128.

22.20. Using Table 22.1 and Table 22.12, determine the required hash algorithm and the length of the RSA modulus that should be employed when using the RSA signature for verifying a client certificate in the SSL protocol in order to establish a fresh, shared key for 3DES.

22.21. Using Table 22.1 and Table 22.12, determine the required hash algorithm and the length of ECP that should

be employed when using the ECDSA signature for verifying a client certificate in the SSL protocol in order to establish a fresh, shared key for AES-128.

22.22. Using Table 22.1 and Table 22.125, describe the required hash algorithm and the length of ECP when using the ECDSA signature for verifying a client certificate in the SSL protocol in order to establish a fresh, shared key for AES-256.

22.23. Using Table 22.1and Table 22.12, describe the required hash algorithm and the length of EC2N when using the ECDSA signature for verifying a client certificate in the SSL protocol in order to establish a fresh, shared key for AES-256.

22.24. A single public key is all that is needed in the application of public key cryptography.

(a) True

(b) False

22.25. An individual's private key is known only to them and the person with whom they are communicating.

(a) True

(b) False

22.26. One difference between public key cryptography and symmetric key cryptography is the number of keys.

(a) True

(b) False

22.27. If an individual signs a message with their private key, this act carries with it non-repudiation.

(a) True

(b) False

22.28. Public key cryptography can be used to exchange messages that result in a symmetric cipher key.

(a) True

(b) False

22.29. The use of public key cryptography is much faster than the use of symmetric key cryptography.

(a) True

(b) False

22.30. The calculations involved in the Diffie-Hellman algorithm are

(a) Simple arithmetic

(b) Modular arithmetic

(c) Linear algebra

22.31. The Diffie-Hellman algorithm is used to generate a secret key that is shared by two communicating individuals.

(a) True

(b) False 22.32. The problem which states that given g^x and g^y , it is mathematically hard to distinguish the difference between $g^{xy} \bmod p$ and $g^r \bmod p$, where r is random is known as the (a) DDH (b) DLP (c) CDH 22.33.

Among other advantages, the Diffie-Hellman protocol provides authentication. (a) True (b) False 22.34. The RSA public key cryptography algorithm involves which of the following? (a) Encryption (b) Decryption (c) Key generation (d) All of the above (e) None of the above

22.35. The size of the modulus n employed in the RSA algorithm is an indication of the size of the key. (a) True (b) False 22.36. The modulus employed in the RSA algorithm is composed of two primes. It is safer to have one prime much larger than another. (a) True (b) False

22.37. While digital signatures can be used for authentication, they cannot be used for non-repudiation. (a) True (b) False 22.38. When RSA signatures are employed, the processes of encryption and decryption provide sufficient information so that anyone who knows the public key can verify the signature. (a) True (b) False

22.39. The security of the DSS is predicated upon the hardness of the (a) DDH (b) DLP (c) CDH (d) None of the above 22.40. Since public keys are by definition public, there is no need to have a public key infrastructure for their authentication. (a) True (b) False 22.41. Public key cryptography is more useful than symmetric key cryptography because (a) There are more keys involved (b)

The computation is easier (c) All of the above (d) None of the above

22.42. Which of the following techniques employ symmetric cryptography after public key cryptography is used to establish a shared secret?

- (a) SSL
- (b) PGP
- (c) IPsec
- (d) All of the above
- (e) None of the above

22.43. To obtain the same strength, the keys for AES and RSA bear the following relationship:

- (a) Both keys are the same length
- (b) The AES key is shorter than the RSA key
- (c) The RSA key is shorter than the AES key

22.44. The two commonly used families of ECC are useful because they are both very efficient in software.

- (a) True
- (b) False

22.45. In the D-H key exchange protocol, D-H may be used over ECC.

- (a) True
- (b) False

22.46. Certicom.com sponsors a challenge in which the problem is given n , find two primes p and q such that $pq = n$.

- (a) True
- (b) False

22.47. The recommended key sizes for D-H and RSA are typically smaller than those of ECC.

(a) True

(b) False

22.48. The authenticity of public keys is based upon a

(a) Public key certificate

(b) Public key infrastructure

(c) All of the above

(d) None of the above

22.49. A signed statement specifying a key and the identity of the person/organization using it is called a

(a) Certificate authority

(b) Certificate

(c) None of the above

22.50. When a computer leaves the factory it contains the CA's public key in a certificate.

(a) True

(b) False

22.51. Alice can verify Amazon's public key using her private key.

(a) True

(b) False

22.52. If a website does not have any security, then only HTTP can be safely used.

(a) True

(b) False 22.53. The presence of a lock at the bottom of a website is normally an indication that SSL is being used.

(a) True (b) False (c) None of the above 22.54. By

clicking on the proper icons in a browser, one can actually see the certificate of a website. (a) True (b) False

22.55. The X.509 certificate format contains a category called Extensions. This category contains the CRL which is

the (a) Certificate record length (b) Certificate revocation list (c) Constraint record list 22.56. The number of classes of digital signatures introduced by Verisign is (a) 3 (b) 5 (c) 7 (d) None of the above 22.57. Verisign's class of digital signatures for online business transactions between companies is (a) 2 (b) 4 (c) 6 (d) None of the above 22.58. Verisign could be referred to as a trusted root authority. (a) True (b) False 22.59. Verisign, with its various classes of digital signatures, is the only certificate authority contained within a computer when it is manufactured. (a) True (b) False 22.60. The X.509 authentication service standard specifies a cryptographic algorithm. (a) True (b) False 22.61. The importance of the CRL stems from the fact that a host/router/switch cannot be configured to check traffic against this list. (a) True (b) False 22.62. Suite B of the NSA security standards is considered more secure than Suite A. (a) True (b) False 22.63. The NSA Suite B of security standards contains which of the following? (a) SHA-512 (b) AES with 128 bit keys (c) ECDH for key agreement (d) All of the above

22.64. Within the U.S. Government, SHA-384 can be used for top secret material.

(a) True

(b) False

22.65. The following protocols are specified by the Entity Authentication Standard in public key algorithms for generating and verifying digital signatures:

(a) ECP

(b) MAP

(c) UAEP

(d) None of the above

22.66. Like symmetric key cryptography, public key cryptography is also vulnerable to side channel attacks.

(a) True

(b) False

22.67. The viable standards for email security include which of the following?

- (a) S/MIME
- (b) MD5
- (c) PGP
- (d) All of the above

22.68. Both of the standards, PGP/MIME and OpenPGP, use MIME to accommodate more media (such as images) and structure in their messages.

- (a) True

- (b) False

22.69. OpenPGP supports cryptographic algorithms that encompass which of the following?

- (a) Symmetric cryptography

- (b) Public key cryptography

- (c) Hash

- (d) All of the above

- (e) None of the above

22.70. ElGamal is an algorithm that supports symmetric key cryptography.

- (a) True

- (b) False

22.71. IDEA is an algorithm that supports public key cryptography.

- (a) True

- (b) False

22.72. MD5 is a hash algorithm.

- (a) True

- (b) False

22.73. PGP combines some of the best features of both symmetric and public key cryptography.

- (a) True
- (b) False

22.74. The data compression employed in PGP enhances its resistance to cryptanalysis.

- (a) True
 - (b) False
- 22.75. A software package that turns a computer into a secure phone is known as (a) IDEAPhone (b) PGPfone (c) OpenPGPfone
- 22.76. S/MIME provides authentication through encryption and confidentiality with digital signatures. (a) True (b) False
- 22.77. The signature algorithm employed in both S/MIMEv3 and OpenPGP is based upon DSS or RSA. (a) True (b) False

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

CHAPTER 23 PROBLEMS

- 23.1. Using a table, compare the differences and similarities that exist between the datagram transport layer security (DTLS) and TLS, including protocols employed, encryption methods and the like.
- 23.2. Outline in tabular form the differences between SSL 3.0 and TLS 1.0 for generating a set of keys for the record protocol.
- 23.3. Use screen captures to illustrate the EV-SSL representations in IE, Chrome, Firefox, and Safari.
- 23.4. Using a table, compare the following properties for both the handshake and record protocols: confidentiality, the message authentication code, and the key derivation process.
- 23.5. Determine the key block lengths required to support a secure channel for the record protocol when AES-128 in CBC mode and SHA-1 are used.
- 23.6. Determine the key block lengths required to support a secure channel for the record protocol when AES-128 in CBC mode and SHA-256 are used.
- 23.7. Determine the key block lengths required to support a secure channel for the record protocol when AES-256 in CBC mode and SHA-256 are used.
- 23.8. Determine the key block lengths required to support a secure channel for the record protocol when 3DES in CBC mode using 112-bit key and SHA-1 are used.
- 23.9. Determine the key block lengths required to support a secure channel for the record protocol when 3DES in CBC mode using 168-bit key and SHA-1 are used.
- 23.10. Will a web server and a client host each use the same set of keys for protecting packets delivered to one another? If so, why, and if not, why not?
- 23.11. When the client side uses a password for authentication, describe how the SSL/TLS protects this password.

