

GLOBAL
EDITION



Business Data Networks and Security

TENTH EDITION

Raymond R. Panko • Julia A. Panko

ALWAYS LEARNING

PEARSON

BUSINESS DATA NETWORKS AND SECURITY

Tenth Edition

Global Edition

BUSINESS DATA NETWORKS AND SECURITY

Raymond R. Panko

University of Hawai`i at Mānoa

Julia L. Panko

Weber State University

PEARSON

Boston Columbus Hoboken Indianapolis New York San Francisco
Amsterdam Cape Town Dubai London Madrid Milan Munich Paris Montreal Toronto
Delhi Mexico City Sao Paulo Sydney Hong Kong Seoul Singapore Taipei Tokyo

Editor-in-Chief: Stephanie Wall
Head of Learning Asset Acquisition,
Global Editions: Laura Dent
Director of Marketing: Maggie Moylan
Executive Marketing Manager: Anne Fahlgren
Acquisitions Editor, Global Editions:
Debapriya Mukherjee
Assistant Project Editor, Global Editions:
Paromita Banerjee
Project Manager: Tom Benfatti

Acquisitions Editor: Nicole Sam
Program Manager: Denise Vaughn
Program Manager Team Lead: Ashley Santora
Project Manager Team Lead: Judy Leale
Senior Production Manufacturing Controller,
Global Editions: Trudy Kimber
Cover Designer: Jon Boylan, Lumina Datamatics
Cover Image: © mamanamsai/Shutterstock
Full Service Project Management: Integra

Credits and acknowledgments borrowed from other sources and reproduced, with permission, in this textbook appear on the appropriate page within text. All the icons in figures are courtesy to iStockphoto.

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose. All such documents and related graphics are provided "as is" without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services. The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screen shots may be viewed in full within the software version specified. Microsoft® and Windows® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

Pearson Education Limited
Edinburgh Gate
Harlow
Essex CM20 2JE
England
and Associated Companies throughout the world

Visit us on the World Wide Web at: www.pearsonglobaleditions.com

© Pearson Education Limited 2015

The rights of Raymond R. Panko and Julia L. Panko to be identified as authors of this work have been asserted by them in accordance with the Copyright, Designs and Patents Act 1988.

Authorized adaptation from the United States edition, entitled Business Data Networks and Security, 10th Edition, ISBN 978-0-13-354401-5 by Raymond R. Panko and Julia L. Panko, published by Pearson Education © 2015.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without either the prior written permission of the publisher or a license permitting restricted copying in the United Kingdom issued by the Copyright Licensing Agency Ltd, Saffron House, 6–10 Kirby Street, London EC1N 8TS.

All trademarks used herein are the property of their respective owners. The use of any trademark in this text does not vest in the author or publisher any trademark ownership rights in such trademarks, nor does the use of such trademarks imply any affiliation with or endorsement of this book by such owners.

ISBN 10: 1-292-07541-4
ISBN 13: 978-1-292-07541-9

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library

Typeset in Palatino LT Std by Integra
Printed and bound by Courier Westford in the United States of America

To Sal Aurigemma. A great partner in crime in research and teaching.

BRIEF CONTENTS

Preface for Students 21

About the Authors 24

<i>Chapter 1</i>	Welcome to the Cloud	25
<i>Chapter 1a</i>	Hands On: A Few Internet Tools	64
<i>Chapter 1b</i>	Design Exercise: A Small Home Network	65
<i>Chapter 2</i>	Network Standards	70
<i>Chapter 2a</i>	Hands-On: Wireshark Packet Capture	104
<i>Chapter 3</i>	Network Security	110
<i>Chapter 4</i>	Network and Security Management	152
<i>Chapter 4a</i>	Hands-On: Microsoft Office Visio	186
<i>Chapter 5</i>	Ethernet (802.3) Switched LANs	190
<i>Chapter 5a</i>	Hands-On: Cutting and Connectorizing UTP	224
<i>Chapter 5b</i>	Hands-On: Ethernet Switching	231
<i>Chapter 6</i>	Wireless LANs I	234
<i>Chapter 6a</i>	Using Xirrus Wi-Fi Inspector	268
<i>Chapter 7</i>	Wireless LANs II	277
<i>Chapter 8</i>	TCP/IP Internetworking I	307
<i>Chapter 9</i>	TCP/IP Internetworking II	338
<i>Chapter 10</i>	Carrier Wide Area Networks (WANs)	365
<i>Chapter 11</i>	Networked Applications	397

Glossary 428

Index 455

Online Modules

(available at www.pearsonglobaleditions.com/Panko)

<i>Module A</i>	More on TCP
<i>Module B</i>	More on Modulation
<i>Module C</i>	More on Telecommunications
<i>Module D</i>	Directory Servers

