

# Computer and Communication Networks

SECOND EDITION

NADER F. MIR

FREE SAMPLE CHAPTER



SHARE WITH OTHERS

# COMPUTER AND COMMUNICATION NETWORKS

Second Edition

*This page intentionally left blank*

# COMPUTER AND COMMUNICATION NETWORKS

Second Edition

Nader F. Mir



PRENTICE  
HALL

Upper Saddle River, NJ • Boston • Indianapolis • San Francisco  
New York • Toronto • Montreal • London • Munich • Paris • Madrid  
Capetown • Sydney • Tokyo • Singapore • Mexico City

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The author and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at [corpsales@pearsoned.com](mailto:corpsales@pearsoned.com) or (800) 382-3419.

For government sales inquiries, please contact [governmentsales@pearsoned.com](mailto:governmentsales@pearsoned.com).

For questions about sales outside the United States, please contact [international@pearsoned.com](mailto:international@pearsoned.com).

Visit us on the Web: [informit.com/ph](http://informit.com/ph)

*Library of Congress Catalog-in-Publication Data*

Mir, Nader F.

Computer and communication networks / Nader F. Mir.—Second edition.

pages cm

Includes bibliographical references and index.

ISBN 978-0-13-381474-3 (hardcover : alk. paper)—ISBN 0-13-381474-2

(hardcover : alk. paper)

1. Computer networks. 2. Data transmission systems. I. Title.

TK5105.5.M567 2015

004.6—dc23

2014037209

Copyright © 2015 Pearson Education, Inc.

All rights reserved. Printed in the United States of America. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. To obtain permission to use material from this work, please submit a written request to Pearson Education, Inc., Permissions Department, One Lake Street, Upper Saddle River, New Jersey 07458, or you may fax your request to (201) 236-3290.

ISBN-13: 978-0-13-381474-3

ISBN-10: 0-13-381474-2

Text printed in the United States on recycled paper at Courier in Westford, Massachusetts.

First printing, December 2014

**Editor-in-Chief**

Mark L. Taub

**Senior Acquisitions Editor**

Trina MacDonald

**Development Editor**

Songlin Qiu

**Managing Editor**

John Fuller

**Full-Service Production Manager**

Julie B. Nahil

**Project Manager**

Vicki Rowland

**Indexer**

Ted Laux

**Proofreader**

Andrea Fox

**Publishing Coordinator**

Olivia Basegio

**Cover Designer**

Chuti Prasertsith

**Compositor**

diacriTech, Inc.

*To Shahrzad and Navid*

*This page intentionally left blank*

# Contents

---

*Preface* xxiii

*About the Author* xxxvii

## **PART I: Fundamental Concepts** 1

- 1 Packet-Switched Networks** 3
  - 1.1 Basic Definitions in Networks 4
    - 1.1.1 Packet Switching Versus Circuit Switching 5
    - 1.1.2 Data, Packets, and Frames 6
    - 1.1.3 The Internet and ISPs 7
    - 1.1.4 Classification of ISPs 9
  - 1.2 Types of Packet-Switched Networks 11
    - 1.2.1 Connectionless Networks 11
    - 1.2.2 Connection-Oriented Networks 13
  - 1.3 Packet Size and Optimizations 15
  - 1.4 Foundation of Networking Protocols 17
    - 1.4.1 Five-Layer TCP/IP Protocol Model 18
    - 1.4.2 Seven-Layer OSI Model 20
  - 1.5 Addressing Scheme in the Internet 21
    - 1.5.1 IP Addressing Scheme 22
    - 1.5.2 Subnet Addressing and Masking 24
    - 1.5.3 Classless Interdomain Routing (CIDR) 26



1.6	Equal-Sized Packets Model	28
1.7	Summary	28
1.8	Exercises	29
1.9	Computer Simulation Project	34
<b>2</b>	<b>Overview of Networking Devices</b>	<b>37</b>
2.1	Network Interface Cards (NICs)	39
2.2	Switching and Routing Devices	40
2.2.1	Layer 1 Devices	41
2.2.2	Layer 2 Devices	42
2.2.3	Layer 3 Devices	44
2.3	Wireless Switching and Routing Devices	47
2.3.1	Wireless Access Points and Base Stations	47
2.3.2	Wireless Routers and Switches	48
2.3.3	Antennas in Wireless Devices	49
2.4	Modems	50
2.4.1	Basic Modulation: ASK, FSK, and PSK	51
2.4.2	Practical Modulation: 4-QAM and QPSK	53
2.4.3	Digital Subscriber Line (DSL) Modems	55
2.4.4	Cable Modems	57
2.5	Multiplexers	58
2.5.1	Frequency-Division Multiplexing (FDM)	59
2.5.2	Time-Division Multiplexing	61
2.6	Summary	66
2.7	Exercises	67
2.8	Computer Simulation Project	69
<b>3</b>	<b>Data Links and Link Interfaces</b>	<b>71</b>
3.1	Data Links	72
3.1.1	Data Link Types	73
3.2	Link Encoder	75
3.3	Error Detection and Correction on Links	77
3.3.1	Error Detection Methods	78
3.3.2	Cyclic Redundancy Check (CRC) Algorithm	79
3.4	Flow Control on Links	85
3.4.1	Stop-and-Wait Flow Control	85
3.4.2	Sliding-Window Flow Control	88

3.5	Link Access by Multiple Users	92
3.5.1	Carrier Sense Multiple Access (CSMA)	93
3.6	Wireless Channel Access by Multiple Users	97
3.6.1	Frequency-Division Multiple Access	99
3.6.2	Time-Division Multiple Access	99
3.6.3	Orthogonal Frequency-Division Multiple Access	99
3.6.4	Single-Carrier Frequency-Division Multiple Access	100
3.6.5	Code-Division Multiple Access	100
3.6.6	Other Multiple-Access Methods	104
3.7	Link Aggregation	107
3.7.1	Link Aggregation Applications	107
3.7.2	Link Aggregation Control Protocol (LACP)	108
3.8	Summary	109
3.9	Exercises	110
3.10	Computer Simulation Project	114
<b>4</b>	<b>Local Area Networks and Networks of LANs</b>	<b>115</b>
4.1	LANs and Basic Topologies	116
4.2	LAN Protocols	117
4.2.1	Logical-Link Control (LLC)	118
4.2.2	Media Access Control (MAC)	118
4.3	Networks of LANs	121
4.3.1	LAN Networking with Layer 1 Devices	121
4.3.2	LAN Networking with Layer 2 Devices	123
4.3.3	Networking with Layer 2 and 3 Devices	128
4.4	MAC/IP Address Conversion Protocols	130
4.4.1	Address Resolution Protocol (ARP)	130
4.4.2	Reverse Address Resolution Protocol (RARP)	132
4.5	Spanning-Tree Protocol (STP)	133
4.6	Virtual LANs (VLANs)	136
4.6.1	VLAN Switches	137
4.6.2	VLAN Trunking Protocol (VTP) and IEEE 802.1Q	138
4.7	Wireless LANs	139
4.7.1	Infrared LANs	140
4.7.2	Spread-Spectrum LANs	141
4.7.3	Narrowband RF LANs	141
4.7.4	Home RF and Bluetooth LANs	141

4.8	IEEE 802.11 Wireless LAN Standard	142
4.8.1	IEEE 802.11 Physical Layer	144
4.8.2	802.11 MAC Layer	145
4.8.3	WiFi Networks	149
4.9	Case Study: DOCSIS, a Cable TV Protocol	151
4.10	Summary	152
4.11	Exercises	153
4.12	Computer Simulation Project	157
<b>5</b>	<b>Wide-Area Routing and Internetworking</b>	<b>159</b>
5.1	IP Packets and Basic Routing Policies	160
5.1.1	Packet Fragmentation and Reassembly	163
5.1.2	Internet Control Message Protocol (ICMP)	164
5.1.3	Obtaining and Assigning IP Addresses	165
5.1.4	Dynamic Host Configuration Protocol (DHCP)	167
5.1.5	Network Address Translation (NAT)	169
5.1.6	Universal Plug and Play (UPnP)	172
5.2	Path Selection Algorithms	173
5.2.1	Dijkstra's Algorithm	174
5.2.2	Bellman-Ford Algorithm	176
5.2.3	Packet Flooding Algorithm	177
5.2.4	Deflection Routing Algorithm	178
5.3	Intradomain Routing Protocols	178
5.3.1	Open Shortest Path First (OSPF) Protocol	180
5.3.2	Routing Information Protocol (RIP)	183
5.4	Interdomain Routing Protocols	188
5.4.1	Autonomous System (AS)	189
5.4.2	Border Gateway Protocol (BGP)	189
5.5	Internet Protocol Version 6 (IPv6)	196
5.5.1	IPv6 Addressing Format	197
5.5.2	Extension Header	198
5.5.3	Packet Fragmentation	198
5.5.4	Other Features of IPv6	199
5.6	Congestion Control at the Network Layer	199
5.6.1	Unidirectional Congestion Control	201
5.6.2	Bidirectional Congestion Control	202
5.6.3	Random Early Detection (RED)	203
5.6.4	A Quick Estimation of Link Blocking	205
5.6.5	Lee's Serial and Parallel Connection Rules	206

- 5.7 Summary 207
- 5.8 Exercises 209
- 5.9 Computer Simulation Project 213
  
- 6 Multicast Routing and Protocols 215**
  - 6.1 Basic Definitions and Techniques 216
    - 6.1.1 IP Multicast Addresses 217
    - 6.1.2 Basic Multicast Tree Algorithms 218
    - 6.1.3 Classification of Multicast Protocols 220
  - 6.2 Local and Membership Multicast Protocols 221
    - 6.2.1 Internet Group Management Protocol (IGMP) 221
  - 6.3 Intradomain Multicast Protocols 223
    - 6.3.1 Multicast Backbone (MBone) 224
    - 6.3.2 Distance Vector Multicast Routing Protocol (DVMRP) 224
    - 6.3.3 Multicast OSPF (MOSPF) Protocol 225
    - 6.3.4 Protocol-Independent Multicast (PIM) 227
    - 6.3.5 Core-Based Trees (CBT) Protocol 230
  - 6.4 Interdomain Multicast Protocols 231
    - 6.4.1 Multiprotocol BGP (MBGP) 231
    - 6.4.2 Multicast Source Discovery Protocol (MSDP) 234
    - 6.4.3 Border Gateway Multicast Protocol (BGMP) 236
  - 6.5 Summary 237
  - 6.6 Exercises 238
  - 6.7 Computer Simulation Project 241
  
- 7 Wireless Wide Area Networks and LTE Technology 243**
  - 7.1 Infrastructure of Wireless Networks 244
  - 7.2 Cellular Networks 246
    - 7.2.1 Cellular Network Devices and Operation 247
    - 7.2.2 Handoff 253
  - 7.3 Mobile IP Management in Cellular Networks 259
    - 7.3.1 Home Agents and Foreign Agents 260
    - 7.3.2 Agent Discovery Phase 261
    - 7.3.3 Registration 262
    - 7.3.4 Mobile IP Routing 263
    - 7.3.5 Generations of Cellular Networks 267
  - 7.4 Long-Term Evolution (LTE) Technology 268
    - 7.4.1 LTE Networking Devices 269
    - 7.4.2 Call Establishment in LTE Cells 271

7.4.3	Handoff in LTE	271
7.4.4	Downlink and Uplink Schemes in LTE	273
7.4.5	Frequency Reuse	273
7.5	Wireless Mesh Networks (WMNs) with LTE	277
7.5.1	Applications of Mesh Networks	277
7.5.2	Physical and MAC Layers of WMNs	279
7.6	Characterization of Wireless Channels	280
7.6.1	Capacity Limits of Wireless Channels	283
7.6.2	Channel Coding	283
7.6.3	Flat-Fading Countermeasures	284
7.6.4	Intersymbol Interference Countermeasures	284
7.7	Summary	285
7.8	Exercises	286
7.9	Computer Simulation Project	288
<b>8</b>	<b>Transport and End-to-End Protocols</b>	<b>289</b>
8.1	Overview of the Transport Layer	290
8.1.1	Interaction of Transport Layer and Adjacent Layers	291
8.1.2	Transport Layer Protocols	294
8.2	User Datagram Protocol (UDP)	295
8.2.1	UDP Segments	295
8.2.2	Applications of UDP	297
8.3	Transmission Control Protocol (TCP)	298
8.3.1	TCP Segment	299
8.3.2	A TCP Connection	301
8.3.3	Window-Based Transmission and Sliding Window in TCP	305
8.3.4	Applications of TCP	306
8.4	Mobile Transport Protocols	307
8.4.1	UDP for Mobility	307
8.4.2	TCP for Mobility	307
8.5	TCP Congestion Control	309
8.5.1	Additive Increase, Multiplicative Decrease Control	309
8.5.2	Slow-Start Method	311
8.5.3	Fast Retransmit and Fast Recovery Methods	312
8.6	Summary	315
8.7	Exercises	316
8.8	Computer Simulation Project	319

<b>9</b>	<b>Basic Network Applications and Management</b>	<b>321</b>
9.1	Overview of the Application Layer	322
9.1.1	Client/Server Model	323
9.1.2	Graphical User Interface (GUI)	324
9.2	Domain Name System (DNS)	325
9.2.1	Domain Name Space	325
9.2.2	Name/Address Mapping	327
9.2.3	DNS Message Format	329
9.3	Electronic Mail (E-Mail)	330
9.3.1	Basic E-Mail Structure and Definitions	330
9.3.2	Simple Mail Transfer Protocol (SMTP)	333
9.3.3	Post Office Protocol, Version 3 (POP3)	334
9.3.4	Internet Mail Access Protocol (IMAP)	335
9.4	World Wide Web (WWW)	335
9.4.1	Hypertext Transfer Protocol (HTTP)	336
9.4.2	Web Caching (Proxy Server)	341
9.4.3	Webmail	342
9.5	Remote Login Protocols	342
9.5.1	TELNET Protocol	343
9.5.2	Secure Shell (SSH) Protocol	344
9.6	File Transfer and FTP	346
9.6.1	File Transfer Protocol (FTP)	346
9.6.2	Secure Copy Protocol (SCP)	346
9.7	Peer-to-Peer (P2P) Networking	347
9.7.1	P2P File Sharing Protocols	348
9.7.2	P2P Database Sharing Protocols	353
9.7.3	Estimation of Peer Connection Efficiency	355
9.8	Network Management	356
9.8.1	Elements of Network Management	358
9.8.2	Structure of Management Information (SMI)	359
9.8.3	Management Information Base (MIB)	359
9.8.4	Simple Network Management Protocol (SNMP)	360
9.9	Summary	362
9.10	Exercises	363
9.11	Computer Simulation Projects	366

## 10 Network Security 369

- 10.1 Overview of Network Security 370
  - 10.1.1 Elements of Network Security 370
  - 10.1.2 Classification of Network Attacks 371
- 10.2 Security Methods 375
- 10.3 Symmetric-Key Cryptography 377
  - 10.3.1 Data Encryption Standard (DES) 377
  - 10.3.2 Advanced Encryption Standard (AES) 379
- 10.4 Public-Key Cryptography 380
  - 10.4.1 RSA Algorithm 381
  - 10.4.2 Diffie-Hellman Key-Exchange Protocol 382
- 10.5 Authentication 383
  - 10.5.1 Hash Function 383
  - 10.5.2 Secure Hash Algorithm (SHA) 385
- 10.6 Digital Signatures 387
- 10.7 Security of IP and Wireless Networks 387
  - 10.7.1 IP Security and IPsec 387
  - 10.7.2 Security of Wireless Networks and IEEE 802.11 389
- 10.8 Firewalls and Packet Filtering 391
  - 10.8.1 Packet Filtering 393
  - 10.8.2 Proxy Server 395
- 10.9 Summary 396
- 10.10 Exercises 397
- 10.11 Computer Simulation Project 399

## PART II: Advanced Concepts 401

### 11 Network Queues and Delay Analysis 403

- 11.1 Little's Theorem 404
- 11.2 Birth-and-Death Process 406
- 11.3 Queueing Disciplines 408
- 11.4 Markovian FIFO Queueing Systems 409
  - 11.4.1  $M/M/1$  Queueing Systems 409
  - 11.4.2 Systems with Limited Queueing Space:  $M/M/1/b$  414
  - 11.4.3  $M/M/a$  Queueing Systems 415
  - 11.4.4 Models for Delay-Sensitive Traffic:  $M/M/a/a$  420
  - 11.4.5  $M/M/\infty$  Queueing Systems 422

11.5	Non-Markovian and Self-Similar Models	424
11.5.1	Pollaczek-Khinchin Formula and $M/G/1$	424
11.5.2	$M/D/1$ Models	427
11.5.3	Self-Similarity and Batch-Arrival Models	427
11.6	Networks of Queues	428
11.6.1	Burke's Theorem	428
11.6.2	Jackson's Theorem	433
11.7	Summary	437
11.8	Exercises	438
11.9	Computer Simulation Project	444
<b>12</b>	<b>Advanced Router and Switch Architectures</b>	<b>445</b>
12.1	Overview of Router Architecture	446
12.2	Input Port Processor (IPP)	447
12.2.1	Packet Parser	448
12.2.2	Packet Partitioner	449
12.2.3	Input Buffer	450
12.2.4	Routing Table (IPv4 and IPv6)	450
12.2.5	Multicast Scheduler	452
12.2.6	Forwarding Table and Packet Encapsulator	452
12.3	Output Port Processor (OPP)	453
12.3.1	Output Buffer	453
12.3.2	Reassembler and Resequencer	454
12.3.3	Error Control	454
12.4	Central Controller	454
12.4.1	Contention Resolution Unit	455
12.4.2	Congestion Controller	457
12.5	Switch Fabric	457
12.5.1	Complexity of Switch Fabrics	458
12.5.2	Crossbar Switch Fabrics	459
12.5.3	Clos Switch Fabrics	460
12.5.4	Concentration and Expansion Switch Fabrics	465
12.5.5	Shared-Memory Switch Fabrics	468
12.5.6	Performance Improvement in Switch Fabrics	469
12.6	Multicasting Packets in Routers	475
12.6.1	Tree-Based Multicast Algorithm	476
12.6.2	Packet Recirculation Multicast Algorithm	479



12.7	Summary	480
12.8	Exercises	481
12.9	Computer Simulation Project	484
<b>13</b>	<b>Quality of Service and Scheduling in Routers</b>	<b>485</b>
13.1	Overview of Quality of Service (QoS)	486
13.2	Integrated Services QoS	486
13.2.1	Traffic Shaping	488
13.2.2	Admission Control	494
13.2.3	Resource Reservation Protocol (RSVP)	495
13.3	Differentiated Services QoS	495
13.3.1	Per-Hop Behavior (PHB)	497
13.4	Resource Allocation	497
13.4.1	Management of Resources	498
13.4.2	Classification of Resource-Allocation Schemes	499
13.4.3	Fairness in Resource Allocation	500
13.5	Packet Scheduling	501
13.5.1	First-In, First-Out Scheduler	502
13.5.2	Priority Queueing Scheduler	503
13.5.3	Fair Queueing Scheduler	507
13.5.4	Weighted Fair Queueing Scheduler	508
13.5.5	Deficit Round-Robin Scheduler	511
13.5.6	Earliest Deadline First Scheduler	512
13.6	Summary	512
13.7	Exercises	513
13.8	Computer Simulation Project	517
<b>14</b>	<b>Tunneling, VPNs, and MPLS Networks</b>	<b>519</b>
14.1	Tunneling	520
14.1.1	Point-to-Point Protocol (PPP)	521
14.1.2	IPv6 Tunneling and Dual-Stack Lite	522
14.2	Virtual Private Networks (VPNs)	524
14.2.1	Remote-Access VPN	526
14.2.2	Site-to-Site VPN	526
14.2.3	Security in VPNs	528
14.3	Multiprotocol Label Switching (MPLS)	528
14.3.1	Labels and Label Switch Routers (LSRs)	529
14.3.2	Label Binding and Switching	531

14.3.3	Routing in MPLS Domains	534
14.3.4	MPLS Packet Format	536
14.3.5	Multi-Tunnel Routing	537
14.3.6	Traffic Engineering	538
14.3.7	MPLS-Based VPNs	539
14.4	Summary	540
14.5	Exercises	540
14.6	Computer Simulation Project	543
<b>15</b>	<b>All-Optical Networks, WDM, and GMPLS</b>	<b>545</b>
15.1	Overview of Optical Networks	546
15.1.1	Fiber Optic Links	547
15.1.2	SONET/SDH Standards	547
15.1.3	Generalized MPLS (GMPLS) Protocol	548
15.1.4	Passive Optical Networks (PONs)	551
15.2	Basic Optical Networking Devices	553
15.2.1	Tunable Lasers	553
15.2.2	Optical Buffers or Delay Elements	553
15.2.3	Optical Amplifiers	553
15.2.4	Optical Filters	554
15.2.5	Wavelength-Division Multiplexer (WDM)	555
15.2.6	Optical Switches	556
15.3	Large-Scale Optical Switches	558
15.3.1	Crossbar Optical Switches	559
15.3.2	Spanke-Beneš Optical Switch	560
15.4	Structure of Optical Cross Connects (OXC)s	560
15.4.1	Structure of Wavelength Routing Nodes	561
15.5	Routing in All-Optical Networks	563
15.5.1	Wavelength Routing Versus Broadcasting	564
15.5.2	Blocking Estimation over Lightpaths	565
15.6	Wavelength Allocation in Networks	567
15.6.1	Wavelength Allocation without Dependency	568
15.6.2	Wavelength Allocation with Dependency	569
15.7	Case Study: An All-Optical Switch	569
15.7.1	Self-Routing in SSN	571
15.7.2	Wavelength Assignment in SSN	571
15.8	Summary	572
15.9	Exercises	573
15.10	Computer Simulation Project	575

<b>16 Cloud Computing and Network Virtualization</b>	<b>577</b>
16.1 Cloud Computing and Data Centers	578
16.1.1 Platforms and APIs	581
16.1.2 Cloud Computing Service Models	581
16.1.3 Data Centers	583
16.1.4 Virtualization in Data Centers	584
16.2 Data Center Networks (DCNs)	588
16.2.1 Load Balancer	589
16.2.2 Traffic Engineering	591
16.2.3 DCN Architectures	591
16.2.4 Multicast Methods	594
16.3 Network Virtualization	595
16.3.1 Network Virtualization Components	596
16.4 Overlay Networks	600
16.5 Summary	601
16.6 Exercises	602
16.7 Computer Simulation Projects	605
<b>17 Software-Defined Networking (SDN) and Beyond</b>	<b>607</b>
17.1 Software-Defined Networking (SDN)	608
17.1.1 Separation of Control and Data Planes	609
17.1.2 Programmability of the Control Plane	612
17.1.3 Standardization of Application Programming Interfaces (APIs)	613
17.2 SDN-Based Network Model	613
17.2.1 Control Plane	614
17.2.2 Data Plane Interface (OpenFlow Protocol)	615
17.3 Small-Size SDN Architectures	620
17.3.1 Scalability of SDN	620
17.3.2 Multicasting in SDN-Based Networks	621
17.4 SDN Architectures for Clouds	621
17.4.1 Software-Defined Compute and Storage	621
17.4.2 Application Delivery in Data Centers by SDN	622
17.5 Network Functions Virtualization (NFV)	623
17.5.1 Abstract Model of NFV	624
17.5.2 Distributed NFV-Based Networks	626
17.5.3 Virtualized Services	627

17.6	Information-Centric Networking (ICN)	627
17.6.1	Named Objects	628
17.6.2	ICN Routing and Network Management	628
17.6.3	ICN Security	631
17.7	Network Emulators for Advanced Networks	632
17.7.1	Mininet	632
17.8	Summary	635
17.9	Exercises	636
17.10	Computer Simulation Projects	638
<b>18</b>	<b>Voice over IP (VoIP) Signaling</b>	<b>641</b>
18.1	Public Switched Telephone Networks (PSTN)	642
18.1.1	SS7 Network	644
18.1.2	Circuit-Switched Networks	647
18.2	Overview of Voice over IP (VoIP)	649
18.3	H.323 Protocol	652
18.3.1	Main Components of H.323 Protocol	652
18.3.2	H.323 Protocol Organization	653
18.3.3	RAS Signaling	655
18.3.4	Call Signaling	659
18.3.5	Control Signaling	662
18.3.6	Conference Calling with H.323 Protocol	665
18.4	Session Initiation Protocol (SIP)	666
18.4.1	Main Components of SIP	667
18.4.2	SIP Messages	669
18.4.3	SIP Protocol Organization	671
18.4.4	Registration Process	672
18.4.5	Call Establishment	673
18.4.6	Features and Extensions	674
18.5	Softswitch Methods and MGCP	678
18.6	VoIP and Multimedia Internetworking	679
18.6.1	SIP to H.323 Internetworking	679
18.6.2	SIP to PSTN Internetworking	681
18.6.3	Wireless Cellular Multimedia Internetworking	682
18.7	Summary	684
18.8	Exercises	685
18.9	Computer Simulation Projects	689

**19 Media Exchange and Voice/Video Compression 693**

- 19.1 Overview of Data Compression 694
- 19.2 Digital Voice and Compression 695
  - 19.2.1 Sampling 695
  - 19.2.2 Quantization and Encoding 696
- 19.3 Still Images and JPEG Compression 701
  - 19.3.1 Raw-Image Sampling and DCT 702
  - 19.3.2 Quantization 705
  - 19.3.3 Encoding 706
- 19.4 Moving Images and MPEG Compression 707
  - 19.4.1 MP3 and Streaming Audio 708
- 19.5 Compression Methods with Loss 709
  - 19.5.1 Basics of Information Theory 710
  - 19.5.2 Entropy of Information 710
  - 19.5.3 Shannon's Coding Theorem 711
  - 19.5.4 Compression Ratio and Code Efficiency 713
- 19.6 Compression Methods without Loss 713
  - 19.6.1 Run-Length Encoding 714
  - 19.6.2 Huffman Encoding 715
  - 19.6.3 Lempel-Ziv Encoding 716
- 19.7 Scanned Document Compression 717
- 19.8 Summary 718
- 19.9 Exercises 719
- 19.10 Computer Simulation Project 724

**20 Distributed and Cloud-Based Multimedia Networking 725**

- 20.1 Real-Time Media Exchange Protocols 726
  - 20.1.1 Real-Time Transport Protocol (RTP) 727
  - 20.1.2 Analysis of Jitter in RTP Traffic 731
  - 20.1.3 Real-Time Transport Control Protocol (RTCP) 732
  - 20.1.4 Real Time Streaming Protocol (RTSP) 735
  - 20.1.5 Stream Control Transmission Protocol (SCTP) 735
  - 20.1.6 HTTP-Based Streaming 740
- 20.2 Distributed Multimedia Networking 741
  - 20.2.1 Content Distribution (Delivery) Networks (CDNs) 741
  - 20.2.2 IP Television (IPTV) and VoD 745
  - 20.2.3 Online Gaming 751

20.3	Cloud-Based Multimedia Networking	751
20.3.1	Distributed Media Mini-Clouds	752
20.3.2	Cloud-Based Interactive Voice Response (IVR)	754
20.4	Self-Similarity and Non-Markovian Streaming	756
20.4.1	Self-Similarity with Batch Arrival Models	757
20.5	Summary	759
20.6	Exercises	761
20.7	Computer Simulation Project	764
<b>21</b>	<b>Mobile Ad-Hoc Networks</b>	<b>765</b>
21.1	Overview of Wireless Ad-Hoc Networks	766
21.2	Routing in Ad-Hoc Networks	767
21.2.1	Classification of Routing Protocols	768
21.3	Routing Protocols for Ad-Hoc Networks	769
21.3.1	Destination-Sequenced Distance-Vector (DSDV) Protocol	769
21.3.2	Cluster-Head Gateway Switch Routing (CGSR) Protocol	771
21.3.3	Wireless Routing Protocol (WRP)	772
21.3.4	Dynamic Source Routing (DSR) Protocol	773
21.3.5	Temporally Ordered Routing Algorithm (TORA)	774
21.3.6	Associativity-Based Routing (ABR) Protocol	775
21.3.7	Ad-Hoc On-Demand Distance Vector (AODV) Protocol	776
21.4	Security of Ad-Hoc Networks	783
21.4.1	Types of Attacks	783
21.4.2	Criteria for a Secure Routing Protocol	784
21.5	Summary	785
21.6	Exercises	786
21.7	Computer Simulation Projects	787
<b>22</b>	<b>Wireless Sensor Networks</b>	<b>789</b>
22.1	Sensor Networks and Protocol Structures	790
22.1.1	Clustering in Sensor Networks	790
22.1.2	Protocol Stack	791
22.1.3	Sensor Node Structure	793
22.2	Communication Energy Model	794
22.3	Clustering Protocols	799
22.3.1	Classification of Clustering Protocols	800
22.3.2	LEACH Clustering Protocol	800

22.3.3	DEEP Clustering Protocol	801
22.3.4	Reclustering	805
22.4	Routing Protocols	805
22.4.1	Intracluster Routing Protocols	806
22.4.2	Intercluster Routing Protocols	808
22.5	Other Related Technologies	811
22.5.1	ZigBee Technology and IEEE 802.15.4	811
22.6	Case Study: Simulation of a Sensor Network	812
22.6.1	Cluster-Head Constellation and Distribution of Load	812
22.6.2	Optimum Percentage of Cluster Heads	814
22.7	Summary	814
22.8	Exercises	815
22.9	Computer Simulation Projects	815
<b>A</b>	<b>Glossary of Acronyms</b>	<b>817</b>
<b>B</b>	<b>RFCs</b>	<b>823</b>
<b>C</b>	<b>Probabilities and Stochastic Processes</b>	<b>827</b>
C.1	Probability Theory	827
C.1.1	Bernoulli and Binomial Sequential Laws	828
C.1.2	Counting and Sampling Methods	828
C.2	Random Variables	828
C.2.1	Basic Functions	829
C.2.2	Conditional Functions	829
C.2.3	Popular Random Variables	830
C.2.4	Expected Value and Variance	831
C.2.5	A Function of a Random Variable	832
C.3	Multiple Random Variables	832
C.3.1	Basic Functions of Two Random Variables	833
C.3.2	Two Independent Random Variables	833
C.4	Stochastic (Random) Processes	834
C.4.1	IID Random Process	834
C.4.2	Brownian Motion Random Process	834
C.5	Theory of Markov Chains	835
C.5.1	Continuous-Time Markov Chains	835
<b>D</b>	<b>Erlang-B Blocking Probability Table</b>	<b>837</b>
	<i>Index</i>	<i>841</i>

# Preface

---

This textbook represents more than a decade of work. During this time, some material became obsolete and had to be deleted. In my days as a telecommunication engineer and then a university professor, much has changed in the fields of data communications and computer networks. Nonetheless, this text covers both the foundations and the latest advanced topics of computer communications and networking.

