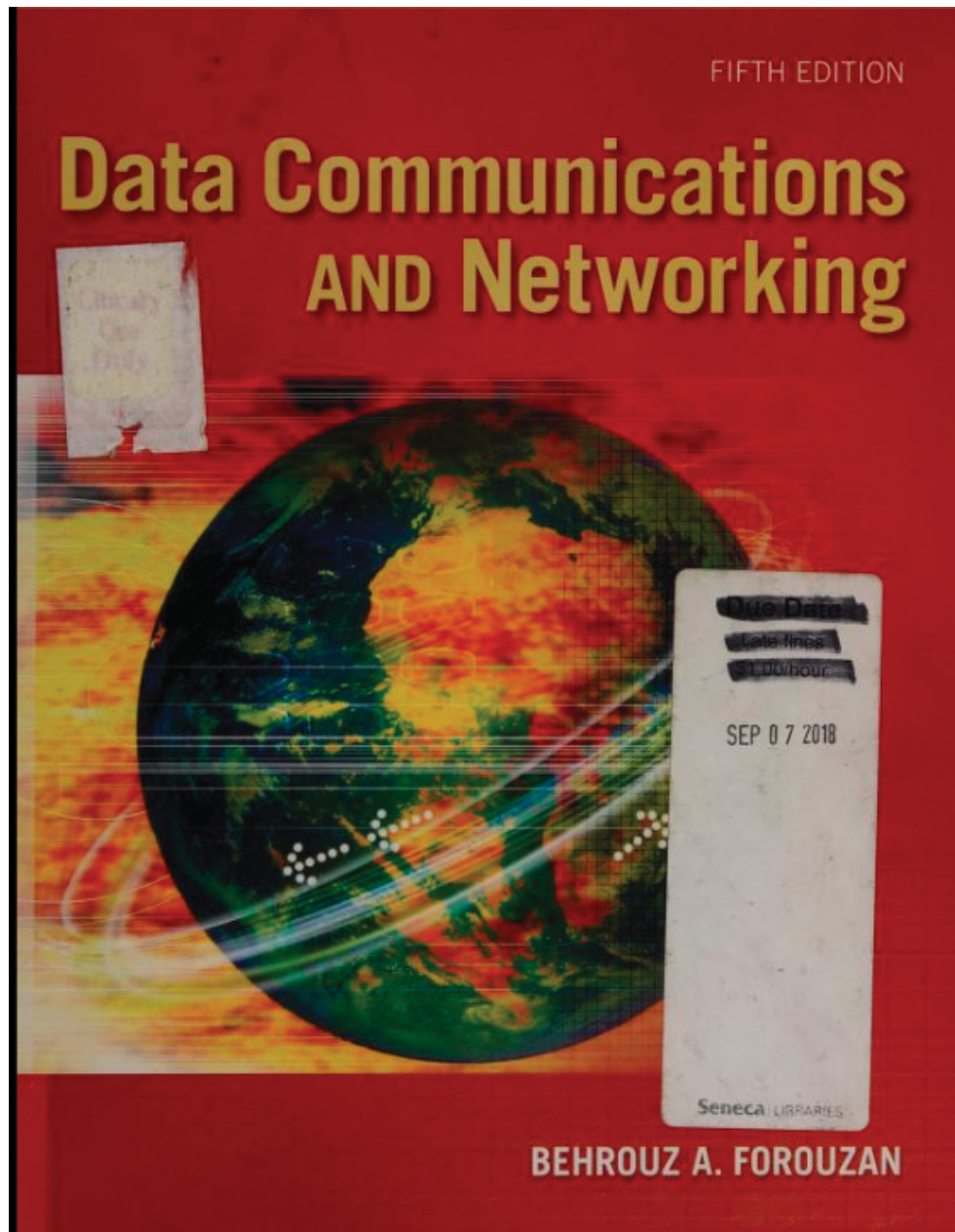




ACRONYMS

2B1Q	two-binary, one-quaternary	BER	Basic Encoding Rules
4B/5B	four binary, five binary	BGP	Border Gateway Protocol
4D-PAM5	4-dimensional, 5-level pulse amplitude modulation	BNC	Bayone-Neill-Concelman
8B/10B	eight binary, ten binary	BOOTP	Bootstrap Protocol
8B6T	eight binary, six ternary	BRI	basic rate interface
AAL	(ATM) application adaptation layer	BSS	basic service set
AAS	adaptive antenna system	CA	Certification Authority
ABM	asynchronous balanced mode	CATV	community antenna TV
ABR	available bit rate	CBC	cipher-block chaining
ACK	acknowledgment	CBR	constant bit rate
ACL	asynchronous connectionless link	CBT	Core-Based Tree
ADM	adaptive DM	CCITT	Consultative Committee for International Telegraphy and Telephony
ADPCM	adaptive DPCM	CCK	complementary code keying
ADSL	asymmetric digital subscriber line	CDMA	code division multiple access
AES	Advanced Encryption Standard	CDPD	cellular digital packet data
AH	authentication header	CDV	cell delay variation
AIMD	additive increase, multiplicative decrease	CEPT	Comité Européen de Post et Telegraphie
AM	amplitude modulation	CGI	common gateway interface
AMI	alternate mark inversion	CHAP	Challenge Handshake Authentication Protocol
AMPS	Advanced Mobile Phone System	CIDR	Classless Interdomain Routing
ANSI	American National Standards Institute	CIR	committed information rate
ANSNET	Advanced Networks and Services Network	CLP	cell loss priority
AP	access point	CLR	cell loss ratio
API	application programming interface	CMS	Cryptographic Message Syntax
APS	automatic protection switching	CMTS	cable modem transmission system
ARP	Address Resolution Protocol	CPE	customer premises equipment
ARPA	Advanced Research Projects Agency	CRC	cyclic redundancy check
ARPANET	Advanced Research Projects Agency Network	CS	convergence sublayer
ARQ	automatic repeat request	CSM	cipher stream mode
AS	authentication server	CSMA	carrier sense multiple access
AS	autonomous system	CSMA/CA	carrier sense multiple access with collision avoidance
ASCII	American Standard Code for Information Interchange	CSMA/CD	carrier sense multiple access with collision detection
ASK	amplitude shift keying	CSNET	Computer Science Network
ASN.1	Abstract Syntax Notation One	CSRC	contributing source
ATM	Asynchronous Transfer Mode	CSS	Cascading Style Sheets
AUI	attachment unit interface	CTS	clear to send
B-frame	bidirectional frame	D-AMPS	digital AMPS
B8ZS	bipolar with 8-zero substitution	DARPA	Defense Advanced Research Projects Agency
BASK	binary amplitude shift keying	dB	decibel
Bc	committed burst size	DC	direct current
BECN	backward explicit congestion notification	DCF	distributed coordination function
		DCT	discrete cosine transform
		DDNS	Dynamic Domain Name System

DDS	digital data service	HDLC	High-level Data Link Control
DE	discard eligibility	HDSL	high bit rate digital subscriber line
DEMUX	demultiplexer	HEC	header error check
DES	Data Encryption Standard	HFC	hybrid-fiber-coaxial
DHCP	Dynamic Host Configuration Protocol	HMAC	hashed MAC (hashed message authentication code)
DHT	distributed hash table	HR-DSSS	high-rate direct-sequence spread spectrum
DiffServ	Differentiated Services	HTML	HyperText Markup Language
DIFS	distributed interframe space	HTTP	HyperText Transfer Protocol
DISC	disconnect	Hz	hertz
DMT	discrete multitone technique	I-frame	inter-coded frame
DNS	Domain Name System	IAB	Internet Architecture Board
DOCSIS	Data Over Cable System Interface Specification	IANA	Internet Assigned Numbers Authority
DPCM	differential PCM	iBGP	internal BGP
DS-<i>n</i>	digital signal- <i>n</i>	ICANN	Internet Corporation for Assigned Names and Numbers
DSL	digital subscriber line	ICMP	Internet Control Message Protocol
DSLAM	digital subscriber line access multiplexer	IEEE	Institute of Electrical and Electronics Engineers
DSS	Digital Signature Standard	IESG	Internet Engineering Steering Group
DSSS	direct sequence spread spectrum	IETF	Internet Engineering Task Force
DTE	data terminal equipment	IFDMA	interleaved FDMA
DVMRP	Distance Vector Multicast Routing Protocol	IFS	interframe space
DWDM	dense wave-division multiplexing	IGMP	Internet Group Management Protocol
EBCDIC	extended binary coded decimal interchange code	IGP	Interior Gateway Protocol
eBGP	external BGP	IKE	Internet Key Exchange
ECB	electronic codebook	ILEC	incumbent local exchange carrier
EGP	Exterior Gateway Protocol	IMAP	Internet Mail Access Protocol
EIA	Electronic Industries Alliance	INTERNIC	Internet Network Information Center
ENQ	enquiry frame	IntServ	Integrated Services
ESP	Encapsulating Security Payload	IP	Internet Protocol
ESS	extended service set	IPCP	Internetwork Protocol Control Protocol
FA	foreign agent	IPng	Internet Protocol, next generation
FCC	Federal Communications Commission	IPSec	IP Security
FCS	frame check sequence	IPv4	Internet Protocol, version 4
FDD	frequency division duplex	IPv6	Internet Protocol, version 6
FDDI	Fiber Distributed Data Interface	IRTF	Internet Research Task Force
FDM	frequency division multiplexing	IS-95	Interim Standard 95
FDMA	frequency division multiple access	ISAKMP	Internet Security Association and Key Management Protocol
FEC	forward error correction	ISDN	Integrated Services Digital Network
FHSS	frequency-hopping spread spectrum	ISN	initial sequence number
FIFO	first-in, first-out	ISO	International Organization for Standardization
FM	frequency modulation	ISOC	Internet Society
FRMR	frame reject	ISP	Internet service provider
FQDN	fully qualified domain name	ITM-2000	Internet Mobile Communication 2000
FSK	frequency shift keying	ITU	International Telecommunications Union
FTP	File Transfer Protocol	ITU-T	ITU, Telecommunication Standardization Sector
GEO	geostationary Earth orbit	IV	initial vector
GIF	graphical interchange format		
GPS	Global Positioning System		
GSM	Global System for Mobile Communication		
HA	home agent		

(Continued on back end sheets)



Data Communications and Networking

Belongs A Forevers

McGraw-Hill Forouzan Networking Series

Titles by Behrouz A. Forouzan:

Data Communications and Networking

TCP/IP Protocol Suite

Computer Networks: A Top-Down Approach

Cryptography and Network Security

Data Communications and Networking

FIFTH EDITION

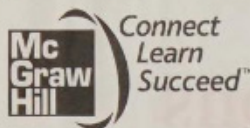
Behrouz A. Forouzan

PROPERTY OF
SENECA COLLEGE
LIBRARIES
@ YORK CAMPUS

WITHDRAWN

PROPERTY OF
SENECA COLLEGE
LIBRARIES
NEWNHAM CAMPUS





DATA COMMUNICATIONS AND NETWORKING, FIFTH EDITION

Published by McGraw-Hill, a business unit of The McGraw-Hill Companies, Inc., 1221 Avenue of the Americas, New York, NY 10020. Copyright © 2013 by The McGraw-Hill Companies, Inc. All rights reserved. Printed in the United States of America. Previous editions © 2007 and 2004. No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written consent of The McGraw-Hill Companies, Inc., including, but not limited to, in any network or other electronic storage or transmission, or broadcast for distance learning.

Some ancillaries, including electronic and print components, may not be available to customers outside the United States.

This book is printed on acid-free paper.

1 2 3 4 5 6 7 8 9 0 DOC/DOC 1 0 9 8 7 6 5 4 3 2

ISBN 978-0-07-337622-6

MHID 0-07-337622-1

Vice President & Editor-in-Chief: *Marty Lange*

Vice President of Specialized Publishing: *Janice M. Roerig-Blong*

Editorial Director: *Michael Lange*

Global Publisher: *Raghothaman Srinivasan*

Senior Marketing Manager: *Curt Reynolds*

Lead Project Manager: *Jane Mohr*

Design Coordinator: *Brenda A. Rolwes*

Cover Designer: *Studio Montage, St. Louis, Missouri*

Cover Image: © *Digital Vision/Getty Images RF*

Buyer: *Kara Kudronowicz*

Media Project Manager: *Prashanthi Nadipalli*

Compositor: *MPS Limited, a Macmillan Company*

Typeface: *10/12 Times Roman*

Printer: *R. R. Donnelley*

All credits appearing on page or at the end of the book are considered to be an extension of the copyright page.

Library of Congress Cataloging-in-Publication Data

Forouzan, Behrouz A.

Data communications and networking / Behrouz A. Forouzan. — 5th ed.
p. cm.