23.12. Does the Firefox browser use the same set of trusted root CA certificates that are installed in a Windows or MAC OS X PC? In addition, when an organization issues certificates by its own CA, describe what a user must do in order to achieve the correct browser behavior when visiting the internal web sites using the organization issued certificates?

23.13. Repeat Problem 23.8 for the Google Chrome browser.

23.14. The set of allowed cipher suites for most browsers includes, by default, RC4 for encryption with a 40 bit key. There was a limited choice of cipher suites for browsers and servers, and cipher suites with RC4 were typically chosen first. Most server implementations do not allow the server administrator to specify a preference order for ciphers. What must a server administrator do to ensure SSL/TLS security between browsers and the server?

23.15. Describe the importance of specifying the key lengths used in the cipher suites for both clients and servers.

23.16. List all crypto schemes available in TLS version 1.2 (RFC 5246). 23.17. SSL/TLS employs the message

authentication code. (a) True (b) False 23.18. SSL/TLS uses two protocols. It first uses the record protocol and then the handshake protocol. (a) True (b) False 23.19.

The handshake protocol uses symmetric key cryptography to establish a shared secret key. (a) True (b) False

23.20. In the handshake protocol, the server is authenticated using the shared secret. (a) True (b) False

23.21. The final step in the handshake protocol is the development of a symmetric key cipher. (a) True (b) False

23.22. The ClientHello employs a nonce, which is nothing more than a random number that is used only once. (a)

True (b) False 23.23. In the handshake protocol, the ClientHello and ServerHello are done in plaintext. (a)

True (b) False 23.24. In the handshake protocol, the ServerHello contains the lowest grade security protocol that can be supported by both client and server (a) True

(b) False 23.25. In the execution of the SSL/TLS process, the record protocol is initiated once all the handshake messages have been exchanged. (a) True (b) False 23.26.

SSL version 2 is the recommended for use in the handshake protocol. (a) True (b) False 23.27. The application layer data in the packet format for the SSL/TLS record protocol is split into multiple sections, each of which has a maximum of (a) 32K bits (b) 64K bits (c) 128K bits

(d) 256K bits 23.28. The number of categories used for Content Type in the record protocol is (a) 2 (b) 3 (c) 4 (d) 5

23.29. The length of the master secret, shared between client and server, in SSL/TLS applications is

- (a) 24 bytes
- (b) 46 bytes
- (c) 64 bytes

23.30. The hashing method used by SSL is the same as that used in TLS.

- (a) True
- (b) False

23.31. Diffie-Hellman and the Digital Signature Algorithm are used to encrypt in SSL/TLS applications.

- (a) True
 - (b) False
- 23.32. The guidelines for EV-SSL are produced by the
- (a) IETF
 - (b) CA/Browser Forum
 - (c) IRS
 - (d) None of the above

23.33. EV-SSL is applicable with

- (a) Firefox
- (b) Linux
- (c) IE7
- (d) All of the above
- (e) None of the above

23.34. OpenSSL can be used by an organization to create its

own CA.

- (a) True
- (b) False

23.35. The core library for OpenSSL is written in the C programming languages.

- (a) True
- (b) False

23.36. A self-signed certificate is a necessary ingredient for creating a CA.

- (a) True
- (b) False

23.37. Prior to installing a new certificate for IIS, the default certificates must be removed.

- (a) True
- (b) False

23.38. When installing a new certificate for IIS, IIS need not have a private key.

- (a) True
- (b) False

23.39. An organization can establish its own CA for its private network by creating a selfsigned root CA certificate and installing it in the organization's host OS/browser.

- (a) True
- (b) False

23.40. A self-signed certificate must be imported into Firefox.

- (a) True
 - (b) False
- 23.41. When shopping at amazon.com, the client's credit card number is encrypted by
- (a) Amazon's public key

(b) Amazon's private key (c) Client's private key (d) A symmetrical key established in the handshake protocol (e) None of the above 23.42. Windows uses the ___ file format certificate. (a) der (b) pem (c) p12 (d) All of the above (e) None of the above 23.43. ___ format file may contain a private key. (a) pem (b) p12 (c) der (d) All of the above (e) None of the above 23.44. Firefox and IE use the same set of trusted root CA certificates. (a) True (b) False 23.45. Apache uses httpd-ssl.conf file for specifying the files that contain the certificate and private key of the website. (a) True (b) False 23.46. When generating keys in handshake protocol, ___ is used to produce a number of keys. (a) RSA (b) Hash (c) Diffie-Hellman (d) All of the above (e) None of the above

24 Chapter 24 - Virtual Private Networks for Network Layer Security

24.6. Describe the differences between the IKE SA and IPsec SA by specifying their purposes and the method of computation.

24.7. Describe the differences between the SSL-based VPN and IPsec-based VPN by comparing their client software, protection mechanisms, protocols and the applications supported.

24.8. Which IPsec mode is better for protection against traffic analysis?

24.9. Compare the similarities and differences between the SSL Hello protocol and the IKE protocol.

24.10. Compare the similarities and differences between IKE phase 2 exchanges and a SSL/TLS session resumption.

24.11. Compare the similarities and differences between an IKE Child SA and a SSL/TLS record protocol.

24.12. Describe the reason IETF developed the IPsec standards since SSL/TLS standards are available for deploying applications.

24.13. Describe the relationship between IKE and ESP.

24.14. Is an encryption key used for encrypting communication between two ends?

24.15. What is the recommended lifetime for IKE Security Associations according to SP 800-77?

24.16. Describe the risk of long lifetimes for IKE Security Associations when the same key derived from a Diffie-Hellman exchange is repetitively used for rekeying.

24.17. Describe the requirements for Diffie-Hellman (DH) groups in generating the required security strength for IPsec ESP tunnels.