CONTENTS

Preface for Students 21

About the Authors 24

Chapter 1 WELCOME TO THE CLOUD 25

■ **BOX 1: By the Numbers** 26

Netflix Dives into the Amazon 26

Hosts, Messages, and Addresses 27

The Internet 28

Netflix Dives into the Amazon 30

Virtualization and Agility 32

Infrastructure as a Service (IaaS) and Software as a Service (SaaS) 33

Clients Move into the Cloud 35

Rain Clouds: Security 36

Networks and the Cloud 36

Service Level Agreements (SLAs): Speed 37

■ **BOX 2: Writing Speeds in Metric Notation** 38

Messages 39

Application Messages 39

Message Fragmentation, Frames, and Packets 39

Single Networks 42

Single-Network Host Addresses 42

Point-to-Point Single Networks, Physical Links, and Data links 43

Wireless Single Networks 46

Switched Single Networks 47

Hybrid Switched/Wireless Single Networks 48

Internet Transmission 49

Hosts on Different Single Networks 49

Creating the Internet 50

Routes and Layer 3 53

■ **BOX 3: "Packet Switching"** 55

Standards Layers 56

Five Layers 56

Layers 1 through 3 (Physical, Data Link, and Internet Layers) 56

Layers 4 and 5 (Transport and Application Layers) 57

- Standards Agencies and Architectures 57
- TCP/IP Supervisory Applications: The Domain Name System (DNS) 59
- Conclusion* 60
- Synopsis 60
- End-of-Chapter Questions* 62

Chapter 1a HANDS ON: A FEW INTERNET TOOLS 64

Chapter 1b DESIGN EXERCISE: A SMALL HOME NETWORK 65

- A Small Home Network* 65
 - Components 65
 - The Wireless Access Router 67
 - Services 68
 - Configuration 68
- Design Exercise* 69

Chapter 2 NETWORK STANDARDS 70

- How Internet Standards Came to Be* 70
 - **BOX 1: April 1 and RFCs** 73
- Introduction* 73
 - Standard = Protocol 73
 - Network Standards 74
 - Recap of Chapter 1 Standards Concepts 75
 - Network Standard Characteristics 77
- Examples of Message Ordering* 79
 - Message Ordering in HTTP 79
 - Message Ordering and Reliability in TCP at the Transport Layer 80
- Examples of Message Syntax* 83
 - Syntax: General Message Organization 83
 - The Ethernet Frame Syntax 85
 - The Internet Protocol (IP) Packet Syntax 86
 - Transmission Control Protocol Segment Syntax 88
 - User Datagram Protocol Datagram Syntax 90
 - Port Numbers 90
 - HTTP Request and Response Message Syntax 92
- Converting Application Messages Into Bits* 94
 - Encoding 94
 - Encoding Text as ASCII 95
 - Converting Integers into Binary Numbers (1s and 0s) 96

Encoding Alternatives	97
Encoding Voice	99
<i>Vertical Communication on Hosts</i>	100
<i>Conclusion</i>	101
Synopsis	101
<i>End-of-Chapter Question</i>	103

Chapter 2a HANDS-ON: WIRESHARK PACKET CAPTURE 104

<i>Introduction</i>	104
<i>Getting Wireshark</i>	104
<i>Using Wireshark</i>	105
Getting Started	105
Starting a Packet Capture	105
Getting Data	106
Stopping Data Collection	107
Looking at Individual Packets	107
Options	109

Chapter 3 NETWORK SECURITY 110

<i>The Target Breach</i>	110
The Attack	111
Damages	113
Perspective	114
<i>Introduction</i>	115
<i>Types of Attacks</i>	115
Malware Attacks	115
Vulnerabilities and Patches	116
Viruses and Worms	117
Other Types of Malware	118
Payloads	119
Attacks on Human Judgment	120
Human Break-Ins (Hacking)	122
Stages in the Attack	123
Denial-of-Service (DOS) Attacks Using Bots	124
Advanced Persistent Threats	125
<i>Types of Attackers</i>	126
Hackers	126
Malware Attackers	128
Employees, Ex-Employees, and Other Insiders	128

- Cyberterrorists and National Governments 128
- Protecting Dialogues Cryptography* 129
 - Symmetric Key Encryption for Confidentiality 130
 - Electronic Signatures: Message Authentication and Integrity 131
 - Host-to-Host Virtual Private Networks (VPNs) 132
- Other Forms of Authentication* 133
 - Terminology and Concepts 133
 - Reusable Passwords 134
 - Other Forms of Authentication 136
- Firewalls* 139
 - Dropping and Logging Provable Attack Packets 140
 - Stateful Packet Inspection (SPI) Firewalls 141
 - Next-Generation Firewalls (NGFWs) 145
- Box: Antivirus Protection* 148
- Conclusion* 149
 - Synopsis 149
 - End-of-Chapter Questions* 151

Chapter 4 NETWORK AND SECURITY MANAGEMENT 152

- Failures in the Target Breach* 152
- Introduction* 154
- Network Quality of Service (QOS)* 155
 - Transmission Speed 156
 - Rated Speed versus Throughput and Aggregate Throughput 156
 - Other Quality-of-Service Metrics 157
 - Service Level Agreements (SLAs) 159
- Network Design* 160
 - Traffic Analysis 161
 - Redundancy 162
 - Momentary Traffic Peaks 163
- Strategic Security Planning Principles* 165
 - Security Is a Management Issue 165
 - The Plan–Protect–Respond Cycle 166
 - Security Planning Principles 167
 - Policy-Based Security 173
- Centralized Network Management* 177
 - Ping 177

The Simple Network Management Protocol (SNMP)	178
Software-Defined Networking (SDN)	180
<i>Centralized Security Management</i>	182
<i>Conclusion</i>	183
Synopsis	183
<i>End-of-Chapter Questions</i>	185