ISBN 978-0-07-337622-6 (alk. paper)

1. Data transmission systems. 2. Computer networks. I. Title.
TK5105.F6617 2012
004.6—dc23

2011047732

www.mhhe.com

WRITE CONTENT

Prologue, xiii

Track Mark, xxi

PART I Overview, 1

Chapter 1 Introduction, 3

Chapter 2 Network Fundamentals, 5

PART II *To my beloved grandson, William.*

Chapter 3 Introduction to the OSI Model, 7

Chapter 4 Data Link Layer, 23

Chapter 5 Network Layer, 35

Chapter 6 Transport Layer, 47

Chapter 7 Session Layer, 59

Chapter 8 Presentation Layer, 61

Chapter 9 Application Layer, 63

PART III Data Link Layer, 23

Chapter 9 Introduction to the Data Link Layer, 23

Chapter 10 Data Link Layer Fundamentals, 25

Chapter 11 Data Link Layer Fundamentals, 27

Chapter 12 Data Link Layer Fundamentals, 29

Chapter 13 Data Link Layer Fundamentals, 31

Chapter 14 Data Link Layer Fundamentals, 33

Chapter 15 Data Link Layer Fundamentals, 35

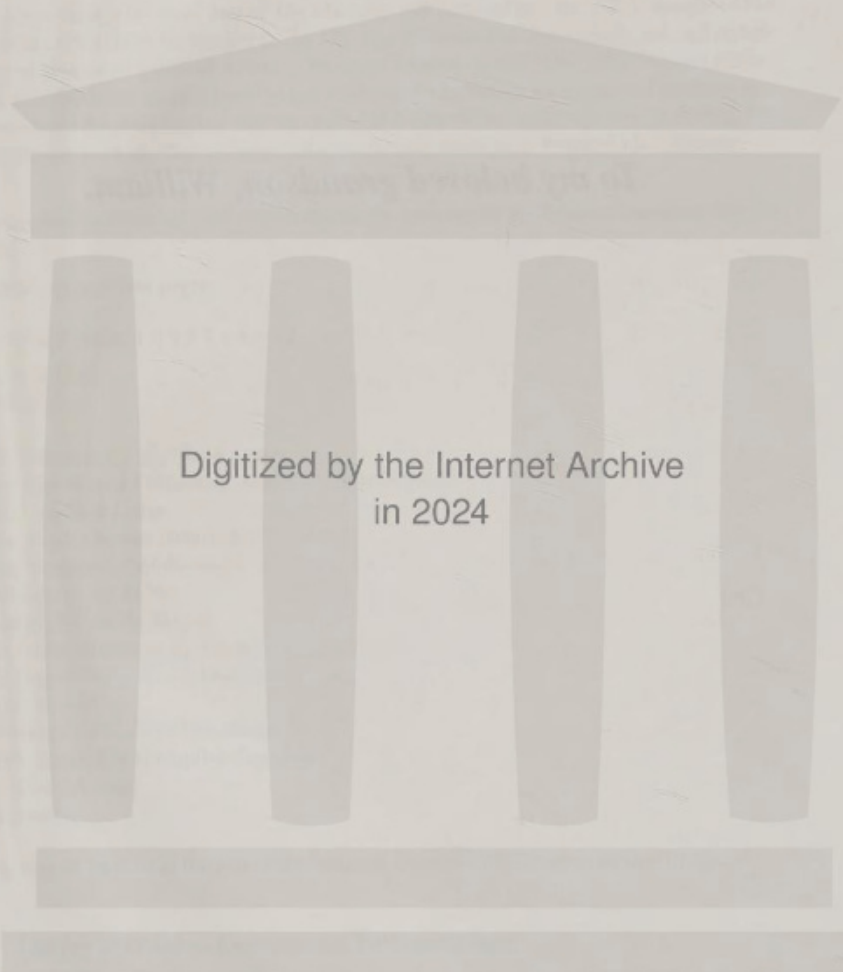
Chapter 16 Data Link Layer Fundamentals, 37

Chapter 17 Data Link Layer Fundamentals, 39

PART IV Network Layer, 35

Chapter 18 Network Layer Fundamentals, 35

Chapter 19 Network Layer Fundamentals, 37



Digitized by the Internet Archive
in 2024

https://archive.org/details/datacommunicatio0000foro_i8a0_5ed

BRIEF CONTENTS

Preface xxix

Trade Mark xxxviii

PART I: Overview 1

Chapter 1 *Introduction* 3

Chapter 2 *Network Models* 31

PART II: Physical Layer 51

Chapter 3 *Introduction to Physical Layer* 53

Chapter 4 *Digital Transmission* 95

Chapter 5 *Analog Transmission* 135

Chapter 6 *Bandwidth Utilization: Multiplexing and Spectrum Spreading* 155

Chapter 7 *Transmission Media* 185

Chapter 8 *Switching* 207

PART III: Data-Link Layer 235

Chapter 9 *Introduction to Data-Link Layer* 237

Chapter 10 *Error Detection and Correction* 257

Chapter 11 *Data Link Control (DLC)* 293

Chapter 12 *Media Access Control (MAC)* 325

Chapter 13 *Wired LANs: Ethernet* 361

Chapter 14 *Other Wired Networks* 387

Chapter 15 *Wireless LANs* 435

Chapter 16 *Other Wireless Networks* 465

Chapter 17 *Connecting Devices and Virtual LANs* 493

PART IV: Network Layer 509

Chapter 18 *Introduction to Network Layer* 511

Chapter 19 *Network-Layer Protocols* 561

Chapter 20 *Unicast Routing* 595

Chapter 21 *Multicast Routing* 639

Chapter 22 *Next Generation IP* 665

PART V: Transport Layer 689

Chapter 23 *Introduction to Transport Layer* 691

Chapter 24 *Transport-Layer Protocols* 735

PART VI: Application Layer 815

Chapter 25 *Introduction to Application Layer* 817

Chapter 26 *Standard Client-Server Protocols* 871

Chapter 27 *Network Management* 929

Chapter 28 *Multimedia* 961

Chapter 29 *Peer-to-Peer Paradigm* 1023

PART VII: Topics Related to All Layers 1051

Chapter 30 *Quality of Service* 1053

Chapter 31 *Cryptography and Network Security* 1077

Chapter 32 *Internet Security* 1123

Appendices A-H available online at
<http://www.mhhe.com/forouzan>

Appendices

Appendix A *Unicode*

Appendix B *Positional Numbering System*

Appendix C *HTML, CSS, XML, and XSL*

Appendix D *A Touch of Probability*

Appendix E *Mathematical Review*

Appendix F *8B/6T Code*

Appendix G *Miscellaneous Information*

Appendix H *Telephone History*

Glossary 1157

References 1193

Index 1199

CONTENTS

Preface xxix

Trade Mark xxxviii

PART I: Overview 1

Chapter 1 *Introduction* 3

- 1.1 DATA COMMUNICATIONS 4
 - 1.1.1 Components 4
 - 1.1.2 Data Representation 5
 - 1.1.3 Data Flow 6
- 1.2 NETWORKS 7
 - 1.2.1 Network Criteria 7
 - 1.2.2 Physical Structures 8
- 1.3 NETWORK TYPES 13
 - 1.3.1 Local Area Network 13
 - 1.3.2 Wide Area Network 14
 - 1.3.3 Switching 15
 - 1.3.4 The Internet 17
 - 1.3.5 Accessing the Internet 18
- 1.4 INTERNET HISTORY 19
 - 1.4.1 Early History 19
 - 1.4.2 Birth of the Internet 20
 - 1.4.3 Internet Today 22
- 1.5 STANDARDS AND ADMINISTRATION 22
 - 1.5.1 Internet Standards 22
 - 1.5.2 Internet Administration 24
- 1.6 END-CHAPTER MATERIALS 25
 - 1.6.1 Recommended Reading 25
 - 1.6.2 Key Terms 25
 - 1.6.3 Summary 26
- 1.7 PRACTICE SET 27
 - 1.7.1 Quizzes 27
 - 1.7.2 Questions 27
 - 1.7.3 Problems 28
- 1.8 SIMULATION EXPERIMENTS 28
 - 1.8.1 Applets 28
 - 1.8.2 Lab Assignments 28

Chapter 2 *Network Models* 31

- 2.1 PROTOCOL LAYERING 32
 - 2.1.1 Scenarios 32
 - 2.1.2 Principles of Protocol Layering 34
 - 2.1.3 Logical Connections 35

2.2	TCP/IP PROTOCOL SUITE	35
2.2.1	Layered Architecture	35
2.2.2	Layers in the TCP/IP Protocol Suite	37
2.2.3	Description of Each Layer	38
2.2.4	Encapsulation and Decapsulation	41
2.2.5	Addressing	42
2.2.6	Multiplexing and Demultiplexing	43
2.3	THE OSI MODEL	44
2.3.1	OSI versus TCP/IP	45
2.3.2	Lack of OSI Model's Success	45
2.4	END-CHAPTER MATERIALS	46
2.4.1	Recommended Reading	46
2.4.2	Key Terms	46
2.4.3	Summary	46
2.5	PRACTICE SET	47
2.5.1	Quizzes	47
2.5.2	Questions	47
2.5.3	Problems	48
PART II: Physical Layer		51
Chapter 3		<i>Introduction to Physical Layer</i>
3.1	DATA AND SIGNALS	54
3.1.1	Analog and Digital Data	55
3.1.2	Analog and Digital Signals	55
3.1.3	Periodic and Nonperiodic	56
3.2	PERIODIC ANALOG SIGNALS	56
3.2.1	Sine Wave	56
3.2.2	Phase	59
3.2.3	Wavelength	61
3.2.4	Time and Frequency Domains	61
3.2.5	Composite Signals	63
3.2.6	Bandwidth	65
3.3	DIGITAL SIGNALS	68
3.3.1	Bit Rate	69
3.3.2	Bit Length	69
3.3.3	Digital Signal as a Composite Analog Signal	70
3.3.4	Transmission of Digital Signals	70
3.4	TRANSMISSION IMPAIRMENT	76
3.4.1	Attenuation	77
3.4.2	Distortion	79
3.4.3	Noise	79
3.5	DATA RATE LIMITS	81
3.5.1	Noiseless Channel: Nyquist Bit Rate	81
3.5.2	Noisy Channel: Shannon Capacity	82
3.5.3	Using Both Limits	83

- 3.6 PERFORMANCE 84
 - 3.6.1 Bandwidth 84
 - 3.6.2 Throughput 85
 - 3.6.3 Latency (Delay) 85
 - 3.6.4 Bandwidth-Delay Product 87
 - 3.6.5 Jitter 88
- 3.7 END-CHAPTER MATERIALS 89
 - 3.7.1 Recommended Reading 89
 - 3.7.2 Key Terms 89
 - 3.7.3 Summary 89
- 3.8 PRACTICE SET 90
 - 3.8.1 Quizzes 90
 - 3.8.2 Questions 90
 - 3.8.3 Problems 91
- 3.9 SIMULATION EXPERIMENTS 94
 - 3.9.1 Applets 94

Chapter 4 *Digital Transmission* 95

- 4.1 DIGITAL-TO-DIGITAL CONVERSION 96
 - 4.1.1 Line Coding 96
 - 4.1.2 Line Coding Schemes 100
 - 4.1.3 Block Coding 109
 - 4.1.4 Scrambling 113
- 4.2 ANALOG-TO-DIGITAL CONVERSION 115
 - 4.2.1 Pulse Code Modulation (PCM) 115
 - 4.2.2 Delta Modulation (DM) 123
- 4.3 TRANSMISSION MODES 125
 - 4.3.1 Parallel Transmission 125
 - 4.3.2 Serial Transmission 126
- 4.4 END-CHAPTER MATERIALS 129
 - 4.4.1 Recommended Reading 129
 - 4.4.2 Key Terms 130
 - 4.4.3 Summary 130
- 4.5 PRACTICE SET 131
 - 4.5.1 Quizzes 131
 - 4.5.2 Questions 131
 - 4.5.3 Problems 131
- 4.6 SIMULATION EXPERIMENTS 134
 - 4.6.1 Applets 134

Chapter 5 *Analog Transmission* 135

- 5.1 DIGITAL-TO-ANALOG CONVERSION 136
 - 5.1.1 Aspects of Digital-to-Analog Conversion 137
 - 5.1.2 Amplitude Shift Keying 138
 - 5.1.3 Frequency Shift Keying 140
 - 5.1.4 Phase Shift Keying 142
 - 5.1.5 Quadrature Amplitude Modulation 146

5.2	ANALOG-TO-ANALOG CONVERSION	147
5.2.1	Amplitude Modulation (AM)	147
5.2.2	Frequency Modulation (FM)	148
5.2.3	Phase Modulation (PM)	149
5.3	END-CHAPTER MATERIALS	151
5.3.1	Recommended Reading	151
5.3.2	Key Terms	151
5.3.3	Summary	151
5.4	PRACTICE SET	152
5.4.1	Quizzes	152
5.4.2	Questions	152
5.4.3	Problems	153
5.5	SIMULATION EXPERIMENTS	154
5.5.1	Applets	154
Chapter 6	<i>Bandwidth Utilization: Multiplexing and Spectrum Spreading</i>	155
6.1	MULTIPLEXING	156
6.1.1	Frequency-Division Multiplexing	157
6.1.2	Wavelength-Division Multiplexing	162
6.1.3	Time-Division Multiplexing	163
6.2	SPREAD SPECTRUM	175
6.2.1	Frequency Hopping Spread Spectrum	176
6.2.2	Direct Sequence Spread Spectrum	178
6.3	END-CHAPTER MATERIALS	180
6.3.1	Recommended Reading	180
6.3.2	Key Terms	180
6.3.3	Summary	180
6.4	PRACTICE SET	181
6.4.1	Quizzes	181
6.4.2	Questions	181
6.4.3	Problems	182
6.5	SIMULATION EXPERIMENTS	184
6.5.1	Applets	184
Chapter 7	<i>Transmission Media</i>	185
7.1	INTRODUCTION	186
7.2	GUIDED MEDIA	187
7.2.1	Twisted-Pair Cable	187
7.2.2	Coaxial Cable	190
7.2.3	Fiber-Optic Cable	192
7.3	UNGUIDED MEDIA: WIRELESS	197
7.3.1	Radio Waves	199
7.3.2	Microwaves	200
7.3.3	Infrared	201

