

CONTENTS

PREFACE

xix

1 INTRODUCTION

1

- 1.1 USES OF COMPUTER NETWORKS 1
 - 1.1.1 Access to Information 2
 - 1.1.2 Person-to-Person Communication 5
 - 1.1.3 Electronic Commerce 6
 - 1.1.4 Entertainment 6
 - 1.1.5 The Internet of Things 7
- 1.2 TYPES OF COMPUTER NETWORKS 7
 - 1.2.1 Broadband Access Networks 8
 - 1.2.2 Mobile and Wireless Access Networks 8
 - 1.2.3 Content Provider Networks 11
 - 1.2.4 Transit Networks 12
 - 1.2.5 Enterprise Networks 13
- 1.3 NETWORK TECHNOLOGY, FROM LOCAL TO GLOBAL 15
 - 1.3.1 Personal Area Networks 15
 - 1.3.2 Local Area Networks 16
 - 1.3.3 Home Networks 18
 - 1.3.4 Metropolitan Area Networks 20
 - 1.3.5 Wide Area Networks 21
 - 1.3.6 Internetworks 25

- 1.4 EXAMPLES OF NETWORKS 26
 - 1.4.1 The Internet 26
 - 1.4.2 Mobile Networks 36
 - 1.4.3 Wireless Networks (WiFi) 43

- 1.5 NETWORK PROTOCOLS 47
 - 1.5.1 Design Goals 47
 - 1.5.2 Protocol Layering 49
 - 1.5.3 Connections and Reliability 53
 - 1.5.4 Service Primitives 56
 - 1.5.5 The Relationship of Services to Protocols 58

- 1.6 REFERENCE MODELS 59
 - 1.6.1 The OSI Reference Model 59
 - 1.6.2 The TCP/IP Reference Model 61
 - 1.6.3 A Critique of the OSI Model and Protocols 64
 - 1.6.4 A Critique of the TCP/IP Reference Model and Protocols 66
 - 1.6.5 The Model Used in This Book 67

- 1.7 STANDARDIZATION 68
 - 1.7.1 Standardization and Open Source 68
 - 1.7.2 Who's Who in the Telecommunications World 69
 - 1.7.3 Who's Who in the International Standards World 71
 - 1.7.4 Who's Who in the Internet Standards World 72

- 1.8 POLICY, LEGAL, AND SOCIAL ISSUES 75
 - 1.8.1 Online Speech 75
 - 1.8.2 Net Neutrality 76
 - 1.8.3 Security 77
 - 1.8.4 Privacy 78
 - 1.8.5 Disinformation 79

- 1.9 METRIC UNITS 80

- 1.10 OUTLINE OF THE REST OF THE BOOK 81

- 1.11 SUMMARY 82

2 THE PHYSICAL LAYER**89**

- 2.1 GUIDED TRANSMISSION MEDIA 90
 - 2.1.1 Persistent Storage 90
 - 2.1.2 Twisted Pairs 91
 - 2.1.3 Coaxial Cable 93
 - 2.1.4 Power Lines 94
 - 2.1.5 Fiber Optics 95
- 2.2 WIRELESS TRANSMISSION 100
 - 2.2.1 The Electromagnetic Spectrum 101
 - 2.2.2 Frequency Hopping Spread Spectrum 103
 - 2.2.3 Direct Sequence Spread Spectrum 103
 - 2.2.4 Ultra-Wideband Communication 104
- 2.3 USING THE SPECTRUM FOR TRANSMISSION 104
 - 2.3.1 Radio Transmission 104
 - 2.3.2 Microwave Transmission 106
 - 2.3.3 Infrared Transmission 107
 - 2.3.4 Light Transmission 108
- 2.4 FROM WAVEFORMS TO BITS 109
 - 2.4.1 The Theoretical Basis for Data Communication 110
 - 2.4.2 The Maximum Data Rate of a Channel 114
 - 2.4.3 Digital Modulation 115
 - 2.4.4 Multiplexing 123
- 2.5 THE PUBLIC SWITCHED TELEPHONE NETWORK 131
 - 2.5.1 Structure of the Telephone System 131
 - 2.5.2 The Local Loop: Telephone Modems, ADSL, and Fiber 134
 - 2.5.3 Trunks and Multiplexing 143
 - 2.5.4 Switching 149
- 2.6 CELLULAR NETWORKS 154
 - 2.6.1 Common Concepts: Cells, Handoff, Paging 155
 - 2.6.2 First-Generation (1G) Technology: Analog Voice 156
 - 2.6.3 Second-Generation (2G) Technology: Digital Voice 158
 - 2.6.4 GSM: The Global System for Mobile Communications 159
 - 2.6.5 Third-Generation (3G) Technology: Digital Voice and Data 162
 - 2.6.6 Fourth-Generation (4G) Technology: Packet Switching 166
 - 2.6.7 Fifth-Generation (5G) Technology 168