24.18. Describe the IPsec crypto requirements specified in SP 800-77.

24.19. Describe the differences that exist between the transport and tunnel modes.

24.20. Does tunnel mode cause any problems with NAT?

24.21. IPsec provides open standards for secure communication over the transport layer.

(a) True

(b) False

24.22. Every protocol running on top of IPv4 and IPv6 is protected by IPsec.

(a) True

(b) False

24.23. IPsec is composed of which of the following components?

(a) IKE

(b) ESP

(c) AH

(d) IPcomp

(e) All of the above 24.24. The authentication header used with IPsec provides confidentiality and integrity. (a)

True (b) False 24.25. The ESP portion of IPsec provides keys for AH. (a) True (b) False 24.26. The IPsec modes are referred to as transport and tunnel. (a) True (b)

False 24.27. The tunnel mode of IPsec provides host-to-host protection. (a) True (b) False 24.28. IPsec provides network-to-network security through a secure channel across insecure networks in the following mode:

(a) Transport (b) Tunnel 24.29. IPsec in the tunnel mode protects internal traffic behind a VPN gateway. (a) True (b) False 24.30. IPsec in the tunnel mode uses a VPN from router-to-router across the Internet. (a) True (b) False

24.31. Which of the following modes can be used by IPsec in the host-to-gateway configuration? (a) Transport (b) Tunnel (c) All of the above 24.32. The tunnel mode employs the original IP header. (a) True (b) False

24.33. The Security Association specifies the methods and modes for packet protection. (a) True (b) False 24.34. An SPI is used to uniquely identify each SA. (a) True (b) False 24.35. ESP adds new header and trailer fields to every packet. (a) True (b) False 24.36. In the implementation of ESP security, if a new header is used,

the TCP/UDP segment and ESP trailer are encrypted and that combination together with the ESP header is authenticated, the mode of operation is the (a) Transport mode (b) Tunnel mode

24.37. The encrypted portion of the ESP packet contains

- (a) The payload
- (b) Padding information
- (c) The next header
- (d) All of the above
- (e) None of the above

24.38. A sender uses AH to support authentication using HMAC.

- (a) True
- (b) False

24.39. Sender and receiver share a secret key, set up by the SA, that is used in the HMAC computation in AH.

- (a) True
- (b) False

24.40. In the IP header, which contains mutable, immutable and predictable fields, the only field that is predictable with loose or strict source routing is the destination address.

- (a) True
- (b) False

24.41. The IP header is the same whether the transport mode or tunnel mode is used.

- (a) True
- (b) False

24.42. When a sliding window is used for the prevention of replay attacks, the sliding window on the recipient's end slides whenever a packet is received.

(a) True

(b) False

24.43. The manual mode for key management in IPsec is performed through the use of preshared symmetric keys which are exchanged online without any hashing.

(a) True

(b) False

24.44. Diffie-Hellman used with IKE can be configured to provide perfect forward secrecy.

(a) True

(b) False

24.45. The cookies used in Photuris are the same as those used in a browser.

(a) True

(b) False

24.46. One of the methods of authentication used with IKE is a RSA digital signature using a DSS private key.

(a) True

(b) False

24.47. IKE employs two phases because it is more economical to do so.

(a) True

(b) False

24.48. A dead peer cannot be detected by the IKE/IPsec protocol.

(a) True

(b) False 24.49. NAT works in conjunction with AH in IKE.

(a) True (b) False 24.50. NAT changes the original IP header in the ESP protocol. (a) True (b) False 24.51. In order for IPsec to work through a NAT, the following UDP

ports must be permitted on the firewall: (a) 50 (b) 500
(c) 4500 (d) All of the above (e) None of the above

24.52. When establishing a VPN in Windows 7/Vista, only the user name and password are required. (a) True (b) False

24.53. The Microsoft VPN is compatible with IPsec/IKE. (a) True (b) False

24.54. L2TP is actually a data link layer protocol. (a) True (b) False

24.55. When using a VPN in Windows 7/Vista, the default gateway is provided by the ISP or an organization. (a) True (b) False

24.56. When applied for use in Windows 7/Vista, the pre-shared secret is more secure than a certificate. (a) True (b) False

24.57. OCSP can be used to obtain the revocation status of a X.509 digital certificate. (a) True (b) False

24.58. Microsoft's Internet security and acceleration (ISA) server provides which of the following? (a) Firewall (b) VPN

(c) IPS (d) All of the above (e) None of the above

24.59. One of the items that ISA supports is VPN monitoring. (a) True (b) False

24.60. A gateway-to-gateway VPN employing a Cisco VPN appliance will employ a RSA public and private key pair.

(a) True

(b) False

24.61. The SCEP used to request a certificate from a CA using a Windows Server has resulted from collaboration between Cisco and Microsoft.

(a) True

(b) False

24.62. The child SA must use a new D-H key in order to derive a session key.

(a) True

(b) False

24.63. When the IKE is used with a pre-shared secret, no Diffie-Hellman is used for establishing a secret key.

(a) True

(b) False

24.64. The responder must save the cookie sent to the initiator in order to verify the cookie sent back by the

initiator.

(a) True

(b) False

24.65. The cookie of IKE is designed for

(a) Authentication

(b) Encryption

(c) Prevent DDoS attacks

(d) All of the above

(e) None of the above

25 Chapter 25 - Network Access Control and Wireless Network Security

13. IEEE Std. 802.1X-2004 IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control, 2004;
<http://standards.ieee.org/getieee802/portfolio.html>.
14. C. De Laat, G. Gross, L. Gommans, J. Vollbrecht, and D. Spence, RFC 2903: Generic AAA Architecture, 2000.
15. B. Aboba and P. Calhoun, RFC 3579: RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP), 2003.
16. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, RFC 3748: Extensible Authentication Protocol (EAP), 2004.
17. B. Aboba, D. Simon, and P. Eronen, RFC 5247: Extensible Authentication Protocol (EAP) Key Management Framework, 2008.
18. F. Bersani and H. Tschofenig, RFC 4764: The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method, 2007.
19. D. Simon, B. Aboba, and R. Hurst, RFC 5216: The EAP-TLS Authentication Protocol, 2008.
20. H. Haverinen and J. Salowey, RFC 4186: Extensible authentication protocol method for global system for mobile communications (GSM) subscriber identity modules (EAP-SIM), 2006.
21. J. Arkko and H. Haverinen, RFC 4187: Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) Is, 2006.
22. N. Cam-Winget, D. McGrew, J. Salowey, and H. Zhou, RFC 4851: The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST), 2007.
23. P. Funk and S. Blake-Wilson, RFC 5281: Extensible authentication protocol tunneled transport layer security authenticated protocol version 0 (EAP-TTLSv0), 2008.
24. NIST, SP 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, 2007; <http://csrc.nist.gov/publications/PubsSPs.html>.

25. C. Rigney, A. Rubens, W. Simpson, and others, RFC 2865: Remote authentication dial in user service, 2000.
26. L. Blunk and J. Vollbrecht, RFC 2284: PPP Extensible Authentication Protocol (EAP), 1998.
27. NIST, SP 800-46 Rev. 1: Guide to Enterprise Telework and Remote Access Security, 2009; <http://csrc.nist.gov/publications/PubsSPs.html>.
28. Cisco Systems, "Cisco NAC Appliance [Cisco NAC Appliance (Clean Access)]"; <http://www.cisco.com/>
29. Joel Snyder, "NAC: What went wrong?", May. 2010;
30. Trusted Computing Group, TCG Spec.: TCG Architecture Overview, Version 1.4, 2007; <http://www>.
31. Trusted Computing Group, TCG Spec.: Federated TNC Version 1.0, Revision 26, 2009; <http://www>.
32. Trusted Computing Group, TCG Spec.: TNC Architecture for Interoperability Specification Version 1.4, Revision 4, 2009;
33. Trusted Computing Group, TCG Spec.: TNC IF-MAP Binding for SOAP Specification, 2009; <http://>
34. Trusted Computing Group, TCG Spec.: TNC IF-T Binding to TLS Version 1.0, Revision 16, 2009; <http://>
35. P. Sangster, H. Khosravi, M. Mani, K. Narayan, and J. Tardo, RFC 5209: Network Endpoint Assessment (NEA): Overview and Requirements, 2008; <http://tools.ietf.org/html/rfc5209>.
36. G. Camarillo, RFC 5694: Peer-to-Peer (P2P) Architecture: Definition, Taxonomy, 2009; <http://tools.ietf.org/html/rfc5792>.
37. R. Sahita, Hanna, R. Hurst, and K. Narayan, RFC 5793: PB-TNC: A Posture Broker (PB) Protocol Compatible with Trusted Network Connect (TNC), 2010; <http://tools.ietf.org/html/rfc5793>.