7.4	END-CHAPTER MATERIALS	202
7.4.1	Recommended Reading	202
7.4.2	Key Terms	202
7.4.3	Summary	203
7.5	PRACTICE SET	203
7.5.1	Quizzes	203
7.5.2	Questions	203
7.5.3	Problems	204
Chapter 8 Switching 207		
8.1	INTRODUCTION	208
8.1.1	Three Methods of Switching	208
8.1.2	Switching and TCP/IP Layers	209
8.2	CIRCUIT-SWITCHED NETWORKS	209
8.2.1	Three Phases	211
8.2.2	Efficiency	212
8.2.3	Delay	213
8.3	PACKET SWITCHING	213
8.3.1	Datagram Networks	214
8.3.2	Virtual-Circuit Networks	216
8.4	STRUCTURE OF A SWITCH	222
8.4.1	Structure of Circuit Switches	222
8.4.2	Structure of Packet Switches	226
8.5	END-CHAPTER MATERIALS	230
8.5.1	Recommended Reading	230
8.5.2	Key terms	230
8.5.3	Summary	230
8.6	PRACTICE SET	231
8.6.1	Quizzes	231
8.6.2	Questions	231
8.6.3	Problems	231
8.7	SIMULATION EXPERIMENTS	234
8.7.1	Applets	234
PART III: Data-Link Layer 235		
Chapter 9 Introduction to Data-Link Layer 237		
9.1	INTRODUCTION	238
9.1.1	Nodes and Links	239
9.1.2	Services	239
9.1.3	Two Categories of Links	241
9.1.4	Two Sublayers	242
9.2	LINK-LAYER ADDRESSING	242
9.2.1	Three Types of addresses	244
9.2.2	Address Resolution Protocol (ARP)	245
9.2.3	An Example of Communication	248

9.3	END-CHAPTER MATERIALS	252
9.3.1	Recommended Reading	252
9.3.2	Key Terms	252
9.3.3	Summary	252
9.4	PRACTICE SET	253
9.4.1	Quizzes	253
9.4.2	Questions	253
9.4.3	Problems	254
Chapter 10 <i>Error Detection and Correction</i> 257		
10.1	INTRODUCTION	258
10.1.1	Types of Errors	258
10.1.2	Redundancy	258
10.1.3	Detection versus Correction	258
10.1.4	Coding	259
10.2	BLOCK CODING	259
10.2.1	Error Detection	259
10.3	CYCLIC CODES	264
10.3.1	Cyclic Redundancy Check	264
10.3.2	Polynomials	267
10.3.3	Cyclic Code Encoder Using Polynomials	269
10.3.4	Cyclic Code Analysis	270
10.3.5	Advantages of Cyclic Codes	274
10.3.6	Other Cyclic Codes	274
10.3.7	Hardware Implementation	274
10.4	CHECKSUM	277
10.4.1	Concept	278
10.4.2	Other Approaches to the Checksum	281
10.5	FORWARD ERROR CORRECTION	282
10.5.1	Using Hamming Distance	283
10.5.2	Using XOR	283
10.5.3	Chunk Interleaving	283
10.5.4	Combining Hamming Distance and Interleaving	284
10.5.5	Compounding High- and Low-Resolution Packets	284
10.6	END-CHAPTER MATERIALS	285
10.6.1	Recommended Reading	285
10.6.2	Key Terms	286
10.6.3	Summary	286
10.7	PRACTICE SET	287
10.7.1	Quizzes	287
10.7.2	Questions	287
10.7.3	Problems	288
10.8	SIMULATION EXPERIMENTS	292
10.8.1	Applets	292
10.9	PROGRAMMING ASSIGNMENTS	292

Chapter 11 *Data Link Control (DLC)* 293

- 11.1 DLC SERVICES 294
 - 11.1.1 Framing 294
 - 11.1.2 Flow and Error Control 297
 - 11.1.3 Connectionless and Connection-Oriented 298
- 11.2 DATA-LINK LAYER PROTOCOLS 299
 - 11.2.1 Simple Protocol 300
 - 11.2.2 Stop-and-Wait Protocol 301
 - 11.2.3 Piggybacking 304
- 11.3 HDLC 304
 - 11.3.1 Configurations and Transfer Modes 305
 - 11.3.2 Framing 305
- 11.4 POINT-TO-POINT PROTOCOL (PPP) 309
 - 11.4.1 Services 309
 - 11.4.2 Framing 310
 - 11.4.3 Transition Phases 311
 - 11.4.4 Multiplexing 312
- 11.5 END-CHAPTER MATERIALS 319
 - 11.5.1 Recommended Reading 319
 - 11.5.2 Key Terms 319
 - 11.5.3 Summary 319
- 11.6 PRACTICE SET 320
 - 11.6.1 Quizzes 320
 - 11.6.2 Questions 320
 - 11.6.3 Problems 321
- 11.7 SIMULATION EXPERIMENTS 323
 - 11.7.1 Applets 323
- 11.8 PROGRAMMING ASSIGNMENTS 323

Chapter 12 *Media Access Control (MAC)* 325

- 12.1 RANDOM ACCESS 326
 - 12.1.1 ALOHA 326
 - 12.1.2 CSMA 331
 - 12.1.3 CSMA/CD 334
 - 12.1.4 CSMA/CA 338
- 12.2 CONTROLLED ACCESS 341
 - 12.2.1 Reservation 341
 - 12.2.2 Polling 342
 - 12.2.3 Token Passing 343
- 12.3 CHANNELIZATION 344
 - 12.3.1 FDMA 344
 - 12.3.2 TDMA 346
 - 12.3.3 CDMA 347
- 12.4 END-CHAPTER MATERIALS 352
 - 12.4.1 Recommended Reading 352
 - 12.4.2 Key Terms 353
 - 12.4.3 Summary 353

12.5	PRACTICE SET	354
12.5.1	Quizzes	354
12.5.2	Questions	354
12.5.3	Problems	356
12.6	SIMULATION EXPERIMENTS	360
12.6.1	Applets	360
12.7	PROGRAMMING ASSIGNMENTS	360

Chapter 13 *Wired LANs: Ethernet* 361

13.1	ETHERNET PROTOCOL	362
13.1.1	IEEE Project 802	362
13.1.2	Ethernet Evolution	363
13.2	STANDARD ETHERNET	364
13.2.1	Characteristics	364
13.2.2	Addressing	366
13.2.3	Access Method	368
13.2.4	Efficiency of Standard Ethernet	370
13.2.5	Implementation	370
13.2.6	Changes in the Standard	373
13.3	FAST ETHERNET (100 MBPS)	376
13.3.1	Access Method	377
13.3.2	Physical Layer	377
13.4	GIGABIT ETHERNET	379
13.4.1	MAC Sublayer	380
13.4.2	Physical Layer	381
13.5	10 GIGABIT ETHERNET	382
13.5.1	Implementation	382
13.6	END-CHAPTER MATERIALS	383
13.6.1	Recommended Reading	383
13.6.2	Key Terms	383
13.6.3	Summary	383
13.7	PRACTICE SET	384
13.7.1	Quizzes	384
13.7.2	Questions	384
13.7.3	Problems	385
13.8	SIMULATION EXPERIMENTS	385
13.8.1	Applets	385
13.8.2	Lab Assignments	386

Chapter 14 *Other Wired Networks* 387

14.1	TELEPHONE NETWORKS	388
14.1.1	Major Components	388
14.1.2	LATAs	388
14.1.3	Signaling	390
14.1.4	Services Provided by Telephone Networks	393
14.1.5	Dial-Up Service	394
14.1.6	Digital Subscriber Line (DSL)	396

14.2	CABLE NETWORKS	397
14.2.1	Traditional Cable Networks	397
14.2.2	Hybrid Fiber-Coaxial (HFC) Network	398
14.2.3	Cable TV for Data Transfer	399
14.3	SONET	400
14.3.1	Architecture	401
14.3.2	SONET Layers	403
14.3.3	SONET Frames	404
14.3.4	STS Multiplexing	412
14.3.5	SONET Networks	415
14.3.6	Virtual Tributaries	420
14.4	ATM	421
14.4.1	Design Goals	422
14.4.2	Problems	422
14.4.3	Architecture	425
14.5	END-CHAPTER MATERIALS	429
14.5.1	Recommended Reading	429
14.5.2	Key Terms	430
14.5.3	Summary	431
14.6	PRACTICE SET	432
14.6.1	Quizzes	432
14.6.2	Questions	432
14.6.3	Problems	433

Chapter 15 *Wireless LANs* 435

15.1	INTRODUCTION	436
15.1.1	Architectural Comparison	436
15.1.2	Characteristics	438
15.1.3	Access Control	438
15.2	IEEE 802.11 PROJECT	439
15.2.1	Architecture	440
15.2.2	MAC Sublayer	441
15.2.3	Addressing Mechanism	446
15.2.4	Physical Layer	448
15.3	BLUETOOTH	451
15.3.1	Architecture	451
15.3.2	Bluetooth Layers	452
15.4	END-CHAPTER MATERIALS	458
15.4.1	Further Reading	458
15.4.2	Key Terms	458
15.4.3	Summary	458
15.5	PRACTICE SET	459
15.5.1	Quizzes	459
15.5.2	Questions	459
15.5.3	Problems	460
15.6	SIMULATION EXPERIMENTS	463
15.6.1	Applets	463
15.6.2	Lab Assignments	463

Chapter 16 *Other Wireless Networks* 465

- 16.1 WiMAX 466
 - 16.1.1 Services 466
 - 16.1.2 IEEE Project 802.16 467
 - 16.1.3 Layers in Project 802.16 467
- 16.2 CELLULAR TELEPHONY 470
 - 16.2.1 Operation 471
 - 16.2.2 First Generation (1G) 473
 - 16.2.3 Second Generation (2G) 474
 - 16.2.4 Third Generation (3G) 480
 - 16.2.5 Fourth Generation (4G) 482
- 16.3 SATELLITE NETWORKS 483
 - 16.3.1 Operation 483
 - 16.3.2 GEO Satellites 485
 - 16.3.3 MEO Satellites 485
 - 16.3.4 LEO Satellites 488
- 16.4 END-CHAPTER MATERIALS 489
 - 16.4.1 Recommended Reading 489
 - 16.4.2 Key Terms 490
 - 16.4.3 Summary 490
- 16.5 PRACTICE SET 491
 - 16.5.1 Quizzes 491
 - 16.5.2 Questions 491
 - 16.5.3 Problems 491

Chapter 17 *Connecting Devices and Virtual LANs* 493

- 17.1 CONNECTING DEVICES 494
 - 17.1.1 Hubs 494
 - 17.1.2 Link-Layer Switches 495
 - 17.1.3 Routers 501
- 17.2 VIRTUAL LANS 502
 - 17.2.1 Membership 504
 - 17.2.2 Configuration 504
 - 17.2.3 Communication between Switches 505
 - 17.2.4 Advantages 506
- 17.3 END-CHAPTER MATERIALS 506
 - 17.3.1 Recommended Reading 506
 - 17.3.2 Key Terms 506
 - 17.3.3 Summary 506
- 17.4 PRACTICE SET 507
 - 17.4.1 Quizzes 507
 - 17.4.2 Questions 507
 - 17.4.3 Problems 507

PART IV: Network Layer 509**Chapter 18 *Introduction to Network Layer* 511**

- 18.1 NETWORK-LAYER SERVICES 512
 - 18.1.1 Packetizing 513
 - 18.1.2 Routing and Forwarding 513
 - 18.1.3 Other Services 514
- 18.2 PACKET SWITCHING 516
 - 18.2.1 Datagram Approach: Connectionless Service 516
 - 18.2.2 Virtual-Circuit Approach: Connection-Oriented Service 517
- 18.3 NETWORK-LAYER PERFORMANCE 522
 - 18.3.1 Delay 522
 - 18.3.2 Throughput 523
 - 18.3.3 Packet Loss 525
 - 18.3.4 Congestion Control 525
- 18.4 IPV4 ADDRESSES 528
 - 18.4.1 Address Space 529
 - 18.4.2 Classful Addressing 530
 - 18.4.3 Classless Addressing 532
 - 18.4.4 Dynamic Host Configuration Protocol (DHCP) 539
 - 18.4.5 Network Address Resolution (NAT) 543
- 18.5 FORWARDING OF IP PACKETS 546
 - 18.5.1 Forwarding Based on Destination Address 547
 - 18.5.2 Forwarding Based on Label 553
 - 18.5.3 Routers as Packet Switches 555
- 18.6 END-CHAPTER MATERIALS 556
 - 18.6.1 Recommended Reading 556
 - 18.6.2 Key Terms 556
 - 18.6.3 Summary 556
- 18.7 PRACTICE SET 557
 - 18.7.1 Quizzes 557
 - 18.7.2 Questions 557
 - 18.7.3 Problems 558
- 18.8 SIMULATION EXPERIMENTS 560
 - 18.8.1 Applets 560
- 18.9 PROGRAMMING ASSIGNMENT 560