- 2.7 CABLE NETWORKS 169
 - 2.7.1 A History of Cable Networks: Community Antenna Television 170
 - 2.7.2 Broadband Internet Access Over Cable: HFC Networks 170
 - 2.7.3 DOCSIS 173
 - 2.7.4 Resource Sharing in DOCSIS Networks: Nodes and Minislots 174
- 2.8 COMMUNICATION SATELLITES 176
 - 2.8.1 Geostationary Satellites 177
 - 2.8.2 Medium-Earth Orbit Satellites 181
 - 2.8.3 Low-Earth Orbit Satellites 181
- 2.9 COMPARING DIFFERENT ACCESS NETWORKS 184
 - 2.9.1 Terrestrial Access Networks: Cable, Fiber, and ADSL 184
 - 2.9.2 Satellites Versus Terrestrial Networks 186
- 2.10 POLICY AT THE PHYSICAL LAYER 187
 - 2.10.1 Spectrum Allocation 187
 - 2.10.2 The Cellular Network 190
 - 2.10.3 The Telephone Network 192
- 2.11 SUMMARY 194

3 THE DATA LINK LAYER 201

- 3.1 DATA LINK LAYER DESIGN ISSUES 202
 - 3.1.1 Services Provided to the Network Layer 203
 - 3.1.2 Framing 205
 - 3.1.3 Error Control 208
 - 3.1.4 Flow Control 209
- 3.2 ERROR DETECTION AND CORRECTION 210
 - 3.2.1 Error-Correcting Codes 212
 - 3.2.2 Error-Detecting Codes 217
- 3.3 ELEMENTARY DATA LINK PROTOCOLS 223
 - 3.3.1 Initial Simplifying Assumptions 223
 - 3.3.2 Basic Transmission and Receipt 224
 - 3.3.3 Simplex Link-Layer Protocols 228

- 3.4 IMPROVING EFFICIENCY 234
 - 3.4.1 Goal: Bidirectional Transmission, Multiple Frames in Flight 234
 - 3.4.2 Examples of Full-Duplex, Sliding Window Protocols 238
- 3.5 DATA LINK PROTOCOLS IN PRACTICE 252
 - 3.5.1 Packet over SONET 253
 - 3.5.2 ADSL (Asymmetric Digital Subscriber Loop) 256
 - 3.5.3 Data Over Cable Service Interface Specification (DOCSIS) 259
- 3.6 SUMMARY 261

4 THE MEDIUM ACCESS CONTROL SUBLAYER 267

- 4.1 THE CHANNEL ALLOCATION PROBLEM 268
 - 4.1.1 Static Channel Allocation 268
 - 4.1.2 Assumptions for Dynamic Channel Allocation 270
- 4.2 MULTIPLE ACCESS PROTOCOLS 271
 - 4.2.1 ALOHA 272
 - 4.2.2 Carrier Sense Multiple Access Protocols 276
 - 4.2.3 Collision-Free Protocols 279
 - 4.2.4 Limited-Contention Protocols 283
 - 4.2.5 Wireless LAN Protocols 287
- 4.3 ETHERNET 290
 - 4.3.1 Classic Ethernet Physical Layer 290
 - 4.3.2 Classic Ethernet MAC Sublayer Protocol 292
 - 4.3.3 Ethernet Performance 296
 - 4.3.4 Switched Ethernet 297
 - 4.3.5 Fast Ethernet 300
 - 4.3.6 Gigabit Ethernet 302
 - 4.3.7 10-Gigabit Ethernet 306
 - 4.3.8 40- and 100-Gigabit Ethernet 307
 - 4.3.9 Retrospective on Ethernet 308
- 4.4 WIRELESS LANS 309
 - 4.4.1 The 802.11 Architecture and Protocol Stack 310
 - 4.4.2 The 802.11 Physical Layer 311