The Internet is a revolutionary communication vehicle by which we all conveniently communicate every day and do business with one another. Because of its complexities at both hardware and software levels, the Internet is a challenge to those who want to study this field. The growing number and variety of communication services introduces other challenges to experts of computer networks. Such experts are in need of effective references having in-depth balanced analysis, architecture, and description, and enabling them to better design emerging communication networks. This book fills the gaps in current available texts.

## Objectives

This textbook offers a mix of theory, architecture, and applications in computer networking. The lack of computer communications books presenting moderate analysis with detailed figures covering both wireline and wireless communication technologies led me to write this book. The main objective of this book is to help readers learn the fundamentals and certain advanced concepts of computer and communication networks, using a unified set of symbols throughout a single textbook. The preparation of this book responds to the explosive demand for learning computer communication science and engineering.



This book targets two groups of people. For people in academia, at both the undergraduate and graduate levels, the book provides a thorough design and performance evaluation of communication networks. The book can also give researchers the ability to analyze and simulate complex communication networks. For engineers who want to work in the communication and networking industry and need a reference covering various angles of computer networks, this book provides a variety of learning techniques: exercises, case studies, and computer simulation projects. The book makes it easy and fun for an engineer to review and learn from a reliable networking reference covering all the necessary concepts and performance models.

## Organization of This Book

The range of topics presented in this text allows instructors to choose the topics best suited for their classes. Besides the explanations provided in each chapter, readers will learn how to model a communication network and how to mathematically analyze it. Readers of this text will benefit from the combination of theory and applications presented in each chapter, with the more theoretical portions of each chapter challenging those readers who are more ambitious.

This book is organized into 22 chapters in two main parts, as follows. The ten chapters of Part I cover the fundamental topics in computer networking, with each chapter serving as a base for the following chapter. Part I of the book begins with an overview of networking, focusing on TCP/IP schemes, describing routing and multicasting in regular networks and wireless networks, and ending with a discussion of network applications, P2P networking, network management, and security. Part I is most appropriate for readers with no experience in computer communications. The 12 chapters in Part II cover detailed analytical aspects and offer a closer perspective of advanced networking protocols: architectures of switches and routers, delay and congestion analysis, label switching, virtual private networks, optical networks, cloud computing, SDN, data compression, voice over IP (VoIP), multimedia networking, ad-hoc networking, and sensor networks. An overview of the 22 chapters is as follows:

- **Chapter 1, Packet-Switched Networks**, introduces computer networks, touching on the need for networks, explaining relevant packet-switched networks, and giving an overview of today's Internet. Fundamental concepts, such as *messages*, *packets*, and *frames* and *packet switching* versus *circuit switching*, are defined. Various types of packet-switched networks are defined, and how a

message can be handled by either *connection-oriented networks* or *connectionless networks* is explained. The second part of the chapter presents basics of the five- and seven-layer Internet Protocol reference models, as well as Internet and addressing scheme. Finally, this chapter presents a detailed analysis of packet size and optimization.

- **Chapter 2, Overview of Networking Devices**, introduces the overall architectures of regular and wireless networking devices. The chapter starts with introducing *network interface cards* (NICs), followed by switching and routing devices, such as hubs, bridges, switches, and routers. These devices are used to switch packets from one path to another. The devices include both wireline and wireless devices used as user, server, or network equipment. Networking modems are used for access to the Internet from remote and residential areas. Finally, multiplexers are used in all layers of a network and are utilized to combine data from multiple lines into one line.
- **Chapter 3, Data Links and Link Interfaces**, focuses on the links and transmission interfaces, the two basic components that networking starts with. This chapter presents both wired and wireless links and describes their characteristics, advantages, and channel access methods. This chapter also presents various *error-detection and correction* techniques at the link level and discusses the integrity of transmitted data. The chapter further presents link-layer *stop-and-wait* and *sliding-window* flow controls. We then proceed to presenting methods of link and then channel access by multiple users, both in regular and wireless environments. Finally, at the end of the chapter, the *link aggregation* method is described. The method combines multiple network links to increase throughput beyond what a single link can sustain. Link aggregation also has a second benefit of providing redundancy in case one of the links fails. We then introduce the well-known *Link Aggregation Control Protocol* (LACP).
- **Chapter 4, Local Area Networks and Networks of LANs**, explores the implementation of small networks, using the functional aspects of the fundamental knowledge gained in Chapters 1, 2, and 3 on basic protocols, devices, and links, respectively. The chapter provides some pointers for constructing a network with those devices and making connections, gives several examples of local area networks (LANs), and explains how such LANs are internetworked. Next, the chapter explores address conversion protocols by which addresses at layers 2 and 3 are converted to one another. The chapter at this point proceeds to the very important topic of the Spanning-Tree Protocol (STP). STP prevents frames or

packets from the looping that causes infinite circulation of frames in a network. *Virtual LANs* (VLANs) are the next topic. A VLAN methodology allows a single LAN to be partitioned into several seemingly and virtually separate LANs. At the end of the chapter, a reader can see an overview of wireless local area networks including WiFi, and wireless LANs and associated standards such as IEEE 802.11.

- **Chapter 5, Wide-Area Routing and Internetworking**, focuses on routing in wide area networks (WANs) and introduces related routing algorithms and protocols. We begin the chapter with some IP packet format and basic routing policies such as the *Internet Control Message Protocol* (ICMP), *Dynamic Host Configuration Protocol* (DHCP), and *Network Address Translation* (NAT). We then proceed to explain path selection algorithms such as the *Open Shortest Path First* (OSPF) protocol, and the *Routing Information Protocol* (RIP) followed by the interdomain routing protocols with a focus on the *Border Gateway Protocol* (BGP) covering both internal BGP (iBGP) and external BGP (eBGP). The chapter then presents IPv6 and its packet format. The chapter finally covers congestion-control algorithms at the network layer: *network-congestion control* and *link-flow control*, and especially looks at *random early detection* for congestion control and describes a useful technique to estimate the link-blocking probability.
- **Chapter 6, Multicast Routing and Protocols**, covers the multicast extension of routing protocols in the Internet. First, the chapter defines basic terms and algorithms: multicast group, multicast addresses, and multicast tree algorithms, which form the next set of foundations for understanding packet multicast in the Internet. Two main classes of protocols are discussed: *intradomain* multicast routing protocols, by which packets are multicast within a domain; and *interdomain* routing protocol, by which packet multicast among domains is managed.
- **Chapter 7, Wireless Wide Area Networks and LTE Technology**, presents the basics of wireless wide area networking. The chapter discusses challenges in designing a wireless network: *management of mobility*, *network reliability*, and *frequency reuse*. The chapter then shifts to cellular networks, one of the main backbones of our wireless wide area networking infrastructure. The *mobile IP* in cellular networks is then presented, in which a mobile user can make a data connection while changing its location. The chapter then focuses on *wireless mesh networks* (WMNs). Finally, the chapter proceeds to the presentation of the fourth-generation wireless wide area networks called *Long-Term Evolution* (LTE).

- **Chapter 8, Transport and End-to-End Protocols**, first looks at the basics of the *transport layer* and demonstrates how a simple file is transferred. This layer handles the details of data transmission. Several techniques for Transmission Control Protocol (TCP) congestion control are discussed. Next, *congestion-avoidance* methods, which are methods of using precautionary algorithms to avoid a possible congestion in a TCP session, are presented. The chapter ends with a discussion of methods of congestion control.
- **Chapter 9, Basic Network Applications and Management**, presents the fundamentals of the *application layer*, which determines how a specific user application should use a network. Among the applications are the *Domain Name System* (DNS); *e-mail protocols*, such as SMTP and Webmail, the *World Wide Web* (WWW), remote login, File Transfer Protocol (FTP), and *peer-to-peer* (P2P) networking. Finally, the chapter proceeds to the presentation of network management techniques and protocol.
- **Chapter 10, Network Security**, focuses on security aspects of networks. After introducing network threats, hackers, and attacks, this chapter discusses *cryptography techniques: public- and symmetric-key protocols, encryption standards, key-exchange algorithms, authentication methods, digital signature* and secure connections, firewalls, IPsec, and security methods for virtual private networks. This chapter also covers some security aspects of wireless networks.
- **Chapter 11, Network Queues and Delay Analysis**, begins Part II of the book by discussing how packets are queued in buffers. Basic modeling theorems are presented such as *Little's theorem*, the *Markov chain theorem*, and *birth and death processes*. Queueing-node models are presented with several scenarios: finite versus infinite queueing capacity, one server versus several servers, and Markovian versus non-Markovian systems. Non-Markovian models are essential for many network applications, as multimedia traffic cannot be modeled by Markovian patterns. In addition, delay analysis, based on networks of queues, is discussed. *Burke's theorem* is applied in both serial and parallel queueing nodes. *Jackson's theorem* is presented for situations in which a packet visits a particular queue more than once, resulting in *loops* or *feedback*.
- **Chapter 12, Advanced Router and Switch Architectures**, looks inside structures of advanced Internet devices such as switches and routers. The chapter begins with general characteristics and block diagrams of switches and routers followed by basic features of *input port processors* (IPPs) and *output port processors* (OPPs) as the interfacing processors to central controllers and switch fabrics.

The details of IPPs and OPPs with several regular IP and IPv6 examples for building blocks such as routing tables, packet parsers, and packet partitioners are presented. A number of switch fabric structures are introduced starting with the building block of *crossbar* switch fabric. In particular, a case study at the end of chapter combines a number of buffered crosspoints to form a buffered crossbar. A number of other switch architectures—both blocking and nonblocking, as well as shared-memory, *concentration-based*, and *expansion-based* switching networks—are presented. The chapter also introduces packet multicast techniques and algorithms used within the hardware of switches and routers.

- **Chapter 13, Quality of Service and Scheduling in Routers**, covers quality-of-service issues in networking. The two broad categories of QoS discussed are the *integrated services approach*, for providing service quality to networks that require maintaining certain features in switching nodes; and the *differentiated services approach* (DiffServ), which is based on providing quality-of-service support to a broad class of applications. These two categories include a number of QoS protocols and architectures, such as *traffic shaping*, *admission control*, *packet scheduling*, *reservation methods*, the *Resource Reservation Protocol* (RSVP), and traffic conditioner and bandwidth broker methods. This chapter also explains fundamentals of resource allocation in data networks.
- **Chapter 14, Tunneling, VPNs, and MPLS Networks**, starts by introducing a useful Internet technique called *tunneling*, used in advanced, secured, and high-speed networking. The chapter explains how networks can be *tunneled* to result in *virtual private networks* (VPNs) by which a private-sector entity tunnels over the public networking infrastructure, maintaining private connections. Another related topic in this chapter is *multiprotocol label switching* (MPLS) networks, in which networks use labels and tunnels to expedite routing.
- **Chapter 15, All-Optical Networks, WDM, and GMPLS**, presents principles of fiber-optic communications and all-optical switching and networking. The optical communication technology uses principles of light emission in a glass medium, which can carry more information over longer distances than electrical signals can carry in a copper or coaxial medium. The discussion on optical networks starts with basic optical devices, such as *optical filters*, *wavelength-division multiplexers* (WDMs), *optical switches*, and *optical buffers* and *optical delay lines*. After detailing optical networks using routing devices, the chapter discusses *wavelength reuse and allocation* as a link in all-optical networks.

*Generalized multiprotocol label switching* (GMPLS) technology, which is similar to MPLS studied in the previous chapter, is applied to optical networks and is also studied in this chapter. The chapter ends with a case study on an optical switching network, presenting a new topology: the *spherical switching network* (SSN).

- **Chapter 16, Cloud Computing and Network Virtualization**, covers basics of cloud computing, large data centers, networking segments of data centers, and virtualization in networking. Data center and cloud computing architectures continue to target support for tens of thousands of servers, massive data storage, terabits per second of traffic, and tens of thousands of tenants. First, the chapter defines basic terms such as *virtualization*, *virtual machines*, and the structure of large data centers constructed from server racks and large data bases. The chapter also presents *data center networks* (DCNs). In a data center, server and storage resources are interconnected with packet switches and routers to construct the DCN.
- **Chapter 17, Software-Defined Networking (SDN) and Beyond**, covers primarily advanced paradigms in control and management of networks. Growth at the infrastructure and applications of the Internet causes profound changes in the technology ecosystems of Internet-related industries. *Software-Defined Networking* (SDN) is a networking paradigm by which a central software program known as “controller” (or SDN controller) determines and controls the overall network behavior resulting in potential improvement in the network performance. This chapter focuses on the fundamentals of SDN and a couple of other alternative innovative networking features, and describes the details of related topics such as OpenFlow switches and flow tables in switches. Protocols such as *network functions virtualization* (NFV) and *Information-Centric Networking* (ICN) are other advanced network control and management topics covered in this chapter. Finally, the chapter concludes with a section that presents network emulators such as the Mininet emulator.
- **Chapter 18, Voice over IP (VoIP) Signaling**, presents the signaling protocols used in voice over IP (VoIP) telephony and multimedia networking. The chapter starts with reviewing the basics of call control and signaling in the traditional Public Switched Telephone Network (PSTN). The chapter then presents two important voice over IP (VoIP) protocols designed to provide real-time service to the Internet, the *Session Initiation Protocol* (SIP) and the *H.323 series*

*of protocols*. At the end of the chapter, a reader can find presentations on a series of internetworking examples between a set of callers, each supplied through a different Internet service provider and a different protocol.

- **Chapter 19, Media Exchange and Voice/Video Compression**, focuses on data-compression techniques for voice and video to prepare digital voice and video for multimedia networking. The chapter starts with the analysis of information-source fundamentals, source coding, and limits of data compression, and explains all the steps of the conversion from raw voice to compressed binary form, such as sampling, quantization, and encoding. The chapter also summarizes the limits of compression and explains typical processes of still-image and video-compression techniques, such as JPEG, MPEG, and MP3.
- **Chapter 20, Distributed and Cloud-Based Multimedia Networking**, presents the transport of real-time voice, video, and data in multimedia networking. The chapter first presents protocols designed to provide real-time transport, such as the *Real-time Transport Protocol* (RTP). Also discussed are the *HTTP-based streaming* which is a reliable TCP-based streaming, and the *Stream Control Transmission Protocol* (SCTP), which provides a general-purpose transport protocol for transporting stream traffic. The next topic is streaming video using *content distribution (delivery) networks* (CDNs). We then present *Internet Protocol television* (IPTV). IPTV is a system through which television services are delivered using the Internet. *Video on demand* (VoD) as a unique feature of IPTV is also described in this chapter. Next, cloud-based multimedia networking is introduced. This type of networking consists of distributed and networked services of voice, video, and data. For example, voice over IP (VoIP), video streaming, or *interactive voice response* (IVR) for recognizing human voice, can be distributed in various clouds of services. The chapter ends with detailed streaming source modeling using self-similarity analysis.
- **Chapter 21, Mobile Ad-Hoc Networks**, presents a special type of wireless network, known as a *mobile ad-hoc network* (MANET). Ad-hoc networks do not need any fixed infrastructure to operate and they support dynamic topology scenarios where no wired infrastructure exists. The chapter explains how a mobile user can act as a routing node and how a packet is routed from a source to its destination without having any static router in the network. The chapter also discusses *table-driven routing protocols* such as DSDV, CGSR, and WRP, and also *source-initiated routing protocols*, as well as DSR, ABR, TORA, and AODV. At the end of the chapter, we discuss the security of ad-hoc networks.

- **Chapter 22, Wireless Sensor Networks**, presents an overview of such sensor networks and describes intelligent sensor nodes, as well as an overview of a protocol stack for sensor networks. The chapter explains how the “power” factor distinguishes the routing protocols of sensor networks from those of computer networks and describes *clustering protocols* in sensor networks. These protocols specify the topology of the hierarchical network partitioned into nonoverlapping *clusters* of sensor nodes. The chapter also presents a typical routing protocol for sensor networks, leading to a detailed numerical case study on the implementation of a clustering protocol. This chapter ends with *ZigBee technology*, based on IEEE standard 802.15.4. This technology uses low-power nodes and is a well-known low-power standard.

## Exercises and Computer Simulation Projects

A number of exercises are given at the end of each chapter. The exercises normally challenge readers to find the directions to solutions in that chapter. The answers to the exercises may be more elusive, but this is typical of real and applied problems in networking. These problems encourage the reader to go back through the text and pick out what the instructor believes is significant.

Besides typical exercises, there are numerous occasions for those who wish to incorporate projects into their courses. The computer simulation projects are normally meant to be a programming project but the reader can use a simulation tool of choice to complete a project. Projects listed at the end of a chapter range from computer simulations to partial incorporation of hardware design in a simulation.

## Appendixes

The book’s appendixes make it essentially self-sufficient. **Appendix A, Glossary of Acronyms**, defines acronyms. **Appendix B, RFCs**, encourages readers to delve more deeply into each protocol presented in the book by consulting the many requests for comments (RFCs) references. **Appendix C, Probabilities and Stochastic Processes**, reviews probabilities, random variables, and random processes. **Appendix D, Erlang-B Blocking Probability Table**, provides a numerically expanded version of the Erlang-B formula presented in Chapter 11. This table can be used in various chapters to estimate traffic blocking, which is one of the main factors in designing a computer network.



## Instructions and Instructor Supplements

This textbook can be used in a variety of ways. An instructor can use Part I of the book for the first graduate or a senior undergraduate course in networking. Part II of the text is aimed at advanced graduate courses in computer networks. An instructor can choose the desired chapters, depending on the need and the content of the course. The following guidelines suggest the adoption of chapters for five different courses:

- *First undergraduate course in Computer Networking*: Chapters 1, 2, 3, 4, and 5 and another chapter such as part of Chapter 6, 7, 8, or 9.
- *First graduate course in Computer Networking*: Chapters 1 through 10 with less emphasis on Chapters 1 and 2.
- *Second graduate course in Advanced Computer Networking*: Chapters 11 through 17.
- *Graduate course in Convergent Data, Voice and Video over IP*: Chapters 7, 9, 16, 18, 19, and 20.
- *Graduate course in Wireless Networking*: Chapters 2, 3, 4, 7, 9, 16, 21, and 22, and other wireless network examples presented in various chapters such the wireless VoIP signaling covered in Chapter 18.

An instructor's solutions manual and other instructional material, such as PowerPoint presentations, will be available to instructors. Instructors should go to Pearson's Instructor Resource Center (<http://www.pearsonhighered.com/educator/profile/ircHomeTab.page>) for access to ancillary instructional materials.

## Acknowledgments

Writing a text is rarely an individual effort. Many experts from industry and academia graciously provided help. I would like to thank them all very warmly for their support. Many of them have given me invaluable ideas and support during this project. I should acknowledge all those scientists, mathematicians, professors, engineers, authors, and publishers who helped me in this project.

I am honored to publish this book with the world's greatest publishing company, Prentice Hall. I wish to express my deep gratitude to everyone there who made an effort to make this project succeed. In particular, I would like to thank editor-in-chief Mark L. Taub and senior acquisitions editor Trina MacDonald for all their advice. Trina, with her outstanding professional talent, provided me with invaluable information and directed me toward the end of this great and challenging project. I would also like to

thank managing editor John Fuller, full-service production manager Julie Nahil, development editor Songlin Qiu, freelance project manager Vicki Rowland, freelance copy editor/proofreader Andrea Fox, and all the other experts for their outstanding work but whom I did not get a chance to acknowledge by name in this section, including the marketing manager, the composers, the indexer, and the cover designer; many thanks to all. Last but not least, I would like to thank Pearson sales representative Ellen Wynn, who enthusiastically introduced the first edition of my manuscript to the publisher.

I am deeply grateful to the technical editors, and all advisory board members of this book. In particular, I thank Professor George Scheets, Professor Zongming Fei, and Dr. Parviz Yegani for making constructive suggestions that helped me reshape the book to its present form. In addition, I would like to especially recognize the following people, who provided invaluable feedback from time to time during the writing phases of the first and second editions of the book. I took all their comments seriously and incorporated them into the manuscript. I greatly appreciate their time spent on this project.

Professor Nirwan Ansari (New Jersey Institute of Technology)  
Professor Mohammed Atiquzzaman (University of Oklahoma)  
Dr. Radu Balan (Siemens Corporate Research)  
Dr. Greg Bernstein (Grotto Networking)  
R. Bradley (About.com)  
Deepak Biala (OnFiber Communications)  
Dr. Robert Cane (VPP, United Kingdom)  
Kevin Choy (Atmel, Colorado)  
Dr. Kamran Eftekhari (University of California, San Diego)  
Professor Zongming Fei (University of Kentucky)  
Dr. Carlos Ferari (JTN-Network Solutions)  
Dr. Jac Grolan (Alcatel)  
Professor Jim Griffioen (University of Kentucky)  
Ajay Kalambor (Cisco Systems)  
Parviz Karandish (Softtek, Inc.)  
Aurna Ketaraju (Intel)  
Dr. Hardeep Maldia (Sermons Communications)  
Will Morse (Texas Safe-Computing)

Professor Sarhan Musa (P. V. Texas A&M University)  
Professor Achille Pattavina (Politecnico di Milano TNG)  
Dr. Robert J. Paul (NsIM Communications)  
Bala Peddireddi (Intel)  
Christopher H. Pham (Cisco Systems)  
Jasmin Sahara (University of Southern California)  
Dipti Sathe (Altera Corporation)  
Dr. Simon Sazeman (Sierra Communications and Networks)  
Professor George Scheets (Oklahoma State University)  
Professor Mukesh Singhal (University of Kentucky)  
Professor Kazem Sohraby (University of Arkansas)  
Dr. Richard Stevansson (BoRo Comm)  
Professor Jonathan Turner (Washington University)  
Kavitha Venkatesan (Cisco Systems)  
Dr. Belle Wei (California State University, Chico)  
Dr. Steve Willmard (SIM Technology)  
Dr. Parviz Yegani (Juniper Networks)  
Dr. Hemeret Zokhil (JPLab)

I am thankful to my graduate students who helped me throughout the long phase of preparing the manuscript of this textbook. Over the past several years, more than 112 of my graduate students read various portions of this book and made constructive comments. I wish them all the best for their honest support and verbal comments on early versions of this book used in my class lectures. I am especially thankful to the following graduate students who voluntarily reviewed some sections of the book while taking my networking courses: Howard Chan, Robert Bergman, Eshetie Liku, Andrew Cole, Jonathan Hui, Lisa Wellington, and Sitthapon Pumpichet. Special thanks to Marzieh Veyseh for making all the information about sensor networks available for Chapter 22.

Last but not least, I am indebted to my parents who opened the door to the best education for me and supported me all my life; and above all, I want to thank my family who supported and encouraged me in spite of all the time it took me away from them to work on this book. It was a long and difficult journey for them.

## How to Contact the Author

Please feel free to send me any feedback at the Department of Electrical Engineering, Charles W. Davidson College of Engineering, San Jose State University, San Jose, California 95192, U.S.A., or via e-mail at [nader.mir@sjsu.edu](mailto:nader.mir@sjsu.edu). I would love to hear from you, especially if you have suggestions for improving this book. I will carefully read all review comments. You can find out more about me at [www.engr.sjsu.edu/nmir](http://www.engr.sjsu.edu/nmir). I hope that you enjoy the text and that you receive from it a little of my enthusiasm for computer communications and networks.

—*Nader F. Mir*  
*San Jose, California*

*This page intentionally left blank*

# About the Author

---

**Nader F. Mir** received the B.Sc. degree (with honors) in electrical engineering in 1985, and the M.Sc. and Ph.D. degrees, both in electrical engineering, from Washington University in St. Louis, Missouri, in 1990 and 1995, respectively.

He is currently a professor, and served as the associate chair, at the Department of Electrical Engineering, Charles W. Davidson College of Engineering, San Jose State University, California. He also serves as the academic coordinator of the university's special graduate programs offered at several Silicon Valley companies such as Lockheed-Martin Space Systems Company.

Dr. Mir is a well-known expert in patent and technology litigation cases in the areas of communications, telecommunications, and computer networks, and has worked as a patent consultant for leading companies in the field such as Google, Cisco, Netflix, Sony, Tekelec, and YouTube (Google).

Dr. Mir is internationally known through his research and scholarly work, and has been invited to speak at a number of major international conferences. He has published more than 100 refereed technical journal and conference articles, all in the field of communications and computer networking. This textbook is now a worldwide adopted university textbook and has been translated into several languages, such as Chinese.

He was granted a successful U.S. Patent (Patent 7,012,895 B1), claiming an invention related to hardware/protocol for use in high-speed computer communication networks.

Dr. Mir has received a number of prestigious national and university awards and research grants. He is the recipient of a university teaching award and also a university

research excellence award. He is also the recipient of a number of outstanding presentation awards from leading international conferences.

He is currently the technical editor of *IEEE Communications Magazine*. He has held several other editorial positions such as editor of *Journal of Computing and Information Technology*, guest editor for computer networking at *CIT Journal*, and editorial board member of the *International Journal of Internet Technology and Secured Transactions*. He is a senior member of the IEEE and has also served as a member of the technical program committee and steering committee for a number of major IEEE communications and networking conferences such as WCNC, GLOBECOM, and ICC and ICCCN conferences.

The areas of his research are: Computer and Communication Networks, TCP/IP Internet, Client/Server, SDN, Cloud Computing, Web, Load Balancing, VoIP, Video and Streaming over IP, Multimedia Networks, Design of Networking Equipment, Modems, Switches and Routers, PSTN, SS7, Wireless and Mobile Networks, and Wireless Sensor Networks.

Prior to his current position, he was an associate professor at his current school, and assistant professor at University of Kentucky in Lexington. From 1994 to 1996, he was a research scientist at the Advanced Telecommunications Institute, Stevens Institute of Technology in New Jersey, working on the design of advanced communication systems and high-speed computer networks. From 1990 to 1994, he was with the Computer and Communications Research Center at Washington University in St. Louis and worked as a research assistant on the design and analysis of a high-speed switching systems project. From 1985 to 1988, he was with Telecommunication Research & Development Center (TRDC), Surrey, and as a telecommunications system research and development engineer, participated in the design of a high-speed digital telephone Private Branch Exchange (PBX), and received the best “design/idea” award.

*This page intentionally left blank*



## CHAPTER 1

---

# Packet-Switched Networks

*Computer and communication networks* provide a wide range of services, from simple networks of computers to remote-file access to digital libraries, voice over IP (VoIP), Internet gaming, cloud computing, video streaming and conferencing, television over Internet, wireless data communication, and networking billions of users and devices. Before exploring the world of computer and communication networks, we need to study the fundamentals of *packet-switched networks* as the first step. Packet-switched networks are the backbone of the data communication infrastructure. Therefore, our focus in this chapter is on the big picture and the conceptual aspects of this backbone highlighted as:

- *Basic definitions in networks*
- *Types of packet-switched networks*
- *Packet size and optimizations*
- *Foundation of networking protocols*
- *Addressing scheme in the Internet*
- *Equal-sized packet model*

We start with the basic definitions and fundamental concepts, such as *messages*, *packets*, and *frames*, and *packet switching* versus *circuit switching*. We learn what the Internet is and how Internet service providers (ISPs) are formed. We then proceed to types of packet-switched networks and how a message can be handled by either *connection-oriented networks* or *connectionless networks*. Because readers must get a good understanding of *packets* as data units, packet size and optimizations are also discussed.

We next briefly describe specific type of networks used in the Internet. Users and networks are connected together by certain rules called *protocols*. The Internet Protocol (IP), for example, is responsible for using prevailing rules to establish paths for packets. Protocols are represented by either the TCP/IP model or the OSI model. The *five-layer TCP/IP model* is a widely accepted Internet backbone protocol structure. In this chapter, we give an overview of these five layers and leave any further details to be discussed in the remaining chapters. Among these five layers, the basics of IP *packets and network addressing* are designated a separate section in this chapter, entitled IP Packets and Addressing. We make this arrangement because basic definitions related to this layer are required in the following few chapters.

As numerous protocols can be combined to enable the movement of packets, the explanation of all other protocols will be spread over almost all upcoming chapters. In the meantime, the reader is cautiously reminded that getting a good grasp of the fundamental material discussed in this chapter is essential for following the details or extensions described in the remainder of the book. At the end of this chapter, the *equal-sized packet protocol model* is briefly introduced.