Chapter 19 *Network-Layer Protocols* 561

- 19.1 INTERNET PROTOCOL (IP) 562
 - 19.1.1 Datagram Format 563
 - 19.1.2 Fragmentation 567
 - 19.1.3 Options 572
 - 19.1.4 Security of IPv4 Datagrams 573
- 19.2 ICMPv4 574
 - 19.2.1 MESSAGES 575
 - 19.2.2 Debugging Tools 578
 - 19.2.3 ICMP Checksum 580

19.3	MOBILE IP	581
19.3.1	Addressing	581
19.3.2	Agents	583
19.3.3	Three Phases	584
19.3.4	Inefficiency in Mobile IP	589
19.4	END-CHAPTER MATERIALS	591
19.4.1	Recommended Reading	591
19.4.2	Key Terms	591
19.4.3	Summary	591
19.5	PRACTICE SET	592
19.5.1	Quizzes	592
19.5.2	Questions	592
19.5.3	Problems	593
19.6	SIMULATION EXPERIMENTS	594
19.6.1	Applets	594
19.6.2	Lab Assignments	594
Chapter 20 <i>Unicast Routing</i> 595		
20.1	INTRODUCTION	596
20.1.1	General Idea	596
20.1.2	Least-Cost Routing	596
20.2	ROUTING ALGORITHMS	598
20.2.1	Distance-Vector Routing	598
20.2.2	Link-State Routing	604
20.2.3	Path-Vector Routing	606
20.3	UNICAST ROUTING PROTOCOLS	611
20.3.1	Internet Structure	611
20.3.2	Routing Information Protocol (RIP)	613
20.3.3	Open Shortest Path First (OSPF)	618
20.3.4	Border Gateway Protocol Version 4 (BGP4)	623
20.4	END-CHAPTER MATERIALS	631
20.4.1	Recommended Reading	631
20.4.2	Key Terms	631
20.4.3	Summary	632
20.5	PRACTICE SET	632
20.5.1	Quizzes	632
20.5.2	Questions	632
20.5.3	Problems	634
20.6	SIMULATION EXPERIMENTS	637
20.6.1	Applets	637
20.7	PROGRAMMING ASSIGNMENT	637
Chapter 21 <i>Multicast Routing</i> 639		
21.1	INTRODUCTION	640
21.1.1	Unicasting	640
21.1.2	Multicasting	640
21.1.3	Broadcasting	643

21.2	MULTICASTING BASICS	643
21.2.1	Multicast Addresses	643
21.2.2	Delivery at Data-Link Layer	645
21.2.3	Collecting Information about Groups	647
21.2.4	Multicast Forwarding	648
21.2.5	Two Approaches to Multicasting	649
21.3	INTRADOMAIN MULTICAST PROTOCOLS	650
21.3.1	Multicast Distance Vector (DVMRP)	651
21.3.2	Multicast Link State (MOSPF)	653
21.3.3	Protocol Independent Multicast (PIM)	654
21.4	INTERDOMAIN MULTICAST PROTOCOLS	657
21.5	IGMP	658
21.5.1	Messages	658
21.5.2	Propagation of Membership Information	659
21.5.3	Encapsulation	660
21.6	END-CHAPTER MATERIALS	660
21.6.1	Recommended Reading	660
21.6.2	Key Terms	660
21.6.3	Summary	660
21.7	PRACTICE SET	661
21.7.1	Quizzes	661
21.7.2	Questions	661
21.7.3	Problems	662
21.8	SIMULATION EXPERIMENTS	663
21.8.1	Applets	663
Chapter 22	<i>Next Generation IP</i>	665
22.1	IPv6 ADDRESSING	666
22.1.1	Representation	666
22.1.2	Address Space	667
22.1.3	Address Space Allocation	668
22.1.4	Autoconfiguration	672
22.1.5	Renumbers	673
22.2	THE IPv6 PROTOCOL	674
22.2.1	Packet Format	674
22.2.2	Extension Header	677
22.3	THE ICMPv6 PROTOCOL	679
22.3.1	Error-Reporting Messages	679
22.3.2	Informational Messages	680
22.3.3	Neighbor-Discovery Messages	681
22.3.4	Group Membership Messages	682
22.4	TRANSITION FROM IPv4 TO IPv6	682
22.4.1	Strategies	683
22.4.2	Use of IP Addresses	684
22.5	END-CHAPTER MATERIALS	684
22.5.1	Recommended Reading	684
22.5.2	Key Terms	685
22.5.3	Summary	685

22.6	PRACTICE SET	685
22.6.1	Quizzes	685
22.6.2	Questions	685
22.6.3	Problems	686
22.7	SIMULATION EXPERIMENTS	688
22.7.1	Applets	688

PART V: Transport Layer 689

Chapter 23 *Introduction to Transport Layer* 691

23.1	INTRODUCTION	692
23.1.1	Transport-Layer Services	693
23.1.2	Connectionless and Connection-Oriented Protocols	703
23.2	TRANSPORT-LAYER PROTOCOLS	707
23.2.1	Simple Protocol	707
23.2.2	Stop-and-Wait Protocol	708
23.2.3	Go-Back- <i>N</i> Protocol (GBN)	713
23.2.4	Selective-Repeat Protocol	720
23.2.5	Bidirectional Protocols: Piggybacking	726
23.3	END-CHAPTER MATERIALS	727
23.3.1	Recommended Reading	727
23.3.2	Key Terms	727
23.3.3	Summary	728
23.4	PRACTICE SET	728
23.4.1	Quizzes	728
23.4.2	Questions	728
23.4.3	Problems	729
23.5	SIMULATION EXPERIMENTS	733
23.5.1	Applets	733
23.6	PROGRAMMING ASSIGNMENT	733

Chapter 24 *Transport-Layer Protocols* 735

24.1	INTRODUCTION	736
24.1.1	Services	736
24.1.2	Port Numbers	736
24.2	USER DATAGRAM PROTOCOL	737
24.2.1	User Datagram	737
24.2.2	UDP Services	738
24.2.3	UDP Applications	741
24.3	TRANSMISSION CONTROL PROTOCOL	743
24.3.1	TCP Services	743
24.3.2	TCP Features	746
24.3.3	Segment	748
24.3.4	A TCP Connection	750
24.3.5	State Transition Diagram	756
24.3.6	Windows in TCP	760
24.3.7	Flow Control	762
24.3.8	Error Control	768
24.3.9	TCP Congestion Control	777

24.3.10	TCP Timers	786
24.3.11	Options	790
24.4	SCTP	791
24.4.1	SCTP Services	791
24.4.2	SCTP Features	792
24.4.3	Packet Format	794
24.4.4	An SCTP Association	796
24.4.5	Flow Control	799
24.4.6	Error Control	801
24.5	END-CHAPTER MATERIALS	805
24.5.1	Recommended Reading	805
24.5.2	Key Terms	805
24.5.3	Summary	805
24.6	PRACTICE SET	806
24.6.1	Quizzes	806
24.6.2	Questions	806
24.6.3	Problems	809

PART VI: Application Layer 815

Chapter 25 *Introduction to Application Layer* 817

25.1	INTRODUCTION	818
25.1.1	Providing Services	819
25.1.2	Application-Layer Paradigms	820
25.2	CLIENT-SERVER PROGRAMMING	823
25.2.1	Application Programming Interface	823
25.2.2	Using Services of the Transport Layer	827
25.2.3	Iterative Communication Using UDP	828
25.2.4	Iterative Communication Using TCP	830
25.2.5	Concurrent Communication	832
25.3	ITERATIVE PROGRAMMING IN C	833
25.3.1	General Issues	833
25.3.2	Iterative Programming Using UDP	834
25.3.3	Iterative Programming Using TCP	837
25.4	ITERATIVE PROGRAMMING IN JAVA	842
25.4.1	Addresses and Ports	843
25.4.2	Iterative Programming Using UDP	846
25.4.3	Iterative Programming Using TCP	857
25.5	END-CHAPTER MATERIALS	865
25.5.1	Recommended Reading	865
25.5.2	Key Terms	866
25.5.3	Summary	866
25.6	PRACTICE SET	866
25.6.1	Quizzes	866
25.6.2	Questions	866
25.6.3	Problems	869
25.7	SIMULATION EXPERIMENTS	869
25.7.1	Applets	869
25.8	PROGRAMMING ASSIGNMENT	870

Chapter 26 *Standard Client-Server Protocols* 871

- 26.1 WORLD WIDE WEB AND HTTP 872
 - 26.1.1 World Wide Web 872
 - 26.1.2 HyperText Transfer Protocol (HTTP) 876
- 26.2 FTP 887
 - 26.2.1 Two Connections 888
 - 26.2.2 Control Connection 888
 - 26.2.3 Data Connection 889
 - 26.2.4 Security for FTP 891
- 26.3 ELECTRONIC MAIL 891
 - 26.3.1 Architecture 892
 - 26.3.2 Web-Based Mail 903
 - 26.3.3 E-Mail Security 904
- 26.4 TELNET 904
 - 26.4.1 Local versus Remote Logging 905
- 26.5 SECURE SHELL (SSH) 907
 - 26.5.1 Components 907
 - 26.5.2 Applications 908
- 26.6 DOMAIN NAME SYSTEM (DNS) 910
 - 26.6.1 Name Space 911
 - 26.6.2 DNS in the Internet 915
 - 26.6.3 Resolution 916
 - 26.6.4 Caching 918
 - 26.6.5 Resource Records 918
 - 26.6.6 DNS Messages 919
 - 26.6.7 Registrars 920
 - 26.6.8 DDNS 920
 - 26.6.9 Security of DNS 921
- 26.7 END-CHAPTER MATERIALS 921
 - 26.7.1 Recommended Reading 921
 - 26.7.2 Key Terms 922
 - 26.7.3 Summary 922
- 26.8 PRACTICE SET 923
 - 26.8.1 Quizzes 923
 - 26.8.2 Questions 923
 - 26.8.3 Problems 924
- 26.9 SIMULATION EXPERIMENTS 927
 - 26.9.1 Applets 927
 - 26.9.2 Lab Assignments 927

Chapter 27 *Network Management* 929

- 27.1 INTRODUCTION 930
 - 27.1.1 Configuration Management 930
 - 27.1.2 Fault Management 932
 - 27.1.3 Performance Management 933
 - 27.1.4 Security Management 933
 - 27.1.5 Accounting Management 934
- 27.2 SNMP 934
 - 27.2.1 Managers and Agents 935

27.2.2	Management Components	935
27.2.3	An Overview	937
27.2.4	SMI	938
27.2.5	MIB	942
27.2.6	SNMP	944
27.3	ASN.1	951
27.3.1	Language Basics	951
27.3.2	Data Types	952
27.3.3	Encoding	955
27.4	END-CHAPTER MATERIALS	955
27.4.1	Recommended Reading	955
27.4.2	Key Terms	956
27.4.3	Summary	956
27.5	PRACTICE SET	956
27.5.1	Quizzes	956
27.5.2	Questions	956
27.5.3	Problems	958
Chapter 28 Multimedia 961		
28.1	COMPRESSION	962
28.1.1	Lossless Compression	962
28.1.2	Lossy Compression	972
28.2	MULTIMEDIA DATA	978
28.2.1	Text	978
28.2.2	Image	978
28.2.3	Video	982
28.2.4	Audio	984
28.3	MULTIMEDIA IN THE INTERNET	986
28.3.1	Streaming Stored Audio/Video	986
28.3.2	Streaming Live Audio/Video	989
28.3.3	Real-Time Interactive Audio/Video	990
28.4	REAL-TIME INTERACTIVE PROTOCOLS	995
28.4.1	Rationale for New Protocols	996
28.4.2	RTP	999
28.4.3	RTCP	1001
28.4.4	Session Initialization Protocol (SIP)	1005
28.4.5	H.323	1012
28.5	END-CHAPTER MATERIALS	1014
28.5.1	Recommended Reading	1014
28.5.2	Key Terms	1015
28.5.3	Summary	1015
28.6	PRACTICE SET	1016
28.6.1	Quizzes	1016
28.6.2	Questions	1016
28.6.3	Problems	1018
28.7	SIMULATION EXPERIMENTS	1021
28.7.1	Applets	1021
28.7.2	Lab Assignments	1021
28.8	PROGRAMMING ASSIGNMENTS	1022

