Don't forget to check out the Online Learning Center, www.mhhe.com/forouzan for additional resources!

Instructors and students using *Data Communications and Networking*, Fourth Edition by Behrouz A. Forouzan will find a wide variety of resources available at the Online Learning Center, www.mhhe.comlforouzan

#### Instructor Resources

Instructors can access the following resources by contacting their McGraw-Hill Repre sentative for a secure password.

- **a** PowerPoint Slides. Contain figures, tables, highlighted points, and brief descriptions of each section.
- O Complete Solutions Manual. Password-protected solutions to all end-of-chapter problems are provided.
- **a** Pageout. A free tool that helps you create your own course website. **D** Instructor Message Board. Allows you to share ideas with other instructors using the text.

#### Student Resources

The student resources are available to those students using the book. Once you have accessed the Online Learning Center, click on "Student" Student Resources," then select a chap ter from the drop down menu that appears. Each chapter has a wealth of materials to help you review communications and networking concepts. Included are:

- **a** Chapter Summaries. Bulleted summary points provide an essential review of major ideas and concepts covered in each chapter.
- **a** Student Solutions Manual. Contains answers for odd-numbered problems. **O** Glossary. Defines key terms presented in the book.
- O Flashcards. Facilitate learning through practice and review.
- **a** Animated Figures. Visual representations model key networking concept
- D Automated Quizzes. Easy-to-use quizzes strengthen learning and emphas
- a Web links. Connect students to additional resources available online.

ging them to life.

por tant ideas from the book.

# **DATA**

# COMMUNICATIONS AND NETWORKING

McGraw-Hill Forouzan Networking Series

Titles by Behrouz A. Forouzan:

Data Communications and Networking TCPflP Protocol Suite Local Area Networks Business Data Communications

# DATA COMMUNICATIONS AND NETWORKING

Fourth Edition

Behrouz A. Forouzan

DeAnza College

with

Sophia Chung Fegan



Boston Burr Ridge, IL Dubuque, IA Madison, WI New York San Francisco S1. Louis Bangkok Bogota Caracas Kuala Lumpur Lisbon London Madrid Mexico City Milan Montreal New Delhi Santiago Seoul Singapore Sydney Taipei Toronto







# Higher Education

#### DATA COMMUNICATIONS AND NETWORKING, FOURTH EDITION

Published by McGraw-Hill, a business unit of The McGraw-Hill Companies. Inc., 1221 Avenue of the Americas, New York, NY 10020. Copyright © 2007 by The McGraw-Hill Companies, Inc. All rights reserved. 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.

1234567890DOC/DOC09876

ISBN-13 978-0-07-296775-3 ISBN-to 0-07-296775-7

Publisher: Alan R. Apt

Developmental Editor: Rebecca Olson

Executive Marketing Manager: Michael Weitz Senior Project Manager: Sheila M. Frank

Senior Production Supervisor: Kara Kudronowicz Senior Media Project Manager: Jodi K. Banowetz Associate Media Producer: Christina Nelson

Senior Designer: David W Hash W. Cover Designer: Rokusek Design

(USE) Cover Image: Women ascending Mount McKinley, Alaska. Mount McKinley (Denali) 12,000 feet,

©Allan Kearney/Getty Images

Compositor: Interactive Composition Corporation

Typeface: 10/12 Times Roman

Printer: R. R. Donnelley Crawfordsville, IN

 $Library\ of\ Congress\ {\tt Cataloging-in-Publication}\ {\bm Cataloging-in-Publication}\ {\bm Data}$ 

Forouzan, Behrouz A.

Data communications and networking I Behrouz A Forouzan. - \_\_4th ed. p. em. - (McGraw-Hill Forouzan networking series)

Includes index.

ISBN 978-0-07-296775-3 - ISBN 0-07-296775-7 (hard eopy : alk. paper) 1. Data transmission systems. 2. Computer networks. I. Title. II. Series.

TK5105.F6617 004.6--dc22

www.mhhe.com 2007 2006000013 CIP

To lny wife, Faezeh, with love Behrouz Forouzan

# **BRIEF CONTENTS**

Preface XXIX

PART 1 Overview 1

**Chapter 1** *Introduction 3* 

Chapter 2 Network Models 27

PART 2

**Chapter 3 Chapter 4 Chapter 5** 

Chapter 6 Chapter 7 Chapter 8

Chapter 9

PART 3

**Chapter 10 Chapter 11 Chapter 12** 

**Chapter 13 Chapter 14 Chapter 15** 

**Chapter 16 Chapter 17 Chapter 18** 

Physical Layer and Media 55

Data and Signals 57

Digital Transmission 101

Analog Transmission 141

Bandwidth Utilization: Multiplexing and

Spreading 161 Transmission Media 191

Switching 213

Using Telephone and Cable Networksfor

Data Transmission 241

**Data Link Layer 265** 

Error Detection and Correction 267

Data Link Control 307

Multiple Access 363

Wired LANs: Ethernet 395

Wireless LANs 421

Connecting LANs, Backbone Networks,

and Virtual LANs 445 Wireless WANs:

Cellular Telephone and Satellite Networks 467 SONETISDH 491	Chapter 23 Chapter 24
	PART 6
	Chapter 25
	Chapter 26
	Chapter 27
	Chapter 28
	Chapter 29 Network Layer 547
	Netvvork Layer: Logical Addressing Network 549
	Netvvork Layer: Internet Protocol Network579
	Netl,vork <sup>Layer</sup> La.ver: Address Mapping, Error Reporting, Network and Multicasting 611
	Network Layer: Delivery, Fonvarding, and Routing 647
	Transport Layer 701
	Process-to-Process Delivery: UDp, TCP,
Virtual-Circuit Nenvorks: Frame Relay	and SCTP 703 Congestion Control and
Networks: and ATM 517 vii	Quality ql'Sen'ice 761
viii BRIEF CONTENTS	Application Layer 795
PART 4 Chapter 19	Domain Name System 797 Remote Logging, Electronic Mail, and File Transfer 817 WWW and HTTP
Chapter 20	851
Chapter 21	Network Management: SNMP 873
Chapter 22	Multimedia 901
PARTS	
PART 7 Security 929	
Chapter 30 Cf}1Jtogra Chapter 31 Network Security	
Chapter 32 Securit}' in the	Internet: IPSec, SSLITLS, PCp, VPN, and wewalls 995

**Appendix A** *Unicode 1029* 

Appendix B Numbering Systems 1037
Appendix C Mathematical Review 1043
Appendix D 8B/6T Code 1055
Appendix E Telephone History 1059
Appendix F Co! Itact Addresses 1061
Appendix G RFCs 1063
Appendix H UDP and TCP Ports 1065
Acron. VII 1s 1067