CHAPTER 25 PROBLEMS

- 25.1. A user/client accesses a resource using the TGS in Kerberos. Describe the key that is most frequently used by

the user/client. What protection measure can be employed to improve the use of this key?

25.2. Describe the authentication procedure differences that exist between a home wireless network and an enterprise wireless network in terms of the key derivation methods and user credentials.

25.3. Describe the purpose of a 4-way handshake in an enterprise wireless network. 25.4. Describe the crypto requirements for an AS in order to provide authentication for an enterprise wireless network. 25.5. Describe the differences that exist between bind a key and seal a key when used in TPM. 25.6. Describe the methods employed to protect (a) a TPM key hierarchy when keys are exported and (b) the use of keys within the hierarchy. 25.7. Most teleworkers use remote access technologies to interface with an organization's non-public computing resources. Identify the security risks that accompany this remote access. 25.8. Describe the basic requirements for protecting client devices and communication channels used in remote access. 25.9. Describe the manner in which to develop a telework security policy that defines remote access requirements. 25.10. Describe the risk of compromising a remote access server by using a telework client device and the strategy for protecting it. 25.11. Describe the manner in which to secure telework client devices against common threats and maintain their security on a regular basis. 25.12. For legacy IEEE 802.11 equipment that does not provide CCMP or WPA2, describe an alternative security protection. 25.13. Compare the security of authentication provided by the two methods: EAP-TLS and EAP-TTLS. 25.14. Describe how to ensure the confidentiality and integrity of communications between access points and authentication servers. 25.15. Describe the risks associated with enabling the ad hoc mode in a PC or device and the attendant security measures. 25.16. Describe the risks associated with connecting a host to an unauthorized AS and the attendant security measures. 25.17. Describe a maximum PMK lifetime on an AS, as specified in NIST SP 800-97. 25.18. Describe the manner in which to segregate the APs from other network components to improve security for critical information assets. 25.19. Host health inspection can be categorized as (a) Agent-less (b) Agent-based (c) Server-/appliance-/peer-based (d) All of the above (e) None of the above 25.20. Agent-less inspection is a peer-to-peer inspection. (a) True (b) False

25.21. There is no need to monitor a healthy host that has

been permitted to join a network.

(a) True

(b) False

25.22. The NAC policies typically deal with which of the following items?

(a) Auditing

(b) Blocking

(c) Monitoring

(d) Security

(e) All of the above

(f) None of the above

25.23. The NAC policy that inspects the logs and activities as they relate to policies is

(a) Monitoring

(b) Auditing

(c) Security

(d) None of the above

25.24. Authentication is required in order to access resources in the network.

(a) True

(b) False

25.25. If a user is known to a network, then the things that user can do are also known to the network and can be found on an

(a) Authentication list

(b) Authorization list

(c) Access control list

(d) None of the above

25.26. Centralized access control provides a single point of failure.

- (a) True
- (b) False

25.27. The authentication scheme based on the Needham-Schroeder protocol is

- (a) NAP
- (b) TPM
- (c) Kerberos
- (d) None of the above

25.28. Kerberos employs a KDC that consists of

- (a) AS
- (b) TGS
- (c) All of the above
- (d) None of the above

25.29. In the Kerberos process, the ticket used to access a resource is called the

- (a) Authentication ticket
- (b) Service ticket
- (c) TGS ticket

25.30. The user accessing a resource must know the shared key used between TGS and the server.

- (a) True
 - (b) False
- 25.31. The user accessing a resource has no knowledge of the shared key between AS and TGS. (a) True
(b) False
- 25.32. A ticket permits mutual authentication between a user and a resource. (a) True (b) False
- 25.33. Kerberos employs public keys that are shared by the parties involved. (a) True (b) False
- 25.34. If the distance among users becomes large in a wide area network and the

network must be divided into realms, a realm in this context is equivalent to a domain in a Microsoft AD tree.

(a) True (b) False 25.35. Kerberos authentication is accomplished using time-stamped increments. (a) True (b) False 25.36. The only encryption scheme used with Kerberos is DES. (a) True (b) False 25.37. Which of the following applications uses Kerberos? (a) MS Windows (b) Mac OS (c) Email (d) FTP (e) All of the above 25.38. A TPM on a laptop motherboard stores passwords, digital keys and certificates. (a) True (b) False 25.39. The function blocks within the TPM are protected by software-based cryptography. (a) True (b) False 25.40. TPM has a limited number of applications. (a) True (b) False

25.41. The authentication server used in conjunction with 802.1X employs such things as (a) AD (b) Kerberos (c) LDAP (d) RADIUS (e) All of the above (f) None of the above

25.42. When a new client is connected to an authenticator using the 802.1X protocol, the authenticator's port is enabled and set to the "authorized" state.

(a) True

(b) False

25.43. 802.1X requires the use of a backend authentication server.

(a) True

(b) False

25.44. EAP was designed for network access authentication in situations where IP layer connectivity may not be available.

(a) True

(b) False

25.45. If a protocol uses EAP, then that protocol defines a means by which EAP messages are encapsulated within it.

(a) True

(b) False

25.46. The RADIUS protocol provides decentralized AAA for a user to access a network service.

(a) True

(b) False

25.47. The authenticator field used to authenticate the reply from a RADIUS server uses

(a) 8 octets

(b) 24 octets

(c) 32 octets

(d) None of the above

25.48. WPA-2 with AES in the counter mode provides good security.

(a) True

(b) False

25.49. Home users with little knowledge of wireless security can use WPS to configure WPA.

(a) True

(b) False

25.50. IBSS is supported by WPS.

(a) True

(b) False

25.51. One of the methods for implementing WPS is Near Field Communication.

(a) True

(b) False

25.52. Which of the following is not a method for implementing WPS?

(a) PIN

(b) BCP

(c) USB

25.53. The out-of-band methods for implementing WPS are NFC and PBC.

(a) True

(b) False 25.54. The current WPS certification covers only PIN, NFC and USB. (a) True (b) False 25.55. Firewalls, switches and routers are all enforcement points for NAC.

(a) True (b) False 25.56. Symantec and McAffie provide products that support NAP solutions. (a) True (b) False 25.57. To achieve remote access control between a SOHO with a Wi-Fi router and a corporate network, a VPN tunnel can be employed. (a) True (b) False 25.58. HCAP is used to provide communication between a NAC posture validation server and an ACS. (a) True (b) False 25.59. CCMP uses ___ key(s) for both encryption and authentication. (a) 1 (b) 2 (c) 3 (d) None of the above 25.60. The message authentication code encrypted by CTR becomes MIC. (a) True (b) False 25.61. CCMP allows the reuse of PN in the nonce for a given session key. (a) True (b) False 25.62. WiFi can use ___ to secure a wireless LAN. (a) WPA (b) WPA2 (c) WEP (d) None of the above 25.63. CCMP uses the same keystream for both CTR and CBC-MAC. (a) True (b) False

26 Chapter 26 - Cyber Threats and Their Defense

1. "An Illustrated Guide to the Kaminsky DNS Vulnerability";
<http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html>.
2. B. Halley, "How DNS cache poisoning works," 2008;
<http://www.networkworld.com/news/tech/2008/102008-tech-update.html?page=1>.
3. K. Davies, "2008 DNS Cache Poisoning Vulnerability," 2008; <http://74.125.47.132/search?q=2008+dns+cache+poisoning+vulnerability>
4. O. Kolkman, J. Schlyter, and E. Lewis, RFC 3757: Domain Name System KEY (DNSKEY) Resource Record (RR) Secure Entry Point (SEP) Flag, 2004.
5. R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, RFC 4033: DNS security introduction and requirements, 2004.
6. R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, RFC 4034: Resource records for the DNS security extensions, 2005.
7. R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, RFC 4035: Protocol modifications for the DNS security extensions, 2005.
8. W. Hardaker, RFC 4509: Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs), 2006.
9. O. Kolkman and R. Gieben, RFC 4641: DNSSEC operational practices, 2005.
10. NIST, SP 800-81r1: Secure Domain Name System (DNS) Deployment Guide, 2010; <http://csrc.nist.gov/publications/PubsSPs.html>.
11. EURid, "Overview of DNSSEC deployment worldwide";
http://www.eurid.eu/files/Insights_DNSSEC1.pdf.
12. dnssec-deployment.org, "TLD deployment Table";
https://www.dnssec-deployment.org/wp-content/uploads/2010/08/TLD-deployment-Table_8_30_10.pdf.
13. D. Kaminsky, "Phreebird";
<http://dankaminsky.com/phreebird/>.