## 1.1 Basic Definitions in Networks

Communication networks have become essential media for homes and businesses. The design of modern computer and communication networks must meet all the requirements for new communication applications. A ubiquitous *broadband network* is the goal of the networking industry. Communication services need to be available anywhere and anytime. The broadband network is required to support the exchange of multiple types of information, such as voice, video, and data, among multiple types of users, while satisfying the performance requirement of each individual application. Consequently, the expanding diversity of high-bandwidth communication applications calls for a unified, flexible, and efficient network. The design goal of modern communication networks is to meet all the networking demands and to integrate capabilities of networks in a broadband network.

*Packet-switched networks* are the building blocks of computer communication systems in which data units known as *packets* flow across networks. The goal of a broadband packet-switched network is to provide flexible communication in handling all kinds of connections for a wide range of applications, such as telephone calls, data transfer, teleconferencing, video broadcasting, and distributed data processing. One obvious example for the form of traffic is *multi-rate* connections, whereby traffic containing several different bit rates flows to a communication node. The form of information in packet-switched networks is always digital bits. This kind of communication infrastructure is a significant improvement over the traditional telephone networks known as *circuit-switched networks*.

### 1.1.1 Packet Switching Versus Circuit Switching

*Circuit-switched networks*, as the basis of conventional telephone systems, were the only existing personal communication infrastructures prior to the invention of packet-switched networks. In the new communication structure, voice and computer data are treated the same, and both are handled in a unified network known as a packet-switched network, or simply an integrated data network. In conventional telephone networks, a circuit between two users must be established for communication to occur. Circuit-switched networks require resources to be reserved for each pair of end users. This implies that no other users can use the already dedicated resources for the duration of network use and thus the reservation of network resources for each user may result in inefficient use of available bandwidth.

Packet-switched networks with a unified, integrated data network infrastructure collectively known as the *Internet* can provide a variety of communication services requiring different bandwidths. The advantage of having a unified, integrated data network is the flexibility to handle existing and future services with remarkably better performance and higher economical resource utilizations. An integrated data network can also derive the benefits of central network management, operation, and maintenance. Numerous requirements for integrated packet-switched networks are explored in later chapters:

- Having robust routing protocols capable of adapting to dynamic changes in network topology
- Maximizing the utilization of network resources for the integration of all types of services

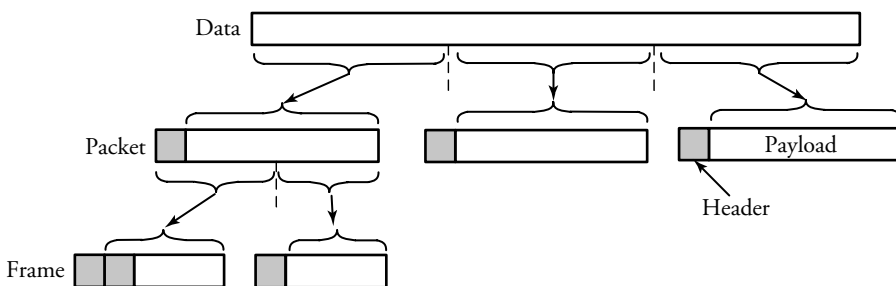
- Providing quality of service to users by means of priority and scheduling
- Enforcing effective congestion-control mechanisms that can minimize dropping packets

Circuit-switched networking is preferred for real-time applications. However, the use of packet-switched networks, especially for the integration and transmission of voice and data, results in the far more efficient utilization of available bandwidth. Network resources can be shared among other eligible users. Packet-switched networks can span a large geographical area and comprise a web of switching *nodes* interconnected through transmission links. A network provides links among multiple users facilitating the transfer of information. To make efficient use of available resources, packet-switched networks dynamically allocate resources only when required.

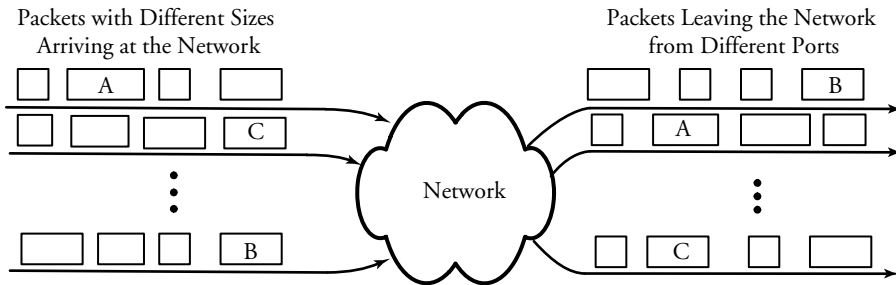
### 1.1.2 Data, Packets, and Frames

A packet-switched network is organized as a multilevel hierarchy. In such a network, digital data are fragmented into one or more smaller units of data, each appended with a *header* to specify control information, such as the source and the destination addresses, while the remaining portion carries the actual data, called the *payload*. This new unit of formatted message is called a *packet*, as shown in Figure 1.1. Packets are forwarded to a data network to be delivered to their destinations. In some circumstances, packets may also be required to be attached together or further partitioned, forming a new packet having a new header. One example of such a packet is referred to as *frame*. Sometimes, a frame may be required to have more than one header to carry out additional tasks in multiple layers of a network.

As shown in Figure 1.2, two packets, A and B, are being forwarded from one side of a network to the other side. Packet-switched networks can be viewed from



**Figure 1.1** Creating packets and frames out of a raw digital data



**Figure 1.2** A packet-switched network receiving various-sized packets to route out

either an external or an internal perspective. The external perspective focuses on the network services provided to the upper layers; the internal perspective focuses on the fundamentals of *network topology*, the structure of communication protocols, and addressing schemes.

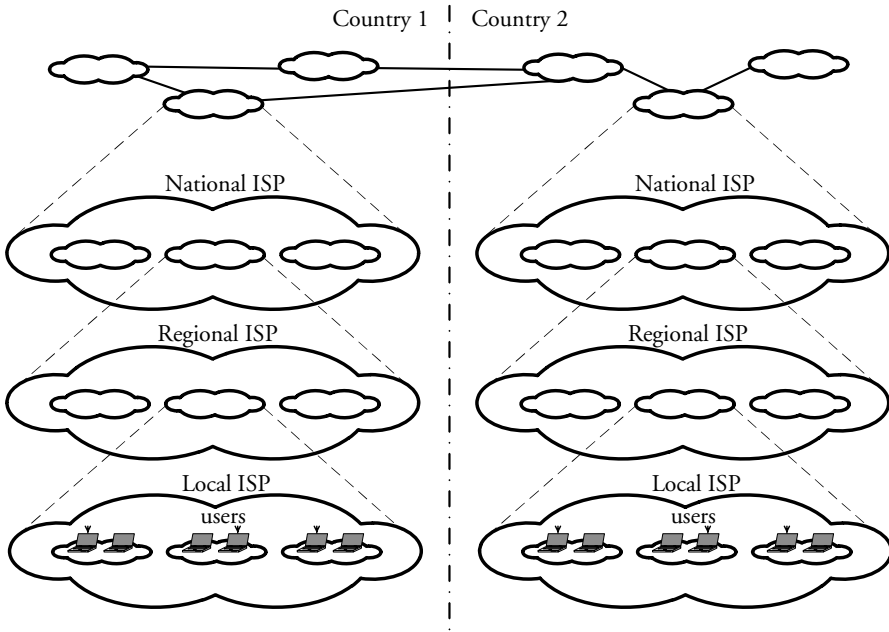
A single packet may even be split into multiple smaller packets before transmission. This well-known technique is called *packet fragmentation*. Apart from measuring the delay and ensuring that a packet is correctly sent to its destination, we also focus on delivering and receiving packets in a correct sequence when the data is fragmented. The primary function of a network is directing the flow of data among the users.

### 1.1.3 The Internet and ISPs

The *Internet* is the collection of hardware and software components that make up our global communication network. The Internet is indeed a collaboration of interconnected communication vehicles that can network all connected communicating devices and equipment and provide services to all distributed applications. It is almost impossible to plot an exact representation of the Internet, since it is continuously being expanded or altered. One way of imagining the Internet is shown in Figure 1.3, which illustrates a big-picture view of the worldwide computer network.

To connect to the Internet, users need the services of an *Internet service provider* (ISP). ISPs consist of various networking devices. One of the most essential networking devices is a *router*. Routers are network “nodes” that can operate to collectively form a network and to also connect ISPs together. Routers contain information about the network routes, and their tasks are to route packets to requested destinations.

Users, networking devices, and servers are connected together by communication *links*. Routers operate on the basis of one or more common *routing protocols*. In



**Figure 1.3** The Internet, a global interconnected network

computer networks, the entities must agree on a protocol, a set of rules governing data communications and defining when and how two users can communicate with each other. Each country has three types of ISPs:

- *National* ISPs
- *Regional* ISPs
- *Local* ISPs

At the top of the Internet hierarchy, national ISPs connect nations or provinces together. The traffic between each two national ISPs is very heavy. Two ISPs are connected together through complex switching nodes called *border routers* (or gateway routers). Each border router has its own system administrator. In contrast, *regional* ISPs are smaller ISPs connected to a national ISP in a hierarchical chart. Each regional ISP can give services to part of a province or a city. The lowest networking entity of the Internet is a local ISP. A local ISP is connected to a regional ISP or directly to a national service provider and provides a direct service to end users called *hosts*. An organization that supplies services to its own employees can also be a local ISP.

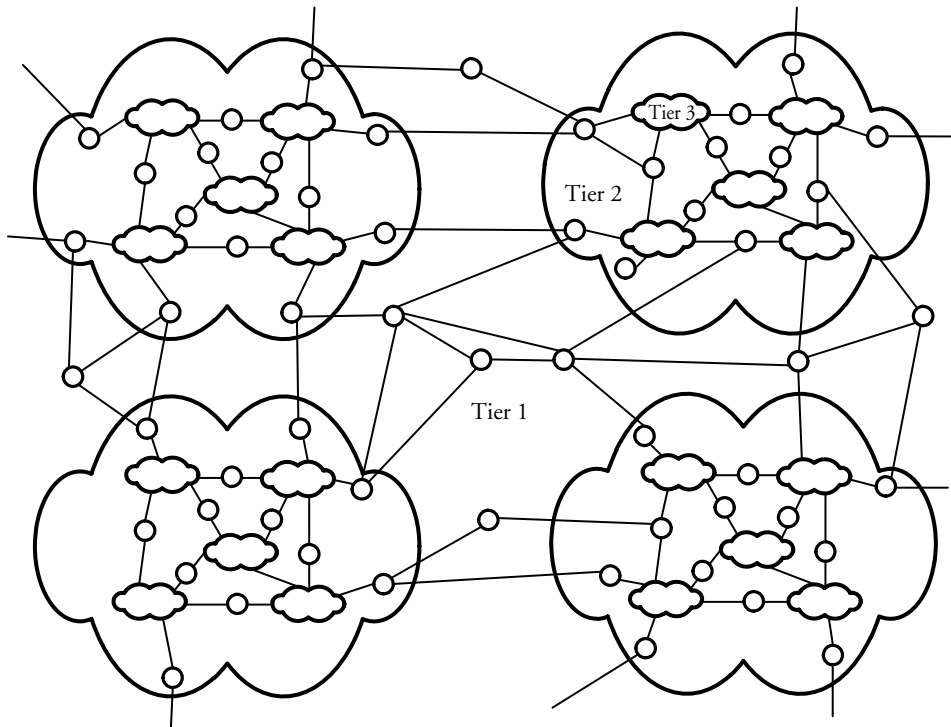
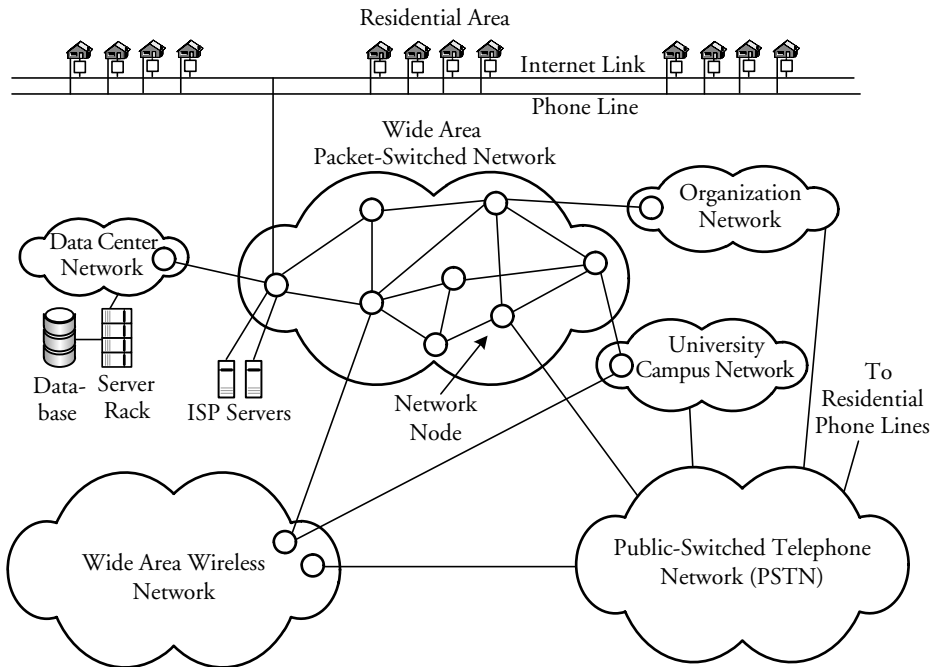


Figure 1.4 Hierarchy of networks from a different angle

Figure 1.4 illustrates a different perspective of the global interconnected network. Imagine the global network in a hierarchical structure. Each ISP of a certain hierarchy or tier manages a number of other network domains at its lower hierarchy. The structure of such networks resembles the hierarchy of nature from the universe to atoms and molecules. Here, Tier 1, Tier 2, and Tier 3 represent, respectively, a national ISP, a regional ISP, and a local ISP.

#### 1.1.4 Classification of ISPs

In most cases, a separate network managed by a network administrator is known as a *domain*, or an *autonomous system*. A domain is shown by a cloud in this book. Figure 1.5 shows several domains. An autonomous system can be administered by an *Internet service provider* (ISP). An ISP provides Internet access to its users. Networks under management of ISPs can be classified into two main categories: *wide area networks* (WANs) and *local area networks* (LANs). A wide area network can be as large as the entire infrastructure of the data network access system known as the Internet.



**Figure 1.5** Overview of various types of Internet service providers (ISPs)

A communication network can also be of wireless type both at LAN or WAN scales. We refer to such networks as *wireless networks*.

Figure 1.5 shows several major WANs each connected to several smaller networks such as a university campus network. Depending on the size of the network, a smaller network can be classified as a LAN or as a WAN. The major WANs are somehow connected together to provide the best and fastest communication for customers. One of the WANs is a wide area wireless network that connects wireless or mobile users to destination users. We notice that aggregated traffic coming from wireless equipment such as smartphone and a mobile laptop in the wide area wireless network is forwarded to a link directed from a major node. The other WAN is the telephone network known as *public-switched telephone network* (PSTN) that provides telephone services.

As an example of the local area network, a university campus network is connected to the Internet via a router that connects the campus to an Internet service provider. ISP users from a residential area are also connected to an access point router of the wide area ISP, as seen in the figure. Service providers have varying policies to overcome the problem of bandwidth allocations on routers. An ISP's *routing server* is conversant with



the policies of all other service providers. Therefore, the “ISP server” can direct the received routing information to an appropriate part of the ISP. Finally, on the left side of Figure 1.5, we see the *data center network* connected to the wide area packet-switched network. Cloud computing data centers contain databases and racks of servers that provide brilliant data processing services; these are discussed in detail in Chapter 16.

Network nodes (devices) such as *routers* are key components that allow the flow of information to be switched over other links. When a link failure occurs in a packet-switched network, the neighboring routers share the fault information with other nodes, resulting in updating of the routing tables. Thus, packets may get routed through alternative paths bypassing the fault. Building the *routing table* in a router is one of the principal challenges of packet-switched networks. Designing the routing table for large networks requires maintaining data pertaining to traffic patterns and network topology information.

## 1.2 Types of Packet-Switched Networks

Packet-switched networks are classified as *connectionless networks* and *connection-oriented networks*, depending on the technique used for transferring information. The simplest form of a network service is based on the connectionless protocol that does not require a call setup prior to transmission of packets. A related, though more complex, service is the connection-oriented protocol in which packets are transferred through an established virtual circuit between a source and a destination.

### 1.2.1 Connectionless Networks

*Connectionless networks, or datagram networks*, achieve high throughput at the cost of additional queuing delay. In this networking approach, a large piece of data is normally fragmented into smaller pieces, and then each piece of data is encapsulated into a certain “formatted” header, resulting in the basic Internet transmission packet, or *datagram*. We interchangeably use packets and datagrams for connectionless networks. Packets from a source are routed independently of one another. In this type of network, a user can transmit a packet anytime, without notifying the network layer. A packet is then sent over the network, with each router receiving the packet forwarding it to the best router it knows, until the packet reaches the destination.

The connectionless networking approach does not require a call setup to transfer packets, but it has error-detection capability. The main advantage of this scheme is its capability to route packets through an alternative path in case a fault is present on the

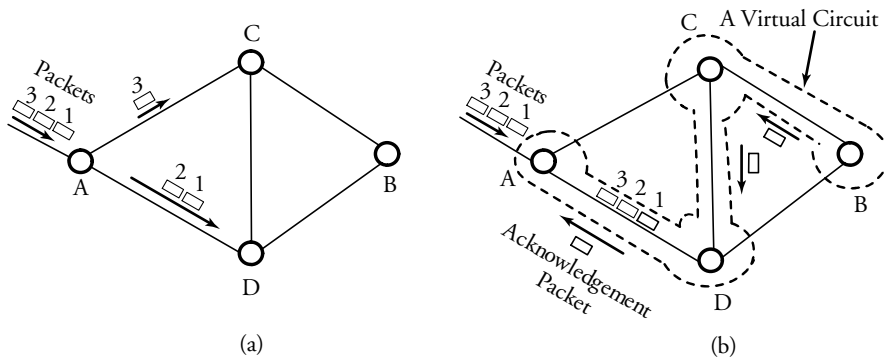
desired transmission link. On the flip side, since packets belonging to the same source may be routed independently over different paths, the packets may arrive out of sequence; in such a case, the misordered packets are resequenced and delivered to the destination.

Figure 1.6 (a) shows the routing of three packets, packets 1, 2, and 3, in a connectionless network from point A to point B. The packets traverse the intermediate nodes in a *store-and-forward* fashion, whereby packets are received and stored at a node on a route; when the desired output port of the node is free for that packet, the output is forwarded to its next node. In other words, on receipt of a packet at a node, the packet must wait in a queue for its turn to be transmitted. Nevertheless, packet loss may still occur if a node's buffer becomes full. The node determines the next hop read from the packet header. In this figure, the first two packets are moving along the path A, D, C, and B, whereas the third packet moves on a separate path, owing to congestion on path A–D.

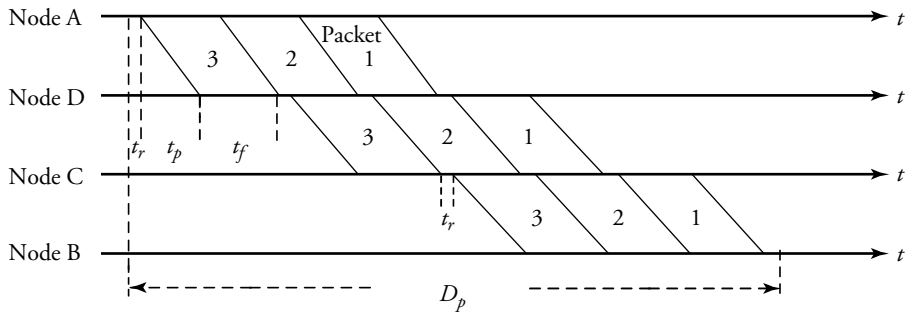
The delay model of the first three packets discussed earlier is shown in Figure 1.7. The total transmission delay for a message three packets long traversing from the source node A to the destination node B can be approximately determined. Let  $t_p$  be the propagation delay between each of the two nodes,  $t_f$  be the time it takes to inject a packet onto a link, and  $t_r$  be the total processing delay for all packets at each node. A packet is processed once it is received at a node. The total transmission delay,  $D_p$  for  $n_b$  nodes and  $n_p$  packets, in general is

$$D_p = [n_p + (n_b - 2)]t_f + (n_b - 1)t_p + n_b t_r. \quad (1.1)$$

In this equation,  $t_r$  includes a certain crucial delay component, primarily known as the *packet-queueing delay* plus some delay due to route finding for it. At this point,



**Figure 1.6** Two models of packet-switched networks: (a) a connectionless network and (b) a connection-oriented network



**Figure 1.7** Signaling delay in a connectionless network

we focus only on  $t_p$  and  $t_f$ , assume  $t_r$  is known or given, and will discuss the queuing delay and all components of  $t_r$  in later chapters, especially in Chapter 11.

**Example.** Figure 1.7 shows a timing diagram for the transmission of three (instead of two) packets on path A, D, C, B in Figure 1.6(a). Determine the total delay for transferring these three packets from node A to node B.

**Solution.** Assume that the first packet is transmitted from the source, node A, to the next hop, node D. The total delay for this transfer is  $t_p + t_f + t_r$ . Next, the packet is similarly transferred from node D to the next node to ultimately reach node B. The delay for each of these jumps is also  $t_p + t_f + t_r$ . However, when all three packets are released from node A, multiple and simultaneous transmissions of packets become possible. This means, for example, while packet 2 is being processed at node A, packet 3 is processed at node D. Figure 1.7 clearly shows this parallel processing of packets. Thus, the total delay for all three packets to traverse the source and destination via two intermediate nodes is  $D_p = 3t_p + 5t_f + 4t_r$ .

Connectionless networks demonstrate the efficiency of transmitting a large message as a whole, especially in noisy environments, where the error rate is high. It is obvious that the large message should be split into packets. Doing so also helps reduce the maximum delay imposed by a single packet on other packets. In fact, this realization resulted in the advent of connectionless packet switching.

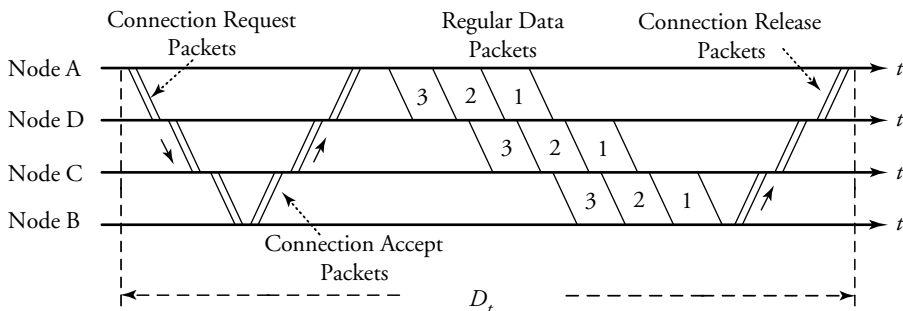
## 1.2.2 Connection-Oriented Networks

In *connection-oriented networks*, or *virtual-circuit networks*, a route setup between a source and a destination is required prior to data transfer, as in the case of conventional telephone networks. In this networking scheme, once a connection or a path

is initially set up, network resources are reserved for the communication duration, and all packets belonging to the same source are routed over the established connection. After the communication between a source and a destination is finished, the connection is terminated using a connection-termination procedure. During the call setup, the network can offer a selection of options, such as best-effort service, reliable service, guaranteed delay service, and guaranteed bandwidth service, as explained in various sections of upcoming chapters.

Figure 1.6 (b) shows a connection-oriented - network. The connection set-up procedure shown in this figure requires three packets to move along path A, D, C, and B with a prior connection establishment. During the connection set-up process, a virtual path is dedicated, and the forwarding routing tables are updated at each node in the route. Figure 1.6 (b) also shows acknowledgement packets in connection-oriented networks initiated from destination node B to source node A to acknowledge the receipt of previously sent packets to source node. The acknowledgement mechanism is not typically used in connectionless networks. Connection-oriented packet switching typically reserves the network resources, such as the buffer capacity and the link bandwidth, to provide guaranteed quality of service and delay. The main disadvantage in connection-oriented packet-switched networks is that in case of a link or switch failure, the call set-up process has to be repeated for all the affected routes. Also, each switch needs to store information about all the flows routed through the switch.

The total delay in transmitting a packet in connection-oriented packet switching is the sum of the connection set-up time and the data-transfer time. The data-transfer time is the same as the delay obtained in connectionless packet switching. Figure 1.8 shows the overall delay for the three packets presented in the previous example. The transmission of the three packets starts with *connection request packets* and then



**Figure 1.8** Signaling delay in a connection-oriented packet-switched network

*connection accept packets*. At this point, a circuit is established, and a partial path bandwidth is reserved for this connection. Then, the three packets are transmitted. At the end, a *connection release packet* clears and removes the established path.

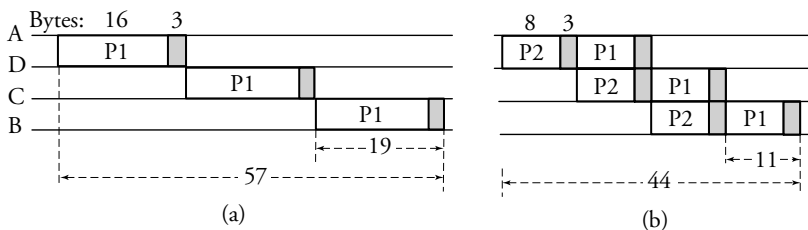
The estimation of total delay time,  $D_t$ , to transmit  $n_p$  packets is similar to the one presented for connectionless networks. For connection-oriented networks, the total time consists of two components:  $D_p$ , which represents the time to transmit packets, and  $D_c$ , which represents the time for the control packets. The control packets' time includes the transmission delay for the connection request packet, the connection accept packet, and the connection release packet:

$$D_t = D_p + D_c. \tag{1.2}$$

Another feature, called *cut-through switching*, can significantly reduce the delay. In this scheme, the packet is forwarded to the next hop as soon as the header is received and the destination is parsed. We see that the delay is reduced to the aggregate of the propagation times for each hop and the transfer time of one hop. This scheme is used in applications in which retransmissions are not necessary. Optical fiber transmission has a very low loss rate and hence uses cut-through switching to reduce the delay in transmitting a packet. We will further explain the concept of cut-through switching and its associated devices in Chapters 2 and 12.

### 1.3 Packet Size and Optimizations

Packet size has a substantial impact on the performance of data transmission. Consider Figure 1.9, which compares the transmission of a 16-byte message from node A to node B through nodes D and C. Assume that for this transmission we would like to compare the transmission of the message with two different packet



**Figure 1.9** Comparison of two cases of transmitting data: (a) using three packets and (b) using six packets

sizes but each requiring the same-size packet header of 3 bytes. In the first scheme shown in part (a) of the figure, the message is converted to a packet, P1, with 16-byte payload and 3-byte header. When the packet is received by node B, a total of 57-byte units have elapsed. If the message is fragmented into two packets, P1 and P2, of 8 bytes each as shown in part (b) of the figure, the total elapsed time becomes 44-byte units of delay.

The reason for the time reduction in the second case is the parallel transmission of two packets at nodes D and C. The parallel transmission of multiple packets can be understood better by referring again to Figure 1.7 or 1.8 in which the times of packets 2 and 1 are coinciding on the times of packets 3 and 2 in nodes D or C. The trend of delay reduction using smaller packets, however, is reversed at a certain point, owing to the dominance of packet overhead when a packet becomes very small.

To analyze packet size optimization, consider a link with a speed of  $s$  b/s or a rate of  $\mu$  packets per second. Assume that packets of size  $d + h$  are sent over this link at the rate  $\lambda$  packets per second, where  $d$  and  $h$  are the sizes of the packet data and the packet header, respectively, in bits. Clearly,

$$\mu = \frac{s}{d + h}. \quad (1.3)$$

We define *link utilization* to be  $\rho = \lambda/\mu$ . Then the percentage of link utilization used by data,  $\rho_d$ , is obtained by

$$\rho_d = \rho \left( \frac{d}{d + h} \right). \quad (1.4)$$

The average delay per packet,  $D$ , can be calculated by using  $\mu - \lambda$ , where this term exhibits how close the offered load is to the link capacity:

$$D = \frac{1}{\mu - \lambda}. \quad (1.5)$$

Using Equations (1.3) and (1.4), we can rewrite the average delay per packet as

$$D = \frac{1}{\mu(1 - \rho)} = \frac{d + h}{s(1 - \rho)} = \frac{d + h}{s \left[ 1 - \frac{\rho_d}{d}(d + h) \right]}. \quad (1.6)$$

Apparently, the optimum size of a packet depends on several contributing factors. Here, we examine one of the factors by which the delay and the packet size become optimum. For optimality, consider  $d$  as one possible variable, where we want

$$\frac{\partial D}{\partial d} = 0. \quad (1.7)$$

This releases the two optimum values (we skip from the detail of derivation):

$$d_{opt} = h \left( \frac{\sqrt{\rho_d}}{1 - \sqrt{\rho_d}} \right) \quad (1.8)$$

and

$$D_{opt} = \frac{h}{s} \left( \frac{\sqrt{\rho_d}}{1 - \sqrt{\rho_d}} \right)^2. \quad (1.9)$$

Note that here,  $d_{opt}$  and  $D_{opt}$  are optimized values of  $d$  and  $D$ , respectively, given only the mentioned variables. The optimality of  $d$  and  $D$  can also be derived by using a number of other factors that will result in a more accurate approach.