Chapter 29 *Peer-to-Peer Paradigm* 1023

- 29.1 INTRODUCTION 1024
 - 29.1.1 P2P Networks 1024
 - 29.1.2 Distributed Hash Table (DHT) 1026
- 29.2 CHORD 1029
 - 29.2.1 Identifier Space 1029
 - 29.2.2 Finger Table 1029
 - 29.2.3 Interface 1030
 - 29.2.4 Applications 1036
- 29.3 PASTRY 1036
 - 29.3.1 Identifier Space 1036
 - 29.3.2 Routing 1037
 - 29.3.3 Application 1041
- 29.4 KADEMLIA 1041
 - 29.4.1 Identifier Space 1041
 - 29.4.2 Routing Table 1041
 - 29.4.3 K-Buckets 1044
- 29.5 BITTORRENT 1045
 - 29.5.1 BitTorrent with a Tracker 1045
 - 29.5.2 Trackerless BitTorrent 1046
- 29.6 END-CHAPTER MATERIALS 1047
 - 29.6.1 Recommended Reading 1047
 - 29.6.2 Key Terms 1047
 - 29.6.3 Summary 1047
- 29.7 PRACTICE SET 1048
 - 29.7.1 Quizzes 1048
 - 29.7.2 Questions 1048
 - 29.7.3 Problems 1048

PART VII: Topics Related to All Layers 1051**Chapter 30** *Quality of Service* 1053

- 30.1 DATA-FLOW CHARACTERISTICS 1054
 - 30.1.1 Definitions 1054
 - 30.1.2 Sensitivity of Applications 1054
 - 30.1.3 Flow Classes 1055
- 30.2 FLOW CONTROL TO IMPROVE QOS 1055
 - 30.2.1 Scheduling 1056
 - 30.2.2 Traffic Shaping or Policing 1058
 - 30.2.3 Resource Reservation 1061
 - 30.2.4 Admission Control 1062
- 30.3 INTEGRATED SERVICES (INTSERV) 1062
 - 30.3.1 Flow Specification 1062
 - 30.3.2 Admission 1063
 - 30.3.3 Service Classes 1063
 - 30.3.4 Resource Reservation Protocol (RSVP) 1063
 - 30.3.5 Problems with Integrated Services 1065
- 30.4 DIFFERENTIATED SERVICES (DFFSERV) 1066
 - 30.4.1 DS Field 1066

30.4.2	Per-Hop Behavior	1067
30.4.3	Traffic Conditioners	1067
30.5	END-CHAPTER MATERIALS	1068
30.5.1	Recommended Reading	1068
30.5.2	Key Terms	1068
30.5.3	Summary	1068
30.6	PRACTICE SET	1069
30.6.1	Quizzes	1069
30.6.2	Questions	1069
30.6.3	Problems	1070
30.7	SIMULATION EXPERIMENTS	1075
30.7.1	Applets	1075
30.8	PROGRAMMING ASSIGNMENTS	1075
Chapter 31	<i>Cryptography and Network Security</i>	1077
31.1	INTRODUCTION	1078
31.1.1	Security Goals	1078
31.1.2	Attacks	1079
31.1.3	Services and Techniques	1081
31.2	CONFIDENTIALITY	1081
31.2.1	Symmetric-Key Ciphers	1081
31.2.2	Asymmetric-Key Ciphers	1092
31.3	OTHER ASPECTS OF SECURITY	1097
31.3.1	Message Integrity	1097
31.3.2	Message Authentication	1099
31.3.3	Digital Signature	1100
31.3.4	Entity Authentication	1105
31.3.5	Key Management	1108
31.4	END-CHAPTER MATERIALS	1114
31.4.1	Recommended Reading	1114
31.4.2	Key Terms	1114
31.4.3	Summary	1114
31.5	PRACTICE SET	1115
31.5.1	Quizzes	1115
31.5.2	Questions	1115
31.5.3	Problems	1117
31.6	SIMULATION EXPERIMENTS	1121
31.6.1	Applets	1121
31.7	PROGRAMMING ASSIGNMENTS	1122
Chapter 32	<i>Internet Security</i>	1123
32.1	NETWORK-LAYER SECURITY	1124
32.1.1	Two Modes	1124
32.1.2	Two Security Protocols	1126
32.1.3	Services Provided by IPSec	1129
32.1.4	Security Association	1130
32.1.5	Internet Key Exchange (IKE)	1132
32.1.6	Virtual Private Network (VPN)	1133

32.2	TRANSPORT-LAYER SECURITY	1134
32.2.1	SSL Architecture	1135
32.2.2	Four Protocols	1138
32.3	APPLICATION-LAYER SECURITY	1140
32.3.1	E-mail Security	1141
32.3.2	Pretty Good Privacy (PGP)	1142
32.3.3	S/MIME	1147
32.4	FIREWALLS	1151
32.4.1	Packet-Filter Firewall	1152
32.4.2	Proxy Firewall	1152
32.5	END-CHAPTER MATERIALS	1153
32.5.1	Recommended Reading	1153
32.5.2	Key Terms	1154
32.5.3	Summary	1154
32.6	PRACTICE SET	1154
32.6.1	Quizzes	1154
32.6.2	Questions	1155
32.6.3	Problems	1155
32.7	SIMULATION EXPERIMENTS	1156
32.7.1	Applets	1156
32.7.2	Lab Assignments	1156

Appendices A-H available online at
<http://www.mhhe.com/forouzan>

Appendices

Appendix A *Unicode*

Appendix B *Positional Numbering System*

Appendix C *HTML, CSS, XML, and XSL*

Appendix D *A Touch of Probability*

Appendix E *Mathematical Review*

Appendix F *8B/6T Code*

Appendix G *Miscellaneous Information*

Appendix H *Telephone History*

Glossary 1157

References 1193

Index 1199

CHAPTER 2

Network Models

The second chapter is a preparation for the rest of the book. The next five parts of the book is devoted to one of the layers in the TCP/IP protocol suite. In this chapter, we first discuss the idea of network models in general and the TCP/IP protocol suite in particular.

Two models have been devised to define computer network operations: the TCP/IP protocol suite and the OSI model. In this chapter, we first discuss a general subject, protocol layering, which is used in both models. We then concentrate on the TCP/IP protocol suite, on which the book is based. The OSI model is briefly discuss for comparison with the TCP/IP protocol suite.

- ❑ The first section introduces the concept of protocol layering using two scenarios. The section also discusses the two principles upon which the protocol layering is based. The first principle dictates that each layer needs to have two opposite tasks. The second principle dictates that the corresponding layers should be identical. The section ends with a brief discussion of logical connection between two identical layers in protocol layering. Throughout the book, we need to distinguish between logical and physical connections.
- ❑ The second section discusses the five layers of the TCP/IP protocol suite. We show how packets in each of the five layers (physical, data-link, network, transport, and application) are named. We also mention the addressing mechanism used in each layer. Each layer of the TCP/IP protocol suite is a subject of a part of the book. In other words, each layer is discussed in several chapters; this section is just an introduction and preparation.
- ❑ The third section gives a brief discussion of the OSI model. This model was never implemented in practice, but a brief discussion of the model and its comparison with the TCP/IP protocol suite may be useful to better understand the TCP/IP protocol suite. In this section we also give a brief reason for the OSI model's lack of success.

2.1 PROTOCOL LAYERING

We defined the term *protocol* in Chapter 1. In data communication and networking, a protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively. When communication is simple, we may need only one simple protocol; when the communication is complex, we may need to divide the task between different layers, in which case we need a protocol at each layer, or **protocol layering**.

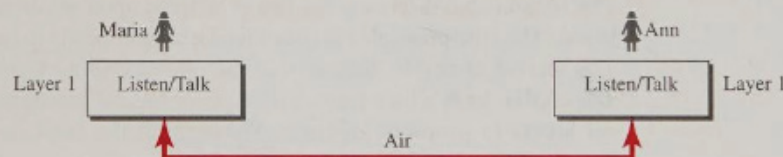
2.1.1 Scenarios

Let us develop two simple scenarios to better understand the need for protocol layering.

First Scenario

In the first scenario, communication is so simple that it can occur in only one layer. Assume Maria and Ann are neighbors with a lot of common ideas. Communication between Maria and Ann takes place in one layer, face to face, in the same language, as shown in Figure 2.1.

Figure 2.1 A single-layer protocol



Even in this simple scenario, we can see that a set of rules needs to be followed. First, Maria and Ann know that they should greet each other when they meet. Second, they know that they should confine their vocabulary to the level of their friendship. Third, each party knows that she should refrain from speaking when the other party is speaking. Fourth, each party knows that the conversation should be a dialog, not a monolog: both should have the opportunity to talk about the issue. Fifth, they should exchange some nice words when they leave.

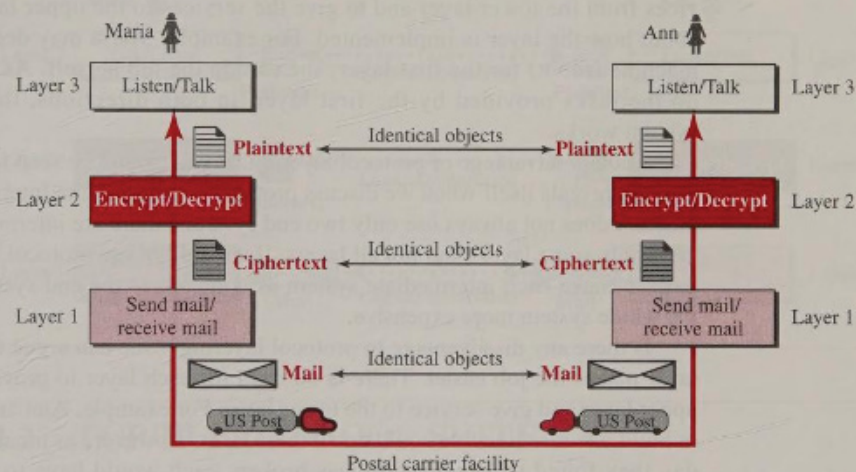
We can see that the protocol used by Maria and Ann is different from the communication between a professor and the students in a lecture hall. The communication in the second case is mostly monolog; the professor talks most of the time unless a student has a question, a situation in which the protocol dictates that she should raise her hand and wait for permission to speak. In this case, the communication is normally very formal and limited to the subject being taught.

Second Scenario

In the second scenario, we assume that Ann is offered a higher-level position in her company, but needs to move to another branch located in a city very far from Maria. The two friends still want to continue their communication and exchange ideas because

they have come up with an innovative project to start a new business when they both retire. They decide to continue their conversation using regular mail through the post office. However, they do not want their ideas to be revealed by other people if the letters are intercepted. They agree on an encryption/decryption technique. The sender of the letter encrypts it to make it unreadable by an intruder; the receiver of the letter decrypts it to get the original letter. We discuss the encryption/decryption methods in Chapter 31, but for the moment we assume that Maria and Ann use one technique that makes it hard to decrypt the letter if one does not have the key for doing so. Now we can say that the communication between Maria and Ann takes place in three layers, as shown in Figure 2.2. We assume that Ann and Maria each have three machines (or robots) that can perform the task at each layer.

Figure 2.2 A three-layer protocol



Let us assume that Maria sends the first letter to Ann. Maria talks to the machine at the third layer as though the machine is Ann and is listening to her. The third layer machine listens to what Maria says and creates the plaintext (a letter in English), which is passed to the second layer machine. The second layer machine takes the plaintext, encrypts it, and creates the ciphertext, which is passed to the first layer machine. The first layer machine, presumably a robot, takes the ciphertext, puts it in an envelope, adds the sender and receiver addresses, and mails it.

At Ann's side, the first layer machine picks up the letter from Ann's mail box, recognizing the letter from Maria by the sender address. The machine takes out the ciphertext from the envelope and delivers it to the second layer machine. The second layer machine decrypts the message, creates the plaintext, and passes the plaintext to the third-layer machine. The third layer machine takes the plaintext and reads it as though Maria is speaking.

Protocol layering enables us to divide a complex task into several smaller and simpler tasks. For example, in Figure 2.2, we could have used only one machine to do the job of all three machines. However, if Maria and Ann decide that the encryption/decryption done by the machine is not enough to protect their secrecy, they would have to change the whole machine. In the present situation, they need to change only the second layer machine; the other two can remain the same. This is referred to as *modularity*. Modularity in this case means independent layers. A layer (module) can be defined as a black box with inputs and outputs, without concern about how inputs are changed to outputs. If two machines provide the same outputs when given the same inputs, they can replace each other. For example, Ann and Maria can buy the second layer machine from two different manufacturers. As long as the two machines create the same ciphertext from the same plaintext and vice versa, they do the job.

One of the advantages of protocol layering is that it allows us to separate the services from the implementation. A layer needs to be able to receive a set of services from the lower layer and to give the services to the upper layer; we don't care about how the layer is implemented. For example, Maria may decide not to buy the machine (robot) for the first layer; she can do the job herself. As long as Maria can do the tasks provided by the first layer, in both directions, the communication system works.

Another advantage of protocol layering, which cannot be seen in our simple examples but reveals itself when we discuss protocol layering in the Internet, is that communication does not always use only two end systems; there are intermediate systems that need only some layers, but not all layers. If we did not use protocol layering, we would have to make each intermediate system as complex as the end systems, which makes the whole system more expensive.

Is there any disadvantage to protocol layering? One can argue that having a single layer makes the job easier. There is no need for each layer to provide a service to the upper layer and give service to the lower layer. For example, Ann and Maria could find or build one machine that could do all three tasks. However, as mentioned above, if one day they found that their code was broken, each would have to replace the whole machine with a new one instead of just changing the machine in the second layer.

2.1.2 Principles of Protocol Layering

Let us discuss two principles of protocol layering.

First Principle

The first principle dictates that if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction. For example, the third layer task is to listen (in one direction) and *talk* (in the other direction). The second layer needs to be able to encrypt and decrypt. The first layer needs to send and receive mail.