References 1107

Index IIII

#### **Preface xxix**

#### **PART 1 Overview 1**

#### **Chapter 1** *Introduction 3*

#### 1.1 DATA COMMUNICATIONS 3

Components 4

Data Representation 5

DataFlow 6

#### 1.2 NETWORKS 7

Distributed Processing 7

Network Criteria 7

Physical Structures 8

Network Models 13

Categories of Networks 13

Interconnection of Networks: Internetwork IS

#### 1.3 THE INTERNET 16

A Brief History 17

The Internet Today 17

#### 1.4 PROTOCOLS AND STANDARDS 19

Protocols 19

Standards 19

Standards Organizations 20

**Internet Standards 21** 

#### 1.5 RECOMMENDED READING 21

Books 21

Sites 22

RFCs 22

**1.6 KEY TERMS 22** 

**1.7 SUMMARY 23** 

1.8 PRACTICE SET 24

**Review Questions 24** 

Exercises 24

Research Activities 25

#### Chapter 2 Network Models 27

#### 2.1 LAYERED TASKS 27

Sender, Receiver, and Carrier 28

Hierarchy 29

#### 2.2 THE OSI MODEL 29

Layered Architecture 30

Peer-to-Peer Processes 30

**Encapsulation 33** 

#### 2.3 LAYERS IN THE OSI MODEL 33

Physical Layer 33

Data Link Layer 34

Network Layer 36

Transport Layer 37

Session Layer 39

Presentation Layer 39

Application Layer 41

Summary of Layers 42

#### 2.4 TCP/IP PROTOCOL SUITE 42

Physical and Data Link Layers 43

Network Layer 43

Transport Layer 44

**Application Layer 45** 

#### 2.5 ADDRESSING 45

Physical Addresses 46

Logical Addresses 47

Port Addresses 49

Specific Addresses 50

#### 2.6 RECOMMENDED READING 50

Books 51

Sites 51

RFCs 51

#### **2.7 KEY IERMS 51**

2.8 SUMMARY 52

#### 2.9 PRACTICE SET 52

**Review Questions 52** 

Exercises 53

Research Activities 54

#### PART 2 Physical Layer and Media 55

#### Chapter 3 Data and Signals 57

#### 3.1 ANALOG AND DIGITAL 57

Analog and Digital Data 57

Analog and Digital Signals 58

Periodic and Nonperiodic Signals 58

#### 3.2 PERIODIC ANALOG SIGNALS 59

Sine Wave 59

Phase 63

Wavelength 64

Time and Frequency Domains 65

Composite Signals 66

Bandwidth 69

#### 3.3 DIGITAL SIGNALS 71

Bit Rate 73

Bit Length 73

Digital Signal as a Composite Analog Signal 74

Transmission of Digital Signals 74

#### 3.4 TRANSMISSION IMPAIRMENT 80

Attenuation 81

Distortion 83

Noise 84

#### 3.5 DATA RATE LIMITS 85

Noiseless Channel: Nyquist Bit Rate 86 Noisy Channel: Shannon Capacity 87

Using Both Limits 88

3.6 PERFORMANCE 89

Bandwidth 89

Throughput 90

Latency (Delay) 90

Bandwidth-Delay Product 92

Jitter 94

#### 3.7 RECOMMENDED READING 94

Books 94

**3.8 KEYTERMS 94** 

**3.9 SUMMARY 95** 

#### 3.10 PRACTICE SET 96

**Review Questions 96** 

Exercises 96

#### **Chapter 4** Digital Transmission 101

#### 4.1 DIGITAL-TO-DIGITAL CONVERSION 101

Line Coding 101

Line Coding Schemes 106

**Block Coding 115** 

Scrambling 118

#### 4.2 ANALOG-TO-DIGITAL CONVERSION 120

Pulse Code Modulation (PCM) 121

Delta Modulation (DM) 129

#### 4.3 TRANSMISSION MODES 131

Parallel Transmission 131

Serial Transmission 132

#### 4.4 RECOMMENDED READING 135

Books 135

**4.5 KEYTERMS 135** 

4.6 SUMMARY 136

#### 4.7 PRACTICE SET 137

**Review Questions 137** 

Exercises 137

Chapter 5 Analog TranSl1'lission 141

#### 5.1 DIGITAL-TO-ANALOG CONVERSION 141

Aspects of Digital-to-Analog Conversion 142

Amplitude Shift Keying 143

Frequency Shift Keying 146

Phase Shift Keying 148

Quadrature Amplitude Modulation 152

#### 5.2 ANALOG-TO-ANALOG CONVERSION 152

Amplitude Modulation 153

Frequency Modulation 154

Phase Modulation 155

xii CONTENTS

#### 5.3 RECOMMENDED READING 156

Books 156

**5.4 KEY IERMS 157** 

**5.5 SUMMARY 157** 

#### 5.6 PRACTICE SET 158

**Review Questions 158** Exercises 158

#### **Chapter 6** Ba17chridth Utili::.ation: Multiplexing

and Spreading 161

#### 6.1 MULTIPLEXING 161

Frequency-Division Multiplexing 162

Wavelength-Division Multiplexing 167

Synchronous Time-Division Multiplexing 169

Statistical Time-Division Multiplexing 179

#### 6.2 SPREAD SPECTRUM 180

Frequency Hopping Spread Spectrum (FHSS) 181

Direct Sequence Spread Spectrum 184

#### 6.3 RECOMMENDED READING 185

Books 185

**6.4 KEY IERMS 185** 

6.5 SUMMARY 186

#### 6.6 PRACTICE SET 187

**Review Questions 187** 

Exercises 187

#### **Chapter 7** Transmission Media 191

#### 7.1 GUIDED MEDIA 192

Twisted-Pair Cable 193

Coaxial Cable 195

Fiber-Optic Cable 198

#### 7.2 UNGUIDED MEDIA: WIRELESS 203

Radio Waves 205

Microwaves 206

Infrared 207

#### 7.3 RECOMMENDED READING 208

Books 208

7.4 KEY IERMS 208

7.5 SUMMARY 209

#### 7.6 PRACTICE SET 209

**Review Questions 209** 

Exercises 210

#### Chapter 8

Syvitching 213

#### 8.1 CIRCUIT-SWITCHED NETWORKS 214

Three Phases 217

Efficiency 217

Delay 217

Circuit-Switched Technology in Telephone Networks 218

#### 8.2 DATAGRAM NETWORKS 218

Routing Table 220

Efficiency 220

Delay 221

Datagram Networks in the Internet 221

8.3 VIRTUAL-CIRCUIT NETWORKS 221

Addressing 222

Three Phases 223

Efficiency 226

Delay in Virtual-Circuit Networks 226

Circuit-Switched Technology in WANs 227

8.4 STRUCTURE OF A SWITCH 227

Structure of Circuit Switches 227

Structure of Packet Switches 232

8.5 RECOMMENDED READING 235

Books 235

8.6 KEY TERMS 235

8.7 SUMMARY 236

8.8 PRACTICE SET 236

**Review Questions 236** 

Exercises 237

#### Chapter 9 Using Telephone and Cable Networks for Data Transm, ission 241

#### 9.1 1ELEPHONE NETWORK 241

Major Components 241

LATAs 242

Signaling 244

Services Provided by Telephone Networks 247

9.2 DIAL-UP MODEMS 248

Modem Standards 249

9.3 DIGITAL SUBSCRIBER LINE 251

ADSL 252

ADSL Lite 254

HDSL 255

**SDSL 255** 

**VDSL 255** 

Summary 255

9.4 CABLE TV NETWORKS 256

Traditional Cable Networks 256

Hybrid Fiber-Coaxial (HFC) Network 256

9.5 CABLE TV FOR DATA TRANSFER 257

Bandwidth 257

Sharing 259

CM and CMTS 259

Data Transmission Schemes: DOCSIS 260

9.6 RECOMMENDED READING 261

Books 261

9.7 KEY TERMS 261

9.8 SUMMARY 262

9.9 PRACTICE SET 263

**Review Questions 263** 

Exercises 264

xiv CONTENTS

#### 10.1 INTRODUCTION 267

Types of Errors 267

Redundancy 269

**Detection Versus Correction 269** 

Forward Error Correction Versus Retransmission 269

Coding 269

Modular Arithmetic 270

#### 10.2 BLOCK CODING 271

Error Detection 272

Error Correction 273

Hamming Distance 274

Minimum Hamming Distance 274

#### 10.3 LINEAR BLOCK CODES 277

Minimum Distance for Linear Block Codes 278

Some Linear Block Codes 278

#### 10.4 CYCLIC CODES 284

Cyclic Redundancy Check 284

Hardware Implementation 287

Polynomials 291

Cyclic Code Analysis 293

Advantages of Cyclic Codes 297

Other Cyclic Codes 297

#### 10.5 CHECKSUM 298

Idea 298

One's Complement 298

Internet Checksum 299

#### 10.6 RECOMMENDED READING 30 I

Books 301

RFCs 301

10.7 KEY IERMS 301

10.8 SUMMARY 302

#### 10.9 PRACTICE SET 303

**Review Questions 303** 

Exercises 303

#### **Chapter 11** *Data Link Control 307*

#### 11.1 FRAMING 307

Fixed-Size Framing 308

Variable-Size Framing 308

#### 11.2 FLOW AND ERROR CONTROL 311

Flow Control 311

Error Control 311

#### 11.3 PROTOCOLS 311

#### 11.4 NOISELESS CHANNELS 312

Simplest Protocol 312

Stop-and-Wait Protocol 315

#### 11.5 NOISY CHANNELS 318

Stop-and-Wait Automatic Repeat Request 318 *Go-Back-N* Automatic Repeat Request 324

11.8

11.9

11.10 11.11

Selective Repeat Automatic Repeat Request Piggybacking

339

HDLC 340

Configurations and Transfer Modes 340 Frames 341

Control Field 343

POINT-TO-POINT

PROTOCOL 346 Framing 348

Transition Phases 349 Multiplexing 350 Multilink PPP 355

11.6 11.7

RECOMMENDED READING 357 Books 357 KEY TERMS 357 SUMMARY 358 PRACTICE SET 359 Review Questions 359 Exercises 359 Access 363 CONTENTS XV

**Chapter 12** *Multiple* 

332

#### 12.1 RANDOMACCESS 364

ALOHA 365

Carrier Sense Multiple Access (CSMA) 370

Carrier Sense Multiple Access with Collision Detection (CSMAlCD) 373

Carrier Sense Multiple Access with Collision Avoidance (CSMAlCA) 377 12.2

#### **CONTROLLED ACCESS 379**

Reservation 379

Polling 380

Token Passing 381

#### 12.3 CHANNELIZATION 383

Frequency-Division Multiple Access (FDMA) 383

Time-Division Multiple Access (TDMA) 384

Code-Division Multiple Access (CDMA) 385

#### 12.4 RECOMMENDED READING 390

Books 391

12.5 KEY TERMS 391

12.6 SUMMARY 391

#### 12.7 PRACTICE SET 392

Review Questions 392

Exercises 393

Research Activities 394

#### **Chapter 13** *Wired LANs: Ethernet 395*

#### 13.1 IEEE STANDARDS 395

Data Link Layer 396

Physical Layer 397

#### 13.2 STANDARD ETHERNET 397

MAC Sublayer 398

Physical Layer 402

#### 13.3 CHANGES IN THE STANDARD 406

Bridged Ethernet 406

Switched Ethernet 407

Full-Duplex Ethernet 408

#### 13.4 FAST ETHERNET 409

MAC Sublayer 409

Physical Layer 410

#### 13.5 GIGABIT ETHERNET 412

MAC Sublayer 412

Physical Layer 414

Ten-Gigabit Ethernet 416

#### 13.6 RECOMMENDED READING 417

Books 417

13.7 KEY TERMS 417

13.8 SUMMARY 417

#### 13.9 PRACTICE SET 418

**Review Questions 418** 

Exercises 419

#### Chapter 14 Wireless LANs 421

#### 14.1 IEEE 802.11 421

Architecture 421

MAC Sublayer 423

Addressing Mechanism 428

Physical Layer 432

#### **14.2 BLUETOOTH 434**

Architecture 435

Bluetooth Layers 436

Radio Layer 436

Baseband Layer 437

L2CAP 440

Other Upper Layers 441

#### 14.3 RECOMMENDED READING 44 I

Books 442

**14.4 KEYTERMS 442** 

14.5 SUMMARY 442

#### 14.6 PRACTICE SET 443

**Review Questions 443** 

Exercises 443

## **Chapter 15** Connecting LANs, Backbone Networks, and Virtual LANs 445

#### 15.1 CONNECTING DEVICES 445

Passive Hubs 446

Repeaters 446

Active Hubs 447

Bridges 447

Two-Layer Switches 454

Routers 455

Three-Layer Switches 455

Gateway 455

#### 15.2 BACKBONE NETWORKS 456

Bus Backbone 456

Star Backbone 457

Connecting Remote LANs 457

CONTENTS xvii

Membership 461

Configuration 461

Communication Between Switches 462

IEEE Standard 462

Advantages 463

15.4 RECOMMENDED READING 463

Books 463

Site 463

15.5 KEY TERMS 463

15.6 SUMMARY 464

15.7 PRACTICE SET 464

**Review Questions 464** 

Exercises 465

#### Chapter 16 Wireless WANs: Cellular Telephone and

Satellite Networks 467

#### 16.1 CELLULAR TELEPHONY 467

Frequency-Reuse Principle 467

Transmitting 468

Receiving 469

Roaming 469

First Generation 469

Second Generation 470

Third Generation 477

#### 16.2 SATELLITE NETWORKS 478

Orbits 479

Footprint 480

Three Categories of Satellites 480

**GEO Satellites 481** 

MEO Satellites 481

LEO Satellites 484

#### 16.3 RECOMMENDED READING 487

Books 487

16.4 KEY TERMS 487

16.5 SUMMARY 487

16.6 PRACTICE SET 488

**Review Questions 488** 

Exercises 488

#### Chapter 17 SONETISDH 491

#### 17.1 ARCHITECTURE 491

Signals 491

**SONET Devices 492** 

Connections 493

17.2 SONET LAYERS 494

Path Layer 494

Line Layer 495

Section Layer 495

Photonic Layer 495

Device-Layer Relationships 495

xviii CONTENTS

#### 17.3 SONET FRAMES 496

Frame, Byte, and Bit Transmission 496 STS-I Frame Format 497 Overhead Summary 501 Encapsulation 501

#### 17.4 STS MULTIPLEXING 503 Byte Interleaving 504 Concatenated Signal 505 AddlDrop Multiplexer 506 17.5 SONET NETWORKS 507 Linear Networks 507 Ring Networks 509 Mesh Networks 510 17.6 VIRTUAL TRIBUTARIES 512 Types of VTs 512 17.7 RECOMMENDED READING 513 Books 513 17.8 KEY IERMS 513 17.9 SUMMARY 514 17.10 PRACTICE SET 514 **Review Questions 514** Exercises 515 **Chapter 18** *Virtual-Circuit Networks: Frame Relm' and* ATM 517 **18.1 FRAME RELAY 517** Architecture 518 Frame Relay Layers 519 Extended Address 521 FRADs 522 **VOFR 522** LMI 522 Congestion Control and Quality of Service 522 18.2 ATM 523 Design Goals 523 Problems 523 Architecture 526 Switching 529 ATM Layers 529 Congestion Control and Quality of Service 535 18.3 ATM LANs 536 ATM LAN Architecture 536 LAN Emulation (LANE) 538 Client/Server Model 539 Mixed Architecture with Client/Server 540 18.4 RECOMMENDED READING 540 Books 541 18.5 KEY IERMS 541 18.6 SUMMARY 541 18.7 PRACTICE SET 543 **Review Questions 543** Exercises 543