## 1.4 Foundation of Networking Protocols

As discussed earlier in this chapter, users and networks are connected together by certain rules and regulations called *network communication protocols*. The Internet Protocol (IP), for example, is responsible for using prevailing rules to establish paths for packets. Communication protocols are the intelligence behind the driving force of packets and are tools by which a network designer can easily expand the capability of networks. One growth aspect of computer networking is clearly attributed to the ability to conveniently add new features to networks. New features can be added by connecting more hardware devices, thereby expanding networks. New features can also be added on top of existing hardware, allowing the network features to expand.

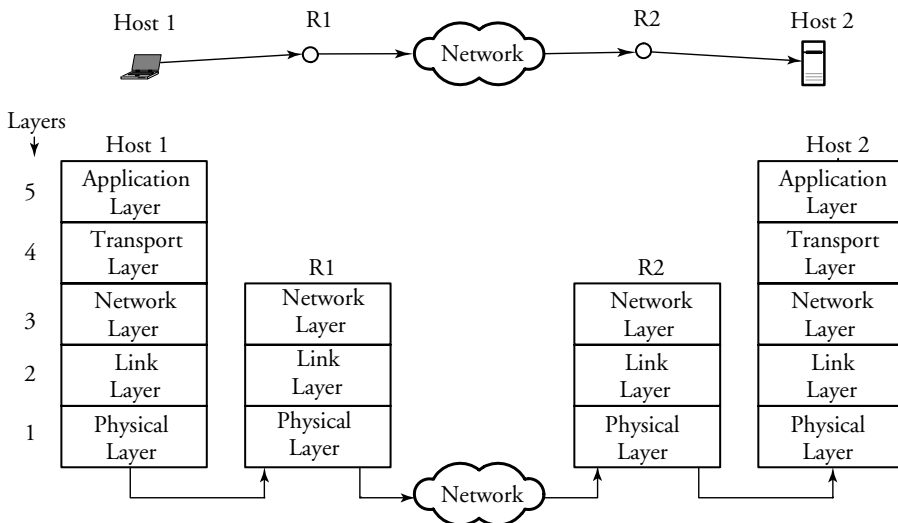
Protocols of communication networks are represented by either the TCP/IP model or its older version, the OSI model. The *five-layer TCP/IP model* is a widely accepted Internet backbone protocol structure. In this section, we describe the basics of these five layers and leave further details to be discussed in the remaining chapters.

However, among these five layers, the basics of IP *packets and network addressing* are designated a separate section, 1.5 IP Packets and Addressing. As stated before, we make this arrangement because basic definitions related to this layer are required in the following chapters, mostly in Part I of this book.

### 1.4.1 Five-Layer TCP/IP Protocol Model

The basic structure of communication networks is represented by the *Transmission Control Protocol/Internet Protocol (TCP/IP)* model. This model is structured in five layers. An end system, an intermediate network node, or each communicating user or program is equipped with devices to run all or some portions of these layers, depending on where the system operates. These five layers, shown in Figure 1.10, are as follows:

1. Physical layer
2. Link layer
3. Network layer
4. Transport layer
5. Application layer



**Figure 1.10** Hierarchy of the five-layer communication protocol model



*Layer 1*, known as the *physical layer*, defines electrical aspects of activating and maintaining physical links in networks. The physical layer represents the basic network hardware. The physical layer also specifies the type of medium used for transmission and the network topology. The details of this layer are explained in later chapters, especially in Chapters 3, 4, 6, 13, 15, 17, and 20.

*Layer 2*, the *link layer*, provides a reliable synchronization and transfer of information across the physical layer for accessing the transmission medium. Layer 2 specifies how packets access links and are attached to additional headers to form frames when entering a new networking environment, such as a LAN. Layer 2 also provides error detection and flow control. This layer is discussed further in Chapters 3 and 4 and the discussion is extended in almost all other chapters.

*Layer 3*, the *network layer* (IP) specifies the networking aspects. This layer handles the way that addresses are assigned to packets and the way that packets are supposed to be forwarded from one end point to another. Some related parts of this layer are described in Chapters 5, 6, and 7, and the discussion is extended in other chapters such as Chapters 10, 12, 13, 14, 15, 16, 21, and 22.

*Layer 4*, the *transport layer*, lies just above the network layer and handles the details of data transmission. Layer 4 is implemented in the end points but not in network routers and acts as an interface protocol between a communicating device and a network. Consequently, this layer provides logical communication between processes running on different hosts. The concept of the transport layer is discussed in Chapter 8, and the discussion is extended in other chapters such as Chapters 9, 14, 17, 18, 20, 21, and 22.

*Layer 5*, the *application layer*, determines how a specific user application should use a network. Among such applications are the *Simple Mail Transfer Protocol* (SMTP), *File Transfer Protocol* (FTP), and the *World Wide Web* (WWW). The details of layer 5 are described in Chapter 9, and descriptions of other advanced applications such as voice over IP (VoIP) are extended in other chapters such as Chapters 18, 19, and 20.

The transmission of a given message between two users is carried out by (1) flowing the data down through each and all layers of the transmitting end, (2) sending it to certain layers of protocols in the devices between two end points, and (3) when the message arrives at the other end, letting the data flow up through the layers of the receiving end until it reaches its destination.

## Hosts

A network *host* is a computing device connected to a computer network and is assigned a network layer address. A host can offer information resources, services, and applications to users or other nodes on the network. Figure 1.10 illustrates a

scenario in which different layers of protocols are used to establish a connection between two hosts. A message is transmitted from host 1 to host 2, and, as shown, all five layers of the protocol model participate in making this connection. The data being transmitted from host 1 is passed down through all five layers to reach router R1. Router R1 is located as a gateway to the operating regions of host 1 and therefore does not involve any tasks in layers 4 and 5. The same scenario is applied at the other end: router R2. Similarly, router R2, acting as a gateway to the operating regions of host 2, does not involve any tasks in layers 4 and 5. Finally at host 2, the data is transmitted upward from the physical layer to the application layer.

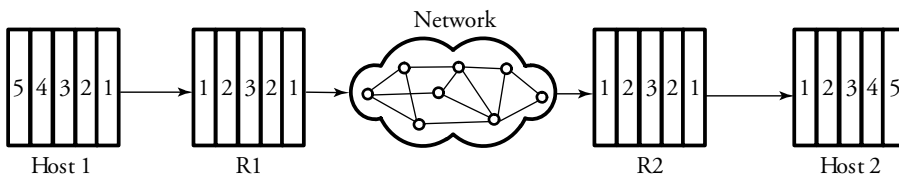
The main idea of the communication protocol stack is that the process of communication between two end points in a network can be partitioned into layers, with each layer adding its own set of special related functions. Figure 1.11 shows a different way of realizing protocol layers used for two hosts communicating through two routers. This figure illustrates a structural perspective of a communication setup and identifies the order of fundamental protocol layers involved.

## 1.4.2 Seven-Layer OSI Model

The *open systems interconnection* (OSI) model was the original standard description for how messages should be transmitted between any two points. To the five TCP/IP layers, OSI adds the following two layers below the application layer:

1. *Layer 5, the session layer*, which sets up and coordinates the applications at each end
2. *Layer 6 the presentation layer*, which is the operating system part that converts incoming and outgoing data from one presentation format to another

The tasks of these two additional layers are dissolved into the application and transport layers in the newer five-layer TCP/IP model. The OSI model is becoming less popular. TCP/IP is gaining more attention, owing to its stability and its ability to offer better communication performance. Therefore, this book focuses on the five-layer model.

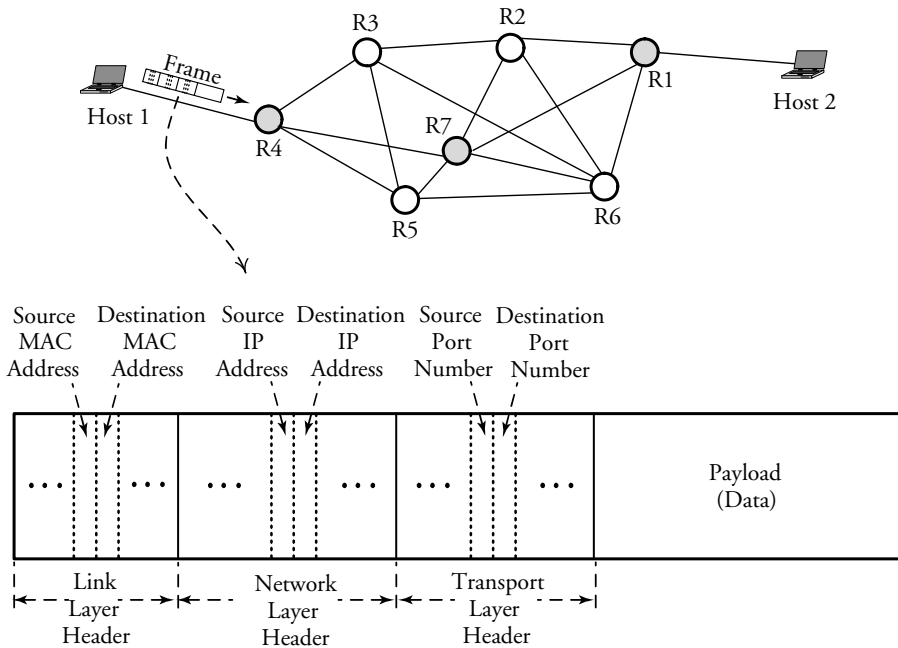


**Figure 1.11** Structural view of protocol layers for two hosts communicating through two routers

## 1.5 Addressing Scheme in the Internet

An addressing scheme is clearly a requirement for communications in a computer network. With an addressing scheme, packets are forwarded from one location to another. Each of the three layers, 2, 3, and 4, of the TCP/IP protocol stack model produces a header, as indicated in Figure 1.12. In this figure, host 1 communicates with host 2 through a network of seven nodes, R1 through R7, and a payload of data encapsulated in a frame by the link layer header, the network layer header, and the transport layer header is carried over a link. Within any of these three headers, each source or destination is assigned an address as identification for the corresponding protocol layer. The three types of addresses are summarized as follows.

- *Link layer (layer 2) address.* A 6-byte (48-bit) field called Media Access Control (MAC) address that is represented by a 6-field hexadecimal number, such as 89-A1-33-2B-C3-84, in which each field is two bytes long. Every input or output of a networking device has an interface to its connected link, and every interface has a unique MAC address. A MAC address is known only locally at the link level. Normally, it is safe to assume that no two interfaces share the same MAC address. A link layer header contains both MAC addresses of a source interface and a destination interface, as seen in the figure.
- *Network layer (layer 3) address.* A 4-byte (32-bit) field called Internet Protocol (IP) address that is represented by a 4-field dot-separated number, such as 192.2.32.83, in which each field is one byte long. Every entity in a network must have an IP address in order to be identified in a communication. An IP address can be known globally at the network level. A network layer header contains both IP addresses of a source node and a destination node, as seen in the figure.
- *Transport layer (layer 4) address.* A 2-byte (16-bit) field called port number that is represented by a 16-bit number, such as 4,892. The port numbers identify the two end hosts' ports in a communication. Any host can be running several network applications at a time and thus each application needs to be identified by another host communicating to a targeted application. For example, source host 1 in Figure 1.12 requires a port number for communication to uniquely identify an application process running on the destination host 2. A transport layer header contains the port numbers of a source host and a destination host, as seen in the figure. Note that a transport-layer "port" is a logical port and not an actual or a physical one, and it serves as the end-point application identification in a host.

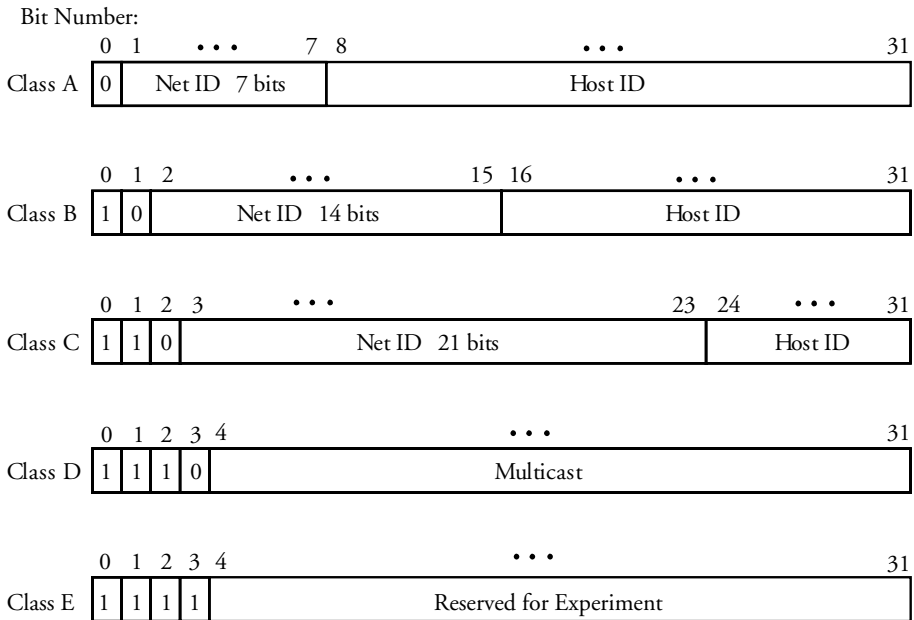


**Figure 1.12** A typical frame structure that is forwarded over a link

The details of the link layer header, including the MAC addresses and all other of the header's fields are described in Chapter 4. The details of the network layer header fields, including the IP addresses and all other of the header's fields are presented in Chapter 5. Finally, the details of the transport layer header, including the port numbers and all other of the header's fields are explained in Chapter 8. In the meanwhile, some of the basic IP addressing schemes are presented in the next section, as understanding IP addressing will help us better understand the upcoming networking concepts.

### 1.5.1 IP Addressing Scheme

The IP header has 32 bits assigned for addressing a desired device on the network. An IP address is a unique identifier used to locate a device on the IP network. To make the system scalable, the address structure is subdivided into the *network* ID and the *host* ID. The network ID identifies the network the device belongs to; the host ID identifies the device. This implies that all devices belonging to the same network have a single network ID. Based on the bit positioning assigned to the network ID and the host ID, the IP address is further subdivided into classes A, B, C, D (multicast), and E (reserved), as shown in Figure 1.13.



**Figure 1.13** Classes of IP addresses

Consider the lengths of corresponding fields for each class shown in this figure:

- Class A starts with 0 followed by 7 bits of network ID and 24 bits of host ID.
- Class B starts with 10 followed by 14 bits of network ID and 16 bits of host ID.
- Class C starts with 110 followed by 21 bits of network ID and 8 bits of host ID.
- Class D starts with 1110 followed by 28 bits. Class D is used only for multicast addressing by which a group of hosts form a multicast group and each group requires a multicast address. Chapter 6 is entirely dedicated to multicast techniques and routing.
- Class E starts with 1111 followed by 28 bits. Class E is reserved for network experiments only.

For ease of use, the IP address is represented in *dot-decimal* notation. The address is grouped into four dot-separated bytes. For example, an IP address with 32 bits of all 0s can be shown by a dot-decimal form of 0.0.0.0 where each 0 is the representation of 00000000 in a logic bit format.

A detailed comparison of IP addressing is shown in the Table 1.1. Note that in this table, each of the “number of available network addresses” and the “number of available

**Table 1.1** Comparison of IP addressing schemes

Class	Bits to Start	Size of Network ID Field	Size of Host ID Field	Number of Available Network Addresses	Number of Available Host Addresses per Network	Start Address	End Address
A	0	7	24	126	16,777,214	0.0.0.0	127.255.255.255
B	10	14	16	16,382	65,534	128.0.0.0	191.255.255.255
C	110	21	8	2,097,150	254	192.0.0.0	223.255.255.255
D	1110	N/A	N/A	N/A	N/A	224.0.0.0	239.255.255.255
E	1111	N/A	N/A	N/A	N/A	240.0.0.0	255.255.255.255

host addresses per network” has already been decreased by 2. For example, in class A, the size of the network ID field is indicated in the table to be  $N = 7$ ; however, the number of available network addresses is presented as  $2^N - 2 = 128 - 2 = 126$ . The subtraction of 2 adjusts for the use of the all-bits-zero network ID (0 in decimal) and the all-bits-one network ID (127 in decimal). These two network IDs, 0 and 127, are reserved for management and cannot be available for any other use. The same argument is true for the number of available host addresses, where with the size of the host ID field indicated as  $N = 24$ , we can have  $2^N - 2 = 16,777,216 - 2 = 16,777,214$  host addresses per network available for use. The last two columns of the table show the start address and the end address of each class, including the reserved addresses explained earlier.

**Example.** A host has an IP address of 10001000 11100101 11001001 00010000. Find the class and decimal equivalence of the IP address.

**Solution.** The host’s IP address belongs to class B, since it starts with 10. Its decimal equivalent is 136.229.201.16.

## 1.5.2 Subnet Addressing and Masking

The concept of subnetting was introduced to overcome the shortcomings of IP addressing. Managing a large number of hosts is an enormous task. For example, a company that uses a class B addressing scheme can support up to 65,535 hosts on one network. If the company has more than one network, a multiple-network address scheme, or *subnet scheme*, is used. In this scheme, the host ID of the original IP address is subdivided into *subnet ID* and *host ID*, as shown in Figure 1.14.

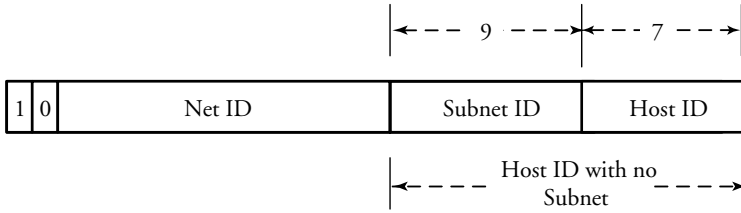


Figure 1.14 A subnet ID and host ID in class B addressing

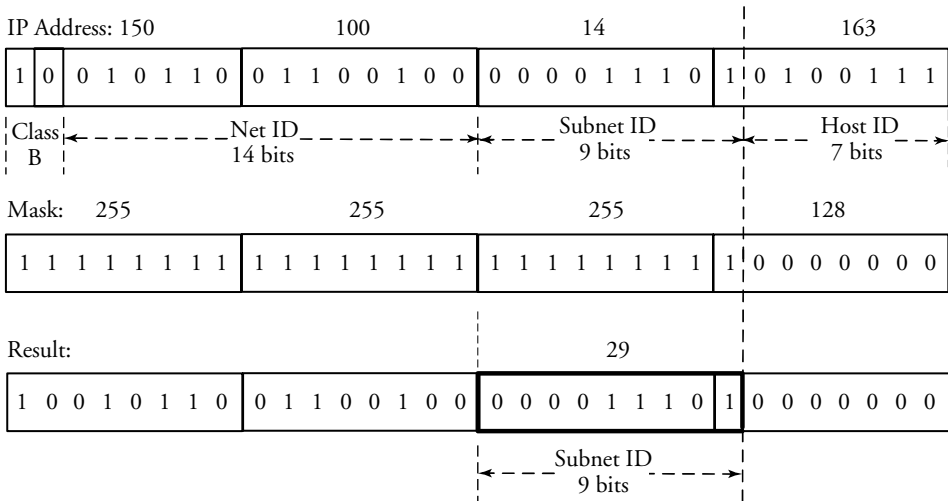


Figure 1.15 An example of subnet and masking

Depending on the network size, different values of subnet ID and host ID can be chosen. Doing so would prevent the outside world from being burdened by a shortage of new network addresses. To determine the subnetting number, a subnet *mask*—logic AND function—is used. The subnet mask has a field of all 0s for the host ID and a field of all 1s for the remaining field.

**Example.** Given an IP address of 150.100.14.163 and a subnet mask of 255.255.255.128, determine the maximum number of hosts per subnet.

**Solution.** Figure 1.15 shows the details of the solution. Masking 255.255.255.128 on the IP address results in 150.100.14.128. Clearly, the IP address 150.100.14.163 is a class B address. In a class B address, the lower 16 bits are assigned to the subnet and host fields. Applying the mask, we see that the maximum number of hosts is  $2^7 = 128$ .

**Example.** A router attached to a network receives a packet with the destination IP address 190.155.16.16. The network is assigned an address of 190.155.0.0. Assume that the network has two subnets with addresses 190.155.16.0 and 190.155.15.0 and that both subnet ID fields have 8 bits. Demonstrate the details of routing the packet.

**Solution.** When it receives the packet, the router determines to which subnet the packet needs to be routed, as follows: The destination IP address is 190.155.16.16, the subnet mask used in the router is 255.255.255.0, and the result is 190.155.16.0. The router looks up its routing table for the next subnet corresponding to the subnet 190.155.16.0, which is subnet 2. When the packet arrives at subnet 2, the router determines that the destination is on its own subnet and routes the packet to its destination.

### 1.5.3 Classless Interdomain Routing (CIDR)

The preceding section described an addressing scheme requiring that the address space be subdivided into five classes. However, giving a certain class C address space to a certain university campus does not guarantee that all addresses within the space can be used and therefore might waste some addresses. This kind of situation is inflexible and would exhaust the IP address space. Thus, the classful addressing scheme consisting of classes A, B, C, D, and E results in an inefficient use of the address space.

A new scheme, with no restriction on the classes, emerged. *Classless interdomain routing* (CIDR) is extremely flexible, allowing a variable-length *prefix* to represent the network ID and the remaining bits of the 32-bit address to represent the hosts within the network. For example, one organization may choose a 20-bit network ID, whereas another organization may choose a 21-bit network ID, with the first 20 bits of these two network IDs being identical. This means that the address space of one organization contains that of another one.

CIDR results in a significant increase in the speed of routers and has greatly reduced the size of routing tables. A routing table of a router using the CIDR address space has entries that include a pair of network IP addresses and the mask. *Supernetting* is a CIDR technique whereby a single routing entry is sufficient to represent a group of adjacent addresses. Because of the use of a variable-length prefix, the routing table may have two entries with the same prefix. To route a packet that



matches both of these entries, the router chooses between the two entries, using the longest-prefix-match technique.

**Example.** Assume that a packet with destination IP address 205.101.0.1 is received by router R1, as shown in Figure 1.16. Find the final destination of the packet.

**Solution.** In the table entries of router R1, two routes, L1 and L2, belonging to 205.101.8.0/20 and 205.101.0.0/21, respectively, are initially matched with the packet's IP address. CIDR protocol then dictates that the longer prefix must be the eligible match. As indicated at the bottom of this figure, link L1, with its 21-bit prefix, is selected, owing to a longer match. This link eventually routes the packet to the destination network, N3.

CIDR allows us to reduce the number of entries in a router's table by using an *aggregate technique*, whereby all entries that have some common partial prefix can be combined into one entry. For example, in Figure 1.16, the two entries 205.101.8.0/20 and 205.101.0.0/21 can be combined into 205.101.0.0/20, saving one entry in the table. Combining entries in routing tables not only saves space but also enhances the speed of the routers, as each time, routers need to search among fewer addresses.

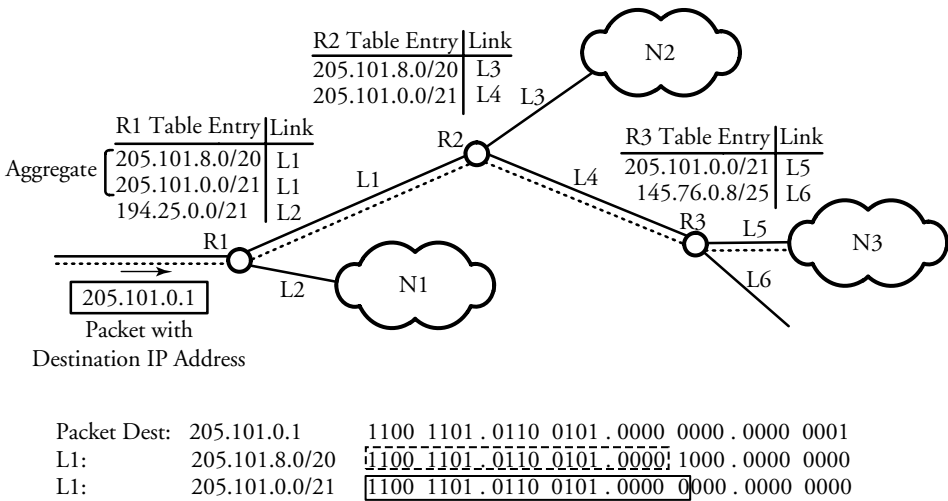


Figure 1.16 CIDR routing

## 1.6 Equal-Sized Packets Model

A networking model in which packets are of equal size can also be constructed. Equal-sized packets, or *cells*, bring a tremendous amount of simplicity to the networking hardware, since buffering, multiplexing, and switching of cells become extremely simple. However, a disadvantage of this kind of networking is the typically high overall ratio of header to data. This issue normally arises when the message size is large and the standard size of packets is small. As discussed in Section 1.3, the dominance of headers in a network can cause delay and congestion.

One of the networking technologies established using the equal-sized packets model is *asynchronous transfer mode* (ATM). The objective of ATM technology is to provide a homogeneous backbone network in which all types of traffic are transported with the same small fixed-sized *cells*. One of the key advantages of ATM systems is flexible processing of packets (cells) at each node. Regardless of traffic types and the speed of sources, the traffic is converted into 53-byte ATM cells. Each cell has a 48-byte data payload and a 5-byte header. The header identifies the virtual channel to which the cell belongs. However, because the high overall ratio of header to data in packets results in huge delays in wide area networks, ATM is rarely deployed in networking infrastructure and therefore we do not expand our discussion on ATM beyond this section.

## 1.7 Summary

This chapter established a conceptual foundation for realizing all upcoming chapters. First, we clearly identified and defined all basic key terms in networking. We showed a big-picture view of computer networks in which from one side, mainframe servers can be connected to a network backbone, and from the other side, home communication devices are connected to a backbone network over long-distance telephone lines. We illustrated how an Internet service provider (ISP) controls the functionality of networks. ISPs have become increasingly involved in supporting packet-switched networking services for carrying all sorts of data, not just voice, and the cable TV industry.

The transfer of data in packet-switched networks is organized as a multilevel hierarchy, with digital messages fragmented into units of formatted messages, or packets. In some circumstances, such as local area networks, packets must be modified further, forming a smaller or larger packet known as a frame. Two types of packet-switched networks are networks using connectionless protocol, in which no particular advanced connection is required, and networks using connection-oriented protocol, in which an advance dedication of a path is required.

A packet's size can be optimized. Using the percentage of link utilization by data,  $\rho_d$ , as a main variable, we showed that the optimized packet size and the optimized packet delay depend on  $\rho_d$ . The total delay of packet transfer in a connectionless network may be significantly smaller than the one for a connection-oriented network since if you have a huge file to transfer, the set-up and tear-down times may be small compared to the file transfer time.

This chapter also covered a tremendous amount of fundamental networking protocol material. We presented the basic structure of the Internet network protocols and an overview of the TCP/IP layered architecture. This architectural model provides a communication service for peers running on different machines and exchanging messages.

We also covered the basics of protocol layers: the *network layer* and the structure of IPv4 and IPv6. IP addressing is further subdivided as either *classful* or *classless*. Classless addressing is more practical for managing routing tables. Finally, we compared the equal-sized packet networking environment to IP networks. Although packet multiplexing is easy, the traffic management is quite challenging.

The next chapter focuses on the fundamental operations of networking devices and presents an overview of the hardware foundations of our networking infrastructure. Networking devices are used to construct a computer network.

## 1.8 Exercises

1. We transmit data directly between two servers 6,000 km apart through a geostationary satellite situated 10,000 km from Earth exactly between the two servers. The data enters this network at 100Mb/s.
  - (a) Find the propagation delay if data travels at the speed of light ( $2.3 \times 10^8$  m/s).
  - (b) Find the number of bits in transit during the propagation delay.
  - (c) Determine how long it takes to send 10 bytes of data and to receive 2.5 bytes of acknowledgment back.
2. We would like to analyze a variation of Exercise 1 where servers are placed in substantially closer proximity to each other still using satellite for communication. We transmit data directly between two servers 60 m apart through a geostationary satellite situated 10,000 km from Earth exactly between the two servers. The data enters this network at 100Mb/s.
  - (a) Find the propagation delay if data travels at the speed of light ( $2.3 \times 10^8$  m/s).
  - (b) Find the number of bits in transit during the propagation delay.
  - (c) Determine how long it takes to send 10 bytes of data and to receive 2.5 bytes of acknowledgment back.

3. Stored on a flash memory device is a 200 megabyte (MB) message to be transmitted by an e-mail from one server to another, passing three nodes of a *connectionless network*. This network forces packets to be of size 10KB, excluding a packet header of 40 bytes. Nodes are 400 miles apart, and servers are 50 miles away from their corresponding nodes. All transmission links are of type 100Mb/s. The processing time at each node is 0.2 seconds.
  - (a) Find the propagation delays per packet between a server and a node and between nodes.
  - (b) Find the total time required to send this message.
4. Equation (1.2) gives the total delay time for connection-oriented networks. Let  $t_p$  be the packet propagation delay between each two nodes,  $t_{f1}$  be the data packet transfer time to the next node, and  $t_{r1}$  be the data packet processing time. Also, let  $t_{f2}$  be the control-packet transfer time to the next node, and  $t_{r2}$  be the control-packet processing time. Give an expression for  $D$  in terms of all these variables.
5. Suppose that a 200MB message stored on a flash memory device attached to a server is to be uploaded to a destination server through a connection-oriented packet-switched network with three serially connected nodes. This network forces packets to be of size 10KB, including a packet header of 40 bytes. Nodes are 400 miles apart from each other and each server is 50 miles away from its corresponding node. All transmission links are of type 100Mb/s. The processing time at each node is 0.2 seconds. For this purpose, the signaling packet is 500 bits long.
  - (a) Find the total connection request/accept process time.
  - (b) Find the total connection release process time.
  - (c) Find the total time required to send this message.
6. We want to deliver a 12KB message by uploading it to the destination's Web site through a 10-node path of a *virtual-circuit packet-switched network*. For this purpose, the signaling packet is 500 bits long. The network forces packets to be of size 10KB including a packet header of 40 bytes. Nodes are 500 miles apart. All transmission links are of type 1Gb/s. The processing time at each node is 100 ms per packet and the propagation speed is  $2.3 \times 10^8$  m/s.
  - (a) Find the total connection request/accept process time.
  - (b) Find the total connection release process time.
  - (c) Find the total time required to send this message.