Second Principle

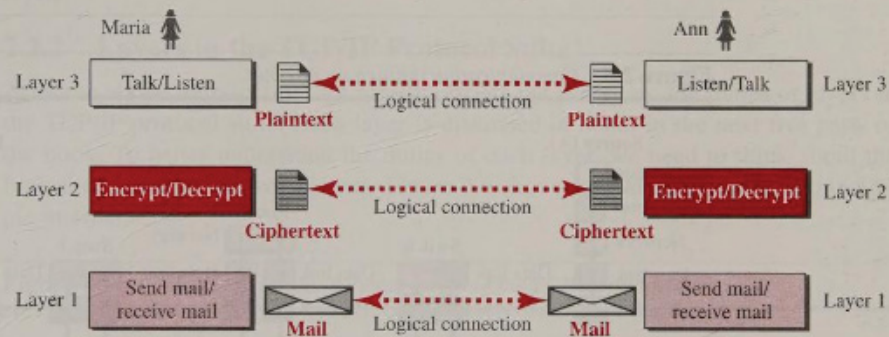
The second principle that we need to follow in protocol layering is that the two objects under each layer at both sites should be identical. For example, the object under layer 3 at both sites should be a plaintext letter. The object under layer 2 at

both sites should be a ciphertext letter. The object under layer 1 at both sites should be a piece of mail.

2.1.3 Logical Connections

After following the above two principles, we can think about logical connection between each layer as shown in Figure 2.3. This means that we have layer-to-layer communication. Maria and Ann can think that there is a logical (imaginary) connection at each layer through which they can send the object created from that layer. We will see that the concept of logical connection will help us better understand the task of layering we encounter in data communication and networking.

Figure 2.3 Logical connection between peer layers

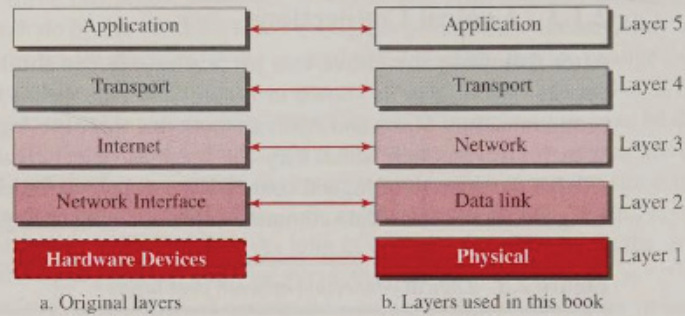
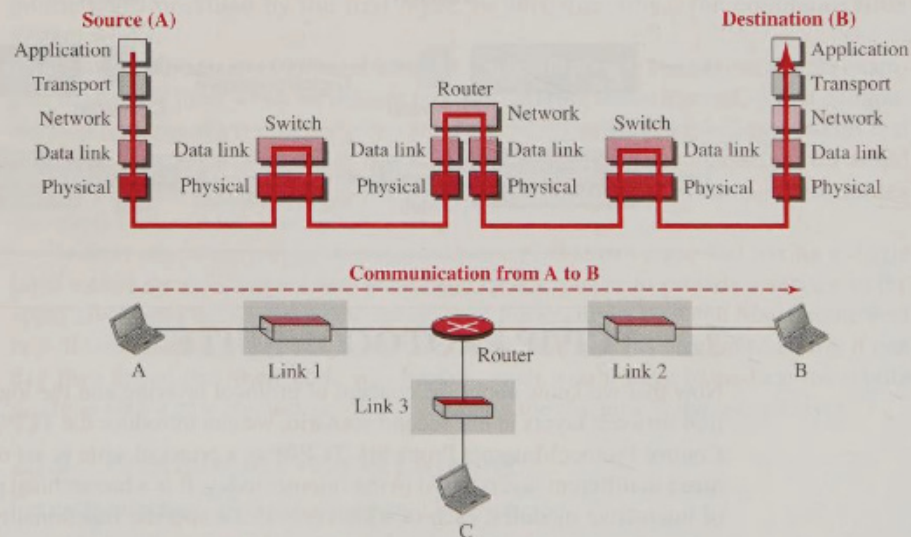


2.2 TCP/IP PROTOCOL SUITE

Now that we know about the concept of protocol layering and the logical communication between layers in our second scenario, we can introduce the TCP/IP (Transmission Control Protocol/Internet Protocol). TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internet today. It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality. The term *hierarchical* means that each upper level protocol is supported by the services provided by one or more lower level protocols. The original TCP/IP protocol suite was defined as four software layers built upon the hardware. Today, however, TCP/IP is thought of as a five-layer model. Figure 2.4 shows both configurations.

2.2.1 Layered Architecture

To show how the layers in the TCP/IP protocol suite are involved in communication between two hosts, we assume that we want to use the suite in a small internet made up of three LANs (links), each with a link-layer switch. We also assume that the links are connected by one router, as shown in Figure 2.5.

Figure 2.4 Layers in the TCP/IP protocol suite**Figure 2.5** Communication through an internet

Let us assume that computer A communicates with computer B. As the figure shows, we have five communicating devices in this communication: source host (computer A), the link-layer switch in link 1, the router, the link-layer switch in link 2, and the destination host (computer B). Each device is involved with a set of layers depending on the role of the device in the internet. The two hosts are involved in all five layers; the source host needs to create a message in the application layer and send it down the layers so that it is physically sent to the destination host. The destination host needs to receive the communication at the physical layer and then deliver it through the other layers to the application layer.

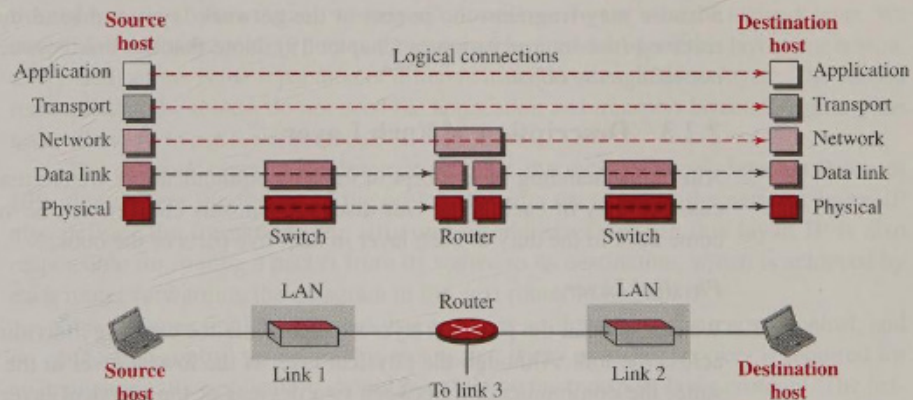
The router is involved in only three layers; there is no transport or application layer in a router as long as the router is used only for routing. Although a router is always involved in one network layer, it is involved in n combinations of link and physical layers in which n is the number of links the router is connected to. The reason is that each link may use its own data-link or physical protocol. For example, in the above figure, the router is involved in three links, but the message sent from source A to destination B is involved in two links. Each link may be using different link-layer and physical-layer protocols; the router needs to receive a packet from link 1 based on one pair of protocols and deliver it to link 2 based on another pair of protocols.

A link-layer switch in a link, however, is involved only in two layers, data-link and physical. Although each switch in the above figure has two different connections, the connections are in the same link, which uses only one set of protocols. This means that, unlike a router, a link-layer switch is involved only in one data-link and one physical layer.

2.2.2 Layers in the TCP/IP Protocol Suite

After the above introduction, we briefly discuss the functions and duties of layers in the TCP/IP protocol suite. Each layer is discussed in detail in the next five parts of the book. To better understand the duties of each layer, we need to think about the logical connections between layers. Figure 2.6 shows logical connections in our simple internet.

Figure 2.6 Logical connections between layers of the TCP/IP protocol suite



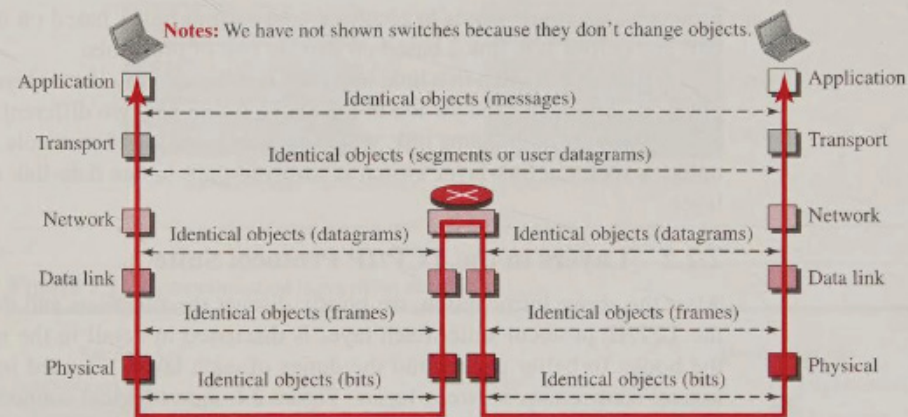
Using logical connections makes it easier for us to think about the duty of each layer. As the figure shows, the duty of the application, transport, and network layers is end-to-end. However, the duty of the data-link and physical layers is hop-to-hop, in which a hop is a host or router. In other words, the domain of duty of the top three layers is the internet, and the domain of duty of the two lower layers is the link.

Another way of thinking of the logical connections is to think about the data unit created from each layer. In the top three layers, the data unit (packets) should not be

changed by any router or link-layer switch. In the bottom two layers, the packet created by the host is changed only by the routers, not by the link-layer switches.

Figure 2.7 shows the second principle discussed previously for protocol layering. We show the identical objects below each layer related to each device.

Figure 2.7 *Identical objects in the TCP/IP protocol suite*



Note that, although the logical connection at the network layer is between the two hosts, we can only say that identical objects exist between two hops in this case because a router may fragment the packet at the network layer and send more packets than received (see fragmentation in Chapter 19). Note that the link between two hops does not change the object.

2.2.3 Description of Each Layer

After understanding the concept of logical communication, we are ready to briefly discuss the duty of each layer. Our discussion in this chapter will be very brief, but we come back to the duty of each layer in next five parts of the book.

Physical Layer

We can say that the physical layer is responsible for carrying individual bits in a frame across the link. Although the physical layer is the lowest level in the TCP/IP protocol suite, the communication between two devices at the physical layer is still a logical communication because there is another, hidden layer, the transmission media, under the physical layer. Two devices are connected by a transmission medium (cable or air). We need to know that the transmission medium does not carry bits; it carries electrical or optical signals. So the bits received in a frame from the data-link layer are transformed and sent through the transmission media, but we can think that the logical unit between two physical layers in two devices is a *bit*. There are several protocols that transform a bit to a signal. We discuss them in Part II when we discuss the physical layer and the transmission media.

Data-link Layer

We have seen that an internet is made up of several links (LANs and WANs) connected by routers. There may be several overlapping sets of links that a datagram can travel from the host to the destination. The routers are responsible for choosing the *best* links. However, when the next link to travel is determined by the router, the data-link layer is responsible for taking the datagram and moving it across the link. The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wireless WAN. We can also have different protocols used with any link type. In each case, the data-link layer is responsible for moving the packet through the link.

TCP/IP does not define any specific protocol for the data-link layer. It supports all the standard and proprietary protocols. Any protocol that can take the datagram and carry it through the link suffices for the network layer. The data-link layer takes a datagram and encapsulates it in a packet called a *frame*.

Each link-layer protocol may provide a different service. Some link-layer protocols provide complete error detection and correction, some provide only error correction. We discuss wired links in Chapters 13 and 14 and wireless links in Chapters 15 and 16.

Network Layer

The network layer is responsible for creating a connection between the source computer and the destination computer. The communication at the network layer is host-to-host. However, since there can be several routers from the source to the destination, the routers in the path are responsible for choosing the best route for each packet. We can say that the network layer is responsible for host-to-host communication and routing the packet through possible routes. Again, we may ask ourselves why we need the network layer. We could have added the routing duty to the transport layer and dropped this layer. One reason, as we said before, is the separation of different tasks between different layers. The second reason is that the routers do not need the application and transport layers. Separating the tasks allows us to use fewer protocols on the routers.

The network layer in the Internet includes the main protocol, Internet Protocol (IP), that defines the format of the packet, called a datagram at the network layer. IP also defines the format and the structure of addresses used in this layer. IP is also responsible for routing a packet from its source to its destination, which is achieved by each router forwarding the datagram to the next router in its path.

IP is a connectionless protocol that provides no flow control, no error control, and no congestion control services. This means that if any of these services is required for an application, the application should rely only on the transport-layer protocol. The network layer also includes unicast (one-to-one) and multicast (one-to-many) routing protocols. A routing protocol does not take part in routing (it is the responsibility of IP), but it creates forwarding tables for routers to help them in the routing process.

The network layer also has some auxiliary protocols that help IP in its delivery and routing tasks. The Internet Control Message Protocol (ICMP) helps IP to report some problems when routing a packet. The Internet Group Management Protocol (IGMP) is another protocol that helps IP in multitasking. The Dynamic Host Configuration Protocol (DHCP) helps IP to get the network-layer address for a host. The Address Resolution Protocol (ARP) is a protocol that helps IP to find the link-layer address of a host or

a router when its network-layer address is given. ARP is discussed in Chapter 9, ICMP in Chapter 19, and IGMP in Chapter 21.