14. A. Heffernan, RFC 2385: Protection of BGP sessions via the TCP MD5 signature option, 1998.

15. M. Wong and W. Schlitt, RFC 4408: Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1, 2006.

16. E. Allman, J. Callas, M. Delany, M. Libbey, J. Fenton, and M. Thomas, RFC 4871: Domainkeys identified mail (DKIM) signatures, 2007.

17. J. Galvin, S. Murphy, S. Crocker, and N. Freed, RFC 1847: Security Multiparts for MIME: Multipart, 1995.

18. J. Callas, L. Donnerhacke, H. Finney, and R. Thayer, "RFC 2440: OpenPGP message format," 1998.

19. G. Appenzeller, L. Martin, and M. Schertler, RFC 5408: Identity-Based Encryption Architecture and Supporting Data Structures, 2009. 20. X. Boyen and L. Martin, RFC 5091: Identity-Based Cryptography Standard (IBCS)(Version 1), Request for Comments (RFC) 5091, 2007. 21. L. Martin and M. Schertler, RFC 5409: Using the Boneh-Franklin identity-based encryption algorithm with the Cryptographic Message Syntax (CMS), 2009. 22. NIST, SP 800-45v2: Guidelines on Electronic Mail Security, 2007; <http://csrc.nist.gov/publications/PubsSPs.html>. 23. "Net threats: State of the Net";

53. Cisco 2008 Annual Security Report, 2009;

54. J. Riden, "HOW FAST-FLUX SERVICE NETWORKS WORK | The Honeynet Project"; <http://www.honeynet.org/node/132>.

55. "MessageLabs Intelligence: 2009 Annual Security Report"; <http://www.message-labs.com/resources/mlireports>.

56. G. Keizer, "Researchers turn Conficker's own P2P protocol against itself," 2009;

57. B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna, Your botnet is my botnet: Analysis of a botnet takeover, CS, UCSB, 2009.

58. Symantec, Symantec Report on the Underground Economy, Symantec Corporation, 2008; <http://eval>.

CHAPTER 26 PROBLEMS

26.1. Summarize the security features provided by DNSSEC using the format of the following table: Keys/RR Key updating Signing Verifying signature Zone Signing Key (ZSK) No interaction with the parent is needed NS RRset, RRSIG(... Signature validity periods on the order of days; Use the public key of ZSK to verify signature,... Key Signing Key (KSK) RRSIG ... DS RR ... NSEC

26.2. Summarize the operations involved in the authentication chain (chain of trust) from a parent zone to a child zone using a pseudo code format. The anchor originates at the root name server.

26.3. Summarize the differences and similarities that exist for the following approaches to email security: SPF, DKIM, S/MIME, and OpenPGP, i.e., for each of these techniques compare such things as the method employed, what it defends, use of compression, use of authentication, integrity, confidentiality, the type of signature, etc.

26.4. In tabular form list the various router attack methods together with a description of each and their corresponding defensive measures.

26.5. Describe the causes for Denial of Service on a DNS server equipped with DNSSEC.

26.6. Describe the relative frequency of use for KSK and ZSK as well as their relative key sizes.

26.7. Describe the differences that exist in the key management models used by OpenPGP and S/MIME to establish trust using digital certificates.

26.8. Describe the reasons why perimeter-based network security technologies, e.g., firewalls, are inadequate, according to NIST SP 800-95, in protecting SOAs.

26.9. Describe the major difficulties in providing secure/reliable web services. 26.10. Describe the mitigation procedures used to address the difficulties identified in Problem 26.5. 26.11. Describe the basic policy for log management. 26.12. Describe how to protect XML content in web service messages. 26.13. Describe how to create and maintain a log management infrastructure. 26.14. Describe the importance of log protection and the associated risks. 26.15. Describe the difference between SIEM and Syslog products. 26.16. When the DNS mapping is forged so that a website's traffic is redirected to a bogus website, this may result from (a) Cache poisoning (b)

Pharming (c) All of the above 26.17. When a fake address record for an Internet domain is inserted into the DNS and accepted by the server, this is known as (a) Cache poisoning (b) Pharming (c) None of the above 26.18. The TTL for cached DNS entries is so short that little damage is done when a DNS cache is poisoned. (a) True (b) False 26.19. An individual who visits a bogus website runs the risk of losing personal information and the control of the computer. (a) True (b) False 26.20. DNS responses from the Internet resulting from DNS queries are generally believed because of the inherent authentication it provides. (a) True (b) False 26.21. The best approach for the prevention of cache poisoning was discovered by Dan Kaminsky. (a) True (b) False 26.22. While open source DNS servers have been compromised with cache poisoning, the TLD servers are immune from this attack. (a) True (b) False 26.23. Randomizing the ___ port of a recursive server is a short term solution for preventing cache poisoning of DNS. (a) Source (b) Destination (c) All of the above (d) None of the above

26.24. Randomizing the source port for a recursive server is effective at preventing cache poisoning for DNS behind a NAT.

(a) True

(b) False

26.25. DNSSEC is an effective protection mechanism for cache poisoning.

(a) True

(b) False

26.26. The goals of DNSSEC are to provide

(a) Authentication

(b) Integrity

(c) Confidentiality

(d) DDoS protection

(e) All of the above

26.27. The RR for DNSSEC that enables the DNS server to inform the client that a particular domain or type does

not exist is

- (a) DNSKEY
- (b) RRSIG
- (c) DS
- (d) NSEC

26.28. If a router is flooded with more packets than it can handle, the router is said to be under a

- (a) Cache poisoning attack
- (b) DoS attack
- (c) Spoofing attack

26.29. Peer IP addresses can often be found using the ICMP traceroute function.

- (a) True
- (b) False

26.30. ICMP can be used to provide session resets between two peer routers.

- (a) True
- (b) False

26.31. Router overload caused by rapid repetitive changes to the BGP routing table is termed a

- (a) Route de-aggregation attack
- (b) Router flapping
- (c) None of the above

26.32. BGP authentication is one of the best techniques for preventing router security problems.

- (a) True
- (b) False

26.33. The following authentication mechanisms are viable

for combating router security problems:

(a) IPsec

(b) BGP MDS

(c) All of the above

(d) None of the above 26.34. Spammers can hide their true identity by sending messages from forged IP addresses. (a)

True (b) False 26.35. Internet domains that employ SPF

are unable to reject messages from unauthorized hosts

prior to receiving the body of the message. (a) True (b)

False 26.36. The domain-level authentication framework for email, known as DKIM, uses symmetric key cryptography and key server technology. (a) True (b) False 26.37. When

DKIM is employed the verification of the source and message contents is performed by (a) MTAs (b) MUAs (c) All of the above (d) None of the above 26.38. While DKIM is

effective against SPAM, there is no confidentiality. (a) True (b) False 26.39. DKIM takes the same approach to message signing as those used with S/MIME and OpenPGP.

(a) True (b) False 26.40. DKIM is compatible with DNSSEC.

(a) True (b) False 26.41. An individual masquerading as a trustworthy entity in some form of electronic communication to obtain sensitive information is said to be phishing.