7. Consider five serial connected nodes A, B, C, D, E and that 100 bytes of data are supposed to be transmitted from node A to E using a protocol that requires packet headers to be 20 bytes long.
  - (a) Ignore  $t_p$ ,  $t_r$ , and all control signals; and sketch and calculate total  $t_f$  in terms of byte-time to transmit the data for cases in which the data is converted into 1 packet, 2 packets, 5 packets, and 10 packets.
  - (b) Put all the results obtained from part (a) together in one plot and estimate where the plot approximately shows the minimum delay (no mathematical work is needed, just indicate the location of the lowest delay transmission on the plot).
8. To analyze the transmission of a 10,000-bit-long packet, we want the percentage of link utilization used by the data portion of a packet to be 72 percent. We also want the ratio of the packet header,  $h$ , to packet data,  $d$ , to be 0.04. The transmission link speed is  $s = 100$  Mb/s.
  - (a) Find the link utilization,  $\rho$ .
  - (b) Find the link capacity rate,  $\mu$ , in terms of packets per second.
  - (c) Find the average delay per packet.
  - (d) Find the optimum average delay per packet.
9. Consider a digital link with a maximum capacity of  $s = 100$  Mb/s facing a situation resulting in 80 percent utilization. Equal-sized packets arrive at 8,000 packets per second. The link utilization dedicated to headers of packets is 0.8 percent.
  - (a) Find the total size of each packet.
  - (b) Find the header and data sizes for each packet.
  - (c) If the header size is not negotiable, what would the optimum size of packets be?
  - (d) Find the delay for each optimally sized packet.
10. Develop a signaling delay chart, similar to Figures 1.7 and 1.8, for circuit-switched networks. From the mentioned steps, get an idea that would result in the establishment of a telephone call over circuit-switched networks.
11. In practice, the optimum size of a packet estimated in Equation (1.7) depends on several other contributing factors.
  - (a) Derive the optimization analysis, this time also including the header size,  $h$ . In this case, you have two variables:  $d$  and  $h$ .
  - (b) What other factors might also contribute to the optimization of the packet size?
12. Specify the class of address and the subnet ID for the following cases:
  - (a) A packet with IP address 127.156.28.31 using mask pattern 255.255.255.0
  - (b) A packet with IP address 150.156.23.14 using mask pattern 255.255.255.128
  - (c) A packet with IP address 150.18.23.101 using mask pattern 255.255.255.128

13. Specify the class of address and the subnet ID for the following cases:
  - (a) A packet with IP address 173.168.28.45 using mask pattern 255.255.255.0
  - (b) A packet with IP address 188.145.23.1 using mask pattern 255.255.255.128
  - (c) A packet with IP address 139.189.91.190 using mask pattern 255.255.255.128
14. Apply CIDR aggregation on the following IP addresses: 150.97.28.0/24, 150.97.29.0/24, and 150.97.30.0/24.
15. Apply CIDR aggregation on the following IP addresses: 141.33.11.0/22, 141.33.12.0/22, and 141.33.13.0/22.
16. Use the subnet mask 255.255.254.0 on the following IP addresses, and then convert them to CIDR forms:
  - (a) 191.168.6.0
  - (b) 173.168.28.45
  - (c) 139.189.91.190
17. A certain organization owns a subnet with prefix 143.117.30.128/26.
  - (a) Give an example of one of the organization's IP addresses.
  - (b) Assume the organization needs to be downsized, and it wants to partition its block of addresses and create three new subnets, with each new block having the same number of IP addresses. Give the CIDR form of addresses for each of the three new subnets.
18. A packet with the destination IP address 180.19.18.3 arrives at a router. The router uses CIDR protocols, and its table contains three entries referring to the following connected networks: 180.19.0.0/18, 180.19.3.0/22, and 180.19.16.0/20, respectively.
  - (a) From the information in the table, identify the exact network ID of each network in binary form.
  - (b) Find the right entry that is a match with the packet.
19. Part of a networking infrastructure consists of three routers R1, R2, and R3 and six networks N1 through N6, as shown in Figure 1.17. All address entries of each router are also given as seen in the figure. A packet with the destination IP address 195.25.17.3 arrives at router R1.
  - (a) Find the exact network ID field of each network in binary form.
  - (b) Find the destination network for the packet (proof needed).
  - (c) Specify how many hosts can be addressed in network N1.

R1 Table Entry	Link	R2 Table Entry	Link	R3 Table Entry	Link
195.25.0.0/21	L11	195.25.24.0/19	L21	111.5.0.0/21	L31
195.25.16.0/20	L12	195.25.16.0/20	L22	Else	L32
195.25.8.0/22	L13	195.25.8.0/22	L23	195.25.16.0/20	L33
135.11.2.0/22	L14				

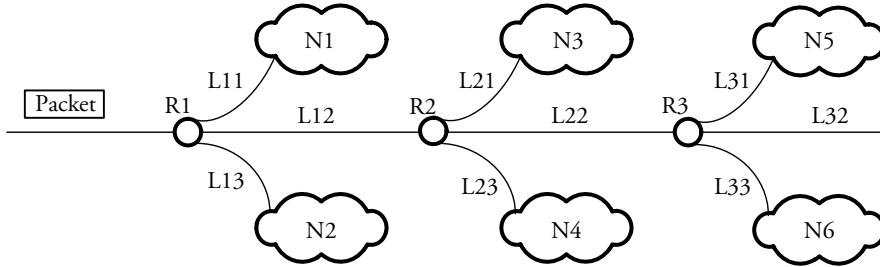


Figure 1.17 Exercise 19 network example

20. Consider an estimated population of 620 million people.
- What is the maximum number of IP addresses that can be assigned per person using IPv4?
  - Design an appropriate CIDR to deliver the addressing in part (a).
21. A router with four output links L1, L2, L3, and L4 is set up based on the following routing table:

Mask Result	Link
192.5.150.16	L3
192.5.150.18	L2
129.95.38.0	L1
129.95.38.15	L3
129.95.39.0	L2
Unidentified	L4

The router has a masking pattern of 255.255.255.240 and examines each packet using the mask in order to find the right output link. For a packet addressed to each of the following destinations, specify which output link is found:

- 192.5.150.18
- 129.95.39.10
- 129.95.38.15
- 129.95.38.149

22. A router with four output links L1, L2, L3, and L4 is set up based on the following routing table:

Mask Result	Link
192.5.150.0	L1
129.95.39.0	L2
129.95.38.128	L3
Unidentified	L4

The router has two masking patterns of 255.255.255.128 and 255.255.255.1 and examines each packet using these masks in the preceding order to find a right output link among L1, L2, and L3. If a mask finds one of the three outputs, the second mask is not used. Link L4 is used for those packets for which none of the masks can determine an output link. For a packet addressed to a destination having each of the following IP addresses, specify which mask pattern finds a link for the packet and then which output port (link) is found:

- (a) 129.95.39.10
- (b) 129.95.38.16
- (c) 129.95.38.149

## 1.9 Computer Simulation Project

1. **Simulation of Networking Packets.** Write a computer program in C or C++ to simulate a “packet.” Each packet must have two distinct parts: header and data. The data is fixed on 10 bytes consisting of all logic 1s. The header is 9 bytes long and consists of three fields only: priority (1 byte), source address (4 bytes), and destination address (4 bytes).
  - (a) For a Packet A, initialize the priority field to be 0, and source and destination addresses to be 10.0.0.1 and 192.0.1.0, respectively.
  - (b) For a Packet B, initialize the priority field to be 1, and source and destination addresses to be 11.1.0.1 and 192.0.1.0, respectively.
  - (c) For a Packet C, initialize the priority field to be 0, and source and destination addresses to be 11.1.0.1 and 192.0.1.0, respectively.
  - (d) Demonstrate that your program can create the packets defined in parts (a), (b), and (c).



- (e) Extend your program such that a comparator looks at the priority fields and destination addresses of any combination of two packets. If the destination addresses are the same, it chooses the packet with the highest priority and leaves the packet with lower priority in a register with incremented priority. Otherwise, it chooses randomly one of the packets and leaves the other one in the register with incremented priority. Show that your program is capable of choosing Packet B.

*This page intentionally left blank*

# Index

---

4G, 258, 581

## A

Abort chunks, 737

ABR (Associative-Based Routing) Protocol, 775–776

Abstract syntax notation one (ASN.1) language, 359

Access networks in IPTV, 747

Access points, 139–140

Accounting, network management for, 358

Accuracy of routing algorithms, 162

ACK frames, 148

ACK/NAK process in DHCP, 169

Acknowledgment (ACK) field, 299, 301, 304, 338

Acknowledgment number field, 299

ACMs (address release messages), 646

Acronyms, 817–822

Active attacks, 783

Ad-hoc networks, 245

MANETs. *See* Mobile ad-hoc networks  
(MANETs)

WMN support for, 279

Ad Hoc On-Demand Distance Vector (AODV)  
protocol

new nodes for, 782–783

route discovery and establishment in, 778–781

route maintenance in, 781–782

routing process in, 778–779

Adaptability of routing algorithms, 162

Adapters for ARP, 132

Adaptive modulation, 284

Adaptive protocols, 768

Adaptive reservation schemes, 500

Additional information field, 329–330

Additive increase, multiplicative decrease (AIMD)  
congestion control, 309–311

Address autoconfiguration procedure, 266–267

Address field, 147

Address family identifier field, 186

Address mapping in DNS, 327–329

Address release messages (ACMs), 646

Address Resolution Protocol (ARP), 39, 130–132

Addresses

distributed hash table objects, 353

Internet, 21–22

IP. *See* IP addresses

MAC, 21–22, 130–133, 153

in mobile IP, 260–261

routing tables. *See* Routing tables

Admission control, 494–495

Admission in RAS signaling, 657

ADSL (asymmetric DSL), 56

ADUs (application data units), 728

Advanced Encryption Standard (AES) protocol,  
379–380

Agent address field, 361

Agents

mobile IP, 260–261

network management, 358

SIP, 671–683

Aggregate switches, 130, 589

Aggregate technique in CIDR, 27

Aggregation, link, 107–109

AIMD (Additive increase, multiplicative decrease)  
congestion control, 309–311

- Alerting call-signaling messages, 659
- All-optical networks, 563–566
- All-optical switches, 563, 569–572
- Aloha-based protocols, 105–106
- American Standard Code for Information Interchange (ASCII), 331
- Amplifiers in optical networks, 553–554
- Amplitude shift keying (ASK), 52–53
- Answer field, 329
- Answer messages (ANMs), 646–647
- Antennas, 48–49, 75
- Anycast addresses, 198
- AODV. *See* Ad Hoc On-Demand Distance Vector (AODV) protocol
- APIs (application programming interfaces), 324–325
  - cloud computing, 579, 581
  - ICN, 628
  - software-defined networking, 613
- Application data units (ADUs), 728
- Application delivery in software-defined networking, 622–623
- Application layer, 321–322
  - DNS, 325–330
  - e-mail, 330–335
  - FTP, 346–347
  - network management, 356–362
  - overview, 323–325
  - packet filtering, 394–395
  - peer-to-peer networks, 347–356
  - remote login protocols, 342–346
  - in TCP/IP protocol model, 19
  - WWW, 335–342
- Application programming interfaces (APIs), 324–325
  - cloud computing, 579, 581
  - ICN, 628
  - software-defined networking, 613
- Application service providers (ASPs), 622–623
- Application-specific type RTCP packets, 732
- Arbitration units, 456
- Area ID field, 182
- ARP (Address Resolution Protocol), 39, 130–132
- ARQ (automatic repeat request)
  - in channel coding, 283–284
  - in sliding window flow control, 92
  - in stop-and-wait flow control, 87–88
  - in TCP, 298
- AS (autonomous system), 189
- ASCII (American Standard Code for Information Interchange), 331
- ASK (amplitude shift keying), 52–53
- ASN.1 (abstract syntax notation one) language, 359
- ASNs (autonomous system numbers), 189
- ASPs (application service providers), 622–623
- Associative-Based Routing (ABR) Protocol, 775–776
- Associativity in ABR, 775–776
- Associativity ticks, 775–776
- Asymmetric cryptography, 380
- Asymmetric DSL (ADSL), 56
- Asynchronous MAC protocols, 118
- Asynchronous Transfer Mode (ATM) technology, 28
- Attacks
  - on ad-hoc networks, 783–784
  - categories, 371–375
- Attenuation, bit, 78
- Audio
  - conferencing, 582, 751
  - IVR databases, 754–755
  - streaming, 708–709
- Authentication, 383
  - categories, 377
  - cellular networks, 254
  - digital signatures for, 387
  - hash functions, 383–384
  - SHA, 385–387
- Authentication field, 182
- Authentication data field, 388
- Authentication type field, 182
- Authentication Web portals (AWPs), 620
- Authenticity
  - in ad-hoc networks, 784
  - in security, 370
- Authoritative servers, 328
- Authority field, 329–330
- Authorization in ad-hoc networks, 785
- Automatic discovery of services, 767
- Automatic repeat request (ARQ)
  - in channel coding, 283–284
  - in sliding window flow control, 92
  - in stop-and-wait flow control, 87–88
  - in TCP, 298
- Automatic updates for layer 2 devices, 125
- Autonomous system (AS), 189
- Autonomous system numbers (ASNs), 189
- Availability in cloud computing, 579

- Average queue length in RED, 204
- Await-reply packets, 776
- AWPs (authentication Web portals), 620
- B**
- B (bidirectional) frames, 708
- Back-off mode, 94
- Back-off time, 143
- Back-pressure signaling, 201
- Backbones, 224
- Balance equations in queueing, 416–420
- Bandwidth
  - ADSL, 56
  - link aggregation, 107
  - RAS signaling, 657–658
  - TCP, 309
- Bandwidth brokers, 496
- Base station controllers (BSCs), 247, 250, 253
- Base stations
  - cellular networks, 246–247
  - ICR, 808
  - LTE (eNodeB), 267–272, 752, 753, 756
  - media mini-clouds, 752–753, 756
  - mobile IP in, 307
  - sensor networks, 791
  - wireless, 48
- Batch arrival models
  - queueing, 427–428
  - self-similarity with, 757–759
- Batches of traffic units, 757
- Bellman-Ford algorithm, 176–177, 185
- Bernoulli random variables, 830
- Bernoulli trials, 828
- Best-effort models, 486, 498
- BGMP (Border Gateway Multicast Protocol), 236–237
- BGP (border gateway protocol), 188–189
  - details, 192–195
  - MBGP, 231–234
  - in MPLS, 529
  - packets, 190–192
- BGP Identifier field, 190
- Bidirectional (B) frames, 708
- Bidirectional congestion control, 200–201
- Big Data in data centers, 584
- Billing, network management for, 358
- Binary exponential backoff, 119
- Binomial coefficients, 474
- Binomial random variables, 830
- Binomial trials, 828
- Bipoint connections, 474
- Birth-and-death process
  - in *M/M/1/a* queueing systems, 417–418
  - overview, 406–408
- Bit attenuation, 78
- Bit-sliced organization, 471
- BitTorrent file sharing protocol, 349–352
- Black-and-white images, 702
- Black-hole attacks, 784
- Blades, 578
- Blocking
  - Clos network estimates, 462–463
  - over lightpaths, 565–566
  - link, 205–207
  - TDM, 62
- Blocking switches, 458, 559
- Blue-tooth communications, 72
- Bluetooth LANs, 141
- Bodies
  - e-mail, 331
  - HTTP, 339–340
- Boolean splitting multicast algorithm, 475
- Border Gateway Multicast Protocol (BGMP), 236–237
- Border gateway protocol (BGP), 188–189
  - details, 192–195
  - MBGP, 231–234
  - in MPLS, 529
  - packets, 190–192
- Border routers, 7
- Bridge port extensions (BPEs), 599
- Bridge protocol data units (BPDUs), 134–135
- Bridges
  - in LANs, 42–43, 121, 123, 128
  - in wireless networks, 142
- Broadband networks, 4
- Broadcast-and-prune algorithm, 220
- Broadcast translated circuits (BTCs), 475
- Broadcasts
  - in optical networks, 560
  - in star topologies, 117
  - in switching networks, 458
  - vs. wavelength routing, 564
- Brownian random process, 758, 834–835
- Browsers, 336
- BSCs (base station controllers), 247, 250, 253
- BTCs (broadcast translated circuits), 475
- Bucket depth in traffic shaping, 493

- Buffered switching networks, 458, 471–475
- Buffers
  - ARP, 39–40
  - input port processors, 450
  - optical networks, 553, 557
  - output port processors, 453–454
- Burk's theorem, 428–432
- Bursts in multimedia networking, 757–759
- Bus topology, 116–117
- Busy states in queuing, 408
- BYE packets, 732
- Bytestreams in TCP, 298
- C**
- Cable modem termination system (CMTS), 151–152
- Cable modems, 51, 57–58
- Cable TV (CATV) systems, 151–152
- Caching, Web, 341–342
- Call agents, 678
- Call establishment
  - cellular networks, 250–251
  - LTE, 270
  - SIP, 673–674
- Call-on-hold feature, 675
- Call Proceeding messages, 659–661
- Call progress messages (CPMs), 646–647
- Call signaling, 654, 659–662
- Calls in cellular networks. *See* Cellular networks
- Cantor switch fabrics, 470–471
- Capabilities exchange in control signaling, 662–663
- Capability Option Negotiation field, 233
- Capacity in wireless channels, 283
- Carrier protocols, 521
- Carrier Sense Multiple Access (CSMA) protocol, 93–97
- Cascaded nodes, Burk's theorem for, 428–431
- Case studies
  - all-optical switches, 569–572
  - sensor network simulation, 812–814
- CATV (Cable TV) systems, 151–152
- CBT (core-based trees) protocol, 230–231
- CC (complete call) messages, 253
- CCK (complementary code keying), 145
- CCN (Content-Centric Networking), 628, 630
- CDF (cumulative distribution function), 829, 833
- CDMA (code-division multiple access), 100–104
- CDNs (content distribution [delivery] networks), 741–745
- Cell sectoring, 277
- Cell splitting, 276
- Cells, ATM, 28
- Cellular networks, 72, 246
  - call establishment and termination, 250–251
  - devices and operation, 247–249
  - generations, 267–268
  - handoffs, 253–259
  - mobile IP management, 259–268
  - multimedia networking, 682–684
  - paging, 253
  - registration and IMSI assignment, 250–251
  - roaming, 252–253
- Central controllers, 44–45, 454–455
  - congestion controllers, 457
  - contention resolution units, 455–457
- Central media coordinators, 756
- Central schedulers for input buffers, 450
- Centralized access, 146
- Centralized clustering, 800
- Centralized protocols
  - ad-hoc networks, 768
  - MAC, 118
- Centralized routing
  - intradomain routing protocols, 179
  - in sensor networks, 806
- Certificates in SHA, 386
- CFE (contention-free end) frames, 148
- CGSR (Cluster-Head Gateway Switch Routing) protocol, 771–772
- Channels
  - ADSL, 56
  - cable modem, 57
  - cellular networks, 248
  - coding, 283–284
  - FDM, 59
  - handoffs, 253–254
  - TDM, 61–64
  - wireless access, 97–107
  - for wireless links, 280–285
- Chapman-Kolmogorov theory, 256, 836
- Checksum bits, 454
- Checksum field, 182
- Checksums, 454
  - Internet, 79
  - in IP packets, 161
  - in TCP segments, 300
  - in UDP segments, 296–297
- Chipping rate in CDMA, 101
- Choke packets, 201–202

- Chords in distributed hash tables, 354–355
- Chunks
  - BitTorrent, 350–351
  - SCTP, 736–737
- CIC (circuit identification code), 645
- CIDR (Classless Interdomain Routing), 26–27, 194
- Ciphersuites, 386
- Ciphertext, 377
- Circuit identification code (CIC), 645
- Circuit-switched networks, 5–6, 642, 647–649
- Cladding for optical cable, 74
- Classes of IP address, 23
- Classifiers, packet, 501
- Classless Interdomain Routing (CIDR), 26–27, 194
- Clear packets, 775
- Clear to Send (CTS) frames, 148
- Client/server model, 323–325
- Clients
  - application buffers, 740
  - BitTorrent, 350
  - TCP buffers, 740
  - VTP modes, 139
- Clipping in TDM, 64–65
- Clos networks
  - blocking estimates for, 462–463
  - five-stage, 464–465
- Clos switch fabric, 460–462
- Cloud-based multimedia networking, 751–752
  - IVR, 754–756
  - mini-clouds, 752–753
- Cloud computing, 577–578, 725–726
  - content servers, 746
  - data center networks, 588–595
  - data centers, 578–588
  - service models, 581–583
  - software-defined networking, 621–623
- Cluster-Head Gateway Switch Routing (CGSR)
  - protocol, 771–772
- Cluster heads, 771, 812–814
- Cluster-member tables, 771
- Clustering, 799–800
  - classification of, 800
  - DEEP, 801–805
  - LEACH, 800–801
  - in sensor networks, 790–791
- CMTS (cable modem termination system), 151–152
- Coaxial cable, 74
- Cochannel cells, 273–275
- Code-division multiple access (CDMA), 100–104
- Code efficiency in compression, 713
- Code field in ICMP, 164
- Coding for flat fading, 284
- Cognitive radios, 279
- Cohen, Bram, 349
- Collisions
  - Carrier Sense Multiple Access protocol, 93–97
  - wireless environments, 106
- Collocated foreign addresses, 262
- Combined switching networks, 469
- Command field, 186–187
- Commodification in cloud computing, 579
- Common SCTP headers, 736
- Communication energy model, 794–799
- Community clouds, 580
- Complementary code keying (CCK), 145
- Complements of events, 827
- Complete call (CC) messages, 253
- Complexity of switching networks, 458
- Compression, 693–694
  - digital voice, 695–701
  - lossless, 713–717
  - lossy, 709–713
  - moving images, 707–709
  - overview, 694–695
  - scanned documents, 717–718
  - still images, 701–707
- Compression ratio, 713
- Concentration switches, 465–468
- Conditional functions in probability, 829
- Conferencing
  - ad-hoc networks, 767
  - H.323 protocol, 665–666
- Confidentiality in security, 370
- Configuration, network management for, 358
- Congestion, 199–201
  - bidirectional, 202–203
  - link blocking, 205–207
  - RED, 203–205
  - TCP. *See* Transmission Control Protocol (TCP)
  - unidirectional, 201–202
- Congestion controllers, 457
- Congestion threshold, 312
- Congestion window, 309–310
- Connect call-signaling messages, 659, 662
- Connection accept packets, 15
- Connection-oriented networks, 11–15
- Connection-oriented services, 294
- Connection release packet, 15

- Connection request packets, 14
  - Connection rules in link blocking, 205–207
  - Connectionless networks, 11–13
  - Connectionless routing, 776
  - Connectionless services, 294
  - Connections
    - HTTP, 338
    - P2P networks, 355–356
    - reliability, 259
    - TCP, 301–305
  - Constellation diagrams, 54
  - Content centers in cloud-based multimedia, 752
  - Content-Centric Networking (CCN), 628, 630
  - Content control servers, 741–742
  - Content distribution (delivery) networks (CDNs), 741–745
  - Content providers, 741
  - Contention-access MAC protocols, 119–121
  - Contention access method for links, 92–93
  - Contention-free end (CFE) frames, 148
  - Contention resolution
    - central controllers, 455–457
    - optical networks, 557–558
  - Continuous probability functions, 829–830
  - Continuous-time Markov chains, 835–836
  - Continuous time stochastic processes, 834
  - Contributing source count (CC) field, 729
  - Contributing source identifier (CSRC) field, 730
  - Control channels in cellular networks, 248
  - Control chunks, 737
  - Control frames, 148
  - Control planes in software-defined networking, 609–615
  - Control segments, 653
  - Control signals, 654, 662–665, 802
  - Controlled-load service classes, 487
  - Controllers in routers, 454–457
  - Convergence
    - RIP, 187
    - routing algorithms, 163
  - Cookie acknowledgment chunks, 738
  - Copy switch fabric, 475–476
  - Core-based trees (CBT) protocol, 230–231
  - Core networks in IPTV, 746–747
  - Core of optical cable, 74
  - Core points
    - CBT, 230–231
    - sparse-mode algorithm, 220
  - Core switches, 130, 589
  - Costs, routing, 173, 179
  - Count field, 733
  - Count-to-infinity restrictions, 187
  - Counters in OpenFlow, 617
  - Counting in probability, 828
  - Couplers in optical networks, 556, 560
  - CPMs (call progress messages), 646–647
  - CRC field
    - IEEE 802.11, 148
    - SSH Packets, 345
  - CRCs. *See* Cyclic redundancy checks (CRCs)
  - Cross connect tables, 550
  - Crossbar switching, 459–460
    - buffers, 471–475
    - in optical networks, 559–560
  - Crossovers in optical networks, 558
  - Crosspoints
    - crossbar switch fabrics, 459–460
    - multipath buffered crossbars, 471–472
  - Crosstalk, 77, 558
  - Cryptography. *See also* Encryption
    - overview, 375–377
    - public-key, 380–383
    - symmetric-key, 377–380
  - CSMA (Carrier Sense Multiple Access) protocol, 93–97
  - CSMA/CA method, 143
  - CTS (Clear to Send) frames, 148
  - Cumulative distribution function (CDF), 829, 833
  - Cumulative number of packets lost field, 734
  - Customer edge routers, 539
  - Cut-through switching, 15, 43–44
  - Cyclic redundancy checks (CRCs), 79–80
    - effectiveness, 83
    - implementing, 84
    - at receivers, 81–82
    - in routers, 454
    - at transmitters, 80
- ## D
- Data-acquisition phase in ICR, 810
  - Data-carrying frames, 148
  - Data center networks (DCNs), 10, 580, 588–589
    - architectures, 591–594
    - load balancers, 589–591
    - multicast methods, 594–595
    - traffic engineering, 591
  - Data centers (DCs)
    - overview, 578–581, 583–584



- platforms and APIs, 581
- service models, 581–583
- virtualization, 584–588
- Data/CFE-ACK frames, 149
- Data/CFE ACK/CFE-Poll frames, 149
- Data/CFE-Poll frames, 149
- Data Encryption Standard (DES) protocol, 377–379
- Data field, 120
- Data finders in ICN, 630
- Data frames, 148
- Data links, 71–73
  - encoders, 75–77
  - error detection and correction in, 77–85
  - flow control, 85–92
  - link aggregation, 107–109
  - multiple user access, 92–97
  - types, 73–75
  - wireless. *See* Wireless links
- Data over Cable Service Interface Specification (DOCSIS), 151–152, 552
- Data planes, 609–611, 615–619
- Data transfer phase for TCP, 303–304
- Database description packets, 182
- Database sharing in P2P networks, 347, 353–355
- Datagram networks, 11–13
- Datagrams, 11, 325
- DCF (distributed coordination function) algorithm, 146–147
- DCNs. *See* Data center networks (DCNs)
- DCs. *See* Data centers (DCs)
- DCT (discrete cosine transform) process, 701–705
- Decentralized clustering, 800
- Decentralized Energy-Efficient Cluster Propagation (DEEP) protocol, 801–805
- Decision-feedback equalizers (DFEs), 285
- Decryption
  - AES, 380
  - RSA, 382
- DEEP (Decentralized Energy-Efficient Cluster Propagation) protocol, 801–805
- Deep fading, 282
- Deficit round-robin (DRR) scheduler, 511
- Deflected packets, 458
- Deflection routing, 178, 557–558
- Delay
  - connectionless networks, 12–13
  - CSMA, 95–96
  - optical networks, 553
  - packet size in, 15–17
  - priority queues, 506
  - queueing systems for, 419–420
  - software-defined networking, 610
- Delay since last SR field, 734
- DELETE method in HTTP, 339
- Delta routing, 263–264
- Demultiplexers in OFDM, 60
- Denial-of-service attacks, 374–375
- Dense-mode algorithm, 220
- Dense-mode PIM, 227
- Dependency
  - wavelength allocation with, 569
  - wavelength allocation without, 568–569
- DES (Data Encryption Standard) protocol, 377–379
- Designated routers (DRs)
  - IGMP, 221–222
  - PIM, 228–229
- Designated switches, 134–135
- Destination address field
  - Ethernet LAN frames, 120
  - IP packets, 162
  - IPv6 packets, 196
- Destination host unreachable message, 165
- Destination point codes (DPCs), 645
- Destination port field
  - TCP segments, 299
  - UDP segments, 296
- Destination port number field, 736
- Destination ports
  - transport layer, 292
  - UDP, 296
- Destination-Sequenced Distance Vector (DSDV) protocol, 769–771
- DFEs (decision-feedback equalizers), 285
- DFT (discrete Fourier transform), 60
- DHCP (Dynamic Host Configuration Protocol), 167–169
- DHTs (distributed hash tables), 353–355
- Differentiated services code points (DSCPs), 497
- Differentiated services (DS) QoS, 495–497
- Diffie-Hellman key-exchange protocol, 382–383
- DiffServ field, 497
- Diffused configuration, 140
- DIFS (distributed IFS coordination function), 147
- Digital certificates, 386
- Digital modulation techniques, 50–51
- Digital signatures, 377, 387
- Digital subscriber line (DSL) modems, 51, 55–57