Chapter 4a HANDS-ON: MICROSOFT OFFICE VISIO 186

<i>What is Visio?</i>	186
<i>Using Visio</i>	186

Chapter 5 ETHERNET (802.3) SWITCHED LANs 190

<i>Ethernet Begins</i>	190
<i>Introduction</i>	191
Local Area Networks	191
Switched Technology	192
Ethernet Standards Development	194
Physical and Data Link Layer Operation	195
<i>Ethernet Physical Layer Standards</i>	196
Signaling	196
4-Pair Unshielded Twisted Pair Copper Wiring	199
Serial and Parallel Transmission	200
UTP Installation Limitations	201
Optical Fiber	202
Multimode Optical Fiber Quality Standards	205
Link Aggregation (Bonding)	206
Ethernet Physical Layer Standards and Network Design	207
<i>Ethernet Data Link Layer Standards</i>	209
The Ethernet Frame	209
Basic Ethernet Data Link Layer Switch Operation	212
<i>Advanced Ethernet Switch Operation</i>	214
The Rapid Spanning Tree Protocol (RSTP)	214
Priority	216
Manageability	216
Power over Ethernet (POE)	217
<i>Ethernet Security</i>	218
Port-Based Access Control (802.1X)	218
Man in the Middle Attack in an Ethernet LAN	219

- Conclusion 221
- Synopsis 221
- End-of-Chapter Questions 222

Chapter 5a HANDS-ON: CUTTING AND CONNECTORIZING UTP 224

- Introduction 224
- Solid and Stranded Wiring 224
 - Solid-Wire UTP versus Stranded-Wire UTP 224
 - Relative Advantages 225
 - Adding Connectors 225
- Cutting the Cord 225
- Stripping the Cord 226
- Working with the Exposed Pairs 226
 - Pair Colors 226
 - Untwisting the Pairs 226
 - Ordering the Pairs 227
 - Cutting the Wires 227
- Adding the Connector 228
 - Holding the Connector 228
 - Sliding in the Wires 228
 - Some Jacket Inside the Connector 228
- Crimping 228
 - Pressing Down 228
 - Making Electrical Contact 228
 - Strain Relief 229
- Testing 229
 - Testing with Continuity Testers 229
 - Testing for Signal Quality 229

Chapter 5b HANDS-ON: ETHERNET SWITCHING 231

- The Exercise 231
 - What You Will Need 231
 - Creating the Network 232
 - Creating a Loop 232

Chapter 6 WIRELESS LANs I 234

- Introduction 235
 - OSI Standards 235
 - 802.11 versus Wi-Fi 235
 - Wireless LAN Operation 236

<i>Radio Signal Propagation</i>	237
Frequencies	238
Antennas	239
Wireless Propagation Problems	240
<i>Radio Bands, Bandwidth, and Spread Spectrum Transmission</i>	243
Service Bands	243
Signal and Channel Bandwidth	244
The 2.4 GHz and 5 GHz Service Bands	245
<i>Normal and Spread Spectrum Transmission</i>	247
Spread Spectrum Transmission	247
Licensed and Unlicensed Radio Bands	248
Implementing Spread Spectrum Transmission	249
<i>802.11 WLAN Operation</i>	251
Wireless Access Points	251
Basic Service Sets (BSSs)	252
Extended Service Sets (ESSs), Handoffs, and Roaming	253
Media Access Control	254
■ BOX 1: Media Access Control (MAC)	255
<i>802.11 Transmission Standards</i>	257
Characteristics of 802.11g, 802.11a, 802.11n, and 802.11ac	257
Bands and Channel Bandwidth	259
MIMO	260
Beamforming and Multiuser MIMO	261
Speed, Throughput, and Distance	262
Backward Compatibility	263
Standards and Options	264
<i>Wireless Mesh Networking</i>	264
<i>Conclusion</i>	265
Synopsis	265
<i>End-of-Chapter Questions</i>	267

Chapter 6a USING XIRRUS WI-FI INSPECTOR 268

<i>Introduction</i>	268
<i>The Four Windows</i>	268
The Radar Window (Read the Fine Print)	269
Connection Window	271
The Networks Window	271
Signal History	272

- Other Groups on the Ribbon 273
- Tests 273
 - Connection Test 273
 - Speed Test 274
 - Quality Test 275
- Activities 276
 - Activity 276

Chapter 7 WIRELESS LANs II 277

- The TJX Breach* 277
- Introduction* 280
- 802.11i WLAN Security* 280
 - WLAN Security Threats 280
 - The 802.11i WLAN Security Standard 281
 - Pre-Shared Key (PSK) Mode in 802.11i 283
 - 802.1X Mode Operation 286
- Beyond 802.11i Security* 287
 - Rogue Access Points 287
 - Evil Twin Access Points and Virtual Private Networks (VPNs) 288
- 802.11 Wi-Fi Wireless LAN Management* 291
 - Access Point Placement 291
 - Remote Management 292
- Bluetooth* 294
 - **BOX 1: Expressing Power Ratios in Decibels** 295
 - Two Modes of Operation 297
 - One-to-One, Master–Slave Operation 299
 - Bluetooth Profiles 300
- Other Local Wireless Technologies* 301
 - Near Field Communication (NFC) 302
 - Wi-Fi Direct 303
 - Security in Emerging Local Wireless Technologies 303
- Conclusion* 305
 - Synopsis 305
 - End-of-Chapter Questions* 306