(a) True (b) False 26.42. Spear-phishing emails, while a problem, have a low rate of success as a result of their inability to effectively mimic messages from an authoritative source. (a) True (b) False 26.43. Once a phishing website is accessed, it is probably too late to prevent damage to the computer. (a) True (b) False

26.44. Common phishing techniques include (a) A confusing URL (b) A redirection of the URL (c) All of the above

26.45. An individual can be confident that the website being visited is a valid one when HTTPS and a lock are both present in the site.

(a) True

(b) False

26.46. In a web-based attack, the inadequate validation of user input may occur as a result of which of the following?

(a) HTTP response splitting

(b) SQL injection

- (c) XSS
- (d) All of the above

26.47. A number of illegal web-based attack kits can be purchased cheaply on the black market.

- (a) True
- (b) False

26.48. Responsible companies that do business on the Internet do not employ cookies.

- (a) True
- (b) False

26.49. The execution of a malicious script on a victim's browser is an attack known as

- (a) SQL injection
- (b) XSS
- (c) None of the above

26.50. XSS attacks are platform (OS) dependent.

- (a) True
- (b) False

26.51. If the URL for a legitimate website contains additional text, the URL cannot be trusted.

- (a) True
- (b) False

26.52. MySpace allows users to post HTML pages containing scripts.

- (a) True
- (b) False

26.53. IBM Smash that works in conjunction with AJAX can proactively check information through authentication to

ensure that it has come from the right source.

(a) True

(b) False

26.54. When an attacker places another website beneath the buttons on a legitimate website the attack is called a clickjacking attack.

(a) True

(b) False

26.55. ___ is the most effective defense measure for a clickjacking attack.

(a) Not clicking a URL

(b) Disable script in a browser

(c) Filtering untrusted website

(d) None of the above 26.56. The underlying issue that supports the execution of a XSS DNS attack is a short TTL.

(a) True (b) False 26.57. The most effective database

attack appears to be (a) Clickjacking (b) SQL injection

(c) XSS DNS (d) None of the above 26.58. A successful SQL

injection attack can be used to gain administrator

privilege on a system. (a) True (b) False 26.59. A

combination of tools are needed for protection against a SQL injection attack. (a) True (b) False 26.60. The

nodes of a Botnet are called (a) Trojans (b) Zombies (c)

None of the above 26.61. A botnet is an excellent vehicle

for a SQL injection attack because in many situations the

attack appears legitimate on an infected computer. (a)

True (b) False 26.62. Historical data indicates that

iFrame was capable of SQL-injecting thousands of different

websites per day. (a) True (b) False 26.63. The process

in which mal-site operators transfer the task of hosting a

mal-site from one Zombie to another is known as (a)

Fast-flux (b) Domain-name Kiting (c) None of the above

(d) All of the above 26.64. The worm can perform advanced

key logging when infected users access specific web pages.

(a) True (b) False 26.65. From a historical standpoint,

the Storm botnet has managed to eclipse the Srizbi botnet

as the biggest menace on the Internet. (a) True (b) False

26.66. Which of the following networking protocols are

exploited by a DoS attack? (a) Botblast (b) Smurf (c)

SYN Flood (d) All of the above

26.67. The following methods are used to control bots:

- (a) P2P
- (b) IRC
- (c) HTTP
- (d) All of the above
- (e) None of the above

26.68. At least one technique has been developed to defeat one version of the Conficker worm.

- (a) True
- (b) False Emerging Technologies 6

27 Chapter 27 - Network and Information Infrastructure Virtualization

1. "Virtualize Your Business Infrastructure: Benefits of Virtualization, Increase IT Efficiency and Virtual Management";
<http://www.vmware.com/virtualization/index.html>.
2. J.E. Smith and R. Nair, "The architecture of virtual machines," Computer, vol. 38, 2005, pp. 32-38.
3. J. Rutkowska and R. Wojtczuk, "Qubes";
<http://qubes-os.org/trac/>.
4. J. Rutkowska and R. Wojtczuk, "Qubes OS Architecture, Version 0.3," 2010; <http://qubes-os.org/files/doc/arch-spec-0.3.pdf>.
5. J. Sahoo, S. Mohapatra, and R. Lath, "Virtualization: A Survey on Concepts, Taxonomy and Associated Security Issues," 2010 Second International Conference on Computer and Network Technology (ICCNT), 2010, pp. 222-226.
6. K. Adams and O. Agesen, "A comparison of software and hardware techniques for x86 virtualization," Proceedings of the 12th international conference on Architectural support for programming languages and operating systems, 2006, p. 13.
7. J. Fisher-Ogden, "Hardware support for efficient virtualization," UC San Diego Report, USA, 2006.
8. G. Neiger, A. Santoni, F. Leung, D. Rodgers, and R. Uhlig, "Intel virtualization technology: Hardware support for efficient processor virtualization," Intel Technology Journal, vol. 10, 2006, pp. 167-177.
9. R. Uhlig, G. Neiger, D. Rodgers, A.L. Santoni, F.C. Martins, A.V. Anderson, S.M. Bennett, A. Kagi, F.H. Leung, and L. Smith, "Intel virtualization technology," Computer, vol. 38, 2005, pp. 48-56.
10. G. Strongin, "Trusted computing using AMD 'Pacific' and 'Presidio' secure virtual machine technology," Information Security Technical Report, vol. 10, 2005, pp. 120-132.
11. R. Perez, L. van Doorn, and R. Sailer, "Virtualization and Hardware-Based Security," IEEE Security & Privacy, vol. 6, 2008, pp. 24-31.

12. VMware, “Software and Hardware Techniques for x86 Virtualization”; http://www.vmware.com/files/pdf/software_hardware_tech_x86_virt.pdf.
13. M. Rosenblum and T. Garfinkel, “Virtual machine monitors: Current technology and future trends,” Computer, vol. 38, 2005, pp. 39-47.
14. D. Abramson, J. Jackson, S. Muthrasanallur, G. Neiger, G. Regnier, R. Sankaran, I. Schoinas, R. Uhlig, B. Vembu, and J. Wiegert, “Intel virtualization technology for directed I/O,” Intel technology journal, vol. 10, 2006, pp. 179-192.
15. B. Armstrong, “Hyper-V Terminology - Virtual PC Guy’s WebLog - Site Home - MSDN Blogs”; <http://>
16. “What is Xen Hypervisor?”; <http://www.xen.org/files/Marketing/WhatisXen.pdf>.
17. “Xen Overview”; <http://wiki.xensource.com/xenwiki/XenOverview>.
18. T. Shinagawa, H. Eiraku, K. Tanimoto, K. Omote, S. Hasegawa, T. Horie, M. Hirano, K. Kourai, Y. Oyama, E. Kawai, and others, “BitVisor: a thin hypervisor for enforcing i/o device security,” Proceedings of the 2009 ACM SIGPLAN/SIGOPS international conference on Virtual execution environments, 2009, pp. 121-130. 19. “DSP0243: Open Virtualization Format Specification, Version 1.1.0,” 2010; <http://www.dmtf.org/standards/ovf>. 20. N.M. Chowdhury and R. Boutaba, “Network virtualization: state of the art and research challenges,” IEEE Communications magazine, vol. 47, 2009, pp. 20-26. 21. “Network Virtualization for the Campus Solution Overview [Network Virtualization Solutions] - Cisco Systems”;
51. “Unified Computing System - Cisco Systems”; <http://www.cisco.com/en/US/netsol/ns944/index.html#~overview>
52. NIST, SP 800-145: DRAFT A NIST Definition of Cloud Computing, 2011; <http://csrc.nist.gov/publications/PubsSPs.html>.
53. “Cloud Computing and Data Center - Industry Solutions - Cisco Systems”; http://www.cisco.com/web/strategy/government/usfed_data_center.html.

54. NIST, SP 800-144: DRAFT Guidelines on Security and Privacy in Public Cloud Computing, 2011; <http://csrc.nist.gov/publications/PubsSPs.html>.

55. NIST, SP 800-125: Guide to Security for Full Virtualization Technologies, 2011; <http://csrc.nist.gov/publications/PubsSPs.html>.