- Digital video broadcasting (DVB), 746
- Digital voice compression
  - quantization and encoding in, 696–701
  - signal sampling in, 695–696
- Dijkstra's algorithm, 174–176, 180, 226
- Direct paths for wireless links, 280
- Direct routing
  - mobile IP, 263–264
  - sensor networks, 806–807
- Direct-sequence spread spectrum (DSSS)
  - CDMA, 103–104
  - physical layer, 144
- Direct sequences in CDMA, 103
- Directed beam configuration, 140
- Directed diffusion, 806
- Directional antennas, 49
- Directional couplers, 556
- Directional transmission links, 73
- Discarded packets, 458
- Discovery
  - DHCP, 168–169
  - Gatekeeper, 655–656
  - mobile IP agents, 261
  - route. *See* Route discovery
- Discrete cosine transform (DCT) process, 701–705
- Discrete Fourier transform (DFT), 60
- Discrete probability functions, 829
- Discrete-time Markov chains, 835
- Discrete time stochastic processes, 834
- Disengage messages in RAS signaling, 658
- Distance tables, 772
- Distance vector algorithm, 776
- Distance Vector Multicast Routing Protocol (DVMRP), 224–225
- Distance vector routing, 184–185
- Distortion in voice compression, 696–701
- Distributed access, 146
- Distributed coordination function (DCF) algorithm, 146–147
- Distributed denial-of-service attacks, 375
- Distributed hash tables (DHTs), 353–355
- Distributed IFS coordination function (DIFS), 147
- Distributed MAC protocols, 118
- Distributed media mini-clouds, 582, 751
- Distributed multimedia, 725–726
  - CDNs, 741–745
  - IPTV, 745–750
  - mini-clouds, 752–753
  - online gaming, 751
  - real-time exchange protocols, 726–731
  - VoD, 750
- Distributed NFB-based networks, 626–627
- Distributed protocols, 768
- Distributed routing
  - intradomain routing protocols, 179
  - sensor networks, 806
- Distribution networks, 467–468
- Distribution of sensor network loads, 812–814
- Diversity
  - in CDMA frequency, 104
  - for flat fading, 284
- DNS. *See* Domain Name System (DNS) and servers
- DOCSIS (Data over Cable Service Interface Specification), 151–152, 552
- DOCSIS provisioning of EPON (DPoE), 552–553
- Domain name space, 325–327
- Domain Name System (DNS) and servers, 168, 325
  - CDN interactions with, 743–744
  - domain name space in, 325–327
  - H.323 protocol, 654–655
  - hacking attacks on, 371–372
  - message format, 329–330
  - name/address mapping in, 327–329
  - VoIP, 651
- Domains
  - AS, 189
  - highjacking attacks on, 372
- Doppler frequency shift, 282
- Dot-decimal notation, 23
- Downlinks in LTE, 273
- Downstream bandwidth, ADSL, 56
- Downstream on demand, 534
- DPCs (destination point codes), 645
- DPoE (DOCSIS provisioning of EPON), 552–553
- Dropers in DiffServ, 496
- DRR (deficit round-robin) scheduler, 511
- DRs (designated routers)
  - IGMP, 221–222
  - PIM, 228–229
- DS (differentiated services) QoS, 495–497
- DSCPs (differentiated services code points), 497
- DSDV (Destination-Sequenced Distance Vector) protocol, 769–771
- DSL (digital subscriber line) modems, 51, 55–57
- DSR (Dynamic Source Routing) protocol, 773–774
- DSSS (direct-sequence spread spectrum)

- CDMA, 104
  - physical layer, 144
- Dual-stack lite standard, 523
- Duration/connection ID (D/I) field, 147
- DVB (digital video broadcasting), 746
- DVMRP (Distance Vector Multicast Routing Protocol), 224–225
- Dynamic address allocation, 168
- Dynamic Host Configuration Protocol (DHCP), 167–169
- Dynamic intradomain routing protocols, 179
- Dynamic IP address allocation, 167
- Dynamic routes with routers, 45
- Dynamic Source Routing (DSR) protocol, 773–774
- E**
- E-mail (electronic mail), 330
  - IMAP, 335
  - POP, 334
  - SMTP, 333–334
  - structure and definitions, 330–332
  - Webmail, 342
- EAP (Extensible Authentication Protocol), 391
- EAR (energy-aware routing), 810–811
- Earliest deadline first (EDF) scheduler, 511–512
- eBGP (external BGP), 194
- Echo, 78
- Echo cancelers, 78
- Echo messages in OpenFlow, 616
- EDF (earliest deadline first) scheduler, 511–512
- EDFAs (erbium-doped fiber amplifiers), 554
- Edge switches, 129–130, 588
- Efficient scheduling in data center networks, 591
- Egress LSRs, 532
- Electro-optical switches, 556
- Electronic mail (e-mail), 330
  - IMAP, 335
  - POP, 334
  - SMTP, 333–334
  - structure and definitions, 330–332
  - Webmail, 342
- Emulators, network, 632–635
- Encapsulation in VPNs, 521, 524
- Encoded source compression, 695
- Encoders, link, 75–77
- Encoding in compression, 696–701, 706–707
- Encryption
  - ad-hoc networks, 785
  - cryptographic techniques, 377–383
  - SSH, 344
- End-to-end encryption, 376
- End-to-end protocols. *See* Transport and end-to-end protocols
- Endpoint registration in RAS signaling, 656–657
- Energy-aware routing (EAR), 810–811
- Energy consumption control, 583
- Energy-exhaustion attacks, 784
- Engset distributions, 63
- eNodeB (evolved node B) in LTE, 269
- Ensured forwarding PHBs, 497
- Enterprise field, 361
- Entity bodies in HTTP, 339–340
- Entropy in lossy compression, 710–711
- Entry numbers in routing tables, 451
- EPC (Evolved Packet Core), 269, 271, 650
- EPONs (Ethernet passive optical networks), 552
- Equal-sized packet model, 28
- Erbium-doped fiber amplifiers (EDFAs), 554
- Erlang-B blocking estimation, 647–649
- Erlang-B blocking probability, 421–422
- Erlang-B blocking probability table, 837–840
- Erlang-C formula, 418
- Error detection and correction, 77–78
  - ARP, 39–40
  - CRC, 79–85
  - IPv6 packets, 197
  - output port processors, 454
- Error index field, 361
- Error status field, 361
- Ethernet LANs, 119–121
- Ethernet passive optical networks (EPONs), 552
- Ethernet switches, 43
- Events in probability, 827–828
- Evolved node B (eNodeB) in LTE, 269
- Evolved Packet Core (EPC), 269, 271, 650
- Exclude mode in IGMP, 222
- Execute action sets, 617
- Exp field, 536
- Expansion switch fabrics, 467–468
- Expected value, 831–832
- Expedited forwarding PHBs, 497
- Experimenter messages, 616
- Explicit multi-unicast (Xcast) protocol, 595
- Explicit routing, 537, 550
- Exponential random variables, 831
- Express multicast, 237
- Extended highest sequence number received field, 734

- Extensible Authentication Protocol (EAP), 391
- Extension (X) field, 729
- Extension headers in IPv6, 198
- Extensions in SIP, 674–678
- External BGP (eBGP), 194
- Extra data in TCP, 314
- Extranet VPNs, 526
- F**
- Facility call-signaling messages, 659
- Fading, 281–284
- Failures, network management for, 357–358
- Fair-queueing (FQ) scheduler, 507–508
- Fairness index, 500–501
- Fast Fourier transform (FFT), 60, 100
- Fast recovery, congestion control, 313
- Fast retransmit method, 308–309, 313–315
- FAX compression, 717–718
- FCFS (first come, first served) queuing systems, 408
- FDM (frequency-division multiplexing), 59–61
- FDMA (frequency-division multiple access), 99
- Feature messages in SIP, 669
- Features in SIP, 674–678
- FEC (forward equivalence class), 532, 537
- FEC (forward error correction), 283–284
- Feedback models, 433–434
- Femtocells, 269
- FFT (fast Fourier transform), 60, 100
- FHSS (frequency-hopping spread spectrum), 144
- Fiber-optic communications, 73
- Fiber optic links (FOLs), 74, 547
- FIFO (first-in, first-out) queuing systems. *See* Markovian FIFO queuing systems
- FIFO (first-in, first-out) schedulers, 502–503
- File sharing protocols, 348–352
- File Transfer Protocol (FTP), 346–347
- Filters
  - optical networks, 554, 561
  - packet, 391–396
- Finished (FIN) field, 300, 304
- Firewalls
  - operation of, 391–396
  - with VPNs, 527–528
- Firmware in software-defined networking, 610
- First come, first served (FCFS) queuing systems, 408
- First-in, first-out (FIFO) queuing systems. *See* Markovian FIFO queuing systems
- First-in, first-out (FIFO) schedulers, 502–503
- 5-layer TCP/IP protocol model, 18–20
- Five-stage Clos networks, 464–465
- Fixed reservation schemes, 500
- Fixed-size switch elements, 570
- Flag field, 736
- Flags field
  - DNS, 329
  - IP packets, 161
- Flags/code field, 263
- Flat fading, 282
- Flexibility in cloud computing, 579
- Flood attacks, 374–375
- Flood routing, 177–178
- Flooding algorithm, 177–178
- Floodlight controllers, 615
- Flow-based routers, 46
- Flow control, 85
  - sliding-window, 88–92
  - stop-and-wait, 85–88
  - in switching networks, 458
- Flow label field, 196
- Flow tables, 617–618
- FOLs (fiber optic links), 74, 547
- Foreign addresses in mobile IP, 260, 263
- Foreign agents
  - cellular networks, 248
  - mobile IP, 260–261
- Forward equivalence class (FEC), 532, 537
- Forward error correction (FEC), 283–284
- Forwarding tables, 452–453
- Four-level QAM, 55
- FQ (fair-queueing) scheduler, 507–508
- Fraction lost field, 734
- Fragment-free switches, 44
- Fragment offset field, 161
- Fragmentation, packet, 7, 163–164, 198–199
- Frame body field, 148
- Frame check sequence field, 120
- Frame check sequences, 118, 454
- Frame collisions with links, 92
- Frame control (FC) field, 147
- Frame delay analysis, 95–96
- Frame flow control, 39–40
- Frame process units, 39
- Frame-switch mode, 117
- Frames
  - LAN, 116
  - MAC, 147–149
  - MPEG, 707–708
  - packet-switched networks, 6–7

- Frequency borrowing, 276
- Frequency-division multiple access (FDMA), 99
- Frequency-division multiplexing (FDM), 59–61
- Frequency hopping, 103
- Frequency-hopping spread spectrum (FHSS), 144
- Frequency ranges, 72–73
- Frequency reuse in LTE, 273–277
- Frequency shift, 282
- Frequency shift keying (FSK), 52–53
- FTP (File Transfer Protocol), 346–347
- Full-duplex links, 73
- Fully connected optical networking schemes, 594
- Functions
  - probability, 829–830
  - random variable, 832–834
- G**
- G-LSPs (generalized label switch paths), 550–551
- Gaming, online, 751
- Gatekeeper discovery in RAS signaling, 655–656
- Gatekeepers (GKs) in H.323 protocol, 652
- Gateways
  - sockets, 293
  - wireless routers with, 149
- Gaussian (normal) random variables, 831
- General distributions, 424–425
- Generalized label switch paths (G-LSPs), 550–551
- Generalized labels in GMPLS, 549–550
- Generalized multiprotocol label switching (GMPLS) protocol, 548
  - lightpaths, 550–551
  - optical cross connects and generalized labels, 549–550
  - traffic grooming, 551
- Generating polynomials for CRC, 82
- Generator values for CRC, 82–83
- Generators, checking, 81–82
- Generic routing encapsulation (GRE), 527
- Geometric distributions, 413
- Geometric random variables, 830
- Geosynchronous orbit satellite systems, 245
- GET method in HTTP, 339–340
- Get PDUs, 361
- GIF (graphics interchange format) file compression, 703
- GKs (gatekeepers) in H.323 protocol, 652
- Global number of copies in tree algorithms, 476–477
- Global packet resequencers, 454
- Global positioning systems (GPSs), 793, 805
- Global translation title (GTT), 644–645
- Glossary of acronyms, 817–822
- GMPLS (generalized multiprotocol label switching) protocol, 548
  - lightpaths, 550–551
  - optical cross connects and generalized labels, 549–550
  - traffic grooming, 551
- Goodbye packets, 732
- Gopher protocol, 335
- GPSs (global positioning systems), 793, 805
- Grant flows, 473
- Graphical user interfaces (GUIs)
  - cloud computing, 581
  - overview, 324–325
- Graphics interchange format (GIF) file compression, 703
- GRE (generic routing encapsulation), 527
- GTT (global translation title), 644–645
- Guaranteed service classes, 486–487
- Guard space, 205
- Guest machines, 587
- Guided missiles, 73
- Guided transmission links, 73
- GUIs (graphical user interfaces)
  - cloud computing, 581
  - overview, 324–325
- H**
- H.323 protocols, 652
  - call signaling, 659–662
  - components, 652–653
  - conference calling, 665–666
  - control signaling, 662–665
  - organization, 653–655
  - RAS signaling, 655–659
  - SIP to H.323 internetworking, 679–680
- Hacking attacks, 371–372
- Half-duplex links, 73
- Handoffs
  - cellular networks, 253–259
  - LTE, 271–273
- Handshakes, three-way, 337
- Hardware firewalls, 392
- Hash functions, 383–384
- Hash tables, 353–355
- HDSL (high-bit-rate digital subscriber line), 57
- HDTV (high-definition television), 707

- HEAD method in HTTP, 339
  - Headends in IPTV, 746
  - Header length (HL) field
    - IP packets, 160
    - TCP segments, 299
  - Header lines in HTTP, 339–340
  - Headers
    - BGP, 190–192
    - e-mail, 331
    - IPsec, 388
    - IPv4, 160–162
    - IPv6, 196–197
    - LAN, 116
    - MAC, 118
    - MPLS, 530–531, 536
    - OSPF, 181–182
    - packet, 449
    - packet-switched networks, 6–7
    - RIP, 186–187
    - RTCP, 732–734
    - RTP, 729–731
    - SCTP, 736–737
  - Heartbeat acknowledgment chunks, 737
  - Heartbeat request chunks, 737
  - Heavy-tailed distributions, 757, 759
  - HELLO messages, 616, 782–783
  - Hello packets, 181–183
  - HFC (hybrid fiber-coaxial) networks, 57
  - Hidden-terminal problem, 106
  - High-bit-rate digital subscriber line (HDSL), 57
  - High-capacity routers, 46
  - High-definition television (HDTV), 707
  - Highjacking attacks, 372
  - HLR (home location register), 248–250, 252
  - Hold state in RIP, 188
  - Hold Time field, 190
  - Home address field, 263
  - Home agents
    - cellular networks, 248
    - mobile IP, 260–261
  - Home location register (HLR), 248–250, 252
  - Home networks
    - ad hoc, 767
    - IPTV, 746, 748
  - Home RF LANs, 141
  - Home Subscriber Server (HSS), 269
  - Hop limit field, 196
  - Host-based resource allocation, 499
  - Host IDs in IP addresses, 22
  - Host machines, 587
  - Hosts
    - intradomain routing protocols, 179
    - ISP, 8
    - TCP/IP protocol model, 19–20
    - WMNs, 277
  - Hot-potato routing, 178
  - Hotspots in WiFi, 150
  - HSS (home Subscriber Server), 269
  - HTML (Hypertext Markup Language), 336, 755
  - HTTP (Hypertext Transfer Protocol), 172, 336–341
  - HTTP-based streaming, 740–741
  - HTTPS protocol, 341, 386
  - Hubs, 40–41
    - LANs, 121, 123
    - overview, 42
    - star topologies, 117
  - Huffman encoding, 708, 715–716, 718
  - Hurst parameter, 758
  - Hybrid clouds, 579–580
  - Hybrid fiber-coaxial (HFC) networks, 57
  - Hybrid networks, 245
  - Hydrogen release, 614
  - Hyperlinks, 335
  - Hypertext Markup Language (HTML), 336, 755
  - Hypertext Transfer Protocol (HTTP), 172, 336–341
  - Hypervisors, 587–588, 596
- I**
- I components in modulation, 54
  - I (interactive) frames, 708
  - I-TCP (Indirect Transmission Control Protocol), 307–308
  - IaaS (infrastructure as a service), 582
  - IAMs (initial address messages), 253, 645–646
  - iBGP (internal BGP), 194
  - ICANN (Internet Corporation for Assigned Names and Numbers), 165
  - ICMP (Internet Control Message Protocol), 164–165
  - ICN (information-centric networking), 627–628
    - named objects, 628
    - routing and management, 628–631
    - security, 631–632
  - ICR (Intercluster Energy-Conscious Routing), 808–811
  - Identification field
    - DNS, 329

- IP packets, 161
  - mobile IP, 263
- Idle states in queuing, 408
- IEEE 802.3 standard, 119–121
- IEEE 802.11 standard, 142–143
  - MAC layer, 145–149
  - physical layer, 144–145
  - security for, 389–391
    - for WiFi technology, 150–151
- IEEE 802.15.4 standard, 811–812
- IEEE 802.16 standard, 267–268
- IETF (Internet Engineering Task Force), 387, 679
- IFS (interframe space) technique, 146–147
- IGMP (Internet Group Management Protocol), 221–223, 749
- IGP (Interior Gateway Protocol) labels, 536
- IID (independent and identically distributed) processes, 408, 834
- IKE (Internet Key Exchange) daemons, 389
- IMAP (Internet Mail Access Protocol), 335
- IMSI (international mobile subscriber identity), 249–250
- In-phase QAM components, 55
- Include mode in IGMP, 222
- Increased total link bandwidth in link aggregation, 107
- Independent and identically distributed (IID) processes, 408, 834
- Independent events, 828
- Independent random variables, 833–834
- Indirect Transmission Control Protocol (I-TCP), 307–308
- Info field, 351
- Info messages in SIP, 677
- Information-centric networking (ICN), 627–628
  - named objects, 628
  - routing and management, 628–631
  - security, 631–632
- Information-compression process, 696
- Information leakage attacks, 372
- Information-level attacks, 372
- Information-source process, 695
- Information theory for lossy compression, 709–713
- Infrared frequency spectrum, 73
- Infrared LANs, 140–141
- Infrastructure as a service (IaaS), 582
- Ingress LSRs, 534–535
- Initial address messages (IAMs), 253, 645–646
- Initial sequence numbers (ISNs), 299
- Initiation chunks, 737
- Initiation acknowledgment chunks, 737
- Input port buffers, 450, 472–473
- Input port processors (IPPs), 44–45, 447–448
  - forwarding tables and packet encapsulators, 452–453
  - input buffers, 450
  - multicast schedulers, 452
  - OpenFlow, 617–618
  - packet parsers, 448–449
  - packet partitioners, 449–450
  - routing tables, 450–452
- Insertion loss, 554, 558
- Integrated Services Digital Network (ISDN), 644
- Integrated services QoS
  - admission control in, 494–495
  - overview, 486–488
  - RSVP, 495
  - traffic shaping in, 488–494
- Integrity
  - ad-hoc networks, 785
  - security, 370
- Interactive (I) frames, 708
- Interactive voice response (IVR), 582, 751, 754–756
- Interarrival jitter field, 731, 734
- Interchanging phone numbers, 669–670
- Intercluster Energy-Conscious Routing (ICR), 808–811
- Intercluster routing protocols, 805, 808–811
- Interdomain routing protocols, 188–189
  - AS, 189
  - BGMP, 236–237
  - BGP, 189–196
  - MBGP, 231–234
  - MSDP, 234–236
  - multicast, 231–237
- Interest signals, 808
- Interference, 283
- Interframe space (IFS) technique, 146–147
- Interior Gateway Protocol (IGP) labels, 537
- Interleaving, 284
- Internal BGP (iBGP), 194
- International mobile subscriber identity (IMSI), 249–250
- Internet, 7–9
- Internet addressing schemes, 21–22
- Internet checksums, 79
- Internet Control Message Protocol (ICMP), 164–165

- Internet Corporation for Assigned Names and Numbers (ICANN), 165
  - Internet Engineering Task Force (IETF), 387, 679
  - Internet Group Management Protocol (IGMP), 221–223, 749
  - Internet Key Exchange (IKE) daemons, 389
  - Internet Mail Access Protocol (IMAP), 335
  - Internet Protocol (IP) layer
    - addressing in. *See* IP addresses
    - CIDR, 26–27
    - IPv6, 196–199
    - mobile. *See* Mobile IP
    - security, 387–389
    - subnet addressing and masking, 24–26
    - telephony. *See* Voice over IP (VoIP)
  - Internet Protocol television (IPTV), 745–750
  - Internet routing policies
    - algorithm characteristics, 162–163
    - DHCP, 167–169
    - ICMP, 164–165
    - IP addresses, obtaining and assigning, 165–167
    - NAT, 169–172
    - packet fragmentation and reassembly, 163–164
    - UPnP, 172–173
  - Internet service providers (ISPs), 7–9, 189
  - Internetwork nodes, 9–11
  - Interoperability in mobile IP, 259
  - Interpreters in IVR, 754
  - Interruption attacks, 374
  - Intersection of events, 827
  - Intersymbol interference (ISI), 284–285
  - Intracluster communication, 805
  - Intracluster routing protocols, 806–808
  - Intradomain protocols, 178–181
    - CBT, 230–231
    - DVMRP, 224–225
    - Mbone, 224
    - MOSPF, 225–227
    - multicast, 223–224
    - OSPF, 180–183
    - PIM, 227–230
    - RIP, 183–188
  - Intranet VPNs, 526
  - IP. *See* Internet Protocol (IP) layer
  - IP addresses, 21–27, 392
    - DHCP for, 167–169
    - IPv6 source address and destination address, 196
    - LAN, 130–133
    - multicast, 217–218
    - NAT for, 169–172
    - Obtaining and assigning, 165–167
    - RIP, 186
    - RTP, 728
    - SIP, 669–670
    - source address and destination address, 162
  - IP headers in MAC, 118
  - IP routing tables, 45
  - IP Security (IPsec) protocol, 387–389
  - IP version 4 (IPv4), 160–162
    - addressing format in, 22
    - CIDR in, 26
    - classes A, B, C, D, and E in, 23
    - header in, 160
    - mobile IP routing with, 263
    - MSS, 301
    - packet fragmentation in, 163
  - IP version 6 (IPv6), 196–197
    - address interacting with MPLS, 535
    - addressing format in, 197–198
    - extension headers in, 198
    - mobile IP routing with, 266–267
    - MSS, 301
    - packet fragmentation in, 198–199
    - routing table, 451
    - tunneling, 522–523
  - IPPs. *See* Input port processors (IPPs)
  - IPsec (IP Security) protocol, 387–389
  - IPTV (Internet Protocol television), 745–750
  - ISDN (Integrated Services Digital Network), 644
  - ISDN user part (ISUP), 644–645
  - ISI (intersymbol interference), 284–285
  - ISNs (initial sequence numbers), 299
  - Isotropic antennas, 48–49, 104
  - ISPs (Internet service providers), 7–9, 189
  - ISUP (ISDN user part), 644–645
  - Iterative mapping, 328–329
  - IVR (interactive voice response), 582, 751, 754–756
- ## J
- Jackets for optical cable, 74
  - Jackson's theorem, 433–437
  - Jain, Raj, 501
  - Jitter
    - description, 78
    - RTCP, 731–732, 734
  - Join messages, 228



- Join packets, 235
- Joint cumulative density function, 833
- Joint Photographic Experts Group (JPEG) compression, 701–707
- Joint probability functions, 711, 833
- K**
- Keep-alive connections, 338
- Keep-alive packets, 190, 196
- Kendal's notations, 408–409
- Keys
  - ad-hoc networks, 783
  - PBX systems, 647
  - public-key cryptography, 380–383
  - secret-key encryption, 376
  - symmetric-key cryptography, 377–380
- Knockout switching fabrics, 465–467
- L**
- L2F (Layer 2 Forwarding) protocol, 526
- L2TP (Layer 2 Tunneling Protocol), 526–527
- Label-binding, 531–533
- Label Distribution Protocol (LDP), 520, 534–535
- Label switch paths (LSPs), 532–534
- Label switch routers (LSRs), 529–533
- Label value field, 536
- Labels
  - domain names, 325–326
  - GMPLS, 549–550
  - in MPLS, 529–533
- LACP (Link Aggregation Control Protocol), 108–109
- LANs. *See* Local area networks (LANs)
- Large-scale optical switches, 558–560
- Lasers, 73, 553
- Last come, first served (LCFS) queuing
  - systems, 408
- Last-mile networks, 747
- Last SR timestamp field, 734
- Latency. *See* Delay
- Law enforcement, ad-hoc networks for, 767
- Layer 1 devices, 41–42, 121–123
- Layer 2 devices, 42–44
  - LANs, 123–128
  - networking with, 128–130
- Layer 2 Forwarding (L2F) protocol, 526
- Layer 2 Tunneling Protocol (L2TP), 526–527
- Layer 3 devices, 44–47, 128–130
- LBs (load balancers), 589–591
- LBSs (local base stations), 808
- LCFS (last come, first served) queuing
  - systems, 408
- LDP (Label Distribution Protocol), 520, 534–535
- LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol, 800–801
- Leaky-bucket traffic shaping, 489–493
- Least-connect algorithms, 590–591
- Least-cost path, 173–174
- Least-cost-path algorithms
  - Bellman-Ford, 176–177
  - Dijkstra's, 174–176
- Leave group messages, 222
- Leechers in BitTorrent, 350
- Lee's method, 206–207
- Lempel-Ziv encoding, 716–717
- Length field
  - BGP, 190
  - RTCP packets, 733
  - SCTP packets, 736
  - SSH packets, 345–346
- Length/Type field, 120
- Liability, data centers, 583
- Lifetime field, 263
- Light frequency spectrum, 73
- Light networks. *See* Optical networks
- Lightpaths (LPs)
  - blocking over, 565–566
  - GMPLS, 550–551
- Line cards, 447
- Line coding process, 75
- Linear topologies in SDN emulators, 635
- Lines in PSTNs, 643
- Link aggregation, 107–109
- Link Aggregation Control Protocol (LACP), 108–109
- Link-cost tables, 772
- Link costs, 173
- Link encoders, 40
- Link-IDs, 108–109
- Link layer, 19
- Link resiliency provisioning, 107–108
- Link reversal, 775
- Link-state acknowledgment packets, 182
- Link-state multicast, 225
- Link-state request packets, 182
- Link-state routing, 180–181
- Link-state update packets, 182
- Link utilization, 16–17

- Links
    - ARP, 40
    - attacks on, 373
    - blocking, 205–207
    - data. *See* Data links
    - encrypting, 376
    - ISP, 7
    - PSTNs, 643
    - virtual, 597
    - wireless. *See* Wireless links
  - Little's theorem, 404–406
  - Live media streaming, 726–727
  - LLC (logical-link layer), 118
  - LLIDs (logical link identifiers), 553
  - Load balancing, 163
    - cloud computing, 581
    - data centers, 583, 589–591
    - virtual machines, 586
  - Load distribution, 812–814
  - Local area networks (LANs), 9–10, 115–116
    - DOCSIS, 151–152
    - IP addresses for, 130–133
    - layer 1 devices, 121–123
    - layer 2 devices, 123–128
    - networks of, 121–130
    - protocols, 117–121
    - STP, 133–136
    - switches, 43
    - topologies, 116–117
    - VLANs, 136–139, 600, 620
    - wireless, 139–141
  - Local base stations (LBSs), 808
  - Local header decoders, 455
  - Local Internet service providers, 8
  - Local multicasting protocols, 221–223, 749
  - Location-disclosure attacks, 784
  - Location management in cellular networks, 254
  - Location registers in cellular networks, 248–250, 252
  - Location servers in SIP, 668
  - Logical congestion, 199–200
  - Logical link identifiers (LLIDs), 553
  - Logical-link layer (LLC), 118
  - Logical links, 290
  - Logins, remote, 342–346
  - Long Term Evolution (LTE) technology, 268–269
    - call establishment, 270
    - downlinks and uplinks, 273
    - eNodeB, 269
    - frequency reuse, 273–277
    - handoffs, 271–273
    - MME, 683
    - networking devices, 269–270
    - SC-FDMA, 100
  - Lossless compression, 694, 713–714
    - Huffman encoding, 715–716, 718
    - Lempel-Ziv encoding, 716–717
    - run-length encoding, 714–715
  - Lossy compression, 694
    - compression ratio and code efficiency in, 713
    - entropy in, 710–711
    - information theory for, 709–713
    - Shannon's coding theorem in, 711–713
  - Low-earth orbit satellite systems, 245
  - Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol, 800–801
  - Low-frequency spectrum, 72
  - LPs (lightpaths)
    - blocking over, 565–566
    - GMPLS, 550–551
  - LSPs (label switch paths), 532–534
  - LSRs (label switch routers), 529–533
  - LTE. *See* Long Term Evolution (LTE) technology
- M**
- M/D/1* queueing systems, 427
  - M/G/1* queueing systems, 424–427
  - M/M/1* queueing systems, 409
    - M/M/a*, 415–420
    - mean delay and queue length in, 413–414
    - number of packets in, 411–413
    - packet arrival and service model in, 410–413
  - M/M/1/b* queueing systems, 414–415
  - M/M/a* queueing systems, 415–420
  - M/M/1/a* queueing systems, 420–422
  - M/M/∞* queueing systems, 422–424
  - M-P-Q field, 456
  - MAC addresses, 21–22, 130–133, 153
  - MAC frames, 147–149
  - MAC layers
    - IEEE 802.11, 145–149
    - in WMNs, 280
  - MAC (medium access control) protocols
    - contention-access, 119–121
    - EAPON frames, 552
    - for LANs, 118–121
    - in sensor networks, 792
  - MACs (message authentication codes), 385
  - Mail user agents (MUAs), 331