Chapter 8 TCP/IP INTERNETWORKING I 307

- Introduction* 307
- IP Routing* 308
 - Hierarchical IP Addressing 308

Routers, Networks, and Subnets	310
Network and Subnet Masks	311
<i>How Routers Process Packets</i>	313
Switching versus Routing	313
Routing Table	315
Rows Are Routes for All IP Addresses in a Range	315
Step 1: Finding All Row Matches	316
Step 2: Selecting the Best-Match Row	319
Step 3: Sending the Packet Back Out	320
Cheating (Decision Caching)	320
■ BOX 1: Masking When Masks Do Not Break at 8-Bit Boundaries	321
■ BOX 2: The Address Resolution Protocol	322
<i>The Internet Protocol Version 4 (IPv4) Fields</i>	324
The First Row	324
The Second Row	325
The Third Row	325
IP Options	326
<i>IP Version 6 (IPv6)</i>	326
Outgrowing IPv4	326
IPv6	326
Writing 128-Bit IPv6 Addresses	327
The IPv6 Header	329
Extension Headers	330
<i>The Transmission Control Protocol (TCP)</i>	332
Fields in TCP/IP Segments	332
Openings and Abrupt TCP Closes	334
<i>The User Datagram Protocol (UDP)</i>	335
<i>Conclusion</i>	336
Synopsis	336
<i>End-of-Chapter Questions</i>	337

Chapter 9 TCP/IP INTERNETWORKING II 338

<i>Introduction</i>	338
<i>Core TCP/IP Management Tasks</i>	338
IP Subnet Planning	339
Network Address Translation (NAT)	340
The Domain Name System (DNS)	343
Simple Network Management Protocol (SNMP)	346

- Securing Internet Transmission* 349
 - Virtual Private Networks 349
 - IPsec VPNs 350
 - IPsec Transport Mode 350
 - IPsec Tunnel Mode 351
 - Remote-Site-Access and Site-to-Site VPNs 352
 - IPsec Security Associations and Policy Servers 352
 - SSL/TLS VPNs 353
- Managing IP Version 6 (IPV6)* 354
 - Internet Layer Protocol Stacks 354
 - IPv6 Subnetting 355
 - The Domain Name System for IPv6 358
- Other TCP/IP Standards* 359
 - Dynamic Routing Protocols 359
 - Internet Control Message Protocol (ICMP) for Supervisory Messages at the Internet Layer 361
- Conclusion* 362
 - Synopsis 362
 - End-of-Chapter Questions* 363

Chapter 10 CARRIER WIDE AREA NETWORKS (WANs) 365

- LANs and WANs (and MANs)* 366
 - LANs versus MANs and WANs 366
 - Other Aspects of WANs 368
 - Carrier WAN Components and Business Uses 369
 - The Telephone System 370
- Residential Wired Internet Access* 371
 - Residential Asymmetric Digital Subscriber Line (ADSL) Service 371
 - Cable Modem Service 373
 - ADSL versus Cable Modem Service 375
- Cellular Data Service* 375
 - Cellular Service 375
 - Why Cells? 377
 - Cellular Data Speeds 377
- Wired Business WANs* 379
 - Leased Lines 379
 - Reaching the ISP via a Leased Line 380
 - Leased Line Private Corporate WANs 381
 - Public Switched Data Network (PSDN) Carrier WANs 383

Multiprotocol Label Switching (MPLS)	386
WAN Optimization	388
<i>Software Defined Networking (SDN)</i>	391
Concepts and Benefits	391
Forwarding Tables	393
SDN Applications	393
Application Program Interfaces (APIs)	394
<i>Conclusion</i>	395
Synopsis	395
<i>End-of-Chapter Questions</i>	396

Chapter 11 NETWORKED APPLICATIONS 397

<i>GhostNet</i>	397
<i>Introduction</i>	399
Networked Applications	399
The Evolution of Client Devices and Networking	400
Application Security	402
Cross-Site Scripting (XSS)	404
SQL Injection Attacks	405
<i>Electronic Mail (E-Mail)</i>	406
E-Mail Standards	406
Message Body Standards	406
Simple Mail Transfer Protocol (SMTP)	407
Receiving Mail (POP and IMAP)	407
Web-Enabled E-Mail	408
SMTP for Transmission between Mail Hosts	408
Malware Filtering in E-Mail	409
Encryption for Confidentiality in E-Mail Transmission	410
<i>Voice Over IP (VOIP)</i>	412
Basics	412
VoIP Signaling	413
VoIP Transport	414
<i>The World Wide Web</i>	415
HTTP and HTML Standards	415
Complex Webpages	416
<i>Peer-to-Peer (P2P) Application Architectures</i>	417
Traditional Client/Server Applications	417
P2P Applications	418
P2P File-Sharing Applications: BitTorrent	419

P2P Communication Applications: Skype 421
P2P Processing Applications: SETI@Home 423
Privacy Protection: Tor 424
Facilitating Servers and P2P Applications 425
Conclusion 425
Synopsis 425
End-of-Chapter Questions 427

Online Modules

(available at www.pearsonglobaleditions.com/Panko)

Module A MORE ON TCP

Numbering Octets
Ordering TCP Segments upon Arrival
The TCP Acknowledgment Process
Flow Control: Window Size
Review Questions

Module B MORE ON MODULATION

Modulation
Frequency Modulation
Amplitude Modulation
Phase Modulation
Quadrature Amplitude Modulation (QAM)
Review Questions

Module C MORE ON TELECOMMUNICATIONS

Introduction
The PSTN Transport Core and Signaling
The Transport Core
Time Division Multiplexing (TDM) Lines
Leased Lines and Trunk Lines
Asynchronous Transfer Mode (ATM) Transport
Signaling
Communication Satellites
Microwave Transmission
Satellite Transmission
Geosynchronous Earth Orbit (GEO) Satellites