CHAPTER 27 PROBLEMS

27.1. Describe the differences between hosted virtualization and a hypervisor.

27.2. Describe the advantages of hardware-assisted virtualization over other CPU virtualization methods.

27.3. Describe the important issues associated with network segmentation for virtualization security.

27.4. Describe the differences between VRF Lite and VRF.

27.5. Describe the differences between iSCSI and Fiber Channel.

27.6. Describe the differences between FCoE and Fiber Channel.

27.7. Describe the differences in scope and control between the cloud subscriber and cloud provider, for each of the service models: SaaS, PaaS, and IaaS.

27.8. Compare the complexity and security that exists between private and public clouds.

27.9. Describe the manner in which to protect virtual networks, including software-based switches and network configurations, which are part of the virtual environment and allow virtual machines on the same host to communicate efficiently within a data center.

27.10. Describe the manner in which to secure virtual servers and applications for serverside protection in both an IaaS and a hybrid cloud infrastructure.

27.11. Describe the difficulty in identity and access management, as well as the means to protect them in cloud computing.

27.12. In the virtualization environment, the hypervisor permits multiple operating systems to run concurrently on

a host computer.

- (a) True
- (b) False

27.13. In the hosted approach to virtualization, the hypervisors run directly upon the host's hardware.

- (a) True
- (b) False

27.14. Virtualization that runs on top of the operating system is called the bare metal approach.

- (a) True

(b) False 27.15. With hosted virtualization, the virtualization software runs in a manner that makes each VM feel that it has dedicated hardware. (a) True (b) False

27.16. The hypervisor implemented in the virtualization software couples the operating system with the application's physical resources. (a) True (b) False

27.17. In the virtualization environment, the VMM runs in the same layer as the hypervisor. (a) True (b) False

27.18. Hosted virtualization is more efficient than a hypervisor. (a) True (b) False 27.19. A hypervisor need not go through the operating system to obtain access to the hardware resources. (a) True (b) False

27.20. The levels of privilege in the x86 architecture that are given to operating systems and applications in managing access to hardware are known as Rings 1, 2, 3 and 4. (a) True (b) False

27.21. Hardware-assisted virtualization is a

technique employed in full virtualization with binary

translation. (a) True (b) False

27.22. Full virtualization with binary translation is probably the most

established and reliable virtualization technology. (a)

True (b) False

27.23. Intel is the only corporation that

supports hardware-assisted virtualization through its

product known as VT-x. (a) True (b) False

27.24. The virtualization scheme in which a modified guest operating

system runs in parallel with other modified operating

systems is known as (a) Hardware-assisted virtualization

(b) Para-virtualization (c) OS-assisted virtualization

(d) All of the above (e) None of the above

27.25. One of the advantages of para-virtualization is lower

virtualization overhead. (a) True (b) False

27.26. Xen operates in which of the following modes?

- (a) HVM x86
- (b) Para-virtual x86
- (c) All of the above
- (d) None of the above

27.27. VMware operates in which of the following modes?

- (a) HVM x86/BT with 32 bits
- (b) Para-virtual x86 with 64 bits
- (c) All of the above
- (d) None of the above

27.28. The virtual appliance is a prebuilt, preconfigured piece of hardware that works in conjunction with the guest operating system.

- (a) True
- (b) False

27.29. The VMware ESX server host has a maximum limit of 1096 ports on all virtual switches contained within it.

- (a) True
- (b) False

27.30. If two virtual network interface cards are connected to the same vSwitch, communication between the two vNICs can be accomplished directly via layer 2 switching performed by the vSwitch.

- (a) True
- (b) False

27.31. The tools for constructing and maintaining a VMware virtual network infrastructure are provided by VMware's VirtualCenter.

- (a) True
- (b) False

27.32. Hardware-assisted virtualization can accommodate an unmodified guest OS.

(a) True

(b) False

27.33. Which of the following are critical components of the virtualized end-to-end information infrastructure?

(a) Virtualized information services

(b) Virtualized data centers/services for groups

(c) Virtualized private networks

(d) All the above

(e) None of the above

27.34. Which of the following are some of the key challenges in the virtual environment?

(a) Access control

(b) Path isolation

(c) Segmentation

(d) All the above

(e) None of the above

27.35. In simplistic terms, the network virtualization objective is the optimized use of network assets.

(a) True

(b) False 27.36. In a generic sense, the VMware technology that performs the live migration of operational virtual machines from one physical server to another is VMotion.

(a) True (b) False 27.37. VMotion permits virtual machines to be automatically and continuously optimized for use within resource pools. (a) True (b) False 27.38. The element that works with the VMware infrastructure to continuously automate the balancing of virtual machine workloads across a cluster is the (a) VMFS (b) DRS (c) ESX (d) None of the above 27.39. Within the virtualized information infrastructure, NAP/NAC is used to mitigate

threats at the edge before they reach the infrastructure core. (a) True (b) False 27.40. VRFs are used on both the customer's and service provider's edge routers. (a) True (b) False 27.41. A physical router can act like multiple virtual routers. (a) True (b) False 27.42. VRF Lite uses virtual routing tables to tie VLANs together at layer 2. (a) True (b) False 27.43. Two advantages of the virtual infrastructure environment are unified access and centralized services. (a) True (b) False 27.44. FC is a gigabit-speed network technology primarily used in storage networking. (a) True (b) False 27.45. Fiber channel signaling runs on (a) Fiber-optic cables (b) Twisted pair copper wires (c) All of the above (d) None of the above 27.46. The benefits of Fiber Channel over Ethernet include (a) Congestion management (b) Effective handling of traffic bursts (c) The achievement of unified I/O through support for multiple flows on the same cable (d) All of the above (e) None of the above

27.47. FCoE defines IP layer 3 and thus is routable using the IP layer.

(a) True

(b) False

27.48. The newest Intel CPUs and chipsets provide hardware virtualization for the

(a) CPU

(b) Memory

(c) I/O

(d) All of the above

(e) None of the above

27.49. The newest CAN requires ___ driver(s) for connecting to FCoE, iSCSI, and computer cluster networks.

(a) 1

(b) 2

(c) 3

(d) None of the above

27.50. The hardware I/O virtualization requires the capability of handling

- (a) Interrupts
- (b) DMA
- (c) All of the above
- (d) None of the above

27.51. The iSCSI requires ___ hardware to connect a disk array to a network.

- (a) FCoE
- (b) FC
- (c) iSCSI
- (d) None of the above

28 Chapter 28 - Unified Communications and Multimedia Protocols

1. W. Jiang, J. Lennox, S. Narayanan, H. Schulzrinne, K. Singh, and X. Wu, "Integrating Internet telephony services," IEEE Internet Computing, vol. 6, 2002, pp. 64-72.
2. "SIP and MGCP/Megaco Comparison/About SIP/SIP and MGCP Megaco"; <http://www.sipcenter.com/SIP.NSF/HTML/SIP+AND+MGCP+MEGACO>.
3. "SGCP: Simple Gateway Control Protocol"; <http://voip-facts.net/sgcp.php>.
4. F. Andreasen and B. Foster, RFC 3435: Media gateway control protocol (MGCP) version 1.0, 2003.
5. N. Greene, M. Ramalho, and B. Rosen, RFC 2805: Media Gateway Control Protocol Architecture and Requirements, 2000.
6. C. Groves, M. Pantaleo, T. Anderson, and T. Taylor, RFC 3525: Gateway Control Protocol Version 1, 2003.
7. ITU Rec., H. 248.1 Gateway Control Protocol, 2002.
8. S.L. Chou and Y.B. Lin, "Computer Telephony Integration and its applications," IEEE Communications Surveys & Tutorials, vol. 3, 2000, pp. 2-11.
9. M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, RFC 2543: Session Initiation Protocol (SIP), IETF, March, 1999.
10. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, RFC 3261: SIP: Session Initiation Protocol, 2002.
11. ITU Rec., H. 323: Packet-based Multimedia Communications Systems, 2003.
12. A. Johnston, S. Donovan, R. Sparks, C. Cunningham, and K. Summers, RFC 3665: Basic Call Flow Examples, 2003.
13. A. Johnston, S. Donovan, R. Sparks, C. Cunningham, and K. Summers, RFC 3666: Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) Call Flows, 2003.
14. M. Handley, V. Jacobson, and C. Perkins, RFC 4566: SDP:

Session Description Protocol, 2006.