- Mailboxes, 331, 334
- Man-in-the-middle attacks, 372
- Manageability in multicasting, 216
- Managed devices, 358
- Management frames, 148
- Management information base (MIB), 359–360
- Management planes, 609
- Managers in network management, 358
- Manchester encoding method, 77
- MANETs. *See* Mobile ad-hoc networks (MANETs)
- Mapping, name/address, 327–329
- Marginal CDF, 833
- Marginal PDF, 833
- Marginal PMF, 833
- Marker (M) field, 730
- Marker field in BGP, 190
- Markers in DiffServ, 496
- Markov chains, 256
  - in birth-and-death process, 406–407
  - for multipath buffered crossbars, 474–475
  - in probability, 835–836
- Markovian FIFO queueing systems, 409
  - M/M/1/b*, 414–415
  - M/M/1/a*, 420–422
  - M/M/∞*, 422–424
- MASC (Multicast Address-Set Claim)
  - protocol, 236
- Masking, 24–26
- Masquerading attacks, 372
- Master/slave assignment in control signaling, 663
- Matching fields in OpenFlow, 618–619
- Maximum response time field, 223
- Maximum segment size (MSS) option, 300–301, 304, 311
- Maximum transmission units (MTUs)
  - IPv6, 198
  - routing protocols, 163–164
- Maximum window size, 309–310
- MBCs (multipath buffered crossbars), 471–475
- MBGP (multiprotocol BGP), 231–234
- MBone (multicast backbone), 224
- MC-endpoint conference calling, 665
- MCU conference calling, 665
- MCUs (multipoint control units), 652
- MD5 hash algorithm, 385
- Mean delay
  - M/M/1* queueing systems, 413–414
  - M/M/1/a* queueing systems, 419
- Mean number of packets in queueing systems, 415
- Mechanical optical switches, 556
- Media Access Control (MAC) addresses, 21–22
- Media exchange establishment control, 663–665
- Media exchange protocols, 650
- Media exchange segments, 653
- Media exchange sessions, 647
- Media Gateway Control Protocol (MGCP), 678
- Media gateway controllers (MGCs), 653, 668, 678
- Media gateway (MG) routers, 650, 653, 668
- Medium access control. *See* MAC (medium access control) protocols
- Medium orbit satellite systems, 245
- Medium-size routers, 46
- Membership multicasting protocols, 221–223, 749
- Membership queries and reports in IGMP, 222
- Membership-search signals, 802, 804
- Memory control in switch fabrics, 469
- Memory units in sensor networks, 794
- Merging LSPs, 533
- Mesh networks, 277
  - applications, 277–279
  - physical and MAC layers in, 279–280
- Message authentication, 383, 385
- Message authentication codes (MACs), 385
- Message digests, 353, 383
- Message-Id identifiers, 332
- Message signal units (MSUs), 645–646
- Message transfer part (MTP), 644
- Message transmission-list tables, 772–773
- Messages
  - HTTP, 339–340
  - packet-switched networks, 6–7
  - SIP, 669–671
- Meters in DiffServ, 496
- Methods in HTTP, 339
- Metric field, 186–187
- MG (media gateway) routers, 650, 653, 668
- MGCP (Media Gateway Control Protocol), 678
- MGCs (media gateway controllers), 653, 668, 678
- MIB (management information base), 359–360
- Microcells, 277
- Microwave frequency spectrum, 72
- Microwave systems, 72
- Military, ad-hoc networks for, 767
- MIMO (multiple-input multiple-output) systems, 49, 279
- Mini-clouds, 752–753
- Minimal topologies in SDN emulators, 634
- Minimum number of hops, 173

- Mininet SDN emulators, 632–635
- Misrouting attacks, 374
- Mixer relays, 729
- MLD (Multicast Listener Discovery), 221
- MME (mobile management entity), 269, 271–273, 683
- Mobile ad-hoc networks (MANETs), 245, 765
  - ABR protocol, 775–776
  - AODV protocol, 776–783
  - CGSR protocol, 771–772
  - DSDV protocol, 769–771
  - DSR protocol, 773–774
  - overview, 766–767
  - protocol overview, 769
  - routing in, 767–769
  - security of, 783–785
  - TORA protocol, 774–775
  - WRP protocol, 772–773
- Mobile agents, 248
- Mobile cloud computing, 751
- Mobile IP, 259–260
  - agents, 260–261
  - registration in, 262–264
  - routing for, 263–267
- Mobile IPv6, 266
- Mobile management entity (MME), 269, 271–273, 683
- Mobile switching centers (MSCs)
  - cellular networks, 247, 250–252
  - mobile IP, 260–261
- Mobile transport protocols
  - TCP, 307–309
  - UDP, 307
- Modems, 37, 50–51
  - cable, 57–58
  - DSL, 55–57
  - modulation schemes, 51–55
- Modification attacks, 374
- Modulation schemes in modems, 51–55
- Modulation symbols, 54
- Modulo-2 arithmetic, 81–82
- Monochrome images, 702
- MOSPF (multicast OSPF) protocol, 225–227
- Moved Temporarily messages, 676–677
- Moving images compression, 707–709
- Moving Pictures Expert Group (MPEG) compression, 707–709
- MP3 technology, 708–709
- MPLS. *See* Multiprotocol label switching (MPLS)
- MSCs (mobile switching centers)
  - cellular networks, 247, 250–252
  - mobile IP, 260–261
- MSDP (Multicast Source Discovery Protocol), 234–236
- MSS (maximum segment size) option, 300–301, 304, 311
- MSUs (message signal units), 645–646
- MTP (message transfer part), 644
- MTUs (maximum transmission units)
  - IPv6, 198
  - routing protocols, 163–164
- MUAs (Mail user agents), 331
- Multi-carrier modulation, 285
- Multi-hop communication efficiency, 797–799
- Multi-rate connections, 5
- Multi-tunnel routing, 536–538
- Multicast Address-Set Claim (MASC) protocol, 236
- Multicast addresses, 198
- Multicast backbone (MBone), 224
- Multicast Listener Discovery (MLD), 221
- Multicast OSPF (MOSPF) protocol, 225–227
- Multicast schedulers in input port processors, 452
- Multicast Source Discovery Protocol (MSDP), 234–236
- Multicast routing and protocols, 215–216, 475–477
  - classification, 220
  - data center networks, 594–595
  - definitions and techniques, 216–217
  - interdomain, 231–237
  - intradomain, 223–231
  - IP addresses, 217–218
  - local and membership, 221–223
  - software-defined networking, 621
  - switching networks, 458
  - tree algorithms, 218–220
  - tree-based, 476–478
- Multichannel multitransceiver MAC, 280
- Multichannel single-transceiver MAC, 280
- Multihop routing, 806–807
- Multimedia networking, 641, 679
  - compression in. *See* Compression
  - distributed. *See* Distributed multimedia
  - self-similarity and non-Markovian streaming
    - analysis in, 756–759
  - SIP to H.323 internetworking, 679–680
  - SIP to PSTN internetworking, 681–682
  - Voice over IP. *See* Voice over IP (VoIP)
  - wireless cellular internetworking, 682–684

- Multimedia terminals, 650
- Multipath buffered crossbars (MBCs), 471
- Multipath effects, 104
- Multipath switching networks, 458
- Multiple access
  - FDMA, 99
  - miscellaneous methods, 104–105
  - OFDM, 99–100
  - random-access techniques, 105–106
  - SC-FDMA, 100
  - TDMA, 99
- Multiple-input multiple-output (MIMO) systems, 49, 279
- Multiple random variables, 833–834
- Multiple stage switching networks, 458
- Multiple users in data link access, 92–97
- Multiplexers, 37, 58
  - FDM, 59–61
  - TDM, 61–65
- Multipoint control units (MCUs), 652
- Multiprotocol BGP (MBGP), 231–234
- Multiprotocol label switching (MPLS), 519–520, 528–529
  - labels, 529–533
  - multi-tunnel routing, 536–538
  - packet format, 536
  - routing in, 534–536
  - traffic engineering in, 538–539
  - for VPNs, 539–540
- My Autonomous System field, 190, 194
- N**
- N-stage planar architecture, 560
- NAIs (network access interfaces), 747
- Name/address mapping, 327–329
- Name resolution mode in ICN, 629
- Named objects in ICN, 628
- Narrowband RF LANs, 141
- NAT (network address translation), 169–172, 590
- National Internet service providers, 8
- Natural nonreturn-to-zero (NRZ) line coding, 76
- Neighbors in BGP, 192
- Network access interfaces (NAIs), 747
- Network-access servers, 526
- Network address translation (NAT), 169–172, 590
- Network communication protocols, 17–18
  - Internet. *See* Internet Protocol (IP) layer
  - OSI, 20
  - TCP/IP, 18–20
- Network emulators, 632–635
- Network function virtualization (NFV), 614
  - abstract model, 624–626
  - distributed networks, 626–627
  - overview, 623–624
  - virtualized services, 627
- Network IDs, 22–23
- Network interface cards (NICs), 37, 446
  - ARP, 131
  - layer 3 devices, 44–45
  - overview, 39–40
  - virtual, 597–598
- Network latency, 610
- Network layer
  - congestion control at, 199–207
  - TCP/IP protocol model, 19
- Network Layer addresses, 22
- Network Layer Reachability Information (NLRI)
  - field, 190, 192, 233
- Network management, 356–358
  - elements, 358
  - MIB, 359–360
  - SMI, 359
  - SNMP, 360–362
- Network orchestration layer process, 626
- Network queues and delay analysis, 403–404
  - birth-and-death process, 406–408
  - Little's theorem, 404–406
  - $M/M/1/b$ , 414–415
  - $M/M/a$ , 415–420
  - $M/M/a/a$ , 420–422
  - $M/M/\infty$ , 422–424
- Markovian FIFO queueing systems. *See* Markovian FIFO queueing systems
- networks of queues, 428–437
- non-Markovian models, 424–427
- queueing disciplines, 408–409
- self-similarity and batch-arrival models, 427–428
- Network-to-network interfaces (NNIs), 548
- Network/transport-layer packet filtering, 393–394
- Network virtual terminals (NVTs), 343–344
- Networking devices. *See also* individual devices
  - multiplexers, 58–65
  - NICs, 39–40
- Networks. *See also* individual network types
  - cloud-based multimedia, 751–756
  - of queues, 428–437
  - switching. *See* Switch fabrics
  - topologies, 7, 116–117

- Next header field
    - IPsec, 388
    - IPv6 packets, 196
  - Next-header fields in packet headers, 449
  - Next hops in RIP packets, 186
  - NFV (network function virtualization), 614
    - abstract model, 624–626
    - distributed networks, 626–627
    - overview, 623–624
    - virtualized services, 627
  - NIC teaming, 107
  - NICs (network interface cards), 37, 446
    - ARP, 131
    - layer 3 devices, 44–45
    - overview, 39–40
    - virtual, 597–598
  - NNIs (network-to-network interfaces), 548
  - Nodes
    - ad-hoc networks, 782–783
    - cascaded, 428–431
    - optical networks, 560–561
    - packet-switched networks, 6
    - sensor networks, 793–794
  - Noise, 77
  - Non-electro-optical switches, 556
  - Non-least-cost-path routing, 174
  - Non-Markovian models
    - arrival, 427
    - queuing, 424–427
    - streaming analysis, 756–759
  - Non-persistent connections, 338
  - Non-Poisson models
    - arrival, 427
    - queuing, 424
  - Non-preemptive priority queues, 503–505
  - Non-real-time packets, 502
  - Nonblocking switch fabrics, 458
  - Nonpersistent CSMA, 94
  - Nonreturn-to-zero (NRZ) line coding, 76
  - Normal (Gaussian) random variables, 831
  - Normalized method, 314–315
  - Notification packets, 191
  - Notifications in cloud-based multimedia, 752
  - NRZ-inverted line coding, 76
  - NRZ (natural nonreturn-to-zero) line coding, 76
  - NTP timestamp field, 733
  - Number of additional records field, 329
  - Number of answers field, 329
  - Number of authoritative records field, 329
  - Number of questions field, 329
  - NVTs (network virtual terminals), 343–344
  - Nyquist theorem, 696
- O**
- Object names in distributed hash tables, 353
  - Observer-gatekeeper-routed signaling, 660
  - OCs (optical carriers), 548
  - OFDM (orthogonal frequency division multiplexing), 59–61, 99–100, 144–145, 150, 285
  - OFDMA scheme in LTE downlinks, 273
  - Offer process in DHCP, 169
  - OLs (optical links), 547
  - OLSR (Optimized Link State Routing) protocol, 149–150
  - OLTs (optical line terminals), 551–552
  - Omnidirectional configuration, 140
  - On-demand cloud computing, 579
  - 1-persistent CSMA, 94, 119
  - ONF (Open Networking Foundation), 613
  - Online gaming, 751
  - ONUs (optical network units), 551–552, 748
  - Opaque optical switches, 563
  - OPCs (original point codes), 645
  - Open Networking Foundation (ONF), 613
  - Open networks, Jackson's theorem on, 434–437
  - Open packets in BGP, 190, 194, 233
  - Open-routed networking, 630
  - Open Shortest Path First (OSPF) protocol, 610
    - MOSPF, 226
    - operation, 180–183
  - Open systems interconnection (OSI) model, 20
  - OpenDaylight controllers, 614–615
  - OpenFlow protocol, 615–616
    - flow tables, 617–618
    - matching fields, 618–619
    - switches, 616–617
  - Operation error chunks, 737
  - OPPs (output port processors), 44–45, 453–454
  - Optical carriers (OCs), 548
  - Optical cross-connects (OXCs)
    - GMPLS, 549–550
    - structure, 560–563
    - switches, 556
  - Optical fiber, 76
  - Optical line terminals (OLTs), 551–552
  - Optical links (OLs), 547
  - Optical network units (ONUs), 551–552, 748
  - Optical networks, 545–546

- all-optical, 563–566
- amplifiers, 553–554
- contention resolution in, 557–558
- delay elements, 553
- fiber optic links, 547
- filters, 554, 561
- GMPLS protocol, 548–551
- overview, 546–547
- OXC, 560–563
- passive, 551–553
- SONET/SDH standards, 547–548
- switches, 556–560, 569–572
- tunable lasers, 553
- wavelength allocation, 567–569
- WDMs, 555
- Optimal quantizers, 699–700
- Optimality
  - packet size, 15–17
  - routing algorithm, 162
- Optimistic unchoking, 352
- Optimized Link State Routing (OLSR) protocol, 149–150
- Optional Parameters field, 190
- Options field
  - IP packets, 162
  - TCP segments, 300–301
- Options messages in SIP, 677
- Original point codes (OPCs), 645
- Orthogonal frequency division multiplexing (OFDM), 59–61, 99–100, 144–145, 150, 285
- OSI (Open systems interconnection) model, 20
- OSPF (Open Shortest Path First) protocol, 610
  - MOSPF, 226
  - operation of, 180–183
- Other Features messages, 676–678
- Outbound notifications in cloud-based multi-media, 752
- Outcomes in probability, 827
- Output port buffers, 453–454, 473
- Output port processors (OPPs), 44–45, 453–454
- Overlay models, 548
- Overlay networks, 600–601
- OXC (optical cross connects)
  - GMPLS, 549–550
  - structure, 560–563
  - switches, 556
- P**
- P (predictive) frames, 708
- P-CSCF (proxy call session control function), 269, 683
- P field in contention resolution units, 456
- P-persistent CSMA, 94
- P2P (peer-to-peer) networks, 548, 600
  - connection efficiency, 355–356
  - database sharing protocols, 353–355
  - file sharing protocols, 348–352
  - WMNs for, 277
- PaaS (platform as a service), 583
- Packet-by-packet routers, 46
- Packet Data Convergence Protocol (PDCP), 269
- Packet data gateway (PGW), 269, 683
- Packet-drop probability, 204–205
- Packet encapsulators, 452–453
- Packet flooding algorithm, 177–178
- Packet-in messages, 617
- Packet length field, 182
- Packet-mistreatment attacks, 373–374
- Packet-out messages, 617
- Packet queues and delay analysis, 12–13
- Packet-reservation multiple-access (PRMA) scheme, 106
- Packet scheduling, 501–502
  - deficit round-robin, 511
  - earliest deadline first, 511–512
  - fair queueing, 507–508
  - first in, first out, 502–503
  - priority queueing, 503–507
  - weighted fair queueing, 508–511
- Packet-switched networks, 3–4
  - CIDR, 26–27
  - connection-oriented, 13–15
  - connectionless, 11–13
  - equal-sized packet model, 28
  - Internet, 7–9
  - Internet addressing schemes, 21–22
  - IP addresses, 21–27, 162
  - ISPs and internetwork nodes, 9–11
  - messages, packets, and frames in, 6–7
  - networking protocols, 17–21
  - packet size in, 15–17
  - packet switching vs. circuit switching, 5–6
  - packets, 21–22
  - subnets, 24–26
- Packet type field, 733
- Packetized elementary stream (PES), 749–750
- Packets, 5
  - BGP, 190–192

- Packets (*continued*)
  - filtering, 391–396
  - fragmentation and reassembly, 7, 163–164, 198–199
  - IGMP, 223–224
  - IP, 160–163
  - IPTV, 749–750
  - LANs, 116
  - MBGP, 232–233
  - MPLS, 530–531, 536
  - MSDP, 235
  - multicasting, 475–480
  - OSPF, 181–183
  - packet-switched networks, 6–7
  - parsers, 448–449
  - partitioners, 449–450
  - reassemblers, 454
  - RIP, 186–187
  - RTCP, 732–735
  - RTP, 729–731
  - SCTP, 736–737
  - size, 15–17
  - SSH, 345
  - TCP, 299–301
  - TORA, 775
- Pad field, 120
- Pad length field, 388
- Padding field
  - IP packets, 162
  - IPsec headers, 388
  - RTCP packets, 732
  - RTP packets, 729
  - SSH Packets, 345
- Padding in SHA, 385
- Paging in cellular networks, 253
- PAM (pulse amplitude modulation), 696
- PAPR (peak-to-average power ratio), 100
- Parallel connections in link blocking, 206–207
- Parallel nodes, Burk’s theorem on, 431–432
- Parallel-plane switching fabrics, 470–471
- Parallel-to-serial multiplexing, 452
- Pareto distributions, 759
- Parity bits, 79
- Parity check methods, 79
- Parsers, packet, 448–449
- Partial-gatekeeper-routed signaling, 660–661
- Partitioners, packet, 449–450
- Passive attacks, 783
- Passive optical networks (PONs), 551–553
- Path attributes field, 190–192
- Path discovery, 781
- Path loss
  - optical networks, 558
  - wireless links, 280–281
- Path selection algorithms, 173–178
- Path vector routing protocols, 192–193
- Payload data field, 388
- Payload length field, 196
- Payload type field, 730
- PBX (private branch exchange) applications, 647
- PCF (point-coordination function), 147
- PCM (pulse code modulation), 708–709
- PCs (point codes), 645
- PDCCP (Packet Data Convergence Protocol), 269
- PDF (probability density function), 829, 833
- PDU (protocol data units), 360–362, 736
- Peak-to-average power ratio (PAPR), 100
- Peer-to-peer (P2P) networks, 548, 600
  - connection efficiency, 355–356
  - database sharing protocols, 353–355
  - file sharing protocols, 348–352
  - WMNs for, 277
- Peer-to-peer topology, 141
- Peers in BGP, 193
- Pending interest tables (PITs), 630
- Per hop behaviors (PHBs), 496–497
- Performance
  - network management for, 357
  - switch fabrics, 469–475
- Period data in ICR, 808–809
- Permanent addresses in mobile IP, 260
- Permutations in AES, 380
- Persistent connections in HTTP, 338
- PES (packetized elementary stream), 749–750
- PGW (packet data gateway), 269, 683
- Phase shift keying (PSK), 52–53
- PHBs (per hop behaviors), 496–497
- Phone call process in SS7 networks, 645–646
- Phone numbers in SIP, 669–670
- Phone units in IVR, 754
- Photographs, 702
- Photonics, 547
- Physical congestion, 199–200
- Physical layer
  - IEEE 802.11, 144–145
  - TCP/IP protocol model, 19
  - WMNs, 279–280
- Picocells, 269



- Pictures, 702
- PIFS (point IFS coordination function), 147
- PIM (protocol-independent multicast), 227–230, 236, 595, 747
- Pin attacks, 784
- Ping of death, 374
- PITs (pending interest tables), 630
- Pixels, 702, 717–718
- Platform as a service (PaaS), 583
- Platforms in cloud computing, 579, 581
- Plug-and-play protocols, 167
  - LANs, 128
  - UPnP, 172–173
- PMF (probability mass function), 829, 833
- Point codes (PCs), 645
- Point-coordination function (PCF), 147
- Point IFS coordination function (PIFS), 147
- Point-to-point connections, 474
- Point-to-Point Protocol (PPP), 521–522, 526
- Point-to-Point Tunneling Protocol (PPTP), 521, 526
- Pointer fields, 449
- Poisoned-reverse rule, 186
- Poisoning attacks, 372–373
- Poisson random variables, 831
- Polar NRZ line coding, 76
- Policing traffic, 201–202, 488
- Pollaczek-Khinchin formula, 424–427
- Polling feature, 147
- Polynomial CRC interpretation, 82
- PONs (passive optical networks), 551–553
- POP (Post Office Protocol), 334
- Port forwarding, 344–346
- Port numbers
  - NAT, 171
  - RTP, 728
  - transport layer, 21, 292–293
  - UDP, 296
- Port trunking, 107
- POST method in HTTP, 339
- Post Office Protocol (POP), 334
- Power ratio, 500–501
- Power save-poll (PS-Poll) frames, 148
- Power supplies
  - ad-hoc networks, 783
  - sensor networks, 794
- PPM (pulse position modulation), 144, 696
- PPP (Point-to-Point Protocol), 521–522, 526
- PPTP (Point-to-Point Tunneling Protocol), 521, 526
- PQ (priority queuing), 409
  - non-preemptive, 503–505
  - preemptive, 505–507
  - schedulers, 503–507
- Preamble field, 120
- Predictive (P) frames, 708
- Preemption queuing systems, 409
- Preemptive priority queues, 506–507
- Prefixes in CIDR, 26
- Prerecorded media streaming, 726–727
- Presentation layer, 20
- Priority queuing (PQ), 409
  - non-preemptive, 503–505
  - preemptive, 505–507
  - schedulers, 503–507
- Privacy in CDMA, 104
- Private branch exchange (PBX) applications, 647
- Private clouds, 579
- PRMA (packet-reservation multiple-access) scheme, 106
- PRNs (provide roaming number) messages, 253
- Proactive distributed routing, 806
- Probability, 827–828
  - blocking, 421–422, 462–463, 837–840
  - expected value and variance in, 831–832
  - Markov chains in, 835–836
  - random variables in, 828–831
  - stochastic processes, 834–835
  - TDM blocking, 63–64
  - TDM clipping, 65
- Probability density function (PDF), 829, 833
- Probability mass function (PMF), 829, 833
- Processing units, 794
- Progress call-signaling messages, 659
- Protocol, 2
  - Protocol converters, 121
  - Protocol data units (PDUs), 360–362, 736
  - Protocol field, 161
  - Protocol immunization, 785
  - Protocol-independent multicast (PIM), 227–230, 236, 595, 747
- Protocols
  - ad-hoc networks, 769–783
  - LANs, 117–121
  - network management, 358
  - sensor networks, 791–792
  - transport layer, 294
- Provide roaming number (PRNs) messages, 253
- Providing routers, 539
- Provisioning in link aggregation, 107–108

- Proxy call session control function (P-CSCF), 269, 683
  - Proxy servers
    - SIP, 667–668
    - Web, 341–342, 395–396
  - Prune messages, 228
  - Pseudonoise signals, 103
  - PSK (phase shift keying), 52–53
  - Public clouds, 579
  - Public-key encryption, 344, 376, 380–383
  - Public-switched telephone networks (PSTNs), 10
    - circuit-switched networks, 647–649
    - overview, 642–644
    - SIP to PSTN internetworking, 681–682
    - SS7, 644–647
  - Pulse amplitude modulation (PAM), 696
  - Pulse code modulation (PCM), 708–709
  - Pulse position modulation (PPM), 144, 696
  - Pulse-type plots, 312
  - Pulse width modulation (PWM), 696
  - Push (PSH) field, 300, 303
  - PUT method in HTTP, 339
- Q**
- Q components in modulation, 54
  - Q field in contention resolution units, 456
  - QAM (quadrature amplitude modulation), 53–55, 60
  - QoS. *See* Quality of service (QoS)
  - QPSK (quadrature phase shift keying), 53–55, 57–58, 60
  - QRV (querier’s robustness variable), 223
  - Quadrature amplitude modulation (QAM), 53–55, 60
  - Quadrature carriers, 54
  - Quadrature-phase components, 55
  - Quadrature phase shift keying (QPSK), 53–55, 57–58, 60
  - Quality of service (QoS), 485–486
    - differentiated services, 495–497
    - distributed multimedia mini-clouds, 752–753
    - input buffers, 450
    - integrated services, 486–495
    - IPPs, 447
    - network management for, 357
    - overview, 486
    - packet scheduling in, 501–512
    - resource allocation, 497–501
    - for streaming, 744–745
    - WMNs, 279
  - Quantization in compression
    - images, 705–706
    - voice, 696–701
  - Querier’s robustness variable (QRV), 223
  - Query messages, 329, 349
  - Query packets
    - ABR, 776
    - TORA, 775
  - Questions field, 329–330
  - Queue sets, 473
  - Queues
    - delay-sensitive traffic, 420–422
    - multipath buffered crossbars, 472–475
    - priority, 503–507
    - RED, 204–205
- R**
- Radar, 72
  - Radio frequency (RF) spectrum, 72
  - Radio systems, 72
  - Radio waves, 47
  - RADIUS protocol, 391
  - Rake receivers, 103
  - RAMA (root-addressed multicast architecture), 237
  - Random-access techniques
    - TDMA, 99
    - wireless access, 105–106
  - Random early detection (RED) technique, 203–205
  - Random padding field, 345
  - Random processes
    - lossy compression, 709
    - probability, 834–835
  - Random service queuing systems, 409
  - Random variables
    - functions of, 832–834
    - in probability, 828–831
  - Randomizing traffic, 469
  - RARP (Reverse Address Resolution Protocol), 132–133
  - RAS (registration, admission, and status) signaling, 653–659
  - Rate-based resource allocation, 500
  - Raw-image sampling, 702–705
  - RCMs (release complete messages), 646–647
  - Reactive distributed routing, 806
  - Reactive routing protocols, 769, 784

- Real-Time Control Protocol (RTCP), 653, 671, 732–735
- Real-time media exchange protocols, 726–731
- Real-time media transport protocols
  - HTTP-based streaming, 740–741
  - RTCP, 732–735
  - RTSP, 735
  - SCTP, 735–740
- Real-time packets, 502
- Real-time sessions, 728–729
- Real-time Streaming Protocol (RTSP), 666, 735, 749
- Real-time transport protocol (RTP), 653, 666, 671, 727–731, 749
- Rearrangeably nonblocking, 559
- Reassemblers in output port processors, 454
- Reassembly of packets, 163–164
- Receiver report (RR) packets, 732–733
- Receivers, CRC generation at, 81–82
- Recirculation in switching networks, 469
- Reclustering, 805
- Recursive mapping, 328
- RED (random early detection) technique, 203–205
- Redirect messages in ICMP, 165
- Redirect servers in SIP, 668
- Redundancy in data center networks, 589
- Refer messages in SIP, 677–678
- Reflection paths, 280
- Regional handoffs, 255
- Regional Internet service providers, 8
- Register messages in PIM, 229
- Register packets in MSDP, 235
- Registration
  - cellular networks, 249–250
  - mobile IP, 259, 262–264
  - SIP, 672–673
- Registration, admission, and status (RAS) signaling, 653–659
- Registration servers, 668
- Relays in RTP, 728–729
- Release Complete call-signaling messages, 659
- Release complete messages (RCMs), 646–647
- Release messages (RLMs), 646–647
- Reliability of mobile IP, 259
- Reliable data delivery, 145
- Remote-access VPNs, 526
- Remote-controls, 73
- Remote login protocols, 342–346
  - SSH, 344–346
  - TELNET, 343–344
- Rendezvous-based networking, 630–631
- Rendezvous points, 220, 228–229
- Repeaters, 40–41
  - LANs, 121
  - overview, 42
- Replication attacks, 374
- Reply messages, 329
- Reply packets, 776
- Representative routers, 234–236
- Request-expiration timers, 778, 781
- Request ID field, 361
- Request in progress (RIP) message, 659
- Request messages
  - HTTP, 339
  - SIP, 669
- Request process in DHCP, 169
- Request to Send (RTS) frames, 148
- Request-to-send/clear-to-send (RTS/CTS) scheme, 145
- Requests for comments (RFCs), 823–826
- Requests in mobile IP registration, 262
- RERR (route-error) messages, 774, 782
- Rescue operations, ad-hoc networks for, 767
- Resequencers in output port processors, 454
- Reservation access method for links, 92
- Reservation-based protocols, 105–106
- Reservations in RSVP, 495
- Reset (RST) field, 300
- Resource allocation, 497–498
  - classification, 499–500
  - fairness, 500–501
  - managing, 498–499
- Resource availability in RAS signaling, 658
- Resource oriented traffic engineering, 539
- Resource Reservation Protocol (RSVP), 495
- Resources in virtualization, 585
- Response messages
  - HTTP, 339–340
  - SIP, 669
- Responses in mobile IP registration, 262
- Reuse, frequency, 273–277
- Reverse Address Resolution Protocol (RARP), 132–133
- Reverse topologies, 635
- RF (radio frequency) spectrum, 72
- RFCs (requests for comments), 823–826
- RIA (routing information acknowledgment) messages, 253