Low Earth Orbit (LEO) and Medium Earth Orbit (MEO) Satellites

VSAT Satellites

Wiring The First Bank of Paradise Headquarters Building

Facilities

Telephone Wiring

Data Wiring

Plenum Cabling

PBX Services

Carrier Services and Pricing

Basic Voice Services

Advanced Services

Call Waiting

Voice Mail

Telephone Carriers and Regulation

PTTs and Ministries of Telecommunications

AT&T, the FCC, and PUCs

Deregulation

Voice Over IP

Module D DIRECTORY SERVERS

Introduction

Hierarchical Organization

Lightweight Directory Access Protocol (LDAP)

Directory Servers and The Networking Staff

Microsoft's Active Directory (AD)

Active Directory Domains

Domain Controllers

Domains in an Active Directory Tree

Complex Structures

Authentication and Directory Servers

Glossary 428

Index 455

PREFACE FOR STUDENTS

Networking and security are the most exciting careers in information technology. Heck, they are the most exciting careers in the world. Professionals in these fields do not spend their careers just doing the same thing over and over again. Their work is constantly evolving, and personal growth is guaranteed.

HOW TO STUDY NETWORKING

Networking and Security are Different

Some students find networking and security difficult. The problem seems to be that they require a different learning approach than programming and database management. In programming and database, you learn a little, apply it, learn a little more, apply it, shampoo, rinse, repeat. If there is something you don't know, there is probably another way to do it. (Except on exams and homework, of course.)

In networking, you need to know everything to do anything, and it is what you don't know that hurts you. For example, suppose that you want to connect a server to an Ethernet switch. This sounds simple enough. However, should you choose copper wire or optical fiber? If copper wire, what grade of copper wire? If fiber, which OM standard should you choose? Or should you connect the server wirelessly? In your choice, you must include speed, distance, delay, reliability, and cost. Especially cost. Budgets are eternally tight, and networking people never say "cost doesn't matter."

Security is different again. In security, you are not just dealing with design issues and the reliability of technology. You are dealing with human opponents that are engaged with you in a perpetual arms race of protections and new attack methods to get beyond those protections. It is a lot like playing a video game at a high level, but with real-world consequences.

Will employers expect you to know everything when you apply for a job? Of course not. However, they will expect you to know a *lot*. They will sit you down and ask you how to connect a server to an Ethernet switch or something else that requires you to be able to integrate what you have learned. In fact, they will do this for the material in most courses you have taken to get an understanding of how serious you are about work.

You will certainly get questions that require you to troubleshoot a problem. Troubleshooting is hard, and most people intuitively do it wrong. This book will give you a methodology for doing it right and plenty of practice in applying it.

Employers will expect applicants to be up in the field. For Wi-Fi, they may ask you about security, and they don't expect you to stop at 802.11i. Mentioning Ethernet busses and hubs in a design may end the interview. Employers expect applicants to have some knowledge of IPv6 and cloud computing. They will be interested if you know even a little about SDN.

Learning with this Book

Organization of the Book We have tried to write this book to help you learn the material. Most basically, we present the material in short sections with Test Your Understanding (TYU) questions immediately after each section, to help you know if you have understood the section.

Pay special attention to keyterms that are boldfaced. These are the core concepts in the field. And yes, there are a lot of them. Important or frequently-misunderstood concepts are broken out like this for special attention:

A rogue access point is an unauthorized access point set up within a firm by an employee or department.

Figures cover almost all important concepts in the book. There are special study figures that summarize the flow and key points in most sections that are not amenable to illustrations. The PowerPoint presentations are based on these figures. For complex illustrations, the PowerPoint presentations have builds, presenting only part of the figure at each step.

If you see a term that you learned previously but have forgotten, go to the Glossary. In Glossary entries, some page numbers are boldfaced. These are the pages on which the term was defined or characterized. Some terms are introduced more than once and may have two or more page numbers boldfaced.

Studying for Exams Exams are the least popular elements in any course. And yes, you will have dreams about waking up late for an exam for several years after you graduate. However, there are things you can do to make your life easier.

First, study the material. Read a section. Do the TYU questions. In fact, download the homework file (www.pearsonglobaleditions.com/Panko), which has all the questions. Put your answers into the file. The multiple choice questions in the test bank are taken from the material in the TYU questions and thought questions. A good idea is to read the material over before exams instead of just relying on your initial answers, which might not have been exactly perfect, having been based on your first reading.

Late in your study, describe the figures as if you were giving a lecture. If there is something you do not understand, note it and follow up. Take notes on your problems and insights.

At each step, ask yourself why each question and answer is important. This will give you insights and will solidify the material in your memory.

Upper-Division Learning Initial college education focuses on learning isolated facts. Networking and security, like other advanced courses, requires something more. First, it requires the ability to compare and contrast concepts you have learned. In networking and security, there are alternative ways to do almost everything. Understanding individual alternatives is not enough. To select the best alternative, you must understand trade-offs between them. You must also see them in the broader context of the chapter. For 802.11 Wi-Fi, 802.11i provides a lot of protection; but there

are other things you must also do to be secure. Life is about trade-offs. Your studying must reflect that.

Another pain point is learning multi-step procedures. It is important to learn the overall flow, understand how each step relates to the flow, understand each step, and do this all over again until you have both the flow and the details. Processes are difficult to learn because you do not have a framework clearly in mind for fitting individual facts into the bigger picture. In learning processes, it takes several cycles of studying at multiple levels to get both the overall flow and the individual steps.