CONTENTS xix

#### PART 4 Network Layer 547

Chapter 19 Netvl/ark Layer: Logical Addressing 549

#### 19.1 IPv4ADDRESSES 549

Address Space 550

Notations 550

Classful Addressing 552

Classless Addressing 555

Network Address Translation (NAT) 563			
19.2 IPv6 ADDRESSES 566			

Structure 567

Address Space 568

#### 19.3 RECOMMENDED READING 572

Books 572

Sites 572

**RFCs 572** 

#### 19.4 KEY TERMS 572

#### 19.5 SUMMARY 573

#### 19.6 PRACTICE SET 574

**Review Questions 574** 

Exercises 574

Research Activities 577

#### Chapter 20 Network Layer: Internet Protocol 579

#### 20.1 INTERNETWORKING 579

Need for Network Layer 579

Internet as a Datagram Network 581

Internet as a Connectionless Network 582

#### 20.2 IPv4 582

Datagram 583

Fragmentation 589

Checksum 594

Options 594

#### 20.3 IPv6 596

Advantages 597

Packet Format 597

Extension Headers 602

#### 20.4 TRANSITION FROM IPv4 TO IPv6 603

Dual Stack 604

Tunneling 604

Header Translation 605

#### 20.5 RECOMMENDED READING 605

Books 606

Sites 606

RFCs 606

20.6 KEY TERMS 606

20.7 SUMMARY 607

#### 20.8 PRACTICE SET 607

**Review Questions 607** 

Exercises 608

Research Activities 609

xx CONTENTS

# **Chapter 21** Network Layer: Address Mapping, Error Reporting, and Multicasting 611

#### 21.1 ADDRESS MAPPING 611

Mapping Logical to Physical Address: ARP 612

Mapping Physical to Logical Address: RARp, BOOTP, and DHCP 618

#### 21.2 ICMP 621

Types of Messages 621

Message Format 621

Error Reporting 622

Query 625

**Debugging Tools 627** 

#### 21.3 IGMP 630

Group Management 630

IGMP Messages 631

Message Format 631

**IGMP Operation 632** 

Encapsulation 635 Netstat Utility 637

#### 21.4 ICMPv6 638

Error Reporting 638

Query 639

#### 21.5 RECOMMENDED READING 640

Books 641

Site 641

RFCs 641

#### 21.6 KEYTERMS 641

21.7 SUMMARY 642

#### 21.8 PRACTICE SET 643

**Review Questions 643** 

Exercises 644

Research Activities 645

# **Chapter 22** Network Layer: Delivery, Forwarding, and Routing 647

#### 22.1 DELIVERY 647

Direct Versus Indirect Delivery 647

#### 22.2 FORWARDING 648

Forwarding Techniques 648

Forwarding Process 650

**Routing Table 655** 

#### 22.3 UNICAST ROUTING PROTOCOLS 658

Optimization 658

Intra- and Interdomain Routing 659

Distance Vector Routing 660

Link State Routing 666

Path Vector Routing 674

#### 22.4 MULTICAST ROUTING PROTOCOLS 678

Unicast, Multicast, and Broadcast 678

Applications 681

**Multicast Routing 682** 

Routing Protocols 684

#### CONTENTS xxi

#### 22.5 RECOMMENDED READING 694

Books 694

Sites 694

RFCs 694

22.6 KEY 1ERMS 694

22.7 SUMMARY 695

22.8 PRACTICE SET 697

Review Questions 697

Exercises 697

Research Activities 699

#### **PART 5 Transport Layer 701**

**Chapter 23** *Process-fa-Process Delivery: UDp, TCp, and* SeTP *703* 

23.1 PRC	CESS-TO	-PROCESS	<b>DELIVERY</b>	703
----------	---------	----------	-----------------	-----

Client/Server Paradigm 704

Multiplexing and Demultiplexing 707

Connectionless Versus Connection-Oriented Service 707

Reliable Versus Unreliable 708

Three Protocols 708

#### 23.2 USER DATAGRAM PROTOCOL (UDP) 709

Well-Known Ports for UDP 709

User Datagram 710

Checksum 711

UDP Operation 713

Use of UDP 715

23.3 TCP 715

TCP Services 715

TCP Features 719

Segment 721

A TCP Connection 723

Flow Control 728

Error Control 731

Congestion Control 735

23.4 SCTP 736

**SCTP Services 736** 

**SCTP Features 738** 

Packet Format 742

An SCTP Association 743

Flow Control 748

Error Control 751

Congestion Control 753

#### 23.5 RECOMMENDED READING 753

Books 753

Sites 753

**RFCs 753** 

23.6 KEY IERMS 754

23.7 SUMMARY 754

#### 23.8 PRACTICE SET 756

**Review Questions 756** 

Exercises 757

Research Activities 759

xxii CONTENTS

#### Chapter 24 Congestion Control and Quality (~j'Service

#### \_\_767

#### 24.1 DATA IRAFFIC 761

Traffic Descriptor 76]

Traffic Profiles 762

#### **24.2 CONGESTION 763**

Network Performance 764

#### 24.3 CONGESTION CONTROL 765

Open-Loop Congestion Control 766

Closed-Loop Congestion Control 767

#### 24.4 IWO EXAMPLES 768

Congestion Control in TCP 769

Congestion Control in Frame Relay 773

#### 24.5 QUALITY OF SERVICE 775

Flow Characteristics 775

Flow Classes 776

#### 24.6 TECHNIQUES TO IMPROVE QoS 776

Scheduling 776

Traffic Shaping 777 Resource Reservation 780 Admission Control 780

#### 24.7 INTEGRATED SERVICES 780

Signaling 781

Flow Specification 781

Admission 781

Service Classes 781

**RSVP 782** 

Problems with Integrated Services 784

#### 24.8 DIFFERENTIATED SERVICES 785

DS Field 785

#### 24.9 QoS IN SWITCHED NETWORKS 786

QoS in Frame Relay 787

QoS in ATM 789

#### 24.10 RECOMMENDED READING 790

Books 791

24.11 KEY TERMS 791

24.12 SUMMARY 791

#### **24.13 PRACTICE SET 792**

**Review Questions 792** 

Exercises 793

#### PART 6 Application Layer 795

#### Chapter 25 DO/nain Name System 797

#### **25.1 NAME SPACE 798**

Flat Name Space 798

Hierarchical Name Space 798

#### 25.2 DOMAIN NAME SPACE 799

Label 799

Domain Narne 799

25.12 25.13 25.14

	Domain 801		
		DISTRIBUTION OF NAME	EResource Record 811
		SPACE 801 Hierarchy of	REGISTRARS 811
25.3		Name Servers 802	DYNAMIC DOMAIN
23.3		Zone 802	NAME SYSTEM (DDNS)
		Root Server 803	<b>ENCAPSULATION 812</b>
		Primary and Secondary Servers	RECOMMENDED
		803 DNS IN THE INTERNET	READING 812
25.4 25.5			Books 813
		803	Sites 813
		Generic Domains 804	RFCs 813
		Country Domains 805	KEY TERMS 813
		Inverse Domain 805	SUMMARY 813
		RESOLUTION 806	PRACTICE SET 814
		Resolver 806	
25.6 25.7		Mapping Names to Addresses	Review Questions 814 Exercises 815
		807	CONTENTS xxiii
		Mapping Address to Names 807	CONTENTS AAM
25.8		Recursive Resolution 808	
25.9 25.10 25.11	11	Iterative Resolution 808	
	.11	Caching 808	
		DNS MESSAGES 809	
		Header 809	

**TYPES OF RECORDS 811** 

Question Record 811

#### **Chapter 26** Remote Logging, Electronic Mail, and File Transfer 817

#### 26.1 REMOTE LOGGING 817

TELNET 817

#### 26.2 ELECTRONIC MAIL 824

Architecture 824

User Agent 828

Message Transfer Agent: SMTP 834

Message Access Agent: POP and IMAP 837

Web-Based Mail 839

#### 26.3 FILE TRANSFER 840

File Transfer Protocol (FTP) 840

Anonymous FTP 844

#### 26.4 RECOMMENDED READING 845

Books 845

Sites 845

RFCs 845

26.5 KEY IERMS 845

26.6 SUMMARY 846

xxiv CONTENTS

26.7 PRACTICE SET 847 Review Questions 847 Exercises 848 Research Activities 848

#### Chapter 27 WWW and HTTP 851

#### 27.1 ARCHITECTURE 851

Client (Browser) 852

Server 852

**Uniform Resource Locator 853** 

Cookies 853

#### 27.2 WEB DOCUMENTS 854

Static Documents 855

Dynamic Documents 857

Active Documents 860

#### 27.3 HTTP 861

HTTP Transaction 861

Persistent Versus Nonpersistent Connection 868

Proxy Server 868

#### 27.4 RECOMMENDED READING 869

Books 869

Sites 869

**RFCs 869** 

#### 27.5 KEY 1ERMS 869

27.6 SUMMARY 870

#### 27.7 PRACTICE SET 871

**Review Questions 871** 

Exercises 871

#### Chapter 28 Network Management: SNMP 873

#### 28.1 NETWORK MANAGEMENT SYSTEM 873

Configuration Management 874

Fault Management 875

Performance Management 876

Security Management 876

Accounting Management 877

#### 28.2 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) 877

Concept 877

**Management Components 878** 

Structure of Management Information 881

Management Information Base (MIB) 886

Lexicographic Ordering 889

**SNMP 891** 

Messages 893

UDP Ports 895

Security 897

#### 28.3 RECOMMENDED READING 897

Books 897

Sites 897

**RFCs 897** 

28.4 KEY 1ERMS 897

28.5 SUMMARY 898

**CONTENTS** xxv

#### 28.6 PRACTICE SET 899

**Review Questions 899** 

Exercises 899

#### Chapter 29 Multimedia 901

#### 29.1 DIGITIZING AUDIO AND VIDEO 902

Digitizing Audio 902

Digitizing Video 902

#### 29.2 AUDIO AND VIDEO COMPRESSION 903

Audio Compression 903

Video Compression 904

#### 29.3 STREAMING STORED AUDIO/VIDEO 908

First Approach: Using a Web Server 909

Second Approach: Using a Web Server with Metafile 909

Third Approach: Using a Media Server 910

Fourth Approach: Using a Media Server and RTSP 911 29.4 STREAMING LIVE AUDIOIVIDEO 912