- RIP (request in progress) message, 659
- RIP (routing information protocol), 183–188, 769
- Rivest, Shamir, and Adleman (RSA) algorithm, 381–382
- RLMs (release messages), 646–647
- Roaming in cellular networks, 252–253
- Root-addressed multicast architecture (RAMA), 237
- Root points, 220
- Root servers, 327
- Root switches in STP, 134–135
- Round-robin access method, 92
- Round robin algorithms, 590
- Round robin queuing systems, 409
- Round-trip times (RTTs), 310, 313–314, 338
- Rounds in LEACH, 801
- Route costs, 173, 179
- Route-creation process, 775
- Route discovery
  - ABR, 776
  - ad-hoc networks, 785
  - AODV, 778–781
  - DSP, 773–774
  - ICR, 809
  - source-initiated protocols, 769
- Route-error (RERR) messages, 774, 782
- Route maintenance, 781–782
- Route reconstruction, 776
- Route reply (RREP) packets, 774, 779–780
- Route request (RREQ) packets, 773–774, 778–780
- Route selection policy, 195–196
- Route tags in RIP packets, 187
- Router-based resource allocation, 499
- Router ID field, 182
- Router line cards, 447
- Router servers, 10
- Routers
  - architecture, 446–447
  - attacks on, 373
  - central controllers, 454–457
  - data center networks, 589
  - description, 41
  - input port processors for, 446–453
  - for ISPs, 7
  - MBGP, 231–232
  - Mbone, 224
  - MPLS, 539
  - MSDP, 234–236
  - multicasting packets, 475–480
  - output port processors for, 453–454
  - overview, 45–47
  - packet-switched networks, 10
  - RED, 203–205
  - wireless, 48–49, 149
  - WMNs, 277
- Routing and internetworking, 7–8, 159–160
  - ad-hoc networks, 767–769
  - AODV, 778–779
  - congestion control. *See* Congestion
  - ICN, 628–631
  - interdomain routing protocols, 188–196
  - Internet. *See* Internet routing policies
  - intradomain routing protocols, 178–188
  - IP packets and basic policies, 160–163
  - IPv6, 196–199
  - mobile IP, 263–267
  - MPLS domains, 534–536
  - multi-tunnel, 536–538
  - packet-switched networks, 11
  - path selection algorithms, 173–178
  - sensor networks, 805–811
- Routing caching timeouts, 778, 781
- Routing information acknowledgment (RIA) messages, 253
- Routing information protocol (RIP), 183–188, 769
- Routing switch fabric, 475–476
- Routing tables
  - AODV, 777
  - CGSR, 771
  - DSDV, 769–770
  - input port processors, 450–452
  - layer 2 devices, 125
  - overflow attacks on, 784
  - packet-switched networks, 11
  - poisoning attacks on, 372–373
  - RIP, 185–186
  - routers, 447
  - WRP, 772
- RR (receiver report) packets, 732–733
- RREP (route reply) packets, 774, 779–780
- RREQ (route request) packets, 773–774, 778–780
- RSA (Rivest, Shamir, and Adleman) algorithm, 381–382
- RSVP (Resource Reservation Protocol), 495
- RTCP (Real-Time Control Protocol), 653, 671, 732–735
- RTP (real-time transport protocol), 653, 666, 671, 727–731, 749
- RTP timestamp field, 734

- RTS/CTS (request-to-send/clear-to-send)
  - scheme, 145
- RTSP (Real-time Streaming Protocol), 666, 735, 749
- RTTs (round-trip times), 310, 313–314, 338
- Rules in packet filtering, 393
- Run-length encoding, 714–715
- S**
- S field, 536
- SaaS (software as a service), 582
- SAL (service abstraction layer), 614
- Sample space, 709, 827
- Sampling
  - in compression, 695–696, 702–705
  - in probability, 828
- SAP (Session Announcement Protocol), 666
- Satellite systems, 72, 244–245
- SC-FDMA (single-carrier frequency-division multiple access), 100, 273
- Scalability
  - CDMA, 104
  - multicasting, 216
  - software-defined networking, 620–621
  - VPNs, 527
  - WMNs, 279
- Scanned document compression, 717–718
- Scattering paths, 280
- SCCP (signaling connection control part), 644
- Schedulers, multicast, 452
- Schedules
  - data center networks, 591
  - packet, 501–512
- Scheduling discipline, 408
- SCP (Secure Copy Protocol), 346–347
- SCPs (service control points), 642, 644
- SCTP (Stream Control Transmission Protocol), 735–740
- SDES (source descriptor) packets, 732
- SDH (Synchronous Digital Hierarchy) standard, 547–548
- SDMA (space-division multiple access), 104
- SDN. *See* Software-defined networking (SDN)
- SDP (Session Description Protocol), 666–667
- SDSL (symmetric digital subscriber line), 56–57
- Secret-key encryption, 376
- Secure Copy Protocol (SCP), 346–347
- Secure Hash Algorithm (SHA), 385–387
- Secure Shell (SSH) Protocol, 344–346
- Security, 369–370
  - ad-hoc networks, 783–785
  - authentication techniques, 383–385
  - cryptographic techniques, 377–383
  - elements, 370–371
  - firewalls, 391–396
  - ICN, 631–632
  - IP, 387–389
  - mobile IP, 259
  - network management for, 358
  - overview, 375–377
  - public-key cryptography, 380–383
  - symmetric-key cryptography, 377–380
  - threats, 371–375
  - VPNs, 524, 527–528
  - wireless networks, 389–391
- Security Association (SA) tags, 388
- Security parameters index (SPI) field, 388
- Seeds in BitTorrent, 350–351
- Segments
  - TCP, 299–301, 310–311
  - transport layer, 292
  - UDP, 295–297
- Self-organized overlay networks, 601
- Self-organizing sensor networks, 789–790
- Self-routing, 571
- Self-similarity
  - in multimedia, 756–759
  - in queuing models, 427–428
- Self-similarity parameter, 758
- Self-stabilization, 767, 785
- Semi-optical routers, 563
- Send information (SI) messages, 253
- Sender report (SR) packets, 732–734
- Sender's byte count field, 734
- Sender's packet count field, 734
- Sensing units, 793
- Sensor networks, 789–790
  - clustering in, 790–791, 799–805
  - communication energy model, 794–799
  - intercluster routing protocols, 808–811
  - intracluster routing protocols, 806–808
  - node structure for, 793–794
  - power supplies, 794
  - protocol stack for, 791–792
  - related technologies, 811–812
  - routing protocols overview, 805–807
  - simulation of, 812–814
- Sequence control (SC) field, 148

- Sequence number field
  - IPsec, 388
  - RTP packets, 730
  - TCP segments, 299
- Sequences and sequence numbers
  - AODV, 778
  - Shannon's coding theorem, 711-713
  - TCP, 298
- Sequential experiments, 828
- Serial connections, 206-207
- Serial-to-parallel converters, 60
- Serial-to-parallel multiplexing, 452
- Server modes in VTP, 138
- Server racks, 578
- Server-routed networking schemes, 592
- Servers
  - authoritative, 328
  - DNS. *See* Domain Name System (DNS) and servers
  - web, 336, 341-342
- Service abstraction layer (SAL), 614
- Service chaining, 627
- Service control in RAS signaling, 658-659
- Service control points (SCPs), 642, 644
- Service-level agreements (SLAs), 496
- Service models
  - cloud computing, 581-583
  - queueing systems, 410-413
- Service-set identification (SSIDs), 142
- Service sharing queuing systems, 409
- Service switching points (SSPs), 642-643, 647
- Serving Gateway (SGW), 269, 271, 683
- Serving General packet radio Support Node (SGSN), 247-248
- Session Announcement Protocol (SAP), 666
- Session Description Protocol (SDP), 666-667
- Session Initiation Protocol (SIP)
  - call establishment, 673-674
  - components, 667-668
  - features and extensions, 674-678
  - messages, 669-671
  - organization, 671
  - overview, 666-667
  - registration process, 672-673
  - SIP to H.323 internetworking, 679-680
  - SIP to PSTN internetworking, 681-682
- Session layer, 20
- Sessions
  - RTCP, 733
  - RTP, 728-729
- Set and Trap PDUs, 361
- Set-top boxes, 746, 748
- Setup call-signaling messages, 659, 662
- 7-layer OSI model, 20
- SGSN (Serving General packet radio Support Node), 247-248
- SGW (Serving Gateway), 269, 271, 683
- SHA-1 hash codes, 351
- Shadow fading, 281
- Shannon's coding theorem, 711-713
- Shapers, 496
- Shared data buses, 471-472
- Shared-memory switch fabrics, 468-469
- Shared trees, 220, 228-229
- Sharing resources in virtualization, 585
- SHF (super-high frequency) band ranges, 98
- Short IFS (SIFS) interval, 147
- Shortest paths
  - SSN, 571
  - STP, 134-135
- Shutdown chunks, 738
- Shutdown acknowledgment chunks, 738
- Shutdown complete chunks, 738
- SI (send information) messages, 253
- SIFS (short IFS) interval, 147
- Signal regeneration, 42
- Signal sampling, 695-696
- Signal System 7 (SS7) networks, 642-643
  - MSUs, 645-646
  - overview, 644-645
  - phone call process and signaling sessions, 645
- Signal-to-noise ratio (SNR), 280-281, 283
- Signal transfer points (STPs), 642-643
- Signaling
  - SCTP, 738-740
  - SS7 networks, 645-646
- Signaling connection control part (SCCP), 644
- Signaling link selection (SLS), 645
- Signaling protocols in VoIP, 649-650
- Signaling servers, 650
- Signaling Transport (sigtran) group, 679
- Signatures, digital, 387
- Simple Mail Transfer Protocol (SMTP), 333-334
- Simple multicast, 237
- Simple Network Management Protocol (SNMP), 360-362
- Simplicity of routing algorithms, 162

- Single-carrier frequency-division multiple access (SC-FDMA), 100, 273
- Single-key encryption protocols, 377
- Single-path switching networks, 458
- Single-source denial-of-service attacks, 375
- Single-stage switching networks, 458
- Single topologies in SDN emulators, 635
- SIP. *See* Session Initiation Protocol (SIP)
- Site-to-site VPNs, 526–527
- Size, packet, 15–17
- SLAs (service-level agreements), 496
- Sliding-window flow control, 88–92, 305–306
- Slow start congestion control method, 311–312
- SLS (signaling link selection), 645
- Small-size routers, 46
- SMI (structure of management information), 359
- SMTP (Simple Mail Transfer Protocol), 333–334
- SNMP (Simple Network Management Protocol), 360–362
- SNR (signal-to-noise ratio), 280–281, 283
- Social networking protocols, 347
- Sockets in transport layer, 293–294
- Softswitch methods, 678
- Software as a service (SaaS), 582
- Software-defined networking (SDN), 607–608
  - APIs, 613
  - application delivery, 622–623
  - cloud computing, 621–623
  - compute and storage, 621–622
  - control planes, 609–615
  - data planes, 609–611, 615–619
  - information-centric networking, 627–632
  - multicasting, 621
  - network emulators, 632–635
  - network function virtualization, 623–627
  - network model, 613–619
  - overview, 608–609
  - scalability, 620–621
  - small-size architectures, 620–621
- Software firewall programs, 392
- Solar cells, 791
- SONET (Synchronous Optical Networking)
  - standard, 547–548
- Sorted deadline lists, 511–512
- Source-active (SA) packets, 235
- Source address field
  - Ethernet LAN frames, 120
  - IP packets, 162
  - IPv6 packets, 196
- Source-based congestion avoidance, 313–314
- Source coding systems, 695
- Source descriptor (SDS) packets, 732
- Source encoder units, 709
- Source identification in RTCP, 733
- Source-initiated protocols, 769
- Source port field
  - SCTP packets, 736
  - TCP segments, 299
  - UDP segments, 296
- Source ports
  - transport layer, 292
  - UDP, 296
- Source routing, 179
- Space-division multiple access (SDMA), 104
- Spanke-Benes switching networks, 559–560
- Spanning-Tree Protocol (STP), 133–136, 610
- Sparse-mode algorithm, 220
- Sparse-mode PIM, 227–230, 236
- Spatial frequencies, 704
- SPDY protocol, 338
- Speech recognition in IVR, 754
- Speed-up factor in switching networks, 469
- Spherical switching networks (SSNs), 569–572
- Spike noise, 77
- Split-horizon rule, 186
- Spread-spectrum techniques
  - CDMA, 101, 103–104
  - LANs, 141
  - physical layer, 144
- Squared-error distortion, 697
- SR (sender report) packets, 732–734
- SS7 (Signal System 7) networks, 642–643
  - MSUs, 645–646
  - overview, 644–645
  - phone call process and signaling sessions, 645
- SSH (Secure Shell) protocol, 344–346
- SSIDs (service-set identification), 142
- SSNs (spherical switching networks), 569–572
- SSPs (service switching points), 642–643, 647
- SSRC field, 734
- Stability of routing algorithms, 162
- Stages in switching networks, 458
- Star couplers, 556, 560
- Star topology for LANs, 116–117
- Start of frame field, 120
- Stateful packet filtering, 394
- Stateless packet filtering, 394
- Static intradomain routing protocols, 179

- Static protocols, 768
  - Static routes with routers, 45
  - Statistical multiplexing, 64–65
  - Status codes in HTTP response messages, 340
  - Status lines in HTTP response messages, 340
  - Status mode in RAS signaling, 658
  - Steady-state phase in LEACH, 801
  - Still image compression, 701–707
  - Stochastic processes, 834–835
  - Stop-and-go model, 255–259
  - Stop-and-wait flow control, 85–88
  - Store-and-forward operation, 12
  - STP (Spanning-Tree Protocol), 133–136, 610
  - STPs (signal transfer points), 642–643
  - Stream batches, 756
  - Stream Control Transmission Protocol (SCTP), 735–740
  - Streaming
    - audio, 708–709
    - non-Markovian, 756–759
    - QoS for, 744–745
  - Structure of management information (SMI), 359
  - Subcarriers in OFDM, 100
  - Subnet addressing, 24–26
  - Subnet masks, 186, 188
  - Subscribe and Notify messages in SIP, 677
  - Super-high frequency (SHF) band ranges, 98
  - Superframe intervals, 147
  - Supernetting, 26–27
  - Superposition, 436
  - Swarms in BitTorrent, 350–352
  - Switch fabrics
    - buffers, 471–475
    - characteristics, 457–458
    - clos, 460–465
    - complexity, 458
    - concentration and expansion switches, 465–468
    - crossbar, 459–460
    - multipath buffered crossbars, 471–475
    - performance, 469–475
    - router, 44–45
    - shared-memory, 468–469
  - Switch IDs in STP, 134–135
  - Switch modes in VTP, 138–139
  - Switch-routed networking schemes, 592–594
  - Switches
    - OpenFlow, 616–617
    - optical networks, 556–560, 569–572
    - virtual, 599–600
    - VLANs, 137–138
  - Switching and routing devices, 40–41
    - layer 1, 41–42
    - layer 2, 42–44, 124–125
    - layer 3, 44–47
    - wireless, 47–50
  - Switching nodes, 6, 8
  - Switching tiers structures, 129
  - Symmetric digital subscriber line (SDSL), 56–57
  - Symmetric-key cryptography, 376–377
    - AES, 379–380
    - DES, 377–379
  - Synchronization source (SSRC) identifier field
    - RTCP packets, 733
    - RTP packets, 730
  - Synchronize (SYN) field, 300
  - Synchronous Digital Hierarchy (SDH) standard, 547–548
  - Synchronous MAC protocols, 118
  - Synchronous Optical Networking (SONET) standard, 547–548
  - Synchronous TDM, 61–64
  - System capacity in frequency reuse, 274
- ## T
- Table-driven routing protocols, 768
  - Tail-drop policy, 203
  - TCAP (transaction capabilities application part), 645
  - TCAs (traffic-conditioning agreements), 496
  - TCP *See* Transmission Control Protocol (TCP)
  - TCP/IP (Transmission Control Protocol/Internet Protocol) model, 17–20
  - TCP normalized method, 314–315
  - TDM (time-division multiplexing), 61
    - GMPLS, 551–552
    - statistical, 64–65
    - synchronous, 61–64
  - TDMA (time-division multiple access), 99
  - TE (traffic engineering), data center networks, 591
  - Telephone systems, 72. *See also* Cellular networks; Voice over IP (VoIP)
  - Telephony over passive optical networks (TPONs), 553
  - Television systems, 72, 745–750
  - TELNET protocol, 343–344
  - Temporally Ordered Routing Algorithm (TORA), 774–775



- Temporary address field, 263
- Terminal-only-routed signaling, 660
- Terminals in H.323 protocol, 652
- Text-to-speech units, 754
- Thermo-optic switches, 556
- Threats to security
  - ad-hoc networks, 783–784
  - categories, 371–375
- Three-dimensional switches, 475
- Three-way handshakes, 337
- Throughput in TCP, 309, 314
- Time-division multiple access (TDMA), 99
- Time-division multiplexing (TDM), 61
  - GMPLS, 551–552
  - statistical, 64–65
  - synchronous, 61–64
- Time-to-live (TTL) field
  - eBGP, 195
  - ICMP, 165
  - IP packets, 161
  - MPLS packets, 536
- Timeouts in flow control, 87–88
- Timestamp field
  - PDU, 361
  - RTP packets, 730–731
- Token arrival rate, 493
- Token-bucket traffic shaping, 493–494
- Tokens in token-bucket traffic shaping, 493
- Top-of-rack (ToR) in data center networks, 588
- Topologies
  - LANs, 7, 116–117
  - SDN emulators, 634–635
- ToR (top-of-rack) in data center networks, 588
- TORA (Temporally Ordered Routing Algorithm), 774–775
- Torus-shaped topology, 570
- TOS (type of service) field
  - differentiated services QoS, 496
  - OSPF, 181
- Total length field, 161–162
- Total Path Attribute Length field, 190, 192
- Total system delay in queues, 506
- TPONs (telephony over passive optical networks), 553
- Trackers in BitTorrent, 350
- Traffic channels, 248
- Traffic class field, 196
- Traffic classifiers, 496
- Traffic conditioners, 495–496
- Traffic-conditioning agreements (TCAs), 496
- Traffic-congestion case, 498
- Traffic engineering (TE), 528, 538–539, 591
- Traffic grooming, 551
- Traffic oriented traffic engineering, 539
- Traffic policing, 201, 488
- Traffic shaping, 488–494
  - leaky-bucket, 489–493
  - token-bucket, 493–494
- Transaction capabilities application part (TCAP), 645
- Translator relays, 729
- Transmission control blocks, 298
- Transmission Control Protocol (TCP), 298
  - applications of, 306
  - congestion control, 309–315
  - connection setup for, 301–303
  - connection termination, 304–305
  - data transfer phase, 303–304
  - MAC headers, 118
  - for mobility, 307–309
  - vs. SCTP, 738–740
  - segments in, 299–301
- Transmission Control Protocol/Internet Protocol (TCP/IP) model, 17–20
- Transmissions, data link. *See* Data links
- Transmitters, CRC generation at, 80
- Transparent bridges in LANs, 128
- Transparent modes in VTP, 139
- Transport and end-to-end protocols, 289–290
  - congestion control, 309–315
  - mobile, 307–309
  - TCP, 298–306
  - transport layer for, 290–294
  - UDP, 295–298
- Transport layer, 22, 290–291
  - Port number, 21, 292
  - interaction with adjacent layers, 291–294
  - protocols, 294
- Transport mode in IPsec, 389
- Tree algorithms, 218–220, 476–478
- Tree-based routing, 265–266
- Tree topologies in SDN emulators, 635
- Trunks
  - PBX, 647
  - PSTNs, 643
- Tunable dispersion compensators, 553
- Tunable lasers, 553
- Tunable optical filters, 561, 564

- Tunneling
  - IPsec, 389
  - IPv6, 522–523
  - Mbone, 224
  - MPLS, 536–538
  - overview, 519–521
  - PPP, 521–522
  - SSH, 345
- Turbo codes, 284
- Twisted-pair links, 73
- Two-key cryptography, 380
- Two random variable functions, 833–834
- Type data in ICR, 808–809
- Type field
  - BGP, 191
  - ICMP, 164
  - IGMP packets, 222
  - mobile IP, 263
  - OSPF packets, 181
  - SCTP packets, 736
  - SSH Packets, 345–346
- Type of service (ToS) field
  - differentiated services QoS, 496
  - OSPF, 181
- U**
- UDP (User Datagram Protocol), 295
  - applications, 297–298
  - for mobility, 307
  - segments, 295–297
- UDP checksum field, 296–297
- UDP length field, 296
- UE (user equipment) in LTE, 269
- UHF (ultrahigh) band ranges, 98
- UIDs (user information databases), 651
- Ultrahigh (UHF) band ranges, 98
- Ultrapure fused silica, 74
- Unbuffered switching networks, 458
- Unfeasible Routes Length field, 190
- Unguided transmission links, 73
- Unicast addresses, 198
- Unicast IPTV systems, 750
- Unicast routers, 233
- Unidirectional congestion control, 201–202
- Uniform random variables, 831
- Uniform Resource Indicators (URIs), 669–670
- Uniform resource locators (URLs), 172–173, 336
  - CDNs, 743
  - HTTP, 339–340
  - SIP, 666, 669
- Union of events, 827
- UNIs (user-to-network interfaces), 548
- Universal Plug-and-Play (UPnP), 171–172
- Update packets, 182
  - BGP, 190–192
  - MBGP, 232–233
  - TORA, 775
- Updates
  - ad-hoc networks, 785
  - layer 2 devices, 125
  - RIP routing tables, 185–186
- Uplinks in LTE, 273
- UPnP (Universal Plug-and-Play), 172–173
- Upstream bandwidth in ADSL, 56
- Upstream grant processors, 457
- Urgent (URG) field, 300
- Urgent pointer field, 300
- URIs (Uniform Resource Indicators), SIP, 669–670
- URLs (uniform resource locators), 172, 336
  - CDNs, 743
  - HTTP, 339–340
  - SIP, 666, 669
- User Datagram Protocol (UDP), 295
  - applications, 297–298
  - for mobility, 307
  - segments, 295–297
- User equipment (UE) in LTE, 269
- User information databases (UIDs), 651
- User mailboxes, 331, 334
- User-to-network interfaces (UNIs), 548
- User tracking in cellular networks, 254
- Utilization
  - in feedback models, 434
  - link, 16–17
  - in *M/M/1* queuing systems, 412
- V**
- Variables in probability, 828–831
- Variance in probability, 831–832
- VDSL (very high bit-rate digital subscriber line), 57
- VEPAs (virtual Ethernet port aggregators), 598
- Verification tag field, 737
- Version field
  - IP packets, 22
  - IPv6 packets, 196
  - RTCP packets, 732
  - RTP packets, 729

- Version number field
    - OSPF packets, 181
    - RIP packets, 185–186
  - Versions in HTTP, 339–340
  - Very high bit-rate digital subscriber line (VDSL), 57
  - VFNs (virtualized network functions), 624–625, 627
  - Video hub offices (VHOs), 747
  - Video on demand (VoD), 745–750
  - Videoconferencing, 582, 751
  - Virtual agents, 264
  - Virtual-circuit networks, 13–15
  - Virtual Ethernet port aggregators (VEPAs), 598
  - Virtual local area networks (VLANs), 136–139
  - Virtual machines (VMs), 585–587
  - Virtual private clouds (VPCs), 621
  - Virtual private networks (VPNs), 519–520
    - Diffie-Hellman key-exchange protocol for, 382–383
    - MPLS-based, 539–540
    - overview, 524–526
    - remote-access, 526
    - security in, 527–528
    - site-to-site, 526–527
  - Virtual registration, 264
  - Virtualization, 577–578, 595–596
    - components, 596–597
    - data centers, 584–588
    - LANs, 600, 620
    - links, 597
    - NICs, 597–598
    - overlay networks, 600–601
    - switches, 599–600
  - Virtualized network functions (VFNs), 624–625, 627
  - Visiting location register (VLR), 248, 252
  - VLAN Trunking Protocol (VTP), 138–139
  - VLANs (virtual local area networks), 136–139, 600, 620
  - VLR (visiting location register), 248, 252
  - VMs (virtual machines), 585–587
  - VNICs (virtual NICs), 597–598
  - VoD (video on demand), 745–750
  - Voice application servers, 754–755
  - Voice compression
    - quantization and distortion in, 696–701
    - signal sampling in, 695–696
  - Voice Extensible Markup Language (VXML), 754
  - Voice interpreters, 754
  - Voice over IP (VoIP), 641–642
    - H.323 protocols. *See* H.323 protocols
    - multimedia networking, 679–684
    - overview, 649–652
    - PSTNs. *See* Public-switched telephone networks (PSTNs)
    - SIP. *See* Session Initiation Protocol (SIP)
    - softswitch methods and MGCP, 678
  - Voice over LTE (VoLTE), 269
  - VPCs (virtual private clouds), 621
  - VPNs. *See* Virtual private networks (VPNs)
  - vSwitches, 599–600
  - VTP (VLAN Trunking Protocol), 138–139
  - VXML (Voice Extensible Markup Language), 754
- ## W
- WANs (wide area networks), 9–10
    - routing and internetworking. *See* Internet routing policies
    - wireless. *See* Wireless networks
  - WAPs (wireless access points), 47–48, 98, 139–140
  - Wavelength-conversion, 561–562
  - Wavelength-conversion gain, 569
  - Wavelength-division multiplexing (WDM), 555
  - Wavelength in optical networks, 547
    - allocation, 567–569
    - conversion, 558, 560–563
  - Wavelength routers, 560
  - Wavelength routing nodes, 560–563
  - Wavelength routing vs. broadcasting, 564
  - WDM (wavelength-division multiplexing), 555
  - Web, 335–336
    - HTTP, 336–341
    - Web caching, 341–342
    - Web page, 742
    - Web server, 755
    - Web site, 742
    - Webmail, 342
  - Weighted-fair queuing (WFQ), 502, 508–511
  - Weighted round-robin (WRR) scheduler, 509
  - WEP (wired equivalent privacy) standard, 390–391
  - WG (wireless routers with gateway), 49
  - Wide area networks (WANs), 9–10
    - routing and internetworking. *See* Internet routing policies
    - wireless. *See* Wireless networks
  - Wide-sense nonblocking networks, 559
  - Wiener random processes, 834

- WiFi (wireless fidelity) technology, 149-151
    - in distributed media mini-clouds, 753
    - network examples, 158, 278, 622-623
    - in peer-to-peer (P2P) applications, 348
  - WiMAX (worldwide interoperability for micro-wave access) technology, 267-268
  - Window-based resource allocation, 500
  - Window scale option, 301
  - Window size field, 300, 305-306
  - Window size in TCP, 300, 305-306, 310
  - Wired equivalent privacy (WEP) standard, 390-391
  - Wireless access, 97-99
    - CDMA, 100-104
    - FDMA, 99
    - miscellaneous methods, 104-105
    - OFDM, 99-100
    - random-access techniques, 105-106
    - SC-FDMA, 100
    - TDMA, 99
  - Wireless access points (WAPs), 47-48, 98, 139-140
  - Wireless fidelity (WiFi) technology, 149-151
    - in distributed media mini-clouds, 753
    - network examples, 158, 278, 622-623
    - in peer-to-peer (P2P) applications, 348
  - Wireless links, 47
    - channels for, 280-285
    - flat fading in, 284
    - intersymbol interference in, 284-285
    - overview, 74-75
  - Wireless mesh networks (WMNs), 245, 277-280
  - Wireless networks, 10, 243-244
    - ad-hoc. *See* Mobile ad-hoc networks (MANETs)
    - cellular. *See* Cellular networks
    - IEEE 802.11, 142-151
    - infrastructure of, 244-245
    - LANs, 139-141
    - LTE, 268-277
    - mobile IP. *See* Mobile IP
    - security in, 390-391
    - sensor. *See* Sensor networks
    - WiFi, 149-151
    - WMNs, 245, 277-280
  - Wireless routers with gateway (WG), 49
  - Wireless Routing Protocol (WRP), 772-773
  - Wireless switching and routing devices, 47
    - antennas, 48-49
    - routers and switches, 48-49
    - WAPs and base stations, 47-48
  - Withdrawn Routes field, 190
  - WLANs (wireless LANs), 49
  - WMNs (wireless mesh networks), 245, 277-280
  - World Wide Web (WWW), 335-336
    - HTTP, 336-341
    - Web caching, 341-342
    - Web page, 742
    - Web server, 755
    - Web site, 742
    - Webmail, 342
  - Worldwide interoperability for microwave access (WiMAX) technology, 267-268
  - WRP (Wireless Routing Protocol), 772-773
  - WRR (weighted round-robin) scheduler, 509
  - WWW (World Wide Web), 335-336
    - HTTP, 336-341
    - Web caching, 341-342
    - Webmail, 342
- X-Z**
- Xcast (explicit multi-unicast) protocol, 595
  - ZigBee technology, 811-812