Pearson would like to thank and acknowledge Sahil Raj, Punjabi University, for his contributions to the Global Edition. Pearson would also like to thank Fabian Ng Yaw Tong, Ngee Ann Polytechnic; Ng Hu, Multimedia University; and Raihana Md Saidi, Universiti Teknologi MARA for reviewing and providing suggestions that helped in improving the Global Edition content.

ABOUT THE AUTHORS

Ray Panko is a professor of IT management and a Shidler Fellow at the University of Hawai'i's Shidler College of Business. His main courses are networking and security. Before coming to the university, he was a project manager at Stanford Research Institute (now SRI International), where he worked for Doug Englebart, the inventor of the mouse and creator of the first operational hypertext system. He received his B.S. in physics and his M.B.A. from Seattle University. He received his doctorate from Stanford University, where his dissertation was conducted under contract to the Office of the President of the United States. He has been awarded the Shidler College of Business's Dennis Ching award as the outstanding teacher among senior faculty. His e-mail is Ray@Panko.com.

Julia Panko is an assistant professor on the faculty at Weber State University. She received her doctorate from the University of California, Santa Barbara. Her research interests include the twentieth- and twenty-first-century novel, the history and theory of information technology, and the digital humanities. Her dissertation focused on the relationship between information culture and modern and contemporary novels.

Chapter 1

Welcome to the Cloud

LEARNING OBJECTIVES

By the end of this chapter, you should be able to:

- Describe basic networking, including why networks are drawn as clouds, hosts, addresses, the Internet, Internet service providers, transmission speed, and service level agreements.
- Explain how the Internet works, how Netflix uses Amazon Web Services IaaS (Infrastructure as a Service) with virtual machines, and a Google SaaS (Software as a Service).
- Describe messages, fragmentation, multiplexing, and frames versus packets.
- Describe how single point-to-point, wireless, switched, and hybrid wireless-switched networks operate—especially how switches forward incoming frames.
- Describe how internets and router make it possible for hosts on different networks to work together.
- List the five standards layers commonly encountered in networking, describe what each layer does, describe concepts and terms in each layer, identify at which layer a given process is operating, and identify which standards agencies and standards architecture are relevant to that process.

BOX 1

By the Numbers

The Internet is enormous, growing, and changing.

- By 2003, there were already more devices connected to the Internet (computers, phones, etc.) than there were human users.¹
- In 2010, 21% of the world's population used the Internet. In 2013, it was 39%.²
- In 2012, online video viewing overtook DVD and Blu-Ray viewing.³
- From 2011 to 2016, global IP traffic will triple, and the number of connected devices will nearly double.⁴
- In 2016, Cisco expects the Internet to carry one zettabyte of data.⁵ A zettabyte is 1,000,000,000,000,000,000 (one sextillion) bytes.
- By 2020, there will be 50 billion devices connected to the Internet—ten times the number of human users. The great majority of these will be devices talking to other devices, without human involvement.⁶

NETFLIX DIVES INTO THE AMAZON⁷

Figure 1-1 shows that the Internet is often depicted as a cloud. This symbolizes that just as you cannot see inside a cloud, users should be oblivious to what happens inside the Internet. To them, the Internet simply works, like the electrical, water, and telephone systems.

In this course, as you might suspect, you will not be spared the burden of understanding the internals of the Internet and other networks. This knowledge will prepare you to help your employer use networks effectively. Along the way, you will learn a good deal about security, too. Networking is a vast superhighway with great potential for benefits. However, it has some rough neighborhoods.

¹ Suzanne Choney, "US Has More Internet-Connected Gadgets Than People," *nbcnews.com*, January 2, 2003. <http://www.nbcnews.com/technology/us-has-more-internet-connected-gadgets-people-1C7782791>.

² Geneva, "Key ICT Indicators for Developed and Developing Countries and the World (Totals and Penetration Rates)," *International Telecommunications Unions (ITU)*, February 27, 2013.

³ Jared Newman, "Online Video Expected to Overtake DVD, Blu-ray Viewing this Year," *Techhive*, May 27, 2012. http://www.techhive.com/article/252650/online_video_expected_to_overtake_dvd_blu_ray_viewing_this_year.html.

⁴ Larry Hettick, "Cisco: Networked Devices Will Outnumber People 3 to 1 in 2016," *Network World*, June 1, 2012. <http://www.networkworld.com/newsletters/converg/2012/060412convergence1.html>

⁵ Grant Gross, "Cisco: Global Net Traffic to Surpass 1 Zettabyte by 2016, Cisco Says," *Network World*, May 31, 2012. http://www.pcworld.com/article/256522/cisco_global_net_traffic_to_surpass_1_zettabyte_in_2016.html

⁶ Ericsson, "CEO to Shareholders: 50 Billion Connections 2020," press release, April 2010.

