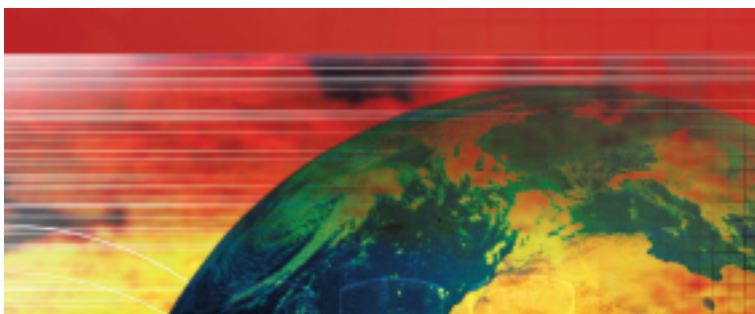
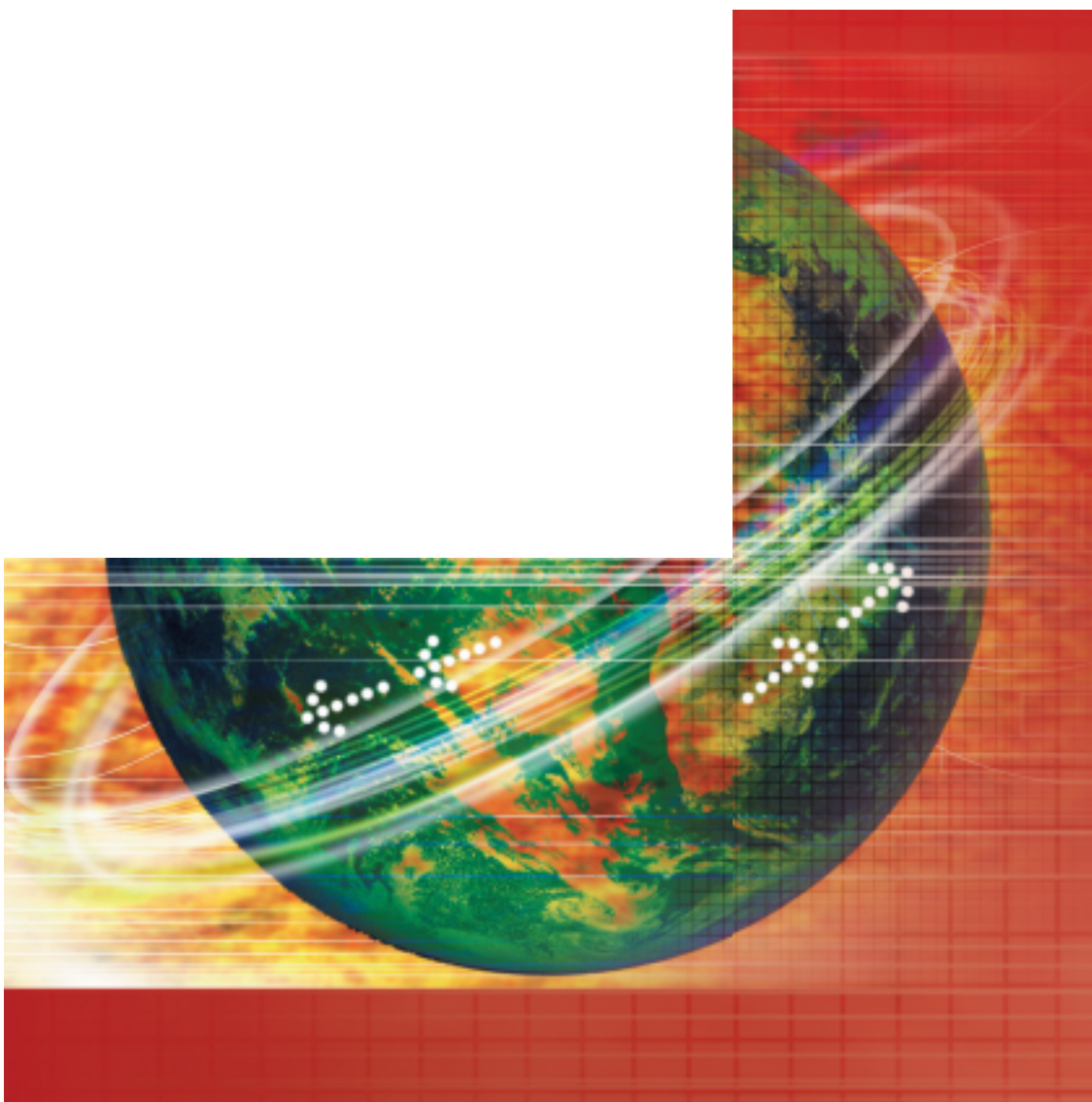


Communications AND Networking

Data

**Communications
AND Networking**



BEHROUZ A. FOROUZAN

Data Communications and Networking

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

F IFTH E DITION

Behrouz A. Forouzan





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.

To my beloved grandson, William.

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*

vii

viii BRIEF CONTENTS

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

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 |

x CONTENTS

ix

| | | |
|-------|-------------------------------------|----|
| 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 *Introduction to Physical Layer* 53

| | | |
|-------|----------------------------|----|
| 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 |

CONTENTS **xi**

| | |
|-------------------------------|----|
| 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

xii CONTENTS

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 *Bandwidth Utilization: Multiplexing and Spectrum Spreading* 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 *Transmission Media* 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 |

CONTENTS **xiii**

| | |
|----------------------------------|------------|
| 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 |

xiv CONTENTS

| | | |
|-------|-----------------------|-----|
| 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 *Error Detection and Correction 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 <i>Media Access Control (MAC)</i> | 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 |

xvi CONTENTS

| | |
|---|------------|
| 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 <i>Wired LANs: Ethernet</i> | 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 |

CONTENTS xvii

| | | |
|--------|------------------------------------|-----|
| 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 |

| | | |
|--|--------------------------------|-----|
| 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 <i>Connecting Devices and Virtual LANs</i> 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 |

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 *Unicast Routing* 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 *Multicast Routing* 639

21.1 INTRODUCTION 640

- 21.1.1 UnICASTING 640
- 21.1.2 Multicasting 640
- 21.1.3 Broadcasting 643

CONTENTS **xxi**

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 *Next Generation IP* 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 Renumbering 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 |

xxii CONTENTS

| | |
|-----------------------------|-----|
| 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 |

CONTENTS xxiii

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 |

xxiv CONTENTS

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 |

CONTENTS **xxv**

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 |

CONTENTS xxvii

| | |
|-----------------------------|------|
| 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 *Cryptography and Network Security 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 *Internet Security 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

T

Technologies related to data communication and networking may be the fastest growing in our culture today. The appearance of some new social networking applications every year is a testimony to this claim. People use the Internet more and more every day. They use the Internet for research, shopping, airline reservations, checking the latest news and weather, and so on.

In this Internet-oriented society, specialists need be trained to run and manage the Internet, part of the Internet, or an organization's network that is connected to the Internet. This book is designed to help students understand the basics of data communications and networking in general and the protocols used in the Internet in particular.

Features

Although the main goal of the book is to teach the principles of networking, it is designed to teach these principles using the following goals:

Protocol Layering

The book is designed to teach the principles of networking by using the protocol layering of the Internet and the TCP/IP protocol suite. Some of the networking principles may have been duplicated in some of these layers, but with their own special details. Teaching these principles using protocol layering is beneficial because these principles are repeated and better understood in relation to each layer. For example, although *addressing* is an issue that is applied to four layers of the TCP/IP suite, each layer uses a different addressing format for different purposes. In addition, addressing has a different domain in each layer. Another example is *framing and packetizing*, which is repeated in several layers, but each layer treats the principle differently.

Bottom-Up Approach

This book uses a bottom-up approach. Each layer in the TCP/IP protocol suite is built on the services provided by the layer below. We learn how bits are moving at the physical layer before learning how some programs exchange messages at the application layer.

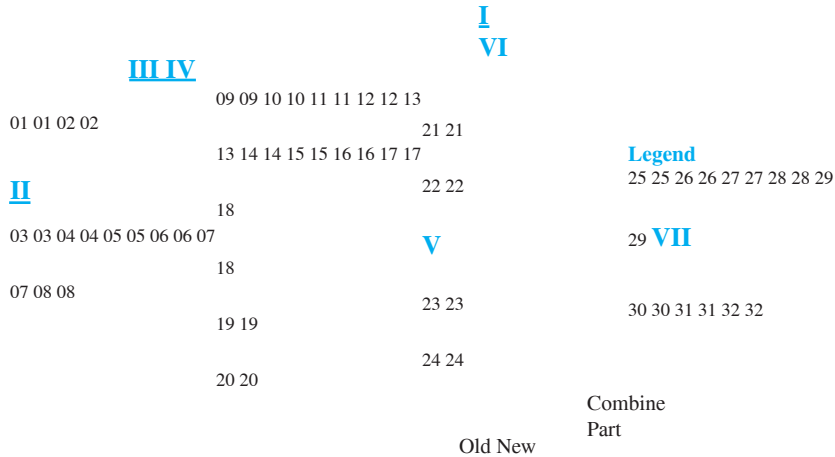
Changes in the Fifth Edition

I have made several categories of changes in this edition.

Changes in the Organization

Although the book is still made of seven parts, the contents and order of chapters have been changed. Some chapters have been combined, some have been moved, some are

new. Sometimes part of a chapter is eliminated because the topic is deprecated. The following shows the relationship between chapters in the fourth and fifth editions.