15. C. Metz, "Internet multimedia: answering basic questions," IEEE internet computing, vol. 9, 2005, pp. 51-55.
16. N. Banerjee, A. Acharya, and S.K. Das, "Seamless SIP-based mobility for multimedia applications," IEEE Network, vol. 20, 2006, pp. 6-13.
17. J. Rosenberg and H. Schulzrinne, RFC 3263: Session Initiation Protocol (SIP): Locating SIP Servers, 2002.
18. A. Gulbrandsen, P. Vixie, and L. Esibov, RFC 2782: A DNS RR for specifying the location of services (DNS SRV), 2000.
19. M. Mealling and R. Daniel, RFC 2915: The naming authority pointer (NAPTR) DNS resource record, 2002.
20. M. Day, J. Rosenberg, and H. Sugano, RFC 2778: A model for presence and instant messaging, 2000.
21. M. Day, S. Aggarwal, G. Mohr, and J. Vincent, RFC 2779: Instant Messaging, 2000.
22. H. Schulzrinne, A. Rao, R. Kanphier, M. Westerlund, and A. Narasimhan, RFC 2326: Real Time Streaming Protocol, 1998.
23. H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, RFC 3550: RTP: A Transport Protocol for RealTime Applications, 2003.
24. R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, RFC 2205: Resource ReSerVation Protocol (RSVP) Version 1 Functional Specification, 1997.
25. ITU Rec., H. 261: Video codec for audiovisual services at p x 64 kbits, 1993.
26. T. Wiegand, G. Sullivan, and A. Luthra, ITU-T H. 264: ISO/IEC 14496-10 AVC Draft ITU-T recommendation and final draft international standard of joint video specification, 2003.
27. N.J. Muller, LANs to WANs: the complete management guide, Artech House Publishers, 2003.
28. H. Schulzrinne and J. Rosenberg, "A Comparison of SIP

and H. 323 for Internet Telephony," Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV), pp. 83-86.

29. I. Dalgic and H. Fang, "Comparison of H. 323 and SIP for IP Telephony Signaling," Proc. of Photonics East.

30. S. Casner and H. Schulzrinne, RFC 3551: RTP profile for Audio and Video Conferences with Minimal Control, 2003.

31. T. Friedman, R. Caceres, and A. Clark, RFC 3611: RTP control protocol extended reports (RTCP XR), November 2003,.

32. J. Wroclawski and others, RFC 2210: The use of RSVP with IETF integrated services, RFC 2210, September 1997, 1997.

33. L. Zhang, S. Deering, D. Estrin, S. Shenker, and D. Zappala, "RSVP: A new resource reservation protocol," IEEE Communications Magazine, vol. 40, 2002, pp. 116-127.

34. Cisco Systems, "Internetworking Technology Handbook";

28.11. The signaling protocol used with IP voice, video and messaging services is signaling system 7.

(a) True

(b) False

28.12. The bridge for translation between IP and PSTN is

(a) SIP

(b) H.323

(c) MGW and MGC

(d) All of the above

(e) None of the above

28.13. H.323 is a signaling protocol developed by

(a) IETF

(b) ITU

(c) None of the above

28.14. Transcoding between dissimilar networks is performed by the MGW.

(a) True

(b) False

28.15. A MGC is also known as a

(a) Softswitch

(b) Call agent

(c) All of the above

(d) None of the above

28.16. The relationship between MGW and MGC is

(a) Master/slave

(b) Peer-to-peer

(c) None of the above

28.17. An IP phone employs Ethernet and supports the SIP protocol.

(a) True

(b) False

28.18. Interoperability between an IP phone and an analog phone is provided by SIP.

(a) True

(b) False

28.19. The following protocols are employed between Microsoft's office communication server and Cisco's unified presence server:

(a) CSTA

(b) SIP

(c) CTI

(d) None of the above

28.20. SIP is a network layer protocol that is ASCII code-based and similar to HTTP.

(a) True

(b) False

28.21. When SIP is used to support the establishment of a call between two parties, the parties must agree upon

(a) Media

(b) Encoding Scheme

(c) All of the above

(d) None of the above 28.22. Within the SIP architecture, the SIP servers include which of the following: (a)

Messaging server (b) Proxy server (c) Registrar server

(d) All of the above (e) None of the above 28.23. A SIP proxy server can act as both a UA server and UA client.

(a) True (b) False 28.24. A SIP server uses DNS to determine an IP address. (a) True (b) False 28.25. Email style addressing is employed by SIP to identify users. (a) True (b) False 28.26. The Real-time Transport Protocol (RTP) is built on top of TCP. (a) True (b) False 28.27.

In a SIP session, the following parameters are specified in order to achieve a minimum QoS for VoIP: (a) Maximum latency (b) Maximum jitter (c) Maximum packet loss (d)

All of the above (e) None of the above 28.28. Although SIP and H.323 are similar, H.323 has an advantage in that it is more scalable. (a) True (b) False 28.29. The sequence number used in RTP can be used to detect packet loss. (a) True (b) False 28.30. The sampling instant for the first octet in a RTP data packet is reflected by the

(a) Sequence number (b) Timestamp (c) None of the above 28.31. RTP provides a mechanism to ensure timely data delivery. (a) True (b) False 28.32. When RTP encapsulation is employed it can be viewed by intermediate routers as well as the end systems. (a) True (b) False 28.33. Data provided by RTCP can be used by a sender to modify its transmission. (a) True (b) False

28.34. A RTP packet uses a different ___ than a RTCP packet.

(a) Round trip time delay

(b) Port number

(c) Inter-arrival jitter

(d) All of the above

(e) None of the above

28.35. An advantage of RTP is the use of a single session for transmitting both audio and video.

(a) True

(b) False

28.36. RSVP is a network layer protocol that is used to reserve resources across a network for integrated services through the Internet.

(a) True

(b) False

28.37. The manner in which RSVP is used is determined by the

(a) MGC

(b) Softswitch

(c) All of the above

(d) None of the above

28.38. The RSVP reservation request flow descriptor consists of flowspec and

(a) Dataspec

(b) Packetspec

(c) Filterspec

(d) All of the above

(e) None of the above

28.39. RSVP handles all layer 3 functions.

(a) True

(b) False

28.40. The two RSVP message types are Path and Rspec.

- (a) True
- (b) False

28.41. A RSVP path message is stored at each router along the path and contains at a minimum the unicast IP address of the previous hop node.

- (a) True
- (b) False

28.42. RTSP is a transport layer protocol.

- (a) True
- (b) False

28.43. The session description protocol (SDP) is used by

- (a) TCP
- (b) SCTP
- (c) RTSP
- (d) All of the above

28.44. The RTSP control messages and media data stream use the same port numbers.

- (a) True
 - (b) False
- 28.45. During a RTSP session, a connectionless transport protocol such as UDP can be employed to issue RTSP requests.
- (a) True
 - (b) False
- 28.46. The admission control is provided by the
- (a) SIP
 - (b) RSVP
 - (c) RTSP
 - (d) All of the above
- 28.47. The RTSP's DESCRIBE method retrieves the description of a presentation or media object identified by the request URL from a media server.
- (a) True
 - (b) False
- 28.48. The packets that meet the classification of the ___ are marked by the Differentiated Services Code Point (DSCP).
- (a) Tspec
 - (b) Rspec
 - (c) Filter spec
 - (d) All of the above