Transport Layer

The logical connection at the transport layer is also end-to-end. The transport layer at the source host gets the message from the application layer, encapsulates it in a transport-layer packet (called a *segment* or a *user datagram* in different protocols) and sends it, through the logical (imaginary) connection, to the transport layer at the destination host. In other words, the transport layer is responsible for giving services to the application layer: to get a message from an application program running on the source host and deliver it to the corresponding application program on the destination host. We may ask why we need an end-to-end transport layer when we already have an end-to-end application layer. The reason is the separation of tasks and duties, which we discussed earlier. The transport layer should be independent of the application layer. In addition, we will see that we have more than one protocol in the transport layer, which means that each application program can use the protocol that best matches its requirement.

As we said, there are a few transport-layer protocols in the Internet, each designed for some specific task. The main protocol, Transmission Control Protocol (TCP), is a connection-oriented protocol that first establishes a logical connection between transport layers at two hosts before transferring data. It creates a logical pipe between two TCPs for transferring a stream of bytes. TCP provides flow control (matching the sending data rate of the source host with the receiving data rate of the destination host to prevent overwhelming the destination), error control (to guarantee that the segments arrive at the destination without error and resending the corrupted ones), and congestion control to reduce the loss of segments due to congestion in the network. The other common protocol, User Datagram Protocol (UDP), is a connectionless protocol that transmits user datagrams without first creating a logical connection. In UDP, each user datagram is an independent entity without being related to the previous or the next one (the meaning of the term *connectionless*). UDP is a simple protocol that does not provide flow, error, or congestion control. Its simplicity, which means small overhead, is attractive to an application program that needs to send short messages and cannot afford the retransmission of the packets involved in TCP, when a packet is corrupted or lost. A new protocol, Stream Control Transmission Protocol (SCTP) is designed to respond to new applications that are emerging in the multimedia. We will discuss UDP, TCP, and SCTP in Chapter 24.

Application Layer

As Figure 2.6 shows, the logical connection between the two application layers is end-to-end. The two application layers exchange *messages* between each other as though there were a bridge between the two layers. However, we should know that the communication is done through all the layers.

Communication at the application layer is between two *processes* (two programs running at this layer). To communicate, a process sends a request to the other process and receives a response. Process-to-process communication is the duty of the application layer. The application layer in the Internet includes many predefined protocols, but

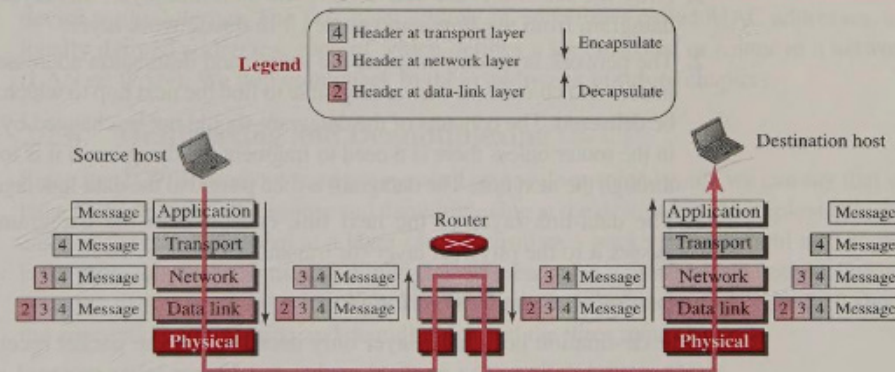
a user can also create a pair of processes to be run at the two hosts. In Chapter 25, we explore this situation.

The Hypertext Transfer Protocol (HTTP) is a vehicle for accessing the World Wide Web (WWW). The Simple Mail Transfer Protocol (SMTP) is the main protocol used in electronic mail (e-mail) service. The File Transfer Protocol (FTP) is used for transferring files from one host to another. The Terminal Network (TELNET) and Secure Shell (SSH) are used for accessing a site remotely. The Simple Network Management Protocol (SNMP) is used by an administrator to manage the Internet at global and local levels. The Domain Name System (DNS) is used by other protocols to find the network-layer address of a computer. The Internet Group Management Protocol (IGMP) is used to collect membership in a group. We discuss most of these protocols in Chapter 26 and some in other chapters.

2.2.4 Encapsulation and Decapsulation

One of the important concepts in protocol layering in the Internet is encapsulation/decapsulation. Figure 2.8 shows this concept for the small internet in Figure 2.5.

Figure 2.8 Encapsulation/Decapsulation



We have not shown the layers for the link-layer switches because no encapsulation/decapsulation occurs in this device. In Figure 2.8, we show the encapsulation in the source host, decapsulation in the destination host, and encapsulation and decapsulation in the router.

Encapsulation at the Source Host

At the source, we have only encapsulation.

1. At the application layer, the data to be exchanged is referred to as a *message*. A message normally does not contain any header or trailer, but if it does, we refer to the whole as the message. The message is passed to the transport layer.
2. The transport layer takes the message as the payload, the load that the transport layer should take care of. It adds the transport layer header to the payload, which contains the identifiers of the source and destination application programs that

want to communicate plus some more information that is needed for the end-to-end delivery of the message, such as information needed for flow, error control, or congestion control. The result is the transport-layer packet, which is called the *segment* (in TCP) and the *user datagram* (in UDP). The transport layer then passes the packet to the network layer.

3. The network layer takes the transport-layer packet as data or payload and adds its own header to the payload. The header contains the addresses of the source and destination hosts and some more information used for error checking of the header, fragmentation information, and so on. The result is the network-layer packet, called a *datagram*. The network layer then passes the packet to the data-link layer.
4. The data-link layer takes the network-layer packet as data or payload and adds its own header, which contains the link-layer addresses of the host or the next hop (the router). The result is the link-layer packet, which is called a *frame*. The frame is passed to the physical layer for transmission.

Decapsulation and Encapsulation at the Router

At the router, we have both decapsulation and encapsulation because the router is connected to two or more links.

1. After the set of bits are delivered to the data-link layer, this layer decapsulates the datagram from the frame and passes it to the network layer.
2. The network layer only inspects the source and destination addresses in the datagram header and consults its forwarding table to find the next hop to which the datagram is to be delivered. The contents of the datagram should not be changed by the network layer in the router unless there is a need to fragment the datagram if it is too big to be passed through the next link. The datagram is then passed to the data-link layer of the next link.
3. The data-link layer of the next link encapsulates the datagram in a frame and passes it to the physical layer for transmission.

Decapsulation at the Destination Host

At the destination host, each layer only decapsulates the packet received, removes the payload, and delivers the payload to the next-higher layer protocol until the message reaches the application layer. It is necessary to say that decapsulation in the host involves error checking.

2.2.5 Addressing

It is worth mentioning another concept related to protocol layering in the Internet, *addressing*. As we discussed before, we have logical communication between pairs of layers in this model. Any communication that involves two parties needs two addresses: source address and destination address. Although it looks as if we need five pairs of addresses, one pair per layer, we normally have only four because the physical layer does not need addresses; the unit of data exchange at the physical layer is a bit, which definitely cannot have an address. Figure 2.9 shows the addressing at each layer.

As the figure shows, there is a relationship between the layer, the address used in that layer, and the packet name at that layer. At the application layer, we normally use names to define the site that provides services, such as *someorg.com*, or the e-mail

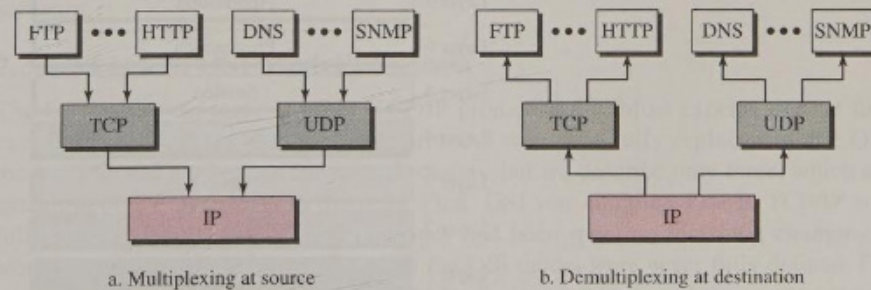
Figure 2.9 Addressing in the TCP/IP protocol suite

Packet names	Layers	Addresses
Message	Application layer	Names
Segment / User datagram	Transport layer	Port numbers
Datagram	Network layer	Logical addresses
Frame	Data-link layer	Link-layer addresses
Bits	Physical layer	

address, such as *somebody@coldmail.com*. At the transport layer, addresses are called port numbers, and these define the application-layer programs at the source and destination. Port numbers are local addresses that distinguish between several programs running at the same time. At the network-layer, the addresses are global, with the whole Internet as the scope. A network-layer address uniquely defines the connection of a device to the Internet. The link-layer addresses, sometimes called MAC addresses, are locally defined addresses, each of which defines a specific host or router in a network (LAN or WAN). We will come back to these addresses in future chapters.

2.2.6 Multiplexing and Demultiplexing

Since the TCP/IP protocol suite uses several protocols at some layers, we can say that we have multiplexing at the source and demultiplexing at the destination. Multiplexing in this case means that a protocol at a layer can encapsulate a packet from several next-higher layer protocols (one at a time); demultiplexing means that a protocol can decapsulate and deliver a packet to several next-higher layer protocols (one at a time). Figure 2.10 shows the concept of multiplexing and demultiplexing at the three upper layers.

Figure 2.10 Multiplexing and demultiplexing

To be able to multiplex and demultiplex, a protocol needs to have a field in its header to identify to which protocol the encapsulated packets belong. At the transport

layer, either UDP or TCP can accept a message from several application-layer protocols. At the network layer, IP can accept a segment from TCP or a user datagram from UDP. IP can also accept a packet from other protocols such as ICMP, IGMP, and so on. At the data-link layer, a frame may carry the payload coming from IP or other protocols such as ARP (see Chapter 9).

2.3 THE OSI MODEL

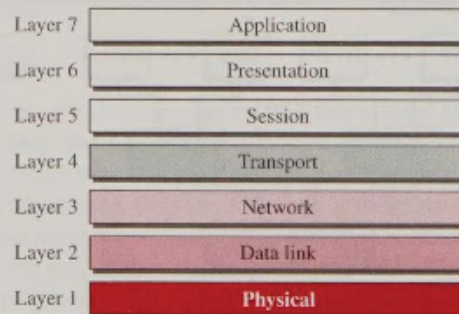
Although, when speaking of the Internet, everyone talks about the TCP/IP protocol suite, this suite is not the only suite of protocols defined. Established in 1947, the **International Organization for Standardization (ISO)** is a multinational body dedicated to worldwide agreement on international standards. Almost three-fourths of the countries in the world are represented in the ISO. An ISO standard that covers all aspects of network communications is the **Open Systems Interconnection (OSI) model**. It was first introduced in the late 1970s.

ISO is the organization; OSI is the model.

An *open system* is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable. The OSI model was intended to be the basis for the creation of the protocols in the OSI stack.

The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network (see Figure 2.11).

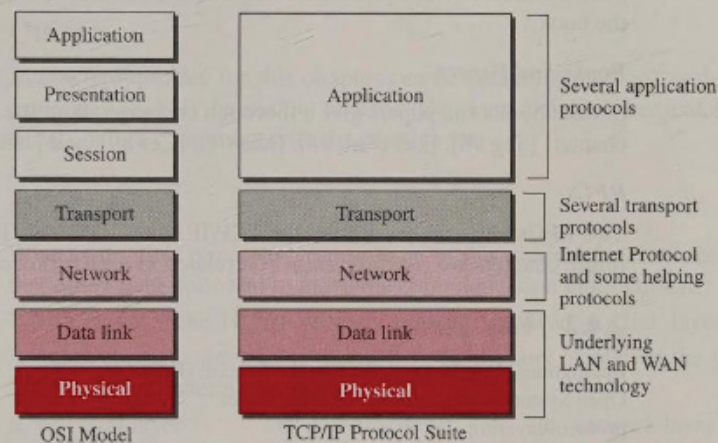
Figure 2.11 The OSI model



2.3.1 OSI versus TCP/IP

When we compare the two models, we find that two layers, session and presentation, are missing from the TCP/IP protocol suite. These two layers were not added to the TCP/IP protocol suite after the publication of the OSI model. The application layer in the suite is usually considered to be the combination of three layers in the OSI model, as shown in Figure 2.12.

Figure 2.12 *TCP/IP and OSI model*



Two reasons were mentioned for this decision. First, TCP/IP has more than one transport-layer protocol. Some of the functionalities of the session layer are available in some of the transport-layer protocols. Second, the application layer is not only one piece of software. Many applications can be developed at this layer. If some of the functionalities mentioned in the session and presentation layers are needed for a particular application, they can be included in the development of that piece of software.