- ❑ Some chapters have been combined into one chapter. Chapters 9, 17, and 18 are combined into one chapter because some topics in each chapter have been deprecated. Chapters 19 and 21 are combined into Chapter 18. Chapters 25, 26, and 27 are also combined into one chapter because the topics are related to each other. Chapters 30 and 31 are also combined because they cover the same issue.
- ❑ Some chapters have been split into two chapters because of content augmentation. For example, Chapter 22 is split into Chapters 20 and 21.
- ❑ Some chapters have been first combined, but then split for better organization. For example, Chapters 23 and 24 are first combined and then split into two chapters again.
- ❑ Some chapters have been moved to better fit in the organization of the book. Chapter 15 now becomes Chapter 17. Chapters 28 and 29 now become Chapters 27 and 28.
- ❑ Some chapters have been moved to fit better in the sequence. For example, Chapter 15 has become Chapter 17 to cover more topics.
- ❑ Some chapters are new. Chapter 9 is an introduction to the data-link layer. Chapter 25 is an introduction to the application layer and includes socket-interface programming in C and Java. Chapter 30 is almost new. It covers QoS, which was part of other chapters in the previous edition.

New and Augmented Materials

Although the contents of each chapter have been updated, some new materials have also been added to this edition:

- ❑ *Peer-to-Peer paradigm* has been added as a new chapter (Chapter 29).
- ❑ *Quality of service* (QoS) has been augmented and added as a new chapter (Chapter 30).
- ❑ Chapter 10 is augmented to include the *forward error correction*. ❑ WiMAX, as the wireless access network, has been added to Chapter 16. ❑ The coverage of the transport-layer protocol has been augmented (Chapter 23). ❑ Socket-interface programming in Java has been added to Chapter 25. ❑ Chapter 28, on multimedia, has been totally revised and augmented.
- ❑ Contents of unicast and multicast routing (Chapters 20 and 21) have gone through a major change and have been augmented.
- ❑ The next generation IP is augmented and now belongs to Chapter 22.

Changes in the End-Chapter Materials

The end-chapter materials have gone through a major change:

- ❑ The practice set is augmented; it has many new problems in some appropriate chapters.
- ❑ Lab assignments have been added to some chapters to allow students to see some data in motion.
- ❑ Some applets have been posted on the book website to allow students to see some problems and protocols in action.
- ❑ Some programming assignments allow the students to write some programs to solve problems.

Extra Materials

Some extra materials, which could not be fit in the contents and volume of the book, have been posted on the book website for further study.

New Organization

This edition is divided into seven parts, which reflects the structure of the Internet model.

Part One: Overview

The first part gives a general overview of data communications and networking. Chapter 1 covers introductory concepts needed for the rest of the book. Chapter 2 introduces

the Internet model.

Part Two: Physical Layer

The second part is a discussion of the physical layer of the Internet model. It is made of six chapters. Chapters 3 to 6 discuss telecommunication aspects of the physical layer.

xxxiii *PREFACE*

Chapter 7 introduces the transmission media, which, although not part of the physical layer, is controlled by it. Chapter 8 is devoted to switching, which can be used in several layers.

Part Three: Data-Link Layer

The third part is devoted to the discussion of the data-link layer of the Internet model. It is made of nine chapters. Chapter 9 introduces the data-link layer. Chapter 10 covers error detection and correction, which can also be used in some other layers. Chapters 11 and 12 discuss issues related to two sublayers in the data-link layer. Chapters 13 and 14 discuss wired networks. Chapters 15 and 16 discuss wireless networks. Chapter 17 shows how networks can be combined to create larger or virtual networks.

Part Four: Network Layer

The fourth part is devoted to the discussion of the network layer of the Internet model. Chapter 18 introduces this layer and discusses the network-layer addressing. Chapter 19 discusses the protocols in the current version. Chapters 20 and 21 are devoted to routing (unicast and multicast). Chapter 22 introduces the next generation protocol.

Part Five: Transport Layer

The fifth part is devoted to the discussion of the transport layer of the Internet model. Chapter 23 gives an overview of the transport layer and discusses the services and duties of this layer. Chapter 24 discusses the transport-layer protocols in the Internet: UDP, TCP, and SCTP.

Part Six: Application Layer

Chapter 25 introduces the application layer and discusses some network programming in both C and Java. Chapter 26 discusses most of the standard client-server programming in the Internet. Chapter 27 discusses network management. Chapter 28 is devoted to the multimedia, an issue which is very hot today. Finally, Chapter 29 is an introduction to the peer-to-peer paradigm, a trend which is on the rise in the today's Internet.

Part Seven: Topics Related to All Layers

The last part of the book discusses the issues that belong to some or all layers. Chapter 30 discusses the quality of service. Chapters 31 and 32 discuss security.

Appendices

The appendices (available online at <http://www.mhhe.com/forouzan>) are intended to

provide a quick reference or review of materials needed to understand the concepts discussed in the book. There are eight appendices that can be used by the students for reference and study:

- ❑ 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

PREFACE xxxiii

- ❑ Appendix F: 8B/6T Code
- ❑ Appendix G: Miscellaneous Information
- ❑ Appendix H: Telephone History

References

The book contains a list of references for further reading.

Glossary and Acronyms

The book contains an extensive glossary and a list of acronyms for finding the corresponding term quickly.

Pedagogy

Several pedagogical features of this text are designed to make it particularly easy for students to understand data communication and networking.

Visual Approach

The book presents highly technical subject matter without complex formulas by using a balance of text and figures. More than 830 figures accompanying the text provide a visual and intuitive opportunity for understanding the material. Figures are particularly important in explaining networking concepts. For many students, these concepts are more easily grasped visually than verbally.

Highlighted Points

I have repeated important concepts in boxes for quick reference and immediate attention.

Examples and Applications

Whenever appropriate, I have included examples that illustrate the concepts introduced in the text. Also, I have added some real-life applications throughout each chapter to motivate students.

End-of-Chapter Materials

Each chapter ends with a set of materials that includes the following:

Key Terms

The new terms used in each chapter are listed at the end of the chapter and their definitions are included in the glossary.

Recommended Reading

This section gives a brief list of references relative to the chapter. The references can be used to quickly find the corresponding literature in the reference section at the end of the book.

Summary

Each chapter ends with a summary of the material covered by that chapter. The summary glues the important materials together to be seen in one shot.

xxxiv PREFACE

Practice Set

Each chapter includes a practice set designed to reinforce salient concepts and encourage students to apply them. It consists of three parts: quizzes, questions, and problems.

Quizzes

Quizzes, which are posted on the book website, provide quick concept checking. Students can take these quizzes to check their understanding of the materials. The feedback to the students' responses is given immediately.

Questions

This section contains simple questions about the concepts discussed in the book. Answers to the odd-numbered questions are posted on the book website to be checked by the student. There are more than 630 questions at the ends of chapters.

Problems

This section contains more difficult problems that need a deeper understanding of the materials discussed in the chapter. I strongly recommend that the student try to solve all of these problems. Answers to the odd-numbered problems are also posted on the book website to be checked by the student. There are more than 600 problems at the ends of chapters.

Simulation Experiments

Network concepts and the flow and contents of the packets can be better understood if they can be analyzed in action. Some chapters include a section to help students experiment with these. This section is divided into two parts: applets and lab assignments.

Applets

Java applets are interactive experiments that are created by the authors and posted on the website. Some of these applets are used to better understand the solutions to some problems; others are used to better understand the network concepts in action.

Lab Assignments

Some chapters include lab assignments that use Wireshark simulation software. The instructions for downloading and using Wireshark are given in Chapter 1. In some other chapters, there are a few lab assignments that can be used to practice sending and receiving packets and analyzing their contents.

Programming Assignments

Some chapters also include programming assignments. Writing a program about a process or procedure clarifies many subtleties and helps the student better understand the concept behind the process. Although the student can write and test programs in any computer language she or he is comfortable with, the solutions are given in Java language at the book website for the use of professors.

PREFACE **xxxv**

Audience

This book is written for both academic and professional audiences. The book can be used as a self-study guide for interested professionals. As a textbook, it can be used for a one-semester or one-quarter course. It is designed for the last year of undergraduate study or the first year of graduate study. Although some problems at the end of the chapters require some knowledge of probability, the study of the text needs only general mathematical knowledge taught in the first year of college.

Instruction Resources

The book contains complete instruction resources that can be downloaded from the book site <http://www.mhhe.com/forouzan>. They include:

Presentations

The site includes a set of colorful and animated PowerPoint presentations for teaching the course.

Solutions to Practice Set

Solutions to all questions and problems are provided on the book website for the use of professors who teach the course.

Solution to Programming Assignments

Solutions to programming assignments are also provided on the book website. The programs are mostly in Java language.

Student Resources

The book contains complete student resources that can be downloaded from the book website <http://www.mhhe.com/forouzan>. They include:

Quizzes

There are quizzes at the end of each chapter that can be taken by the students. Students are encouraged to take these quizzes to test their general understanding of the materials presented in the corresponding chapter.

Solution to Odd-Numbered Practice Set

Solutions to all odd-numbered questions and problems are provided on the book web site for the use of students.

Lab Assignments

The descriptions of lab assignments are also included in the student resources.

Applets

There are some applets for each chapter. Applets can either show the solution to some examples and problems or show some protocols in action. It is strongly recommended that students activate these applets.

Extra Materials

Students can also access the extra materials at the book website for further study.

xxxvi PREFACE

How to Use the Book

The chapters in the book are organized to provide a great deal of flexibility. I suggest the following:

- ❑ Materials provided in Part I are essential for understanding the rest of the book. ❑ Part II (physical layer) is essential to understand the rest of the book, but the professor can skip this part if the students already have the background in engineering and the physical layer.
- ❑ Parts III to VI are based on the Internet model. They are required for understanding the use of the networking principle in the Internet.
- ❑ Part VII (QoS and Security) is related to all layers of the Internet mode. It can be partially or totally skipped if the students will be taking a course that covers these materials.