#### 29.5 REAL-TIME INTERACTIVE AUDIOIVIDEO 912

Characteristics 912

29.6 RTP 916

RTP Packet Format 917

UDPPort 919

29.7 RTCP 919

Sender Report 919

Receiver Report 920

Source Description Message 920

Bye Message 920

Application-Specific Message 920

UDP Port 920

29.8 VOICE OVER IP 920

SIP 920

H.323 923

#### 29.9 RECOMMENDED READING 925

Books 925

Sites 925

29.10 KEY 1ERMS 925

29.11 SUMMARY 926

29.12 PRACTICE SET 927

Review Questions 927

Exercises 927

Research Activities 928

#### PART 7 Security 929

#### Chapter 30 Cryptography 931

#### 30.1 INTRODUCTION 931

**Definitions 931** 

Two Categories 932

#### 30.2 SYMMETRIC-KEY CRYPTOGRAPHY 935

**Traditional Ciphers 935** 

Simple Modem Ciphers 938

xxvi CONTENTS

Modern Round Ciphers 940 Mode of Operation 945

30,3 ASYMMETRIC-KEY CRYPTOGRAPHY 949

RSA 949

Diffie-Hellman 952

30.4 RECOMMENDED READING 956

Books 956

30.5 KEY TERMS 956

30.6 SUMMARY 957

#### 30.7 PRACTICE SET 958

**Review Questions 958** 

Exercises 959

Research Activities 960

#### Chapter 31 Network Security 961

#### 31.1 SECURITY SERVICES 961

Message Confidentiality 962

Message Integrity 962

Message Authentication 962

Message Nonrepudiation 962

**Entity Authentication 962** 

#### 31.2 MESSAGE CONFIDENTIALITY 962

Confidentiality with Symmetric-Key Cryptography 963

Confidentiality with Asymmetric-Key Cryptography 963

#### 31.3 MESSAGE INTEGRITY 964

Document and Fingerprint 965

Message and Message Digest 965

Difference 965

Creating and Checking the Digest 966

Hash Function Criteria 966

Hash Algorithms: SHA-1 967

#### 31.4 MESSAGE AUTHENTICATION 969

**MAC 969** 

#### 31.5 **DIGITAL** SIGNATURE 971

Comparison 971

Need for Keys 972

Process 973

Services 974

Signature Schemes 976

#### 31.6 ENTITY AUTHENTICATION 976

Passwords 976

Challenge-Response 978

#### 31.7 KEY MANAGEMENT 981

Symmetric-Key Distribution 981

Public-Key Distribution 986

#### 31.8 RECOMMENDED READING 990

Books 990

31.9 KEY TERMS 990

31.10 SUMMARY 991

#### **31.11 PRACTICE SET 992**

**Review Questions 992** 

Exercises 993

Research Activities 994

CONTENTS xxvii

#### **Chapter 32** *Security* □ *in the Internet: IPSec, SSUFLS, PGP, VPN, and Firewalls* 995

#### 32.1 IPSecurity (IPSec) 996

Two Modes 996

Two Security Protocols 998

Security Association 1002

Internet Key Exchange (IKE) 1004

Virtual Private Network 1004

32.2 SSLffLS 1008

SSL Services 1008 Security Parameters 1009

Sessions and Connections 1011

Four Protocols 1012

Transport Layer Security 1013

32.3 PGP 1014

Security Parameters 1015

Services 1015

A Scenario 1016

PGP Algorithms 1017

Key Rings 1018

PGP Certificates 1019

32.4 FIREWALLS 1021

Packet-Filter Firewall 1022

Proxy Firewall 1023

32.5 RECOMMENDED READING 1024

Books 1024

32.6 KEY IERMS 1024

32.7 SUMMARY 1025

32.8 PRACTICE SET 1026

**Review Questions 1026** 

Exercises 1026

#### **Appendix A** *Unicode* 1029

A.1 UNICODE 1029

Planes 1030

Basic Multilingual Plane (BMP) 1030

Supplementary Multilingual Plane (SMP) 1032

Supplementary Ideographic Plane (SIP) 1032

Supplementary Special Plane (SSP) 1032

Private Use Planes (PUPs) 1032

A.2 ASCII 1032

Some Properties of ASCII 1036

#### **Appendix B** *Numbering Systems 1037*

**B.I BASE 10: DECIMAL 1037** 

Weights 1038

**B.2 BASE 2: BINARY 1038** 

Weights 1038 Conversion 1038 xxviii CONTENTS

B.3 BASE 16: HEXADECIMAL 1039

Weights 1039

Conversion 1039

A Comparison 1040

BA BASE 256: IP ADDRESSES 1040

Weights 1040

Conversion 1040

#### **B.5 OTHER CONVERSIONS 1041**

Binary and Hexadecimal 1041 Base 256 and Binary 1042

#### C.1 TRIGONOMETRIC FUNCTIONS 1043

Sine Wave 1043

Cosine Wave 1045

Other Trigonometric Functions 1046

Trigonometric Identities 1046

#### C.2 FOURIER ANALYSIS 1046

Fourier Series 1046

Fourier Transform 1048

#### C.3 EXPONENT AND LOGARITHM 1050

Exponential Function 1050 Logarithmic Function 1051

#### **Appendix 0** 8B/6T Code 1055

**Appendix E** *Telephone History 1059* 

Before 1984 1059 Between 1984 and 1996 1059 After 1996 1059

Appendix F Contact Addresses 1061

Appendix G RFCs 1063

**Appendix H** *UDP and TCP Ports 1065* 

Acronyms 1067

Glossary 1071

References 1107

Index 1111



Data communications and networking may be the fastest growing technologies in our culture today. One ofthe ramifications of that growth is a dramatic increase in the number of professions where an understanding of these technologies is essential for success and a proportionate increase in the number and types of students taking courses to learn about them.

#### **Features of the Book**

Several features of this text are designed to make it particularly easy for students to

understand data communications and networking.

#### Structure

We have used the five-layer Internet model as the framework for the text not only because a thorough understanding of the model is essential to understanding most current network ing theory but also because it is based on a structure of interdependencies: Each layer builds upon the layer beneath it and supports the layer above it. In the same way, each con cept introduced in our text builds upon the concepts examined in the previous sections. The Internet model was chosen because it is a protocol that is fully implemented. This text is designed for students with little or no background in telecommunications or data communications. For this reason, we use a bottom-up approach. With this approach, students learn first about data communications (lower layers) before learning about networking (upper layers).

#### Visual Approach

The book presents highly technical subject matter without complex formulas by using a balance of text and figures. More than 700 figures accompanying the text provide a visual and intuitive opportunity for understanding the material. Figures are particularly important in explaining networking concepts, which are based on connections and transmission. Both of these ideas are easy to grasp visually.

#### Highlighted Points

We emphasize important concepts in highlighted boxes for quick reference and imme diate attention.

xxix xxx PREFACE

#### Examples and Applications

When appropriate, we have selected examples to reflect true-to-life situations. For exam ple, in Chapter 6 we have shown several cases of telecommunications in current telephone networks.

#### Recommended Reading

Each chapter includes a list of books and sites that can be used for further reading.

#### Key Terms

Each chapter includes a list of key terms for the student.

#### Summary

Each chapter ends with a summary of the material covered in that chapter. The sum mary provides a brief overview of all the important points in the chapter.

#### Practice Set

Each chapter includes a practice set designed to reinforce and apply salient concepts. It consists of three parts: review questions, exercises, and research activities (only for appropriate chapters). Review questions are intended to test the student's first-level under standing of the material presented in the chapter. Exercises require deeper understanding of the material Research activities are designed to create motivation for further study.

#### **Appendixes**

The appendixes are intended to provide quick reference material or a review of materials needed to understand the concepts discussed in the book.

#### Glossary andAcronyms

The book contains an extensive glossary and a list of acronyms.

#### **Changes in the Fourth Edition**

The Fourth Edition has major changes from the Third Edition, both in the organization and in the contents.

#### Organization

The following lists the changes in the organization of the book:

- 1. Chapter 6 now contains multiplexing as well as spreading.
- 2. Chapter 8 is now totally devoted to switching.
- 3. The contents of Chapter 12 are moved to Chapter 11.
- 4. Chapter 17 covers SONET technology.
- 5. Chapter 19 discusses IP addressing.
- 6. Chapter 20 is devoted to the Internet Protocol.
  - 7. Chapter 21 discusses three protocols: ARP, ICMP, and IGMP.
  - 8. Chapter 28 is new and devoted to network management in the Internet.
  - 9. The previous Chapters 29 to 31 are now Chapters 30 to 32.

PREFACE xxxi

#### **Contents**

We have revised the contents of many chapters including the following: 1. The contents of Chapters 1 to 5 are revised and augmented. Examples are added to clarify the contents.

- 2. The contents of Chapter 10 are revised and augmented to include methods of error detection and correction.
- 3. Chapter 11 is revised to include a full discussion of several control link protocols. 4. Delivery, forwarding, and routing of datagrams are added to Chapter 22. 5. The new transport protocol, SCTP, is added to Chapter 23.
- 6. The contents of Chapters 30, 31, and 32 are revised and augmented to include additional discussion about security issues and the Internet.
- 7. New examples are added to clarify the understanding of concepts.

#### End Materials

- 1. A section is added to the end of each chapter listing additional sources for study. 2. The review questions are changed and updated.
- 3. The multiple-choice questions are moved to the book site to allow students to self-test their knowledge about the contents of the chapter and receive immediate feedback. 4. Exercises are revised and new ones are added to the appropriate chapters. 5. Some chapters contain research activities.

#### Instructional Materials

Instructional materials for both the student and the teacher are revised and augmented. The solutions to exercises contain both the explanation and answer including full col ored figures or tables when needed. The Powerpoint presentations are more compre hensive and

include text and figures.

#### **Contents**

The book is divided into seven parts. The first part is an overview; the last part concerns network security. The middle five parts are designed to represent the five layers of the Internet model. The following summarizes the contents of each part.

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. Chapters 3 to 6 discuss telecommunication aspects of the physical layer. 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. Chapter 9 shows how two public networks, telephone and cable TV, can be used for data transfer.

xxxii PREFACE

Part Three: Data Link Layer

The third part is devoted to the discussion of the data link layer of the Internet model. Chapter 10 covers error detection and correction. Chapters 11, 12 discuss issues related to data link control. Chapters 13 through 16 deal with LANs. Chapters 17 and] 8 are about WANs. LANs and WANs are examples of networks operating in the first two lay ers of the Internet model.

Part Four: Network Layer

The fourth part is devoted to the discussion of the network layer of the Internet model. Chapter 19 covers **IP** addresses. Chapters 20 and 21 are devoted to the network layer protocols such as **IP**, ARP, ICMP, and IGMP. Chapter 22 discusses delivery, forwarding, and routing of packets in the Internet.

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. It also introduces three transport-layer protocols: UDP, TCP, and SCTP. Chapter 24 discusses congestion control and quality of service, two issues related to the transport layer and the previous two layers.

Part Six: Application Layer

The sixth part is devoted to the discussion of the application layer of the Internet model. Chapter 25 is about DNS, the application program that is used by other application programs to map application layer addresses to network layer addresses. Chapter 26 to 29 discuss some common applications protocols in the Internet.

Part Seven: Security

The seventh part is a discussion of security. It serves as a prelude to further study in this subject. Chapter 30 briefly discusses cryptography. Chapter 31 introduces security

aspects. Chapter 32 shows how different security aspects can be applied to three layers of the Internet model.

#### **Online Learning Center**

The McGraw-Hill Online Learning Center contains much additional material. Avail able 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 lec ture materials such as PowerPoint slides, and get additional review from animated fig ures 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.

Additionally, McGraw-Hill makes it easy to create a website for your networking course with an exclusive McGraw-Hill product called PageOut. It requires no prior knowledge of HTML, no long hours, and no design skills on your part. Instead, Page:- Out offers a series of templates. Simply fill them with your course information and

PREFACE xxxiii

click on one of 16 designs. The process takes under an hour and leaves you with a professionally designed website.

Although PageOut offers "instant" development, the finished website provides pow erful features. An interactive course syllabus allows you to post content to coincide with your lectures, so when students visit your PageOut website, your syllabus will direct them to components of Forouzan's Online Learning Center, or specific material of your own.

#### **How to Use the Book**

This book is written for both an academic and a professional audience. 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. The following are some guidelines. **O** Parts one to three are strongly recommended.

**O** Parts four to six can be covered if there is no following course in TCP/IP protocol. **O** Part seven is recommended if there is no following course in network security.

#### Acknowledgments

It is obvious that the development of a book of this scope needs the support ofmany people.

Peer Review

The most important contribution to the development of a book such as this comes from peer reviews. We cannot express our gratitude in words to the many reviewers who spent numerous hours reading the manuscript and providing us with helpful comments and ideas. We would especially like to acknowledge the contributions of the following reviewers for the third and fourth editions of this book.

Farid Ahmed, Catholic University
Kaveh Ashenayi, University of Tulsa
Yoris Au, University of Texas, San Antonio
Essie Bakhtiar, Clayton College & State University
Anthony Barnard, University of Alabama, Brimingham

A.T. Burrell, Oklahoma State University

Scott Campbell, Miami University

Teresa Carrigan, Blackburn College

Hwa Chang, Tufts University

Edward Chlebus, Illinois Institute of Technology

Peter Cooper, Sam Houston State University

Richard Coppins, Virginia Commonwealth University

Harpal Dhillon, Southwestern Oklahoma State University

Hans-Peter Dommel, Santa Clara University

M. Barry Dumas, Baruch College, CUNY

William Figg, Dakota State University

Dale Fox, Quinnipiac University

Terrence Fries, Coastal Carolina University

Errin Fulp, Wake Forest University

#### xxxiv PREFACE

Sandeep Gupta, Arizona State University

George Hamer, South Dakota State University

James Henson, California State University, Fresno

Tom Hilton, Utah State University

Allen Holliday, California State University, Fullerton

Seyed Hosseini Hosseini, University of Wisconsin, Milwaukee

Gerald Isaacs, Carroll College, Waukesha

Hrishikesh Joshi, DeVry University

E.S. Khosravi, Southern University

Bob Kinicki, Worcester Polytechnic University

Kevin Kwiat, Hamilton College

Ten-Hwang Lai, Ohio State University

Chung-Wei Lee, Auburn University

Ka-Cheong Leung, Texas Tech University

Gertrude Levine, Fairleigh Dickinson University

Alvin Sek See Lim, Auburn University

Charles Liu, California State University, Los Angeles

Wenhang Liu, California State University, Los Angeles

Mark Llewellyn, University of Central Florida

Sanchita Mal-Sarkar, Cleveland State University

Louis Marseille, Harford Community College

Kevin McNeill, University of Arizona

Arnold C. Meltzer, George Washington University

Rayman Meservy, Brigham Young University

Prasant Mohapatra, University of California, Davis

Hung Z Ngo, SUNY, Buffalo

Larry Owens, California State University, Fresno

Arnold Patton, Bradley University

Dolly Samson, Hawaii Pacific University

Joseph Sherif, California State University, Fullerton

Robert Simon, George Mason University

Ronald 1. Srodawa, Oakland University

Daniel Tian, California State University, Monterey Bay

Richard Tibbs, Radford University

Christophe Veltsos, Minnesota State University, Mankato

er, proved how a ne developmen tal anager, guided us nk David Hash in

### Overview



Part 1



provides a general idea of what we will see in the rest of the book. Four major concepts are discussed: data communications, networking, protocols and standards, and networking models.