⁷ Sources for this section include the following. Brandon Butler, "Three Lessons from Netflix on How to Live in a Cloud," *NetworkWorld*, October 9, 2013. <http://www.networkworld.com/news/2013/100913-netflix-cloud-274647.html>. Matt Petronzio, "Meet the Man Who Keeps Netflix Afloat in the Cloud," *mashable.com*, May 13, 2013. <http://mashable.com/2013/05/13/netflix-dream-job/>. Kevin Purdy, "How Netflix is Revolutionizing Cloud Computing Just So You Can Watch 'Teen Mom' on Your Phone," *www.itworld.com*, May 10, 2013. <http://www.itworld.com/cloud-computing/355844/netflix-revolutionizing-computer-just-serve-you-movies>. Ashlee Vance, "Netflix, Reed Hastings Survive Missteps to Join Silicon Valley's Elite," *Business Week*, May 9, 2013. <http://www.businessweek.com/articles/2013-05-09/netflix-reed-hastings-survive-missteps-to-join-silicon-valleys-elite>.

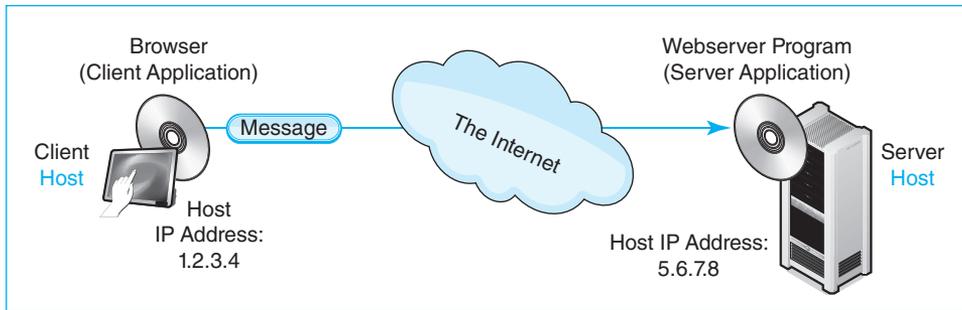


FIGURE 1-1 Internet Communication

Test Your Understanding

1. a) Why is the Internet usually depicted as a cloud? b) What is the significance of this depiction for users?

Hosts, Messages, and Addresses

Hosts Figure 1-1 introduces some basic networking terms. First, any computer attached to a network is a **host**. Hosts include large servers that work with hundreds of users simultaneously. Hosts also include desktop PCs, laptops, tablets, smartphones, smart glasses, and smart watches. In the future, hosts will include interactive walls, tables, and appliances that will turn your entire home into an immersive interactive environment. In a trend called the **Internet of things**, even coffee makers, toasters, medical implants, and many other small and large devices around us will be hosts that communicate through networks to work better. In fact, machine-to-machine communication will eventually dominate traffic on the Internet. The term *host* is not an obvious name for computers that attach to networks, but it is the common name for them in networking.

Any computer attached to a network is a host.

Messages and Addresses Figure 1-1 shows that application programs on different hosts communicate by sending messages to one another. Messages require addresses. For example if you want to send the first author a message, you would send it to his e-mail address, Ray@Panko.com. Hosts also need addresses. On the Internet, these are **Internet Protocol addresses** or **IP addresses**. In Figure 1-1, the IP addresses are 1.2.3.4 for the source host and 5.6.7.8 for the destination host.

Dotted Decimal Notation (DDN) When an IP address is expressed as four numbers separated by dots (periods), this is called **dotted decimal notation (DDN)**. In reality, IP addresses are 32-bit strings of 1s and 0s. Computers have no problem working with long bit strings. Human memory and writing, however, need a crutch to deal with long bit strings. Dotted decimal notation is precisely that—a crutch for inferior biological entities like ourselves. Computers do not use DDN.

32 IP address bits divided into four 8-bit segments	00000001	00000010	00000011	00000100
Segment converted to decimal	1	2	3	4
IP address in dotted decimal notation (DDN)	1.2.3.4			

FIGURE 1-2 Dotted Decimal Notation

Figure 1-2 shows how to convert a 32-bit IP address into dotted decimal notation.

- First, divide the 32 bits into four 8-bit segments.
- Second, treat each segment as a binary number and convert this binary number into a decimal number. For example, the first segment, 00000001 in binary, is 1 in decimal.
- Third, combine the four decimal field values, separating them by dots. This gives 1.2.3.4.

How do you convert a binary number into a decimal number? The fastest way is to go to an Internet search engine and find a binary-to-decimal converter. You then type each 8-bit binary segment's bits into the indicated binary box and hit the convert button. The decimal value appears in the decimal box.

We have been looking at 32-bit IP address. However, this is not the only type of IP address. It is an **IP Version 4 (IPv4)** address. IPv4 is the dominant IP protocol on the Internet today. However, we are beginning to see significant use of **IP Version 6 (IPv6)**. As we will see in Chapter 8, IPv6 addresses are 128 bits long and are represented for human consumption in a very different way.

Test Your Understanding

- a) What is the term we use in networking for any computer attached to a network?
 - b) Is your smartphone a host when you use it to surf the 'Web? c) Are you as a person a host when you use a network? d) How do application programs on different hosts communicate?
- a) What kind of addresses do hosts have on the Internet? b) What kind of address is 128.171.17.13? c) What name do we use for the format 128.171.17.13? d) Who uses this format—humans or computers? e) Convert the following 32-bit binary IP address into DDN (spaces are added for easier reading): 10000000 10101011 00010001 00001101. (Check Figure: 10000000 = 127) f) Convert 5.6.7.138 into a 32-bit IP address. (Check Figure: 5 = 00000101) Show a space between each 8-bit segment. g) What type of IP addresses is 32 bits long? h) What other type of IP address exists, and how long is its addresses?