Website

The McGraw-Hill website contains much additional material, available at www.mhhe.com/forouzan. As students read through *Data Communications and Networking*, they can go online to take self-grading quizzes. They can also access lecture

materials such as PowerPoint slides, and get additional review from animated figures from the book. Selected solutions are also available over the Web. The solutions to odd numbered problems are provided to students, and instructors can use a password to access the complete set of solutions.

McGraw-Hill Create™

Craft your teaching resources to match the way you teach! With McGraw-Hill Create, www.mcgrawhillcreate.com, you can easily rearrange chapters, combine material from other content sources, and quickly upload content you have written like your course syllabus or teaching notes. Find the content you need in Create by searching through thousands of leading McGraw-Hill textbooks. Arrange your book to fit your teaching style. Create even allows you to personalize your book's appearance by selecting the cover and adding your name, school, and course information. Order a Create book and you'll receive a complimentary print review copy in 3–5 business days or a complimentary electronic review copy (eComp) via email in minutes. Go to www.mcgrawhillcreate.com today and register to experience how McGraw-Hill Create empowers you to teach *your* students *your* way.

Electronic Textbook Option

This text is offered through CourseSmart for both instructors and students. CourseSmart is an online resource where students can purchase the complete text online at almost half the cost of a traditional text. Purchasing the eTextbook allows students to take advantage of CourseSmart's web tools for learning, which include full text search, notes and high lighting, and email tools for sharing notes between classmates. To learn more about CourseSmart options, contact your sales representative or visit www.CourseSmart.com.

PREFACE xxxvii

Acknowledgments

It is obvious that the development of a book of this scope needs the support of many people. I would like to acknowledge the contributions from peer reviewers to the development of the book. These reviewers are:

Tricha Anjali, Illinois Institute of Technology
Yoris A. Au, University of Texas at San Antonio
Randy J. Fortier, University of Windsor
Tirthankar Ghosh, Saint Cloud State University
Lawrence Hill, Rochester Institute of Technology
Ezzat Kirmani, Saint Cloud State University
Robert Koeneke, University of Central Florida
Mike O'Dell, University of Texas at Arlington

Special thanks go to the staff of McGraw-Hill. Raghu Srinivasan, the publisher, proved how a proficient publisher can make the impossible, possible. Melinda Bilecki,

the developmental editor, gave help whenever I needed it. Jane Mohr, the project manager, guided us through the production process with enormous enthusiasm. I also thank Dheeraj Chahal, full-service project manager, Brenda A. Rolwes, the cover designer, and Kathryn DiBernardo, the copy editor.

Behrouz A. Forouzan
Los Angeles, CA.
January 2012

T

hroughout the text we have used several trademarks. Rather than insert a trademark symbol with each mention of the trademark name, we acknowledge the trademarks

here and state that they are used with no intention of infringing upon them. Other product names, trademarks, and registered trademarks are the property of their respective owners.

Overview

In the first part of the book, we discuss some general ideas related to both data communications and networking. This part lays the plan for the rest of the book. The part is made of two chapters that prepare the reader for the long journey ahead.

Chapter 1 Introduction

Chapter 2 Network Models

Introduction

D

ata communications and networking have changed the way we do business and the way we live. Business decisions have to be made ever more quickly, and the deci

sion makers require immediate access to accurate information. Why wait a week for that report from Europe to arrive by mail when it could appear almost instantaneously through computer networks? Businesses today rely on computer networks and internet works.

Data communication and networking have found their way not only through business and personal communication, they have found many applications in political and social issues. People have found how to communicate with other people in the world to express their social and political opinions and problems. Communities in the world are not isolated anymore.

But before we ask how quickly we can get hooked up, we need to know how networks operate, what types of technologies are available, and which design best fills which set of needs.

This chapter paves the way for the rest of the book. It is divided into five sections.

- ❑ The first section introduces data communications and defines their components and the types of data exchanged. It also shows how different types of data are represented and how data is flowed through the network.
- ❑ The second section introduces networks and defines their criteria and structures. It introduces four different network topologies that are encountered throughout the book.
- ❑ The third section discusses different types of networks: LANs, WANs, and inter networks (internets). It also introduces the Internet, the largest internet in the world. The concept of switching is also introduced in this section to show how small networks can be combined to create larger ones.
- ❑ The fourth section covers a brief history of the Internet. The section is divided into three eras: early history, the birth of the Internet, and the issues related to the Internet today. This section can be skipped if the reader is familiar with this history.
- ❑ The fifth section covers standards and standards organizations. The section covers

Internet standards and Internet administration. We refer to these standards and organizations throughout the book.

1.1 DATA COMMUNICATIONS

When we communicate, we are sharing information. This sharing can be local or remote. Between individuals, local communication usually occurs face to face, while remote communication takes place over distance. The term *telecommunication*, which includes telephony, telegraphy, and television, means communication at a distance (*tele* is Greek for “far”). The word *data* refers to information presented in whatever form is agreed upon by the parties creating and using the data.

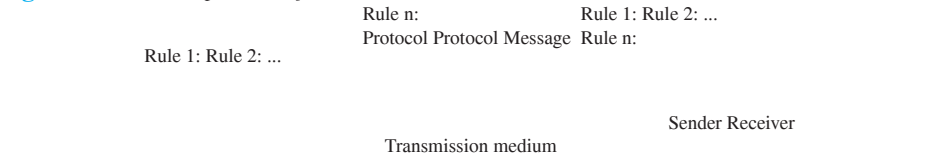
Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

- 1. **Delivery.** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
- 2. **Accuracy.** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
- 3. **Timeliness.** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called *real-time* transmission.
- 4. **Jitter.** Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 ms. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

1.1.1 Components

A data communications system has five components (see Figure 1.1).

Figure 1.1 Five components of data communication



1. Message. The **message** is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video. **2. Sender.** The **sender** is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

CHAPTER 1 INTRODUCTION 5

- 3. Receiver.** The **receiver** is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
- 4. Transmission medium.** The **transmission medium** is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
- 5. Protocol.** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

1.1.2 Data Representation

Information today comes in different forms such as text, numbers, images, audio, and video.

Text

In data communications, text is represented as a bit pattern, a sequence of bits (0s or 1s). Different sets of bit patterns have been designed to represent text symbols. Each set is called a **code**, and the process of representing symbols is called coding. Today, the prevalent coding system is called **Unicode**, which uses 32 bits to represent a symbol or character used in any language in the world. The **American Standard Code for Information Interchange (ASCII)**, developed some decades ago in the United States, now constitutes the first 127 characters in Unicode and is also referred to as **Basic Latin**. Appendix A includes part of the Unicode.

Numbers

Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations. Appendix B discusses several different numbering systems.

Images

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot. The size of the pixel depends on the *resolution*. For example, an image can be divided into 1000 pixels or 10,000 pixels. In the second case, there is a better representation of the image (better

resolution), but more memory is needed to store the image.

After an image is divided into pixels, each pixel is assigned a bit pattern. The size and the value of the pattern depend on the image. For an image made of only black and-white dots (e.g., a chessboard), a 1-bit pattern is enough to represent a pixel.

If an image is not made of pure white and pure black pixels, we can increase the size of the bit pattern to include gray scale. For example, to show four levels of gray scale, we can use 2-bit patterns. A black pixel can be represented by 00, a dark gray pixel by 01, a light gray pixel by 10, and a white pixel by 11.

There are several methods to represent color images. One method is called **RGB**, so called because each color is made of a combination of three primary colors: red, green, and blue. The intensity of each color is measured, and a bit pattern is assigned to

6 PART I OVERVIEW

it. Another method is called **YCM**, in which a color is made of a combination of three other primary colors: yellow, cyan, and magenta.

Audio

Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete. Even when we use a microphone to change voice or music to an electric signal, we create a continuous signal. We will learn more about audio in Chapter 26.

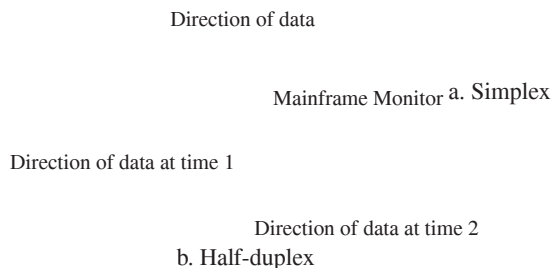
Video

Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion. We will learn more about video in Chapter 26.

1.1.3 Data Flow

Communication between two devices can be simplex, half-duplex, or full-duplex as shown in Figure 1.2.

Figure 1.2 Data flow (simplex, half-duplex, and full-duplex)



Direction of data all the time

c. Full-duplex

Simplex

In **simplex mode**, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive (see Figure 1.2a). Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

CHAPTER 1 INTRODUCTION 7

Half-Duplex

In **half-duplex mode**, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa (see Figure 1.2b). The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

Full-Duplex

In **full-duplex mode** (also called *duplex*), both stations can transmit and receive simultaneously (see Figure 1.2c).

The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions.

One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.

The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

1.2 NETWORKS

A **network** is the interconnection of a set of devices capable of communication. In this definition, a device can be a **host** (or an *end system* as it is sometimes called) such as a large computer, desktop, laptop, workstation, cellular phone, or security system. A device in this definition can also be a **connecting device** such as a router, which connects the network to other networks, a switch, which connects devices together, a modem (modulator-demodulator), which changes the form of data, and so on. These devices in a network are connected using wired or wireless transmission media such as cable or air. When we connect two computers at home using a plug-and-play router, we have created a network, although very small.