Networks exist so that data may be sent from one place to another-the basic con cept of *data communications*. To fully grasp this subject, we must understand the data communication components, how different types of data can be represented, and how to create a data flow.

Data communications between remote parties can be achieved through a process called *networking*, involving the connection of computers, media, and networking devices. Networks are divided into two main categories: local area networks (LANs) and wide area networks (WANs). These two types of networks have different charac teristics and different functionalities. The Internet, the main focus of the book, is a collection of LANs and WANs held together by internetworking devices.

*Protocols and standards* are vital to the implementation of data communications and networking. Protocols refer to the rules; a standard is a protocol that has been adopted by vendors and manufacturers.

*Network models* serve to organize, unify, and control the hardware and software components of data communications and networking. Although the term "network model" suggests a relationship to networking, the model also encompasses data communications.

#### **Chapters**

This part consists of two chapters: Chapter 1 and Chapter 2.

#### Chapter 1

In Chapter 1, we introduce the concepts of data communications and networking. We discuss data communications components, data representation, and data flow. We then move to the structure of networks that carry data. We discuss network topologies, categories of networks, and the general idea behind the Internet. The section on protocols and standards gives a quick overview of the organizations that set standards in data communications and networking.

#### Chapter 2

The two dominant networking models are the Open Systems Interconnection (OSI) and the Internet model (TCP/IP). The first is a theoretical framework; the second is the actual model used in today's data communications. In Chapter 2. we first discuss the OSI model to give a







#### Introduction

Data communications and networking are changing the way we do business and the way we live. Business decisions have to be made ever more quickly, and the decision makers require immediate access to accurate information. Why wait a week for that report from Germany to arrive by mail when it could appear almost instantaneously through computer networks? Businesses today rely on computer networks and internetworks. 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.

The development of the personal computer brought about tremendous changes for business, industry, science, and education. A similar revolution is occurring in data communications and networking. Technological advances are making it possible for communications links to carry more and faster signals. As a result, services are evolving to allow use of this expanded capacity. For example, established telephone services such as conference calling, call waiting, voice mail, and caller **ID** have been extended.

Research in data communications and networking has resulted in new technolo gies. One goal is to be able to exchange data such as text, audio, and video from all points in the world. We want to access the Internet to download and upload information quickly and accurately and at any time.

This chapter addresses four issues: data communications, networks, the Internet, and protocols and standards. First we give a broad definition of data communications. Then we define networks as a highway on which data can travel. The Internet is discussed as a good example of an internetwork (i.e., a network of networks). Finally, we discuss different types of protocols, the difference between protocols and standards, and the organizations that set those standards.

#### 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

3

#### 4 CHAPTER 1 INTRODUCTION

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 com bination of hardware (physical equipment) and software (programs). The effectiveness of a data

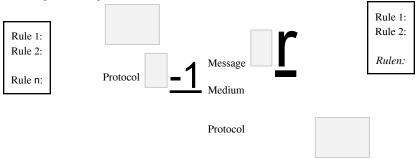
communications system depends on four fundamental characteristics: deliv ery, accuracy, timeliness, and jitter.

- I. 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.
- ■7 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.
- □-\.. 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 3D ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

#### **COinponents**

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

Figure 1.1 Five components of data communication



- I. Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video. 

  Sender. The sender is the device that sends the data message. It can be a com puter, workstation, telephone handset, video camera, and so on.
- ■3. Receiver. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
- □-1.. 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.

SECTION 1.1 DATA COMMUNICATIONS 5

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.

#### **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 (Os or Is).

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 I-bit pattern is enough to represent a pixel.

If an image is not made of pure white and pure black pixels, you can increase the size of the bit pattern to include gray scale. For example, to show four levels of gray scale, you 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 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 6 CHAPTER 1 INTRODUCTION

use a microphone to change voice or music to an electric signal, we create a continuous signal. In Chapters 4 and 5, we learn how to change sound or music to a digital or an analog signal.

#### 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. Again we can change video to a digital or an analog signal, as we will see in Chapters 4 and 5.

#### 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, andfull-duplex)

Direction of data

Monitor

a. Simplex

Direction of data at time I

Direction of data at time 2

b. Half-duplex

c. Full-duplex

Simplex

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 key board 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.

#### 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).

SECTION 1.2 NETWORKS 7

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 m.,lle (als@ called duplex), both stations can transmit	
and receive simul taneously (see Figure 1.2c).	
The full-duplex mode is like atW <d-way bot<="" flowing="" in="" street="" td="" traffic="" with=""><td>th</td></d-way>	th
directions at the same time. In full-duplex mode, si-nals going in one direction shared	re
the capacity of the link: with signals going in the other din-c-on. This sharing ca	ın

occur in two ways: Either the link must contain two physically separate t:nmsmissiIDn paths, one for sending and the other for receiving; or the capacity of the ch:arillilel 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 a set of devices (often referred to as *nodes*) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

### **Distributed Processing**

Most networks use distributed processing, in which a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of a process, separate computers (usually a personal computer or workstation) handle a subset.

### Network Criteria

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

### 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 8 *CHAPTER 1 INTRODUCTION* 

another. Response time is the elapsed time between an inquiry and a response. The per formance 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.

### **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 con nect the two ends, but other options, such as microwave or satellite links, are also possi ble (see Figure 1.3a). When you change television channels by infrared remote control, you 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).

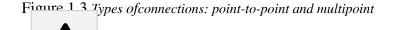
In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

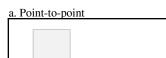
### Physical Topology

The term *physical topology* refers to the way in which a network is laid out physically.: 1\vo or more devices connect to a link; two or more links form a topology. The topology

SECTION 1.2 NETWORKS 9









b. Multipoint

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 (see Figure 1.4).

Figure **1.4** Categories oftopology



Mesh 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 - I 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 (VO) ports (see Figure 1.5) to be connected to the other n-1 stations. 10 CHAPTER 1 INTRODUCTION

Figure 1.5 A fully connected mesh topology (five devices)



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 elimi nating 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 incapaci tate 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.

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 accom modate. 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 con nected device (see Figure 1.6).

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 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 SECTION 1.2 NETWORKS 11

**Figure 1.6** A star topology connecting four stations



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 1.7).

**Figure 1.7** A bus topology connecting three stations



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 ofits 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

12 CHAPTER 1 INTRODUCTION

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 near est 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 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. 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 con nection 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 1.8).

Figure 1.8 A ring topology connecting six stations









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 consider ations (maximum ring length and number of devices). In addition, fault isolation is sim plified. 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.

SECTION 1.2 NETWORKS 13

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.

Hybrid Topology A network can be hybrid. For example, we can have a main star topol ogy with each branch connecting several stations in a bus topology as shown in Figure 1.9.

Figure 1.9 A hybrid topology: a star backbone with three bus networks Hub



#### **Network Models**

Computer networks are created by different entities. Standards are needed so that these heterogeneous networks can communicate with one another. The two best-known stan dards are the OSI model and the Internet model. In Chapter 2 we discuss these two models. The OSI (Open Systems Interconnection) model defines a seven-layer net work; the Internet model defines a five-layer network. This book is based on the Internet model

with occasional references to the OSI model.

### Categories of Networks

Today when we speak of networks, we are generally referring to two primary catego ries: local-area networks and wide-area networks. The category into which a network falls is determined by its size. A LAN normally covers an area less than 2 mi; a WAN can be worldwide. Networks of a size in between are normally referred to as metropolitan area networks and span tens of miles.

#### Local Area Network

A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus (see Figure 1.10). Depending on the needs of an organization and the type of technology used, 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 peripherals. Currently, LAN size is limited to a few kilometers.

14 CHAPTER 1 INTRODUCTION

Figure 1.10 An isolated IAN connecting 12 computers to a hub in a closet



LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data. A common example of a LAN, found in many business environments, links a workgroup of task-related computers, for example, engi neering workstations or accounting PCs. One of the computers may be given a large capacity disk drive and may become a server to clients. Software can be stored on this central server and used as needed by the whole group. In this example, the size of the LAN may be determined by licensing restrictions on the number of users per copy of soft ware, or by restrictions on the number of users licensed to access the operating system.

In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star.

Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps. LANs are discussed at length in Chapters 13, 14, and 15.

Wireless LANs are the newest evolution in LAN technology. We discuss wireless LANs in detail in Chapter 14.

A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. In Chapters 17 and 18 we discuss wide-area networks in greater detail. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. We normally refer to the first as a switched WAN and to the second as a point-to-point WAN (Figure 1.11). The switched WAN connects the end systems, which usually comprise a router (internet working connecting device) that connects to another LAN or WAN. The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (ISP). This type of WAN is often

a. Switched WAN

b. Point-to-point WAN Modem Modem - ISP

Computer

An early example of a switched WAN is X.25, a network designed to provide con mectivity between end users. As we will see in Chapter 18, X.25 is being gradually replaced by a high-speed, more efficient network called Frame Relay. A good example of a switched WAN is the asynchronous transfer mode (ATM) network, which is a net work with fixed-size data unit packets called cells. We will discuss ATM in Chapter 18. Another example of WANs is the wireless WAN that is becoming more and more popular. We discuss wireless WANs and their evolution in Chapter 16.

### Metropolitan Area Networks

A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city. A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer. Another example is the cable TV network that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet. We discuss DSL lines and cable TV networks in Chapter 9.

### Interconnection of Networks: Internetwork

Today, it is very rare to see a LAN, a MAN, or a LAN in isolation; they are con nected to one another. When two or more networks are connected, they become an internetwork, or internet.

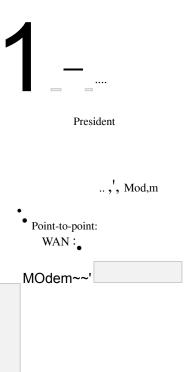
As an example, assume that an organization has two offices, one on the east coast and the other on the west coast. The established office on the west coast has a bus topology LAN; the newly opened office on the east coast has a star topology LAN. The president of the company lives somewhere in the middle and needs to have control over the company

**16** CHAPTER 1 INTRODUCTION

from her horne. To create a backbone WAN for connecting these three entities (two LANs and the president's computer), a switched WAN (operated by a service provider such as a telecom company) has been leased. To connect the LANs to this switched WAN, however, three point-to-point WANs are required. These point-to-point WANs can be a high-speed DSL line offered by a telephone company or a cable modern line offered by a cable TV provider as shown in Figure 1.12.

**Figure 1.12** A heterogeneous network made offour WANs and two LANs







LAN

LAN

### 1.3 THE INTERNET

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. Count the ways you've used the Internet recently. Perhaps you've sent electronic mail (e-mail) to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule-all by using the Internet. Or maybe you researched a medical topic, booked a hotel reservation, chatted with a fellow Trekkie, or comparison-shopped for a car. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.