- 4.4.3 The 802.11 MAC Sublayer Protocol 314
- 4.4.4 The 802.11 Frame Structure 321
- 4.4.5 Services 322
- 4.5 BLUETOOTH 324
 - 4.5.1 Bluetooth Architecture 325
 - 4.5.2 Bluetooth Applications 326
 - 4.5.3 The Bluetooth Protocol Stack 327
 - 4.5.4 The Bluetooth Radio Layer 328
 - 4.5.5 The Bluetooth Link Layers 329
 - 4.5.6 The Bluetooth Frame Structure 330
 - 4.5.7 Bluetooth 5 331
- 4.6 DOCSIS 332
 - 4.6.1 Overview 332
 - 4.6.2 Ranging 333
 - 4.6.3 Channel Bandwidth Allocation 333
- 4.7 DATA LINK LAYER SWITCHING 334
 - 4.7.1 Uses of Bridges 335
 - 4.7.2 Learning Bridges 336
 - 4.7.3 Spanning-Tree Bridges 339
 - 4.7.4 Repeaters, Hubs, Bridges, Switches, Routers, and Gateways 342
 - 4.7.5 Virtual LANs 345
- 4.8 SUMMARY 351

5 THE NETWORK LAYER 359

- 5.1 NETWORK LAYER DESIGN ISSUES 360
 - 5.1.1 Store-and-Forward Packet Switching 360
 - 5.1.2 Services Provided to the Transport Layer 361
 - 5.1.3 Implementation of Connectionless Service 362
 - 5.1.4 Implementation of Connection-Oriented Service 363
 - 5.1.5 Comparison of Virtual-Circuit and Datagram Networks 365
- 5.2 ROUTING ALGORITHMS IN A SINGLE NETWORK 366
 - 5.2.1 The Optimality Principle 368
 - 5.2.2 Shortest Path Algorithm 370

- 5.2.3 Flooding 372
- 5.2.4 Distance Vector Routing 374
- 5.2.5 Link State Routing 377
- 5.2.6 Hierarchical Routing within a Network 382
- 5.2.7 Broadcast Routing 384
- 5.2.8 Multicast Routing 386
- 5.2.9 Anycast Routing 389
- 5.3 TRAFFIC MANAGEMENT AT THE NETWORK LAYER 390
 - 5.3.1 The Need for Traffic Management: Congestion 390
 - 5.3.2 Approaches to Traffic Management 393
- 5.4 QUALITY OF SERVICE AND APPLICATION QOE 406
 - 5.4.1 Application QoS Requirements 406
 - 5.4.2 Overprovisioning 409
 - 5.4.3 Packet Scheduling 410
 - 5.4.4 Integrated Services 417
 - 5.4.5 Differentiated Services 420
- 5.5 INTERNETWORKING 423
 - 5.5.1 Internetworks: An Overview 423
 - 5.5.2 How Networks Differ 424
 - 5.5.3 Connecting Heterogeneous Networks 425
 - 5.5.4 Connecting Endpoints Across Heterogeneous Networks 428
 - 5.5.5 Internetwork Routing: Routing Across Multiple Networks 430
 - 5.5.6 Supporting Different Packet Sizes: Packet Fragmentation 431
- 5.6 SOFTWARE-DEFINED NETWORKING 435
 - 5.6.1 Overview 435
 - 5.6.2 The SDN Control Plane: Logically Centralized Software Control 436
 - 5.6.3 The SDN Data Plane: Programmable Hardware 438
 - 5.6.4 Programmable Network Telemetry 440
- 5.7 THE NETWORK LAYER IN THE INTERNET 441
 - 5.7.1 The IP Version 4 Protocol 444
 - 5.7.2 IP Addresses 448
 - 5.7.3 IP Version 6 461
 - 5.7.4 Internet Control Protocols 470
 - 5.7.5 Label Switching and MPLS 476
 - 5.7.6 OSPF—An Interior Gateway Routing Protocol 479
 - 5.7.7 BGP—The Exterior Gateway Routing Protocol 484
 - 5.7.8 Internet Multicasting 491