1.2.1 Network Criteria

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

8 PART I OVERVIEW

Performance

Performance can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

Performance is often evaluated by two networking metrics: **throughput** and **delay**. We often need more throughput and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

Reliability

In addition to accuracy of delivery, network **reliability** is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

Security

Network **security** issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

1.2.2 Physical Structures

Before discussing networks, we need to define some network attributes.

Type of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections: point-to-point and multipoint.

Point-to-Point

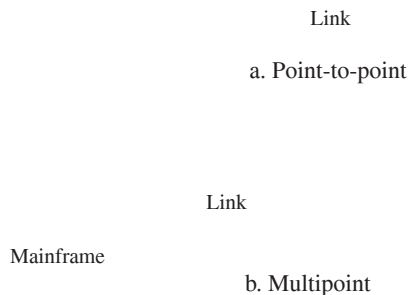
A **point-to-point connection** provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible (see Figure 1.3a). When we change television channels by infrared remote control, we are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint

A **multipoint** (also called **multidrop**) **connection** is one in which more than two specific devices share a single link (see Figure 1.3b).

CHAPTER 1 INTRODUCTION 9

Figure 1.3 Types of connections: point-to-point and multipoint



In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a *spatially shared* connection. If users must take turns, it is a *timeshared* connection.

Physical Topology

The term **physical topology** refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called **nodes**) to one another. There are four basic

topologies possible: mesh, star, bus, and ring.

Mesh Topology

In a **mesh topology**, every device has a dedicated point-to-point link to every other device. The term *dedicated* means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to $n - 1$ nodes, node 2 must be connected to $n - 1$ nodes, and finally node n must be connected to $n - 1$ nodes. We need $n(n - 1)$ physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need $n(n - 1) / 2$ duplex-mode links. To accommodate that many links, every device on the network must have $n - 1$ input/output (I/O) ports (see Figure 1.4) to be connected to the other $n - 1$ stations.

A mesh offers several advantages over other network topologies. First, the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices. Second, a mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system. Third, there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages. Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

10 PART I OVERVIEW

Figure 1.4 *A fully connected mesh topology (five devices)*

$n = 5$
10 links.

The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required. First, because every device must be connected to every other device, installation and reconnection are difficult. Second, the sheer bulk of the

wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate. Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive. For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.

One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Star Topology

In a **star topology**, each device has a dedicated point-to-point link only to a central controller, usually called a **hub**. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device (see Figure 1.5) .

Figure 1.5 *A star topology connecting four stations*

Hub

A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and

CHAPTER 1 INTRODUCTION 11

additions, moves, and deletions involve only one connection: between that device and the hub.

Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead. Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

The star topology is used in local-area networks (LANs), as we will see in Chapter 13. High-speed LANs often use a star topology with a central hub.

Bus Topology

The preceding examples all describe point-to-point connections. A **bus topology**, on the other hand, is multipoint. One long cable acts as a **backbone** to link all the devices in a network (see Figure 1.6).

Figure 1.6 *A bus topology connecting three stations*

Drop line Drop line Drop line
Cable end Cable end Tap Tap Tap

Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given

12 PART I OVERVIEW

length of cable. Adding new devices may therefore require modification or replacement of the backbone.

In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

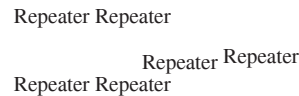
Bus topology was the one of the first topologies used in the design of early local area networks. Traditional Ethernet LANs can use a bus topology, but they are less popular now for reasons we will discuss in Chapter 13.

Ring Topology

In a **ring topology**, each device has a dedicated point-to-point connection with only the

two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along (see Figure 1.7).

Figure 1.7 *A ring topology connecting six stations*



Repeater Repeater
Repeater Repeater
Repeater Repeater

A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally, in a ring a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Ring topology was prevalent when IBM introduced its local-area network, Token Ring. Today, the need for higher-speed LANs has made this topology less popular.

CHAPTER 1 INTRODUCTION 13

1.3 NETWORK TYPES

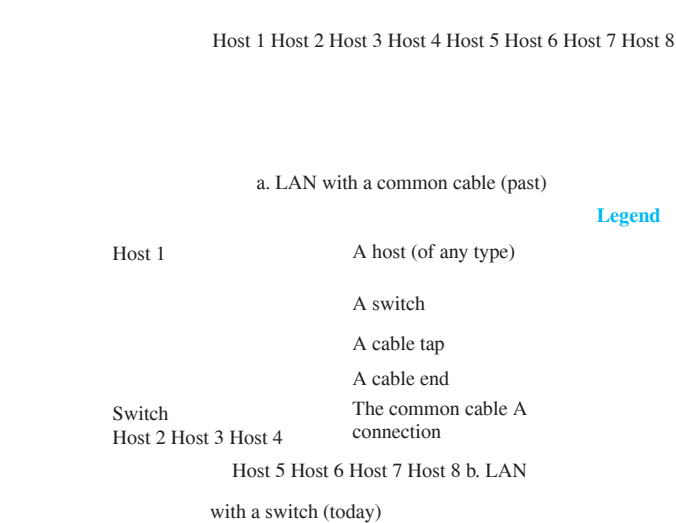
After defining networks in the previous section and discussing their physical structures, we need to discuss different types of networks we encounter in the world today. The criteria of distinguishing one type of network from another is difficult and sometimes confusing. We use a few criteria such as size, geographical coverage, and ownership to make this distinction. After discussing two types of networks, LANs and WANs, we define switching, which is used to connect networks to form an internetwork (a network of networks).

1.3.1 Local Area Network

A **local area network (LAN)** is usually privately owned and connects some hosts in a single office, building, or campus. Depending on the needs of an organization, a LAN can be as simple as two PCs and a printer in someone’s home office, or it can extend throughout a company and include audio and video devices. Each host in a LAN has an identifier, an address, that uniquely defines the host in the LAN. A packet sent by a host to another host carries both the source host’s and the destination host’s addresses.

In the past, all hosts in a network were connected through a common cable, which meant that a packet sent from one host to another was received by all hosts. The intended recipient kept the packet; the others dropped the packet. Today, most LANs use a smart connecting switch, which is able to recognize the destination address of the packet and guide the packet to its destination without sending it to all other hosts. The switch alleviates the traffic in the LAN and allows more than one pair to communicate with each other at the same time if there is no common source and destination among them. Note that the above definition of a LAN does not define the minimum or maximum number of hosts in a LAN. Figure 1.8 shows a LAN using either a common cable or a switch.

Figure 1.8 *An isolated LAN in the past and today*



LANs are discussed in more detail in Part III of the book.

When LANs were used in isolation (which is rare today), they were designed to allow resources to be shared between the hosts. As we will see shortly, LANs today are connected to each other and to WANs (discussed next) to create communication at a

wider level.

1.3.2 Wide Area Network

A **wide area network (WAN)** is also an interconnection of devices capable of communication. However, there are some differences between a LAN and a WAN. A LAN is normally limited in size, spanning an office, a building, or a campus; a WAN has a wider geographical span, spanning a town, a state, a country, or even the world. A LAN interconnects hosts; a WAN interconnects connecting devices such as switches, routers, or modems. A LAN is normally privately owned by the organization that uses it; a WAN is normally created and run by communication companies and leased by an organization that uses it. We see two distinct examples of WANs today: point-to-point WANs and switched WANs.

Point-to-Point WAN

A point-to-point WAN is a network that connects two communicating devices through a transmission media (cable or air). We will see examples of these WANs when we discuss how to connect the networks to one another. Figure 1.9 shows an example of a point-to-point WAN.

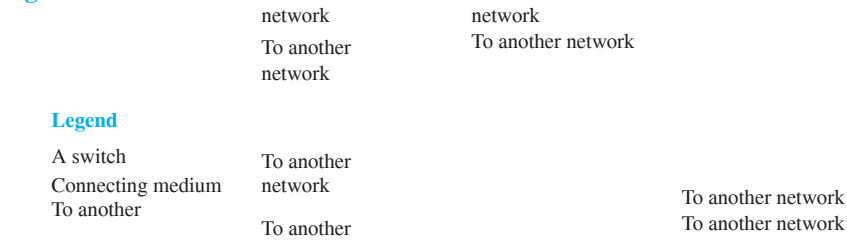
Figure 1.9 *A point-to-point WAN*



Switched WAN

A switched WAN is a network with more than two ends. A switched WAN, as we will see shortly, is used in the backbone of global communication today. We can say that a switched WAN is a combination of several point-to-point WANs that are connected by switches. Figure 1.10 shows an example of a switched WAN.

Figure 1.10 *A switched WAN*

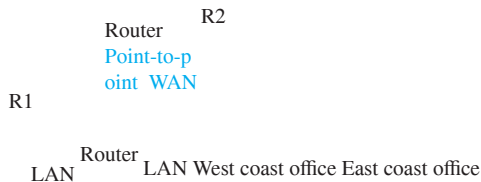


WANs are discussed in more detail in Part II of the book.

Internetwork

Today, it is very rare to see a LAN or a WAN in isolation; they are connected to one another. When two or more networks are connected, they make an **internetwork**, or **internet**. As an example, assume that an organization has two offices, one on the east coast and the other on the west coast. Each office has a LAN that allows all employees in the office to communicate with each other. To make the communication between employees at different offices possible, the management leases a point-to-point dedicated WAN from a service provider, such as a telephone company, and connects the two LANs. Now the company has an internetwork, or a private internet (with lowercase *i*). Communication between offices is now possible. Figure 1.11 shows this internet.