The Internet is a structured, organized system. We begin with a brief history of the Internet. We follow with a description of the Internet today.

SECTION 1.3 THE INTERNET 17

# A Brief History

A network is a group of connected communicating devices such as computers and printers. An internet (note the lowercase letter i) is two or more networks that can communicate with each other. The most notable internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected net works. Private

individuals as well as various organizations such as government agen cies, schools, research facilities, corporations, and libraries in more than 100 countries use the Internet. Millions of people are users. Yet this extraordinary communication sys tem only came into being in 1969. 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 Depart ment 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 elim inating duplication of effort.

In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA pre sented its ideas for 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 *inteiface message processor* (IMP). The IMPs, in tum, would be connected to one another. 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 com munication between the hosts. In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the *Internetting Projec1*. Cerf and Kahn's land mark 1973 paper outlined the protocols to achieve end-to-end delivery of packets. This paper on Transmission Control Protocol (TCP) included concepts such as encapsula tion, the datagram, and the functions of a gateway.

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

### The Internet Today

The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure. It is made up of many wide- and local-area networks joined by connecting devices and switching stations. It is difficult to give an accurate representation of the Internet because it is continually changing-new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed. Today most end users who want Internet connection use the services of Internet service providers (ISPs). There are international service providers, national

18 CHAPTER 1 INTRODUCTION



service providers, regional service providers, and local service providers. The Internet today is run by private companies, not the government. Figure 1.13 shows a conceptual (not geographic) view of the Internet.

Figure 1.13 Hierarchical organization of the Internet



National ISP

#### International Internet Service Providers

At the top of the hierarchy are the international service providers that connect nations together.

#### National Internet Service Providers

The national Internet service providers are backbone networks created and main tained by specialized companies. There are many national ISPs operating in North America; some of the most well known are SprintLink, PSINet, UUNet Technology, AGIS, and internet Mel. To provide connectivity between the end users, these back bone networks are connected by complex switching stations (normally run by a third party) called network access points (NAPs). Some national ISP networks are also connected to one another by private switching stations called *peering points*. These normally operate at a high data rate (up to 600 Mbps).

SECTION 1.4 PROTOCOLS AND STANDARDS 19

#### Regional Internet Service Providers

Regional internet service providers or regional ISPs are smaller ISPs that are connected to one or more national ISPs. They are at the third level of the hierarchy with a smaller data rate.

#### Local Internet Service Providers

Local Internet service providers provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to national ISPs. Most end users are connected to the local ISPs. Note that in this sense, a local ISP can be a company that just provides Internet services, a corporation with a network that supplies services to its own employees, or a nonprofit organization, such as a college or a university, that runs its own network. Each of these local ISPs can be connected to a regional or national service provider.

# 1.4 PROTOCOLS AND STANDARDS

In this section, we define two widely used terms: protocols and standards. First, we define *protocol*, which is synonymous with *rule*. Then we discuss *standards*, which are agreed-upon rules.

### **Protocols**

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities can not simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key

elements of a protocol are syntax, semantics, and timing. **O** Syntax. The term *syntax* refers to the structure or format of the data, meaning the

order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

**O** Semantics. The word *semantics* refers to the meaning of each section of bits. How is a

particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?

**O** Timing. The term *timing* refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

### Standards

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes. Standards provide guidelines 20 CHAPTER 1 INTRODUCTION

to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international com munications. Data communication standards fall into two categories: *de facto* (meaning "by fact" or "by convention") and *de jure* (meaning "by law" or "by regulation").

- O De facto. Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.
- **O** De jure. Those standards that have been legislated by an officially recognized body are de jure standards.

# **Standards Organizations**

Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

#### Standards Creation Committees

While many organizations are dedicated to the establishment of standards, data tele communications in North America rely primarily on those published by the following:

- O International Organization for Standardization (ISO). The ISO is a multinational body whose membership is drawn mainly from the standards creation committees of various governments throughout the world. The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.
- O International Telecommunication Union-Telecommunication Standards Sector (ITU-T). By the early 1970s, a number of countries were defining national standards for telecommunications, but there was still little international compati bility. The United Nations responded by forming, as part of its International Telecommunication Union (ITU), a committee, the Consultative Committee for International Telegraphy and Telephony (CCITT). This committee was devoted to the research and establishment of standards for telecommunications in general and for phone and data systems in particular. On March 1, 1993, the name of this committee was changed to the International Telecommunication Union Telecommunication Standards Sector (ITU-T).
- O American National Standards Institute (ANSI). Despite its name, the American National Standards Institute is a completely private, nonprofit corporation not affili ated with the U.S. federal government. However, all ANSI activities are undertaken

with the welfare of the United States and its citizens occupying primary importance.

- O Institute of Electrical and Electronics Engineers (IEEE). The Institute of Electrical and Electronics Engineers is the largest professional engineering society in the world. International in scope, it aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics, and radio as well as in all related branches of engineering. As one of its goals, the IEEE oversees the develop ment and adoption of international standards for computing and communications.
- O Electronic Industries Association (EIA). Aligned with ANSI, the Electronic Industries Association is a nonprofit organization devoted to the promotion of SECTION 1.5 RECOMMENDED READING 21

electronics manufacturing concerns. Its activities include public awareness education and lobbying efforts in addition to standards development. In the field of information technology, the EIA has made significant contributions by defining physical connection interfaces and electronic signaling specifications for data communication.

#### **Forums**

Telecommunications technology development is moving faster than the ability of stan dards committees to ratify standards. Standards committees are procedural bodies and by nature slow-moving. To accommodate the need for working models and agreements and to facilitate the standardization process, many special-interest groups have devel oped **forums** made up of representatives from interested corporations. The forums work with universities and users to test, evaluate, and standardize new technologies. By concentrating their efforts on a particular technology, the forums are able to speed acceptance and use of those technologies in the telecommunications community. The forums present their conclusions to the standards bodies.

#### Regulatory Agencies

All communications technology is subject to regulation by government agencies such as the **Federal Communications Commission** (FCC) in the United States. The pur pose of these agencies is to protect the public interest by regulating radio, television, and wire/cable communications. The FCC has authority over interstate and interna tional commerce as it relates to communications.

### **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 fol lowed. 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 docu ment (a work in progress) with no official status and a 6-month lifetime. Upon recom mendation 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.

# 1.5 RECOMMENDED READING

For more details about subjects discussed in this chapter, we recommend the following books and sites. 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] discusses standardization in Section 1.6.

22 CHAPTER 1 INTRODUCTION

### **Sites**

The following sites are related to topics discussed in this chapter.

**O** www.acm.org/sigcomm/sos.html This site gives the status of varililus networking standards.

**O** www.ietf.org/ The Internet Engineering Task Force (IETF) home page.

### **RFCs**

The following site lists all RFCs, including those related to IP and TCP. In future chap ters we cite the RFCs pertinent to the chapter material.

O www.ietf.org/rfc.html

# 1.6 KEY TERMS

Advanced Research Projects

Agency (ARPA)

American National Standards

Institute (ANSI)

American Standard Code for

Information Interchange (ASCII) ARPANET

audio

backbone

**Basic Latin** 

bus topology

code

Consultative Committee for

**International Telegraphy** 

and Telephony (CCITT)

data

data communications

de facto standards

de jure standards

delay

distributed processing

Electronic Industries Association (EIA) entity

Federal Communications Commission (FCC)

forum

hub image Institute of Electrical and Electronics Engineers (IEEE) International Organization for Standardization (ISO) International Telecommunication Union-Telecommunication Standards Sector (ITU-T) Internet Internet draft Internet service provider (ISP) Internet standard internetwork or internet local area network (LAN) local Internet service providers mesh topology message metropolitan area network (MAN) multipoint or multidrop connection national Internet service provider network sender network access points (NAPs) node simplex mode performance star topology physical topology syntax point-to-point connection protocol telecommunication receiver throughput regional ISP timing reliability Transmission Control Protocol! Request for Comment (RFC) ROB Internetworking Protocol (TCPIIP) transmission medium ring topology security Unicode video semantics wide area network (WAN) YCM 1.7 SUMMARY SECTION 1.7 SUMMARY 23 O Data communications are the transfer of data from one device to another via some form of transmission medium.

full-duplex mode, or duplex half-duplex mode

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

	t is a set of communication devices connected by media links. <b>O</b> In a teconnection, two and only two devices are connected by a dedicated link. In
_	connection, three or more devices share a link. <b>O</b> Topology refers to the gical arrangement of a network. Devices may be arranged in a mesh, star, opology.
	can be categorized as a local area network or a wide area network. O A a communication system within a building, plant, or campus, or between ngs.
O A WAN is world.	a data communication system spanning states, countries, or the whole
O An interne	et is a network of networks.
O The Intern	et is a collection of many separate networks.
protocol is a s	local, regional, national, and international Internet service providers. <b>O</b> A set of rules that govern data communication; the key elements of a protocol mantics, and timing. <i>DUCTION</i>
0	Standards are necessary to ensure that products from different manufacturers can work together as expected.
0	The ISO, ITD-T, ANSI, IEEE, and EIA are some of the organizations involved in standards creation.
0	Forums are special-interest groups that quickly evaluate and standardize new technologies.
0	A Request for Comment is an idea or concept that is a precursor to an Internet standard.

# 1.8 PRACTICE SET

# **Review Questions**

- 1. Identify the five components of a data communications system.
- ■2. What are the advantages of distributed processing?
  - ■3. What are the three criteria necessary for an effective and efficient network?
  - 4. What are the advantages of a multipoint connection over a point-to-point connection?
- 5. What are the two types of line configuration?
  - 6. Categorize the four basic topologies in terms of line configuration.
- 7. What is the difference between half-duplex and full-duplex transmission modes?  $\square 8$ . Name the four basic network topologies, and cite an advantage of each type.
- 9. For *n* devices in a network, what is the number of cable links required for a mesh, ring, bus, and star topology?
- 10. What are some of the factors that determine whether a communication system is a LAN or WAN?
- 11. What is an internet? What is the Internet?
- 12. Why are protocols needed?

13. Why are standards needed?

### **Exercises**

- 14. What is the maximum number of characters or symbols that can be represented by Unicode?
- 15. A color image uses 16 bits to represent a pixel. What is the maximum number of different colors that can be represented?
- 16. Assume six devices are arranged in a mesh topology. How many cables are needed? How many ports are needed for each device?
- 17. 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

SECTION 1.8 PRACTICE SET 25

- 18. You have two computers connected by an Ethernet hub at home. Is this a LAN, a MAN, or a WAN? Explain your reason.
- 19. In the ring topology in Figure 1.8, what happens if one of the stations is unplugged?
- 20. **In** the bus topology in Figure 1.7, what happens if one of the stations is unplugged?
- 21. Draw a hybrid topology with a star backbone and three ring networks. 22. Draw a hybrid topology with a ring backbone and two bus networks. 23. Performance is inversely related to delay. When you 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
- 24. When a party makes a local telephone call to another party, is this a point-to-point or multipoint connection? Explain your answer.
- 25. Compare the telephone network and the Internet. What are the similarities? What are the differences?

### **Research Activities**

- 26. Using the site \\iww.cne.gmu.edu/modules/network/osi.html, discuss the OSI model.
- 27. Using the site www.ansi.org, discuss ANSI's activities.
- 28. Using the site www.ieee.org, discuss IEEE's activities.
- 29. Using the site www.ietf.org/, discuss the different types of RFCs.



# CHAPTER 2 Network Models

A network is a combination of hardware and software that sends data from one location to another. The hardware consists of the physical equipment that carries signals from one point of the network to another. The software consists of instruction sets that make possible the services that we expect from a network.

We can compare the task of networking to the task of solving a mathematics problem with a computer. The fundamental job of solving the problem with a computer is done by computer hardware. However, this is a very tedious task if only hardware is involved. We would need switches for every memory location to store and manipulate data. The task is much easier if software is available. At the highest level, a program can direct the problem-solving process; the details of how this is done by the actual hardware can be left to the layers of software that are called by the higher levels.