- 5.8 POLICY AT THE NETWORK LAYER 492
 - 5.8.1 Peering Disputes 492
 - 5.8.2 Traffic Prioritization 493

- 5.9 SUMMARY 494

6 THE TRANSPORT LAYER 501

- 6.1 THE TRANSPORT SERVICE 501
 - 6.1.1 Services Provided to the Upper Layers 502
 - 6.1.2 Transport Service Primitives 504
 - 6.1.3 Berkeley Sockets 506
 - 6.1.4 An Example of Socket Programming: An Internet File Server 509
- 6.2 ELEMENTS OF TRANSPORT PROTOCOLS 513
 - 6.2.1 Addressing 514
 - 6.2.2 Connection Establishment 517
 - 6.2.3 Connection Release 523
 - 6.2.4 Error Control and Flow Control 528
 - 6.2.5 Multiplexing 533
 - 6.2.6 Crash Recovery 533
- 6.3 CONGESTION CONTROL 536
 - 6.3.1 Desirable Bandwidth Allocation 536
 - 6.3.2 Regulating the Sending Rate 540
 - 6.3.3 Wireless Issues 544
- 6.4 THE INTERNET TRANSPORT PROTOCOLS: UDP 546
 - 6.4.1 Introduction to UDP 547
 - 6.4.2 Remote Procedure Call 549
 - 6.4.3 Real-Time Transport Protocols 552
- 6.5 THE INTERNET TRANSPORT PROTOCOLS: TCP 557
 - 6.5.1 Introduction to TCP 558
 - 6.5.2 The TCP Service Model 558
 - 6.5.3 The TCP Protocol 561
 - 6.5.4 The TCP Segment Header 562
 - 6.5.5 TCP Connection Establishment 565
 - 6.5.6 TCP Connection Release 567

- 6.5.7 TCP Connection Management Modeling 567
- 6.5.8 TCP Sliding Window 570
- 6.5.9 TCP Timer Management 573
- 6.5.10 TCP Congestion Control 576
- 6.5.11 TCP CUBIC 586
- 6.6 TRANSPORT PROTOCOLS AND CONGESTION CONTROL 587
 - 6.6.1 QUIC: Quick UDP Internet Connections 587
 - 6.6.2 BBR: Congestion Control Based on Bottleneck Bandwidth 588
 - 6.6.3 The Future of TCP 590
- 6.7 PERFORMANCE ISSUES 590
 - 6.7.1 Performance Problems in Computer Networks 591
 - 6.7.2 Network Performance Measurement 592
 - 6.7.3 Measuring Access Network Throughput 593
 - 6.7.4 Measuring Quality of Experience 594
 - 6.7.5 Host Design for Fast Networks 595
 - 6.7.6 Fast Segment Processing 598
 - 6.7.7 Header Compression 601
 - 6.7.8 Protocols for Long Fat Networks 603
- 6.8 SUMMARY 607

7 THE APPLICATION LAYER

613

- 7.1 THE DOMAIN NAME SYSTEM (DNS) 613
 - 7.1.1 History and Overview 614
 - 7.1.2 The DNS Lookup Process 614
 - 7.1.3 The DNS Name Space and Hierarchy 617
 - 7.1.4 DNS Queries and Responses 620
 - 7.1.5 Name Resolution 627
 - 7.1.6 Hands on with DNS 629
 - 7.1.7 DNS Privacy 629
 - 7.1.8 Contention Over Names 631
- 7.2 ELECTRONIC MAIL 632
 - 7.2.1 Architecture and Services 633
 - 7.2.2 The User Agent 635
 - 7.2.3 Message Formats 637

- 7.2.4 Message Transfer 642
- 7.2.5 Final Delivery 647
- 7.3 THE WORLD WIDE WEB 650
 - 7.3.1 Architectural Overview 651
 - 7.3.2 Static Web Objects 659
 - 7.3.3 Dynamic Web Pages and Web Applications 660
 - 7.3.4 HTTP and HTTPS 664
 - 7.3.5 Web Privacy 676
- 7.4 STREAMING AUDIO AND VIDEO 680
 - 7.4.1 Digital Audio 682
 - 7.4.2 Digital Video 684
 - 7.4.3 Streaming Stored Media 687
 - 7.4.4 Real-Time Streaming 694
- 7.5 CONTENT DELIVERY 703
 - 7.5.1 Content and Internet Traffic 705
 - 7.5.2 Server Farms and Web Proxies 707
 - 7.5.3 Content Delivery Networks 711
 - 7.5.4 Peer-to-Peer Networks 715
 - 7.5.5 Evolution of the Internet 721
- 7.6 SUMMARY 725