Figure 1.11 *An internetwork made of two LANs and one point-to-point WAN*



When a host in the west coast office sends a message to another host in the same office, the router blocks the message, but the switch directs the message to the destination. On the other hand, when a host on the west coast sends a message to a host on the east coast, router R1 routes the packet to router R2, and the packet reaches the destination.

Figure 1.12 (see next page) shows another internet with several LANs and WANs connected. One of the WANs is a switched WAN with four switches.

1.3.3 Switching

An internet is a **switched network** in which a switch connects at least two links together. A switch needs to forward data from a network to another network when required. The two most common types of switched networks are circuit-switched and packet-switched networks. We discuss both next.

Circuit-Switched Network

In a **circuit-switched network**, a dedicated connection, called a circuit, is always available between the two end systems; the switch can only make it active or inactive. Figure 1.13 shows a very simple switched network that connects four telephones to each end. We have used telephone sets instead of computers as an end system because circuit switching was very common in telephone networks in the past, although part of the telephone network today is a packet-switched network.

In Figure 1.13, the four telephones at each side are connected to a switch. The switch connects a telephone set at one side to a telephone set at the other side. The thick

16 PART I OVERVIEW

Figure 1.12 *A heterogeneous network made of four WANs and three LANs*

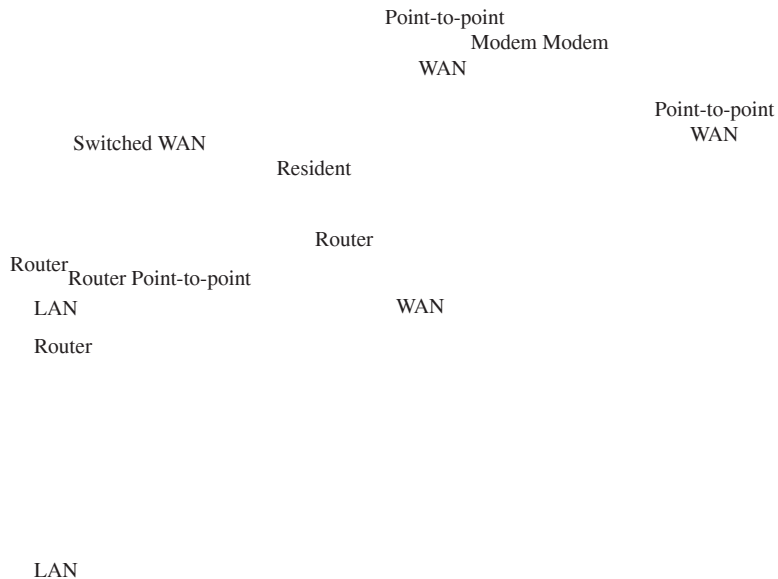


Figure 1.13 *A circuit-switched network*

Low-capacity line
High-capacity line

Switch Switch

line connecting two switches is a high-capacity communication line that can handle four voice communications at the same time; the capacity can be shared between all pairs of telephone sets. The switches used in this example have forwarding tasks but no storing capability.

Let us look at two cases. In the first case, all telephone sets are busy; four people at one site are talking with four people at the other site; the capacity of the thick line is fully used. In the second case, only one telephone set at one side is connected to a telephone set at the other side; only one-fourth of the capacity of the thick line is used. This means that a circuit-switched network is efficient only when it is working at its full capacity; most of the time, it is inefficient because it is working at partial capacity. The reason that we need to make the capacity of the thick line four times the capacity of each voice line is that we do not want communication to fail when all telephone sets at one side want to be connected with all telephone sets at the other side.

CHAPTER 1 INTRODUCTION 17

Packet-Switched Network

In a computer network, the communication between the two ends is done in blocks of data called **packets**. In other words, instead of the continuous communication we see between two telephone sets when they are being used, we see the exchange of individual data packets between the two computers. This allows us to make the switches function for both storing and forwarding because a packet is an independent entity that can be stored and sent later. Figure 1.14 shows a small packet-switched network that connects four computers at one site to four computers at the other site.

Figure 1.14 *A packet-switched network*

Low-capacity line
High-capacity line
Queue Queue
Router

Router

A router in a packet-switched network has a queue that can store and forward the packet. Now assume that the capacity of the thick line is only twice the capacity of the data line connecting the computers to the routers. If only two computers (one at each site) need to communicate with each other, there is no waiting for the packets. However, if packets arrive at one router when the thick line is already working at its full capacity, the packets should be stored and forwarded in the order they arrived. The two simple examples show that a packet-switched network is more efficient than a circuit switched network, but the packets may encounter some delays.

In this book, we mostly discuss packet-switched networks. In Chapter 18, we discuss packet-switched networks in more detail and discuss the performance of these networks.

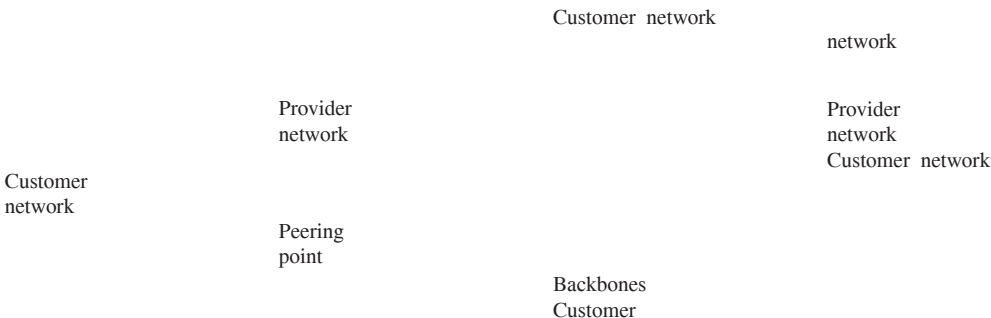
1.3.4 The Internet

As we discussed before, an internet (note the lowercase *i*) is two or more networks that can communicate with each other. The most notable internet is called the **Internet** (uppercase *I*), and is composed of thousands of interconnected networks. Figure 1.15 shows a conceptual (not geographical) view of the Internet.

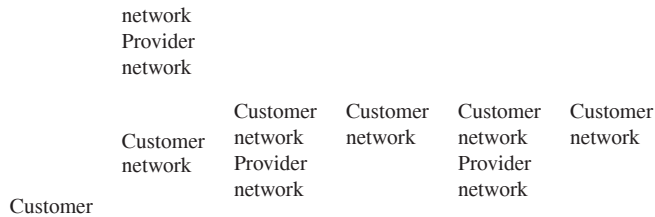
The figure shows the Internet as several backbones, provider networks, and customer networks. At the top level, the *backbones* are large networks owned by some communication companies such as Sprint, Verizon (MCI), AT&T, and NTT. The backbone networks are connected through some complex switching systems, called *peering points*. At the second level, there are smaller networks, called *provider networks*, that use the services of the backbones for a fee. The provider networks are connected to backbones and sometimes to other provider networks. The *customer networks* are

18 PART I OVERVIEW

Figure 1.15 *The Internet today*



Peering



networks at the edge of the Internet that actually use the services provided by the Internet. They pay fees to provider networks for receiving services.

Backbones and provider networks are also called **Internet Service Providers (ISPs)**. The backbones are often referred to as *international ISPs*; the provider networks are often referred to as *national* or *regional ISPs*.

1.3.5 Accessing the Internet

The Internet today is an internetwork that allows any user to become part of it. The user, however, needs to be physically connected to an ISP. The physical connection is normally done through a point-to-point WAN. In this section, we briefly describe how this can happen, but we postpone the technical details of the connection until Chapters 14 and 16.

Using Telephone Networks

Today most residences and small businesses have telephone service, which means they are connected to a telephone network. Since most telephone networks have already connected themselves to the Internet, one option for residences and small businesses to connect to the Internet is to change the voice line between the residence or business and the telephone center to a point-to-point WAN. This can be done in two ways.

- ❑ **Dial-up service.** The first solution is to add to the telephone line a modem that converts data to voice. The software installed on the computer dials the ISP and imitates making a telephone connection. Unfortunately, the dial-up service is

CHAPTER 1 INTRODUCTION 19

very slow, and when the line is used for Internet connection, it cannot be used for telephone (voice) connection. It is only useful for small residences. We discuss dial-up service in Chapter 14.

- ❑ **DSL Service.** Since the advent of the Internet, some telephone companies have upgraded their telephone lines to provide higher speed Internet services to residences or small businesses. The DSL service also allows the line to be used simultaneously for voice and data communication. We discuss DSL in Chapter 14.

Using Cable Networks

More and more residents over the last two decades have begun using cable TV services instead of antennas to receive TV broadcasting. The cable companies have been upgrading their cable networks and connecting to the Internet. A residence or a small business can be connected to the Internet by using this service. It provides a higher speed connection, but the speed varies depending on the number of neighbors that use the same cable. We discuss the cable networks in Chapter 14.

Using Wireless Networks

Wireless connectivity has recently become increasingly popular. A household or a small business can use a combination of wireless and wired connections to access the Internet. With the growing wireless WAN access, a household or a small business can be connected to the Internet through a wireless WAN. We discuss wireless access in Chapter 16.

Direct Connection to the Internet

A large organization or a large corporation can itself become a local ISP and be connected to the Internet. This can be done if the organization or the corporation leases a high-speed WAN from a carrier provider and connects itself to a regional ISP. For example, a large university with several campuses can create an internetwork and then connect the internetwork to the Internet.