Compare this to a service provided by a computer network. For example, the task of sending an e-mail from one point in the world to another can be broken into several tasks, each performed by a separate software package. Each software package uses the services of another software package. At the lowest layer, a signal, or a set of signals, is sent from the source computer to the destination computer.

In this chapter, we give a general idea of the layers of a network and discuss the functions of each. Detailed descriptions of these layers follow in later chapters.

### 2.1 LAYERED TASKS

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal maiL The process of sending a letter to a friend would be complex if there were no services available from the post office. Fig ure 2.1 shows the steps in this task.

27 28 CHAPTER 2 NETWORK MODELS

Figure 2.1 Tasks involved in sending a letter



Sender



The letter is written, The letter is picked up, put in an envelope, and Higher layers removed from the



dropped in a mailbox. envelope, and read.

The letter is carried The letter is carried from the mailbox Middle layers from the post office to a post office. to the mailbox.



The letter is delivered The letter is delivered to a carrier by the post Lower layers from the carrier office. to the post office.



The parcel is carried from the source to the destination.

### Sender, Receiver, and Carrier

In Figure 2.1 we have a sender, a receiver, and a carrier that transports the letter. There is a hierarchy of tasks.

At the Sellder Site

Let us first describe, in order, the activities that take place at the sender site. O Higher layer. The sender writes the letter, inserts the letter in an envelope, writes the sender and receiver addresses, and drops the letter in a mailbox. O Middle layer. The letter is picked up by a letter carrier and delivered to the post office.

O Lower layer. The letter is sorted at the post office; a carrier transports the letter.

011 *the Way* 

The letter is then on its way to the recipient. On the way to the recipient's local post office, the letter may actually go through a central office. In addition, it may be trans ported by truck, train, airplane, boat, or a combination of these.

At the Receiver Site

O Lower layer. The carrier transports the letter to the post office. O Middle layer.

The letter is sorted and delivered to the recipient's mailbox. O Higher layer. The receiver picks up the letter, opens the envelope, and reads it.

SECTION 2.2 THE OS! MODEL 29

# Hierarchy

According to our analysis, there are three different activities at the sender site and another three activities at the receiver site. The task of transporting the letter between the sender and the receiver is done by the carrier. Something that is not obvious immediately is that

the tasks must be done in the order given in the hierarchy. At the sender site, the letter must be written and dropped in the mailbox before being picked up by the letter carrier and delivered to the post office. At the receiver site, the letter must be dropped in the recipient mailbox before being picked up and read by the recipient.

#### Services

Each layer at the sending site uses the services of the layer immediately below it. The sender at the higher layer uses the services of the middle layer. The middle layer uses the services of the lower layer. The lower layer uses the services of the carrier.

The layered model that dominated data communications and networking literature before 1990 was the Open Systems Interconnection (OSI) model. Everyone believed that the OSI model would become the ultimate standard for data communications, but this did not happen. The TCPIIP protocol suite became the dominant commercial archi tecture because it was used and tested extensively in the Internet; the OSI model was never fully implemented.

In this chapter, first we briefly discuss the OSI model, and then we concentrate on TCPIIP as a protocol suite.

# 2.2 THE OSI MODEL

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model. It was first introduced in the late 1970s. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hard ware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

ISO is the organization. OSI is the model.

The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven sep arate but related layers, each of which defines a part of the process of moving information across a network (see Figure 2.2). An understanding of the fundamentals of the OSI model provides a solid basis for exploring data communications.

30 CHAPTER 2 NETWORK MODELS

Figure 2.2 Seven layers of the OSI model

Application
Presentation
Session

Transport

31 Network

21 Data link

1 Physical

# Layered Architecture

The OSI model is composed ofseven ordered layers: physical (layer 1), data link (layer 2), network (layer 3), transport (layer 4), session (layer 5), presentation (layer 6), and application (layer 7). Figure 2.3 shows the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.

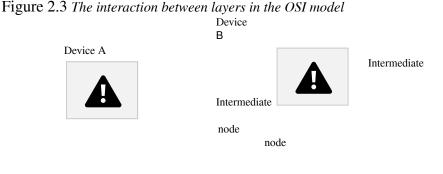
In *developing* the model, the designers distilled the process of transmitting data to its most fundamental elements. They identified which networking functions had related uses and collected those functions into discrete groups that became the layers. Each layer defines a family of functions distinct from those of the other layers. By defining and localizing functionality in this fashion, the designers created an architecture that is both comprehensive and flexible. Most importantly, the OSI model allows complete interoperability between otherwise incompatible systems.

Within a single machine, each layer calls upon the services of the layer just below it. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4. Between machines, layer x on one machine communicates with layer x on another machine. This communication is governed by an agreed-upon series of rules and conventions called protocols. The processes on each machine that communicate at a given layer are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

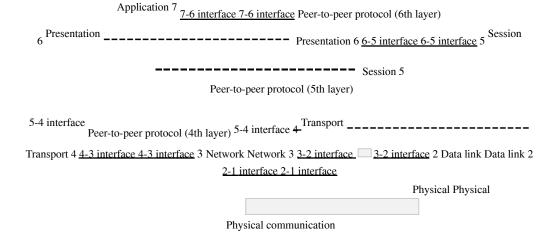
#### **Peer-to-Peer** Processes

At the physical layer, communication is direct: In Figure 2.3, device A sends a stream of bits to device B (through intermediate nodes). At the higher layers, however, com munication must move down through the layers on device A, over to device B, and then

SECTION 2.2 THE OSI MODEL 31



Peer-to-peer protocol Oth layer)



back up through the layers. Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it.

At layer I the entire package is converted to a form that can be transmitted to the receiving device. At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it. For example, layer 2 removes the data meant for it, then passes the rest to layer 3. Layer 3 then removes the data meant for it and passes the rest to layer 4, and so on.

#### Interfaces Between Layers

The passing of the data and network information down through the layers of the send ing device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers. Each interface defines the information and services a layer must provide for the layer above it. Well-defined interfaces and layer functions provide modularity to a network. As long as a layer provides the expected services to the layer above it, the specific implementation of its functions can be modified or replaced without requiring changes to the surrounding layers.

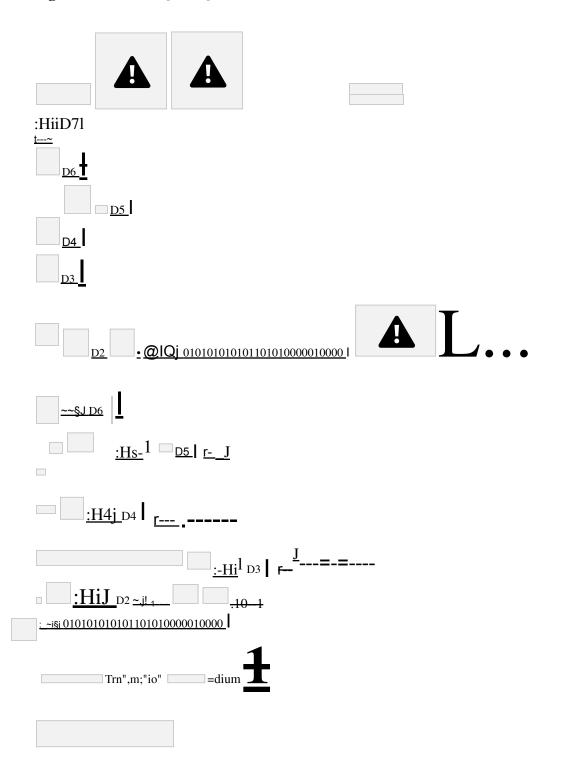
### Organization of the Layers

The seven layers can be thought of as belonging to three subgroups. Layers I, 2, and 3-physical, data link, and network-are the network support layers; they deal with 32 CHAPTER 2 NETWORK MODELS

the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing, and transport timing and reliability). Layers 5, 6, and 7-session, presentation, and application-can be thought of as the user support layers; they allow interoperability among unrelated software systems. Layer 4, the transport layer, links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use. The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

In Figure 2.4, which gives an overall view of the OSI layers, D7 means the data unit at layer 7, D6 means the data unit at layer 6, and so on. The process starts at layer 7 (the application layer), then moves from layer to layer in descending, sequential order. At each layer, a **header**, or possibly a **trailer**, can be added to the data unit. Commonly, the trailer is added only at layer 2. When the formatted data unit passes through the physical layer (layer 1), it is changed into an electromagnetic signal and transported along a physical link.

Figure 2.4 An exchange using the OS! model



Upon reaching its destination, the signal passes into layer 1 and is transformed back into digital form. The data units then move back up through the OSI layers. As each block of data reaches the next higher layer, the headers and trailers attached to it at the corresponding sending layer are removed, and actions appropriate to that layer are taken. By the time it reaches layer 7, the message is again in a form appropriate to the application and is made available to the recipient.

Figure 2.3 reveals another aspect of data communications in the OSI model: encapsula tion. A packet (header and data) at level 7 is encapsulated in a packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5, and so on.

In other words, the data portion of a packet at level N - 1 carries the whole packet (data and header and maybe trailer) from level N. The concept is called *encapsulation*; level N - 1 is not aware of which part of the encapsulated packet is data and which part is the header or trailer. For level N - 1, the whole packet coming from level N is treated as one integral unit.

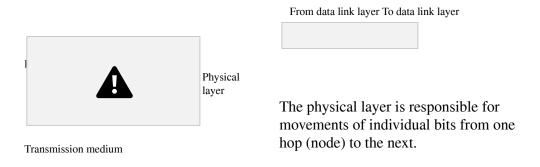
### 2.3 LAYERS IN THE OSI MODEL

In this section we briefly describe the functions of each layer in the OSI model.

### Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physi cal medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur. Figure 2.5 shows the position of the physical layer with respect to the transmission medium and the data link layer.

Figure 2.5 Physical layer



The physical layer is also concerned with the following:

- O Physical characteristics of interfaces and medium. The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
- O Representation of bits. The physical layer data consists of a stream of bits (sequence of Os or 1s) with no interpretation. To be transmitted, bits must be 34 CHAPTER 2 NETWORK MODELS

encoded into signals--electrical or optical. The physical layer defines the type of encoding (how Os and Is are changed to signals).

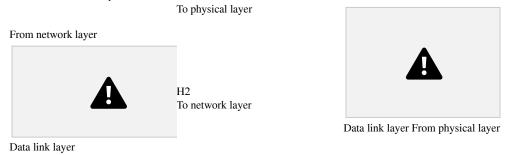
- O Data rate. The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the dura tion of a bit, which is how long it lasts.
- O Synchronization of bits. The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.

- **O** Line configuration. The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.
- O Physical topology. The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology (every device is on a common link), or a hybrid topology (this is a combination of two or more topologies).
- O Transmission mode. The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

### Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reli able link. It makes the physical layer appear error-free to the upper layer (network layer). Figure 2.6 shows the relationship of the data link layer to the network and physicallayers.

Figure 2.6 Data link layer



SECTION 2.3 LAYERS IN THE OSI MODEL 35

The data link layer is responsible for moving frames from one hop (node) to the next.

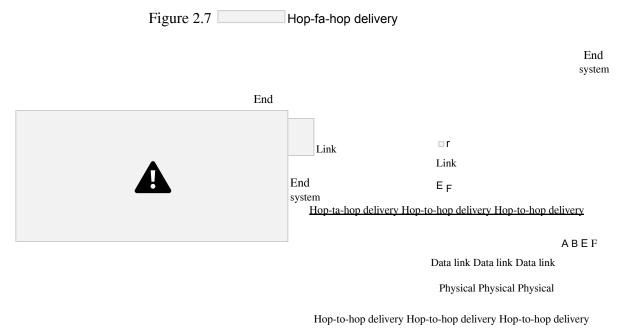
Other responsibilities of the data link layer include the following:

- [I Framing. The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- O Physical addressing. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.
- D Flow control. If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
- O Error control. The data link layer adds reliability to the physical layer by adding

mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.