2.3.2 Lack of OSI Model's Success

The OSI model appeared after the TCP/IP protocol suite. Most experts were at first excited and thought that the TCP/IP protocol would be fully replaced by the OSI model. This did not happen for several reasons, but we describe only three, which are agreed upon by all experts in the field. First, OSI was completed when TCP/IP was fully in place and a lot of time and money had been spent on the suite; changing it would cost a lot. Second, some layers in the OSI model were never fully defined. For example, although the services provided by the presentation and the session layers were listed in the document, actual protocols for these two layers were not fully defined, nor were they fully described, and the corresponding software was not fully

developed. Third, when OSI was implemented by an organization in a different application, it did not show a high enough level of performance to entice the Internet authority to switch from the TCP/IP protocol suite to the OSI model.

2.4 END-CHAPTER MATERIALS

2.4.1 Recommended Reading

For more details about subjects discussed in this chapter, we recommend the following books, and RFCs. The items enclosed in brackets refer to the reference list at the end of the book.

Books and Papers

Several books and papers give a thorough coverage about the materials discussed in this chapter: [Seg 98], [Lei et al. 98], [Kle 04], [Cer 89], and [Jen et al. 86].

RFCs

Two RFCs in particular discuss the TCP/IP suite: RFC 791 (IP) and RFC 817 (TCP). In future chapters we list different RFCs related to each protocol in each layer.

2.4.2 Key Terms

International Organization for Standardization (ISO)
Open Systems Interconnection (OSI) model
protocol layering

2.4.3 Summary

A protocol is a set of rules that governs communication. In protocol layering, we need to follow two principles to provide bidirectional communication. First, each layer needs to perform two opposite tasks. Second, two objects under each layer at both sides should be identical. In a protocol layering, we need to distinguish between a logical connection and a physical connection. Two protocols at the same layer can have a logical connection; a physical connection is only possible through the physical layers.

TCP/IP is a hierarchical protocol suite made of five layers: physical, data link, network, transport, and application. The physical layer coordinates the functions required to transmit a bit stream over a physical medium. The data-link layer is responsible for delivering data units from one station to the next without errors. The network layer is responsible for the source-to-destination delivery of a packet across multiple network links. The transport layer is responsible for the process-to-process delivery of the entire message. The application layer enables the users to access the network.

Four levels of addresses are used in an internet following the TCP/IP protocols: physical (link) addresses, logical (IP) addresses, port addresses, and specific addresses. The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. The IP address uniquely defines a host on the Internet. The port address identifies a process on a host. A specific address is a user-friendly address.

Another model that defines protocol layering is the Open Systems Interconnection (OSI) model. Two layers in the OSI model, session and presentation, are missing from the TCP/IP protocol suite. These two layers were not added to the TCP/IP protocol suite after the publication of the OSI model. The application layer in the suite is usually considered to be the combination of three layers in the OSI model. The OSI model did not replace the TCP/IP protocol suite because it was completed when TCP/IP was fully in place and because some layers in the OSI model were never fully defined.

2.5 PRACTICE SET

2.5.1 Quizzes

A set of interactive quizzes for this chapter can be found on the book website. It is strongly recommended that the student take the quizzes to check his/her understanding of the materials before continuing with the practice set.

2.5.2 Questions

- Q2-1.** What is the first principle we discussed in this chapter for protocol layering that needs to be followed to make the communication bidirectional?
- Q2-2.** Which layers of the TCP/IP protocol suite are involved in a link-layer switch?
- Q2-3.** A router connects three links (networks). How many of each of the following layers can the router be involved with?
a. physical layer **b.** data-link layer **c.** network layer
- Q2-4.** In the TCP/IP protocol suite, what are the identical objects at the sender and the receiver sites when we think about the logical connection at the application layer?
- Q2-5.** A host communicates with another host using the TCP/IP protocol suite. What is the unit of data sent or received at each of the following layers?
a. application layer **b.** network layer **c.** data-link layer
- Q2-6.** Which of the following data units is encapsulated in a frame?
a. a user datagram **b.** a datagram **c.** a segment
- Q2-7.** Which of the following data units is decapsulated from a user datagram?
a. a datagram **b.** a segment **c.** a message
- Q2-8.** Which of the following data units has an application-layer message plus the header from layer 4?
a. a frame **b.** a user datagram **c.** a bit
- Q2-9.** List some application-layer protocols mentioned in this chapter.
- Q2-10.** If a port number is 16 bits (2 bytes), what is the minimum header size at the transport layer of the TCP/IP protocol suite?
- Q2-11.** What are the types of addresses (identifiers) used in each of the following layers?
a. application layer **b.** network layer **c.** data-link layer

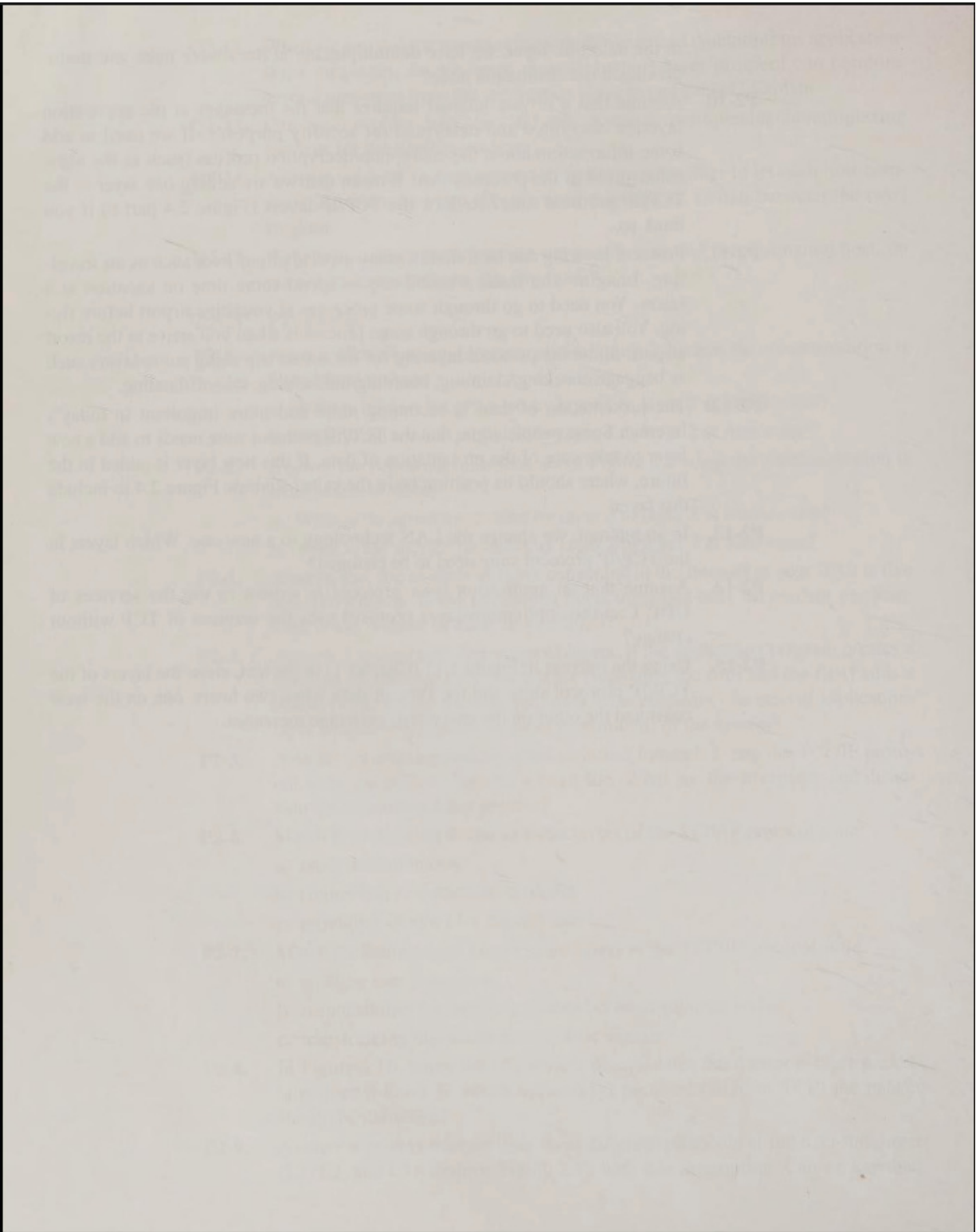
- Q2-12.** When we say that the transport layer multiplexes and demultiplexes application-layer messages, do we mean that a transport-layer protocol can combine several messages from the application layer in one packet? Explain.
- Q2-13.** Can you explain why we did not mention multiplexing/demultiplexing services for the application layer?
- Q2-14.** Assume we want to connect two isolated hosts together to let each host communicate with the other. Do we need a link-layer switch between the two? Explain.
- Q2-15.** If there is a single path between the source host and the destination host, do we need a router between the two hosts?

2.5.3 Problems

- P2-1.** Answer the following questions about Figure 2.2 when the communication is from Maria to Ann:
- a.** What is the service provided by layer 1 to layer 2 at Maria's site?
 - b.** What is the service provided by layer 1 to layer 2 at Ann's site?
- P2-2.** Answer the following questions about Figure 2.2 when the communication is from Maria to Ann:
- a.** What is the service provided by layer 2 to layer 3 at Maria's site?
 - b.** What is the service provided by layer 2 to layer 3 at Ann's site?
- P2-3.** Assume that the number of hosts connected to the Internet at year 2010 is five hundred million. If the number of hosts increases only 20 percent per year, what is the number of hosts in year 2020?
- P2-4.** Assume a system uses five protocol layers. If the application program creates a message of 100 bytes and each layer (including the fifth and the first) adds a header of 10 bytes to the data unit, what is the efficiency (the ratio of application-layer bytes to the number of bytes transmitted) of the system?
- P2-5.** Assume we have created a packet-switched internet. Using the TCP/IP protocol suite, we need to transfer a huge file. What are the advantage and disadvantage of sending large packets?
- P2-6.** Match the following to one or more layers of the TCP/IP protocol suite:
- a.** route determination
 - b.** connection to transmission media
 - c.** providing services for the end user
- P2-7.** Match the following to one or more layers of the TCP/IP protocol suite:
- a.** creating user datagrams
 - b.** responsibility for handling frames between adjacent nodes
 - c.** transforming bits to electromagnetic signals
- P2-8.** In Figure 2.10, when the IP protocol decapsulates the transport-layer packet, how does it know to which upper-layer protocol (UDP or TCP) the packet should be delivered?
- P2-9.** Assume a private internet uses three different protocols at the data-link layer (L1, L2, and L3). Redraw Figure 2.10 with this assumption. Can we say that,

in the data-link layer, we have demultiplexing at the source node and multiplexing at the destination node?

- P2-10.** Assume that a private internet requires that the messages at the application layer be encrypted and decrypted for security purposes. If we need to add some information about the encryption/decryption process (such as the algorithms used in the process), does it mean that we are adding one layer to the TCP/IP protocol suite? Redraw the TCP/IP layers (Figure 2.4 part b) if you think so.
- P2-11.** Protocol layering can be found in many aspects of our lives such as air traveling. Imagine you make a round-trip to spend some time on vacation at a resort. You need to go through some processes at your city airport before flying. You also need to go through some processes when you arrive at the resort airport. Show the protocol layering for the round trip using some layers such as baggage checking/claiming, boarding/unboarding, takeoff/landing.
- P2-12.** The presentation of data is becoming more and more important in today's Internet. Some people argue that the TCP/IP protocol suite needs to add a new layer to take care of the presentation of data. If this new layer is added in the future, where should its position be in the suite? Redraw Figure 2.4 to include this layer.
- P2-13.** In an internet, we change the LAN technology to a new one. Which layers in the TCP/IP protocol suite need to be changed?
- P2-14.** Assume that an application-layer protocol is written to use the services of UDP. Can the application-layer protocol use the services of TCP without change?
- P2-15.** Using the internet in Figure 1.11 (Chapter 1) in the text, show the layers of the TCP/IP protocol suite and the flow of data when two hosts, one on the west coast and the other on the east coast, exchange messages.



The fifth edition of Behrouz Forouzan's ***Data Communications and Networking*** presents a comprehensive and accessible approach to data communications and networking that has made this book a favorite with students and professionals alike. More than 830 figures and 150 tables accompany the text and provide a visual and intuitive opportunity for understanding the material. This unique approach minimizes the need for heavy math content, allowing normally complicated topics to unfold graphically and visually rather than through the presentation of complex formulas.

The new edition has been reorganized to showcase recent developments in the field and minimize or eliminate coverage of deprecated topics. In addition to the updated material included in each chapter, the text now features a chapter on the *peer-to-peer paradigm*, a full chapter on *quality of service (QoS)*, additional coverage of *forward error correction*, coverage of WiMAX, and material on socket-interface programming in Java. The end-of-chapter material has also been significantly enhanced and now includes more than 630 questions, 600 problems, many lab assignments, programming assignments, and online applets that allow students to see problems and protocols in action.

Technologies related to data communications and networking are among the fastest growing in our culture today, and there is no better guide to this rapidly expanding field than Behrouz Forouzan, an author whose visual, student-friendly approach has become a hallmark in computer science instruction.

Be sure to visit the book website at <http://www.mhhe.com/forouzan> for student quizzes, animated PPT lecture slides, applets, programs, student and instructor solutions, and more.

The McGraw-Hill Companies



ISBN 978-0-07-337622-6
MHID 0-07-337622-1