1.4 INTERNET HISTORY

Now that we have given an overview of the Internet, let us give a brief history of the Internet. This brief history makes it clear how the Internet has evolved from a private network to a global one in less than 40 years.

1.4.1 Early History

There were some communication networks, such as telegraph and telephone networks, before 1960. These networks were suitable for constant-rate communication at that time, which means that after a connection was made between two users, the encoded message (telegraphy) or voice (telephony) could be exchanged. A computer network, on the other hand, should be able to handle *bursty* data, which means data received at variable rates at different times. The world needed to wait for the packet-switched network to be invented.

Birth of Packet-Switched Networks

The theory of packet switching for bursty traffic was first presented by Leonard Kleinrock in 1961 at MIT. At the same time, two other researchers, Paul Baran at Rand Institute and Donald Davies at National Physical Laboratory in England, published some papers about packet-switched networks.

ARPANET

In the mid-1960s, mainframe computers in research organizations were stand-alone devices. Computers from different manufacturers were unable to communicate with one another. The **Advanced Research Projects Agency (ARPA)** in the Department of Defense (DOD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.

In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for the **Advanced Research Projects Agency Network (ARPANET)**, a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an *interface message processor* (IMP). The IMPs, in turn, would be connected to each other. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.

By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the *Network Control Protocol* (NCP) provided communication between the hosts.

1.4.2 Birth of the Internet

In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the *Internetworking Project*. They wanted to link dissimilar networks so that a host on one network could communicate with a host on another. There were many problems to overcome: diverse packet sizes, diverse interfaces, and diverse transmission rates, as well as differing reliability requirements. Cerf and Kahn devised the idea of a device called a *gateway* to serve as the intermediary hardware to transfer data from one network to another.

TCP/IP

Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of data. This was a new version of NCP. This paper on transmission control protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway. A radical idea was the transfer of responsibility for error correction from the IMP to the host machine. This ARPA Internet now became the focus of the communication effort. Around this time, responsibility for the ARPANET was handed

over to the Defense Communication Agency (DCA).

In October 1977, an internet consisting of three different networks (ARPANET, packet radio, and packet satellite) was successfully demonstrated. Communication between networks was now possible.

CHAPTER 1 INTRODUCTION 21

Shortly thereafter, authorities made a decision to split TCP into two protocols: **Transmission Control Protocol (TCP)** and **Internet Protocol (IP)**. IP would handle datagram routing while TCP would be responsible for higher level functions such as segmentation, reassembly, and error detection. The new combination became known as TCP/IP.

In 1981, under a Defence Department contract, UC Berkeley modified the UNIX operating system to include TCP/IP. This inclusion of network software along with a popular operating system did much for the popularity of internetworking. The open (non-manufacturer-specific) implementation of the Berkeley UNIX gave every manufacturer a working code base on which they could build their products.

In 1983, authorities abolished the original ARPANET protocols, and TCP/IP became the official protocol for the ARPANET. Those who wanted to use the Internet to access a computer on a different network had to be running TCP/IP.

MILNET

In 1983, ARPANET split into two networks: **Military Network (MILNET)** for military users and ARPANET for nonmilitary users.

CSNET

Another milestone in Internet history was the creation of CSNET in 1981. **Computer Science Network (CSNET)** was a network sponsored by the National Science Foundation (NSF). The network was conceived by universities that were ineligible to join ARPANET due to an absence of ties to the Department of Defense. CSNET was a less expensive network; there were no redundant links and the transmission rate was slower.

By the mid-1980s, most U.S. universities with computer science departments were part of CSNET. Other institutions and companies were also forming their own networks and using TCP/IP to interconnect. The term *Internet*, originally associated with government-funded connected networks, now referred to the connected networks using TCP/IP protocols.

NSFNET

With the success of CSNET, the NSF in 1986 sponsored the **National Science Foundation Network (NSFNET)**, a backbone that connected five supercomputer centers located throughout the United States. Community networks were allowed access to this backbone, a T-1 line (see Chapter 6) with a 1.544-Mbps data rate, thus providing connectivity throughout the United States. In 1990, ARPANET was officially retired and replaced by NSFNET. In 1995, NSFNET reverted back to its original concept of a research network.

ANSNET

In 1991, the U.S. government decided that NSFNET was not capable of supporting the rapidly increasing Internet traffic. Three companies, IBM, Merit, and Verizon, filled the void by forming a nonprofit organization called Advanced Network & Services (ANS) to build a new, high-speed Internet backbone called **Advanced Network Services Network (ANSNET)**.

22 PART I OVERVIEW

1.4.3 Internet Today

Today, we witness a rapid growth both in the infrastructure and new applications. The Internet today is a set of peer networks that provide services to the whole world. What has made the Internet so popular is the invention of new applications.

World Wide Web

The 1990s saw the explosion of Internet applications due to the emergence of the World Wide Web (WWW). The Web was invented at CERN by Tim Berners-Lee. This invention has added the commercial applications to the Internet.

Multimedia

Recent developments in the multimedia applications such as voice over IP (telephony), video over IP (Skype), view sharing (YouTube), and television over IP (PPLive) has increased the number of users and the amount of time each user spends on the network. We discuss multimedia in Chapter 28.

Peer-to-Peer Applications

Peer-to-peer networking is also a new area of communication with a lot of potential. We introduce some peer-to-peer applications in Chapter 29.

1.5 STANDARDS AND ADMINISTRATION

In the discussion of the Internet and its protocol, we often see a reference to a standard or an administration entity. In this section, we introduce these standards and administration entities for those readers that are not familiar with them; the section can be skipped if the reader is familiar with them.

1.5.1 Internet Standards

An **Internet standard** is a thoroughly tested specification that is useful to and adhered to by those who work with the Internet. It is a formalized regulation that must be followed. There is a strict procedure by which a specification attains Internet standard status. A specification begins as an Internet draft. An **Internet draft** is a working document (a work in progress) with no official status and a six-month lifetime. Upon

recommendation from the Internet authorities, a draft may be published as a **Request for Comment (RFC)**. Each RFC is edited, assigned a number, and made available to all interested parties. RFCs go through maturity levels and are categorized according to their requirement level.

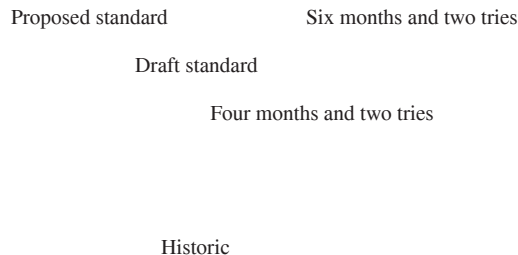
Maturity Levels

An RFC, during its lifetime, falls into one of six *maturity levels*: proposed standard, draft standard, Internet standard, historic, experimental, and informational (see Figure 1.16).

- ❑ **Proposed Standard.** A proposed standard is a specification that is stable, well understood, and of sufficient interest to the Internet community. At this level, the specification is usually tested and implemented by several different groups.

CHAPTER 1 INTRODUCTION 23

Figure 1.16 *Maturity levels of an RFC*



- ❑ **Draft Standard.** A proposed standard is elevated to draft standard status after at least two successful independent and interoperable implementations. Barring difficulties, a draft standard, with modifications if specific problems are encountered, normally becomes an Internet standard.
- ❑ **Internet Standard.** A draft standard reaches Internet standard status after demonstrations of successful implementation.
- ❑ **Historic.** The historic RFCs are significant from a historical perspective. They either have been superseded by later specifications or have never passed the neces

sary maturity levels to become an Internet standard.

- ❑ **Experimental.** An RFC classified as experimental describes work related to an experimental situation that does not affect the operation of the Internet. Such an RFC should not be implemented in any functional Internet service.
- ❑ **Informational.** An RFC classified as informational contains general, historical, or tutorial information related to the Internet. It is usually written by someone in a non-Internet organization, such as a vendor.

Requirement Levels

RFCs are classified into five *requirement levels*: required, recommended, elective, limited use, and not recommended.

- ❑ **Required.** An RFC is labeled *required* if it must be implemented by all Internet systems to achieve minimum conformance. For example, IP and ICMP (Chapter 19) are required protocols.
- ❑ **Recommended.** An RFC labeled recommended is not required for minimum conformance; it is recommended because of its usefulness. For example, FTP (Chapter 26) and TELNET (Chapter 26) are recommended protocols.
- ❑ **Elective.** An RFC labeled elective is not required and not recommended. However, a system can use it for its own benefit.

24 PART I OVERVIEW

- ❑ **Limited Use.** An RFC labeled limited use should be used only in limited situations. Most of the experimental RFCs fall under this category.
- ❑ **Not Recommended.** An RFC labeled not recommended is inappropriate for general use. Normally a historic (deprecated) RFC may fall under this category.

RFCs can be found at <http://www.rfc-editor.org>.

1.5.2 Internet Administration

The Internet, with its roots primarily in the research domain, has evolved and gained a broader user base with significant commercial activity. Various groups that coordinate Internet issues have guided this growth and development. Appendix G gives the addresses, e-mail addresses, and telephone numbers for some of these groups. Figure 1.17 shows the general organization of Internet administration.

Figure 1.17 Internet administration



IRTF IETF

IRSG IESG

Area Area
WG WG WG WG

RG RG
RG RG

ISOC

The **Internet Society (ISOC)** is an international, nonprofit organization formed in 1992 to provide support for the Internet standards process. ISOC accomplishes this through maintaining and supporting other Internet administrative bodies such as IAB, IETF, IRTF, and IANA (see the following sections). ISOC also promotes research and other scholarly activities relating to the Internet.