D Access control. When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Figure 2.7 illustrates hop-to-hop (node-to-node) delivery by the data link layer.



As the figure shows, communication at the data link layer occurs between two adjacent nodes. To send data from A to F, three partial deliveries are made. First, the data link layer at A sends a frame to the data link layer at B (a router). Second, the data *36 CHAPTER 2 NETWORK MODELS* 

link layer at B sends a new frame to the data link layer at E. Finally, the data link layer at E sends a new frame to the data link layer at F. Note that the frames that are exchanged between the three nodes have different values in the headers. The frame from A to B has B as the destination address and A as the source address. The frame from B to E has E as the destination address and B as the source address. The frame from E to F has F as the destination address and E as the source address. The values of the trailers can also be different if error checking includes the header of the frame.

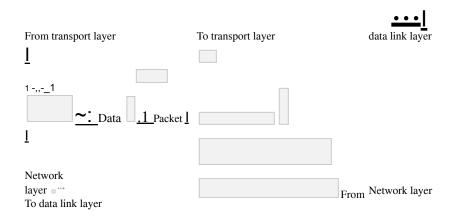
# Network Layer

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

If two systems are connected to the same link, there is usually no need for a net work layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery. Figure 2.8 shows the relationship of the network layer to the data link and transport layers.

Figure 2.8 Network layer





The network layer is responsible for the delivery of individual packets from the source host to the destination host.

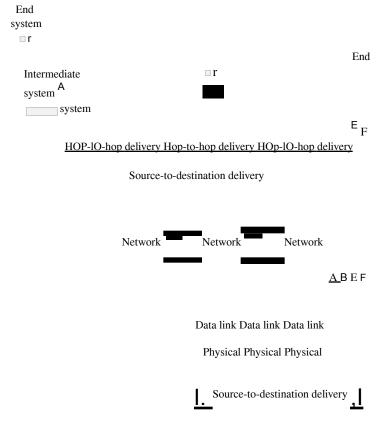
Other responsibilities of the network layer include the following:

- O Logical addressing. The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver. We discuss logical addresses later in this chapter.
- O Routing. When independent networks or links are connected to create *intemetworks* (network of networks) or a large network, the connecting devices (called *routers* SECTION 2.3 LAYERS IN THE OSI MODEL 37

or *switches*) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

Figure 2.9 illustrates end-to-end delivery by the network layer.

Figure 2.9 Source-to-destination delivery



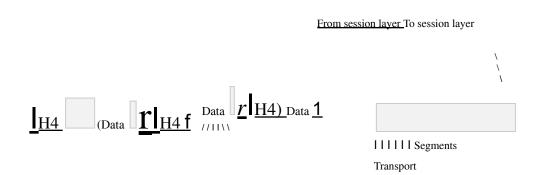
As the figure shows, now we need a source-to-destination delivery. The network layer at A sends the packet to the network layer at B. When the packet arrives at router B, the router makes a decision based on the final destination (F) of the packet. As we will see in later chapters, router B uses its routing table to find that the next hop is router E. The network layer at B, therefore, sends the packet to the network layer at E. The network layer at E, in tum, sends the packet to the network layer at F.

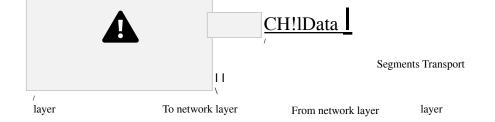
# Transport Layer

The transport layer is responsible for process-to-process delivery of the entire mes sage. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level. Figure 2.10 shows the relationship of the transport layer to the network and session layers.

38 CHAPTER 2 NETWORK MODELS

Figure 2.10 Transport layer





The transport layer is responsible for the delivery of a message from one process to another.

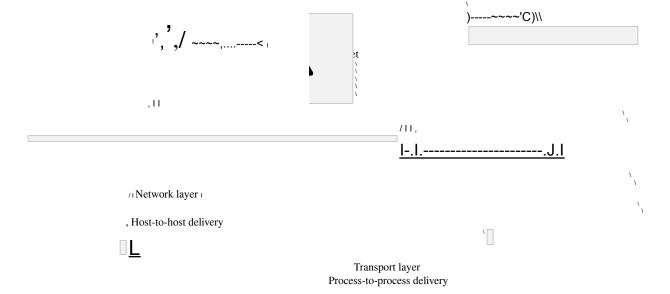
Other responsibilities of the transport layer include the following:

- O Service-point addressing. Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a *service-point address* (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
- O Segmentation and reassembly. A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the trans port layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
- O Connection control. The transport layer can be either connectionless or connection oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
- O Flow control. Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
- O Error control. Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

SECTION 2.3 LAYERS IN THE OSI MODEL 39

Figure 2.11 illustrates process-to-process delivery by the transport layer.





# Session Layer

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network *dialog controller*. It establishes, maintains, and synchronizes the interaction among communicating systems.

The session layer is responsible for dialog control and synchronization.

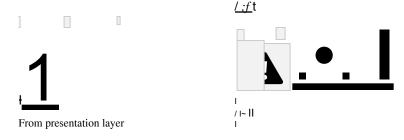
Specific responsibilities of the session layer include the following: **O** Dialog control. The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode. **O** Synchronization. The session layer allows a process to add checkpoints, or syn Chronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent. Figure 2.12 illustrates the relationship of the session layer to the transport and presentation layers.

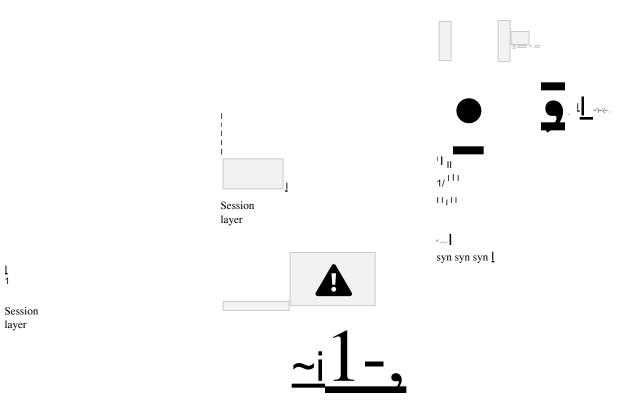
# Presentation Layer

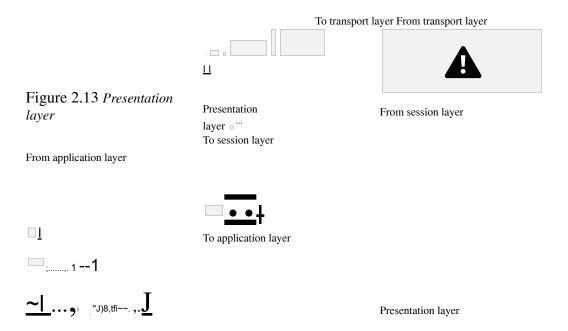
The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. Figure 2.13 shows the relationship between the pre sentation layer and the application and session layers.

40 CHAPTER 2 NETWORK MODELS

Figure 2.12 Session layer







The presentation layer is responsible for translation, compression, and encryption.

Specific responsibilities of the presentation layer include the following: O
Translation. The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The infonnation must be changed to bit streams before being transmitted. Because different computers use different

encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

O Encryption. To carry sensitive information, a system must be able to ensure privacy.

Encryption means that the sender transforms the original information to

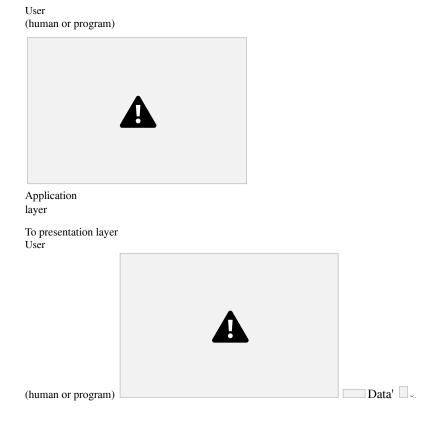
SECTION 2.3 LAYERS IN THE OSI MODEL 41

another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form. O Compression. Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

### **Application Layer**

The application layer enables the user, whether human or software, to access the net work. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distrib uted information services. Figure 2.14 shows the relationship of the application layer to the user and the pre sentation layer. Of the many application services available, the figure shows only three: XAOO (message-handling services), X.500 (directory services), and file transfer, access, and management (FTAM). The user in this example employs XAOO to send an e-mail message.

Figure 2.14 Application layer



The application layer is responsible for providing services to the user.

Specific services provided by the application layer include the following: **O** Network virtual terminal. A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.

#### 42 CHAPTER 2 NETWORK MODELS

- O File transfer, access, and management. This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- **O** Mail services. This application provides the basis for e-mail forwarding and storage.
- O Directory services. This application provides distributed database sources and access for global information about various objects and services.

### Summary of Layers

Figure 2.15 shows a summary of duties for each layer.



Application Presentation To establish, manage, and Session terminate sessions To translate, encrypt, and Transport Network compress data To move packets from source to destination; to provide Data link internetworking To provide reliable process-to process message delivery and error Physical recovery To transmit bits over a medium; to To allow access to network resources provide mechanical and electrical specifications To organize bits into frames; to provide hop-to-hop delivery

# 2.4 TCP/IP PROTOCOL SUITE

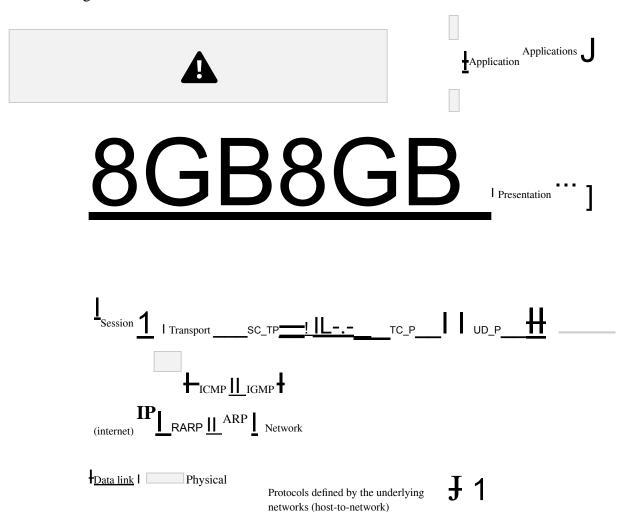
The TCPIIP protocol suite was developed prior to the OSI model. Therefore, the lay ers in the TCP/IP protocol suite do not exactly match those in the

OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the host-to-network layer is equivalent to the combination of the physical and data link layers. The internet layer is equivalent to the network layer, and

the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCPIIP taking care of part of the duties of the session layer. So in this book, we assume that the TCPIIP protocol suite is made of five layers: physical, data link, network, transport, and application. The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model. The three topmost layers in the OSI model, however, are represented in TCPIIP by a single layer called the *application layer* (see Figure 2.16).

SECTION 2.4 TCPIIP PROTOCOL SUITE 43

Figure 2.16 TCPIIP and OSI model



TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdepen dent. Whereas the OSI model specifies which functions belong to each of its layers, the layers of the TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system. The term *hierarchi cal* means that each upper-level protocol is supported by one or more lower-level protocols.

At the transport layer, TCP/IP defines three protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP). At the network layer, the main protocol defined by TCP/IP is the Internetworking Protocol (IP); there are also some other protocols that support data movement in this layer.

# Physical and Data Link Layers

At the physical and data link layers, TCPIIP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCPIIP internetwork can be a local-area network or a wide-area network.

# Network Layer

At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP. Each of these protocols is described in greater detail in later chapters.