8 NETWORK SECURITY

731

- 8.1 FUNDAMENTALS OF NETWORK SECURITY 733
 - 8.1.1 Fundamental Security Principles 734
 - 8.1.2 Fundamental Attack Principles 736
 - 8.1.3 From Threats to Solutions 738
- 8.2 THE CORE INGREDIENTS OF AN ATTACK 739
 - 8.2.1 Reconnaissance 739
 - 8.2.2 Sniffing and Snooping (with a Dash of Spoofing) 742
 - 8.2.3 Spoofing (beyond ARP) 744
 - 8.2.4 Disruption 755

- 8.3 FIREWALLS AND INTRUSION DETECTION SYSTEMS 759
 - 8.3.1 Firewalls 760
 - 8.3.2 Intrusion Detection and Prevention 762

- 8.4 CRYPTOGRAPHY 766
 - 8.4.1 Introduction to Cryptography 767
 - 8.4.2 Two Fundamental Cryptographic Principles 769
 - 8.4.3 Substitution Ciphers 771
 - 8.4.4 Transposition Ciphers 773
 - 8.4.5 One-Time Pads 774

- 8.5 SYMMETRIC-KEY ALGORITHMS 779
 - 8.5.1 The Data Encryption Standard 780
 - 8.5.2 The Advanced Encryption Standard 781
 - 8.5.3 Cipher Modes 783

- 8.6 PUBLIC-KEY ALGORITHMS 787
 - 8.6.1 RSA 788
 - 8.6.2 Other Public-Key Algorithms 790

- 8.7 DIGITAL SIGNATURES 791
 - 8.7.1 Symmetric-Key Signatures 791
 - 8.7.2 Public-Key Signatures 793
 - 8.7.3 Message Digests 795
 - 8.7.4 The Birthday Attack 797

- 8.8 MANAGEMENT OF PUBLIC KEYS 799
 - 8.8.1 Certificates 799
 - 8.8.2 X.509 801
 - 8.8.3 Public Key Infrastructures 802

- 8.9 AUTHENTICATION PROTOCOLS 805
 - 8.9.1 Authentication Based on a Shared Secret Key 806
 - 8.9.2 Establishing a Shared Key: The Diffie-Hellman Key Exchange 811
 - 8.9.3 Authentication Using a Key Distribution Center 813
 - 8.9.4 Authentication Using Kerberos 816
 - 8.9.5 Authentication Using Public-Key Cryptography 819

- 8.10 COMMUNICATION SECURITY 819
 - 8.10.1 IPsec 820
 - 8.10.2 Virtual Private Networks 824
 - 8.10.3 Wireless Security 825

- 8.11 EMAIL SECURITY 829
 - 8.11.1 Pretty Good Privacy 829
 - 8.11.2 S/MIME 833
- 8.12 WEB SECURITY 834
 - 8.12.1 Threats 834
 - 8.12.2 Secure Naming and DNSSEC 835
 - 8.12.3 Transport Layer Security 838
 - 8.12.4 Running Untrusted Code 842
- 8.13 SOCIAL ISSUES 844
 - 8.13.1 Confidential and Anonymous Communication 844
 - 8.13.2 Freedom of Speech 847
 - 8.13.3 Copyright 851
- 8.14 SUMMARY 854

9 READING LIST AND BIBLIOGRAPHY 863

- 9.1 SUGGESTIONS FOR FURTHER READING 863
 - 9.1.1 Introduction and General Works 864
 - 9.1.2 The Physical Layer 865
 - 9.1.3 The Data Link Layer 866
 - 9.1.4 The Medium Access Control Sublayer 867
 - 9.1.5 The Network Layer 868
 - 9.1.6 The Transport Layer 869
 - 9.1.7 The Application Layer 870
 - 9.1.8 Network Security 871

- 9.2 ALPHABETICAL BIBLIOGRAPHY 872

INDEX 891