IAB

The **Internet Architecture Board (IAB)** is the technical advisor to the ISOC. The main purposes of the IAB are to oversee the continuing development of the TCP/IP Protocol Suite and to serve in a technical advisory capacity to research members of the Internet community. IAB accomplishes this through its two primary components, the Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRTF). Another responsibility of the IAB is the editorial management of the RFCs, described

CHAPTER 1 INTRODUCTION **25**

earlier. IAB is also the external liaison between the Internet and other standards organizations and forums.

IETF

The **Internet Engineering Task Force (IETF)** is a forum of working groups managed by the Internet Engineering Steering Group (IESG). IETF is responsible for identifying operational problems and proposing solutions to these problems. IETF also develops and reviews specifications intended as Internet standards. The working groups are collected into areas, and each area concentrates on a specific topic. Currently nine areas have been defined. The areas include applications, protocols, routing, network management next generation (IPng), and security.

IRTF

The **Internet Research Task Force (IRTF)** is a forum of working groups managed by the Internet Research Steering Group (IRSG). IRTF focuses on long-term research topics related to Internet protocols, applications, architecture, and technology.

1.6 END-CHAPTER MATERIALS

1.6.1 Recommended Reading

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

Books

The introductory materials covered in this chapter can be found in [Sta04] and [PD03]. [Tan03] also discusses standardization.

1.6.2 Key Terms

| | |
|--|--|
| Advanced Network Services Network (ANSNET) | full-duplex mode |
| Advanced Research Projects Agency (ARPA) | half-duplex mode |
| Advanced Research Projects Agency Network (ARPANET) | hub |
| American Standard Code for Information Interchange (ASCII) | image |
| audio | internet |
| backbone | Internet |
| Basic Latin | Internet Architecture Board (IAB) |
| bus topology | Internet draft |
| circuit-switched network | Internet Engineering Task Force (IETF) |
| code | Internet Research Task Force (IRTF) |
| Computer Science Network (CSNET) | Internet Service Provider (ISP) |
| data communications | Internet Society (ISOC) |
| delay | Internet standard |
| | internetwork |
| | local area network (LAN) |
| | mesh topology |
| | message |
| | packet-switched network |
| | performance |
| | physical topology |
| | point-to-point connection |
| | protocol |
| | Request for Comment (RFC) |
| | RGB |

26 PART I OVERVIEW

Military Network (MILNET)
multipoint or multidrop connection
National Science Foundation Network (NSFNET)
network
node
packet

1.6.3 Summary

ring topology
simplex mode
star topology
switched network
TCP/IP protocol suite
telecommunication

throughput
Transmission Control Protocol/ Internet Protocol
(TCP/IP)
transmission medium
Unicode
video
wide area network (WAN)
YCM

Data communications are the transfer of data from one device to another via some form of transmission medium. A data communications system must transmit data to the correct destination in an accurate and timely manner. The five components that make up a data communications system are the message, sender, receiver, medium, and protocol. Text, numbers, images, audio, and video are different forms of information. Data flow between two devices can occur in one of three ways: simplex, half-duplex, or full-duplex.

A network is a set of communication devices connected by media links. In a point-to-point connection, two and only two devices are connected by a dedicated link. In a multipoint connection, three or more devices share a link. Topology refers to the physical or logical arrangement of a network. Devices may be arranged in a mesh, star, bus, or ring topology.

A network can be categorized as a local area network or a wide area network. A LAN is a data communication system within a building, plant, or campus, or between nearby buildings. A WAN is a data communication system spanning states, countries, or the whole world. An internet is a network of networks. The Internet is a collection of many separate networks.

The Internet history started with the theory of packet switching for bursty traffic. The history continued when The ARPA was interested in finding a way to connect computers so that the researchers they funded could share their findings, resulting in the creation of ARPANET. The Internet was born when Cerf and Kahn devised the idea of a device called a *gateway* to serve as the intermediary hardware to transfer data from one network to another. The TCP/IP protocol suite paved the way for creation of today's Internet. The invention of WWW, the use of multimedia, and peer-to-peer communication helps the growth of the Internet.

An Internet standard is a thoroughly tested specification. An Internet draft is a working document with no official status and a six-month lifetime. A draft may be published as a Request for Comment (RFC). RFCs go through maturity levels and are categorized according to their requirement level. The Internet administration has

CHAPTER 1 INTRODUCTION 27

evolved with the Internet. ISOC promotes research and activities. IAB is the technical advisor to the ISOC. IETF is a forum of working groups responsible for operational problems. IRTF is a forum of working groups focusing on long-term research topics.

1.7 PRACTICE SET

1.7.1 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.

1.7.2 Questions

Q1-1. Identify the five components of a data communications system. **Q1-2.** What are the three criteria necessary for an effective and efficient network? **Q1-3.** What are the advantages of a multipoint connection over a point-to-point one? **Q1-4.** What are the two types of line configuration?

Q1-5. Categorize the four basic topologies in terms of line configuration. **Q1-6.** What is the difference between half-duplex and full-duplex transmission modes? **Q1-7.** Name the four basic network topologies, and cite an advantage of each type. **Q1-8.** For n devices in a network, what is the number of cable links required for a mesh, ring, bus, and star topology?

Q1-9. What are some of the factors that determine whether a communication system is a LAN or WAN?

Q1-10. What is an internet? What is the Internet?

Q1-11. Why are protocols needed?

Q1-12. In a LAN with a link-layer switch (Figure 1.8b), Host 1 wants to send a message to Host 3. Since communication is through the link-layer switch, does the switch need to have an address? Explain.

Q1-13. How many point-to-point WANs are needed to connect n LANs if each LAN should be able to directly communicate with any other LAN?

Q1-14. When we use local telephones to talk to a friend, are we using a circuit switched network or a packet-switched network?

Q1-15. When a resident uses a dial-up or DLS service to connect to the Internet, what is the role of the telephone company?

Q1-16. What is the first principle we discussed in this chapter for protocol layering that needs to be followed to make the communication bidirectional? **Q1-17.** Explain the difference between an Internet draft and a proposed standard. **Q1-18.** Explain the difference between a required RFC and a recommended RFC. **Q1-19.** Explain the difference between the duties of the IETF and IRTF.

1.7.3 Problems

- P1-1.** What is the maximum number of characters or symbols that can be represented by Unicode?
- P1-2.** A color image uses 16 bits to represent a pixel. What is the maximum number of different colors that can be represented?
- P1-3.** Assume six devices are arranged in a mesh topology. How many cables are needed? How many ports are needed for each device?
- P1-4.** For each of the following four networks, discuss the consequences if a connection fails.
- a.** Five devices arranged in a mesh topology
 - b.** Five devices arranged in a star topology (not counting the hub)
 - c.** Five devices arranged in a bus topology
 - d.** Five devices arranged in a ring topology
- P1-5.** We have two computers connected by an Ethernet hub at home. Is this a LAN or a WAN? Explain the reason.
- P1-6.** In the ring topology in Figure 1.7, what happens if one of the stations is unplugged?
- P1-7.** In the bus topology in Figure 1.6, what happens if one of the stations is unplugged?
- P1-8.** Performance is inversely related to delay. When we use the Internet, which of the following applications are more sensitive to delay?
- a.** Sending an e-mail
 - b.** Copying a file
 - c.** Surfing the Internet
- P1-9.** When a party makes a local telephone call to another party, is this a point-to-point or multipoint connection? Explain the answer.
- P1-10.** Compare the telephone network and the Internet. What are the similarities? What are the differences?

1.8 SIMULATION EXPERIMENTS

1.8.1 Applets

One of the ways to show the network protocols in action or visually see the solution to some examples is through the use of interactive animation. We have created some Java applets to show some of the main concepts discussed in this chapter. It is strongly recommended that the students activate these applets on the book website and carefully examine the protocols in action. However, note that applets have been created only for some chapters, not all (see the book website).

1.8.2 Lab Assignments

Experiments with networks and network equipment can be done using at least two

methods. In the first method, we can create an isolated networking laboratory and use

networking hardware and software to simulate the topics discussed in each chapter. We can create an internet and send and receive packets from any host to another. The flow of packets can be observed and the performance can be measured. Although the first method is more effective and more instructional, it is expensive to implement and not all institutions are ready to invest in such an exclusive laboratory.

In the second method, we can use the Internet, the largest network in the world, as our virtual laboratory. We can send and receive packets using the Internet. The existence of some free-downloadable software allows us to capture and examine the packets exchanged. We can analyze the packets to see how theoretical aspects of networking are put into action. Although the second method may not be as effective as the first method, in that we cannot control and change the packet routes to see how the Internet behaves, the method is much cheaper to implement. It does not need a physical networking lab; it can be implemented using our desktop or laptop. The required software is also free to download.

There are many programs and utilities available for Windows and UNIX operating systems that allow us to sniff, capture, trace, and analyze packets that are exchanged between our computer and the Internet. Some of these, such as *Wireshark* and *Ping Plotter*, have graphical user interface (GUI); others, such as *tracert*, *nslookup*, *dig*, *ipconfig*, and *ifconfig*, are network administration command-line utilities. Any of these programs and utilities can be a valuable debugging tool for network administrators and educational tool for computer network students.

In this book, we mostly use Wireshark for lab assignments, although we occasionally use other tools. It captures live packet data from a network interface and displays them with detailed protocol information. Wireshark, however, is a passive analyzer. It only “measures” things from the network without manipulating them; it doesn’t send packets on the network or perform other active operations. Wireshark is not an intrusion detection tool either. It does not give warning about any network intrusion. It, nevertheless, can help network administrators or network security engineers to figure out what is going on inside a network and to troubleshoot network problems. In addition to being an indispensable tool for network administrators and security engineers, Wireshark is a valuable tool for protocol developers, who may use it to debug protocol implementations, and a great educational tool for computer networking students who can use it to see details of protocol operations in real time. However, note that we can use lab assignments only with a few chapters.

Lab1-1. In this lab assignment we learn how to download and install Wireshark. The instructions for downloading and installing the software are posted on the book website in the lab section for Chapter 1. In this document, we also discuss the general idea behind the software, the format of its window, and how to use it. The full study of this lab prepares the student to use Wireshark in the lab assignments for other chapters.

Network Models

T

he 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

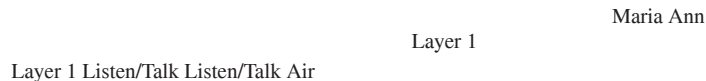
We defined the term *protocol* in Chapter 1. In data communication and networking, a protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively. When communication is simple, we may need only one simple protocol; when 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 far mal and limited to the subject being taught.

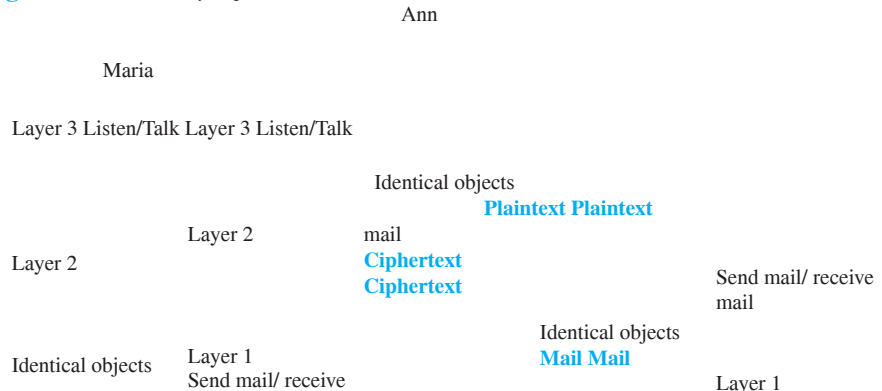
Second Scenario

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

CHAPTER 2 NETWORK MODELS 33

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.

34 PART I OVERVIEW

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 cipher text 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

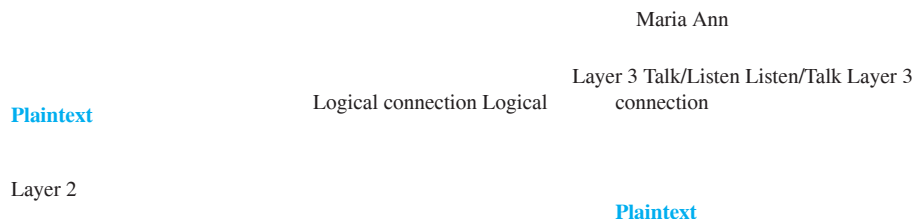
CHAPTER 2 NETWORK MODELS 35

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*





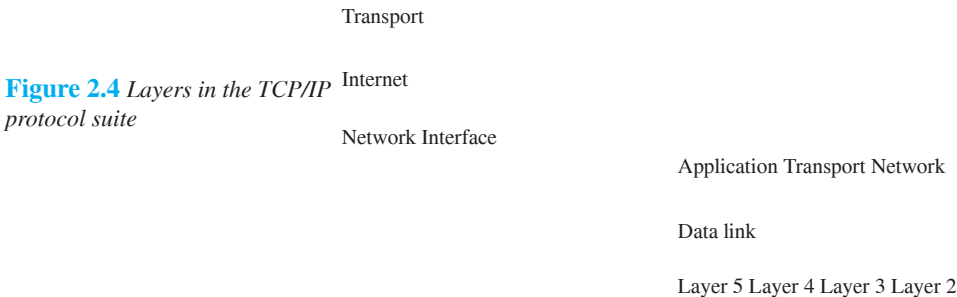
2.2 TCP/IP PROTOCOL SUITE

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 *hier archical* 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.

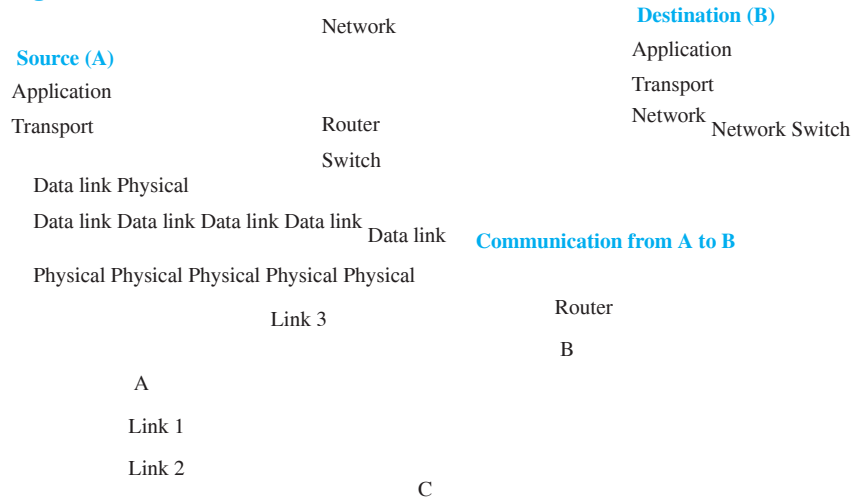
36 PART I OVERVIEW



Application

Layer 1 a. Original layers b. Layers used in this book

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.

CHAPTER 2 NETWORK MODELS 37

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

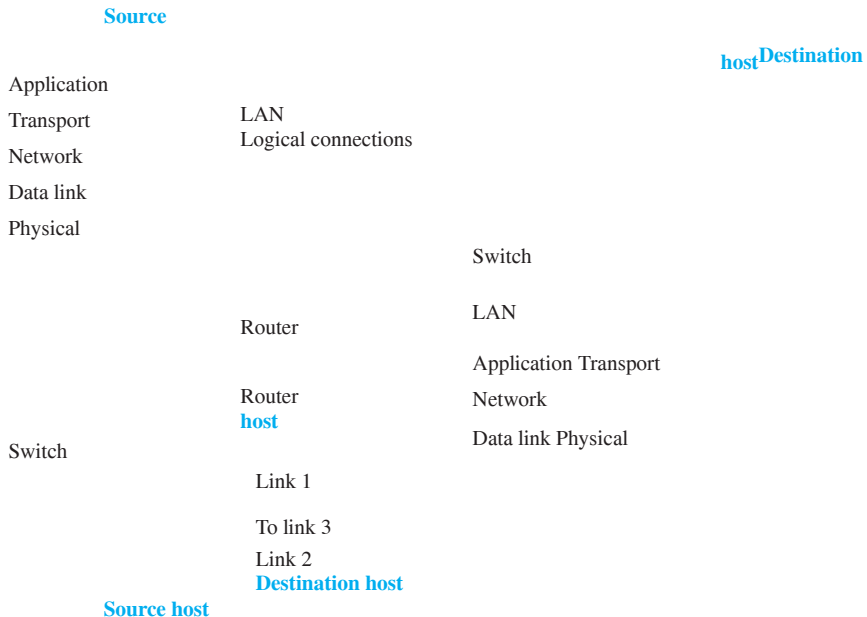
and physical-layer protocols; the router needs to receive a packet from link 1 based on one pair of protocols and deliver it to link 2 based on another pair of protocols.

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.

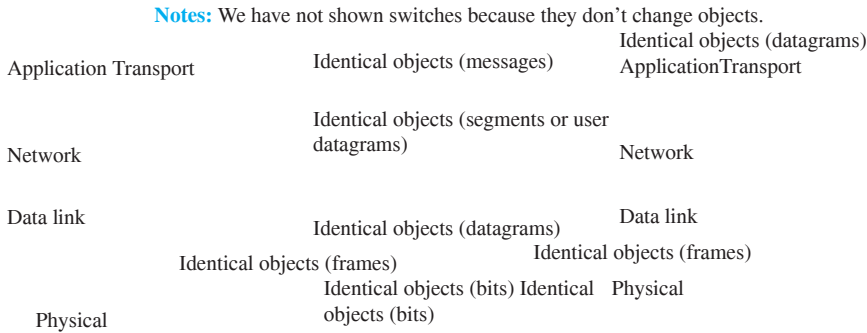
Another way of thinking of the logical connections is to think about the data unit

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 trans

formed 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 net

work 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

40 PART I OVERVIEW

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

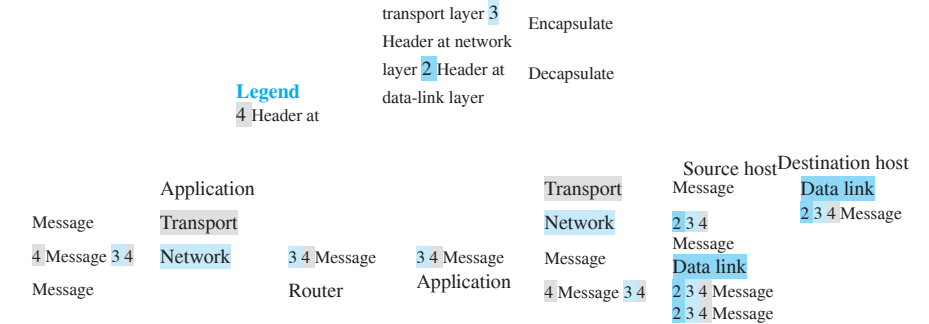
a user can also create a pair of processes to be run at the two hosts. In Chapter 25, we explore this situation.

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