The Internet

Figure 1-3 illustrates that the global Internet is not a single network. Instead, the **Internet** is a collection of thousands of single networks and smaller internets. All of these single networks and smaller internets interconnect to form a single transmission system that in

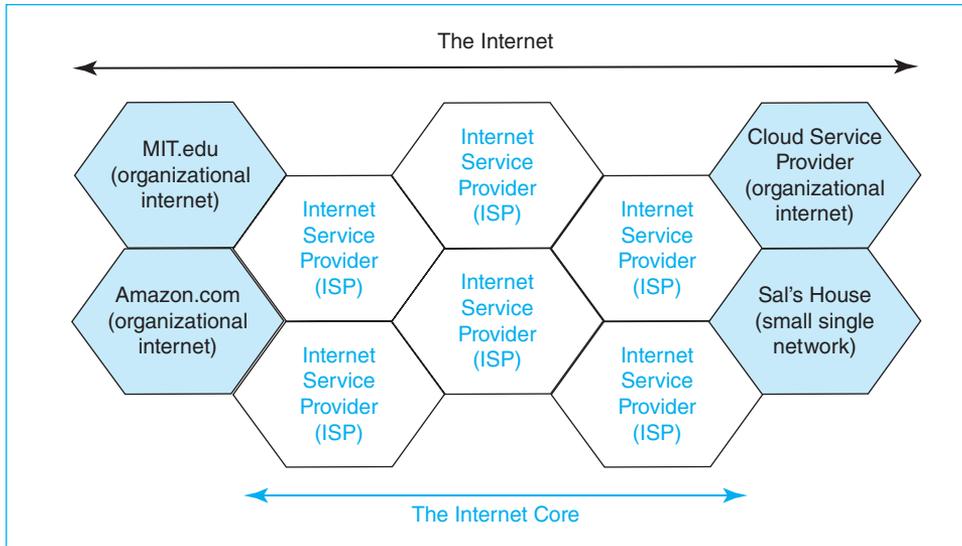


FIGURE 1-3 The Internet's Networks and Smaller Internets

principle allows any Internet host reach any other host.⁸ Some of these single networks and smaller internets are owned by organizations such as Amazon.com or MIT. Smaller networks are owned by families and even individuals. In addition, some internets link these smaller networks and smaller internets together. We call these linking internets **Internet service providers (ISPs)**. ISPs collectively form the **core** of the Internet, which is also called the Internet's backbone.⁹ To use the Internet, a customer must connect to an ISP.

The Internet is a collection of single networks and smaller internets. All of these networks and smaller internets interconnect to form a single transmission system.

At this point, we need to break the narrative to mention in two pieces of terminology we will use in this book.

- First, saying “single networks and internets” is cumbersome. We use the term *network* for both.
- Second, in this book, we spell internet in lowercase for internets in general and internets that are not the global Internet. We capitalize the global Internet.

Who owns the Internet? The surprising answer is, “Nobody.” The ISPs and other organizations own their pieces of the Internet. Who controls the Internet? Again, nobody does. Although the **Internet Engineering Task Force (IETF)** creates standards,

⁸ The original term for *internet* was *catanet*. When things are connected together in computer science, they are said to be concatenated. Fortunately, “catanet” never caught on, saving the Internet from a flood of bad feline jokes.

⁹ For simplicity, the figure shows ISPs as if they served nonoverlapping geographic regions. Actually, ISPs often overlap geographically. National and international ISPs may connect at several geographical locations to exchange messages.

network owners decide which standards to adopt. There is no overall authority to enforce standards or to govern interconnection business practices. Everything is negotiated between the network and internet owners. Who pays for the Internet? You do. Users pay ISPs, who work out arrangements with other ISPs to deliver your messages. You probably pay around \$30 per month to your ISP. Businesses pay thousands or millions of dollars annually. With rare exceptions, no government money sustains the Internet.

Test Your Understanding

4. a) Is the Internet a single network? Explain. b) What is the role of ISPs? c) Who controls the Internet? d) Who funds the Internet?

Netflix Dives into the Amazon

You know personally how individuals use the Internet. The corporate experience is often very different. We will illustrate this by talking about how Netflix uses the Internet. Netflix is a commercial streaming video service with tens of millions of customers around the world. Streaming video places a heavy load on network capacity. For a two-hour high-definition movie, Netflix must deliver five million bits (1s or 0s) each second. This is a total of nine gigabytes for that one movie. On any given night, Netflix accounts for roughly a third of the Internet traffic going into U.S. homes.

Requirements Users expect high video quality, and they will not tolerate delay or unreliability. The Internet was not designed for these requirements. The Internet is a “best effort” delivery system that often has insufficient speed and reliability and that often has too much delay for Netflix users. Netflix had to overcome these limitations.

The Internet is a “best effort” delivery system.

Video streaming also requires vast amounts of server processing capacity beyond the demands of actual streaming. Each movie must be **transcoded** into many streaming formats, and when a customer requests a movie, streaming servers have to select the best transcoded format for that particular customer.

In addition, at the heart of Netflix’s business plan is an application that creates personalized viewing suggestions for individual customers. This requires the analysis of extensive data about the customer’s viewing habits and the choices of other customers with similar viewing profiles.

Outsourcing In 2008, when Netflix was only delivering movies through mailed DVDs, the company suffered a crippling server outage that stopped shipments for several days. That was a wake up call for Netflix. Management realized that reliability would be critical for the online delivery it would soon introduce. It also realized that while Internet delivery would become its core business, managing servers would not. Rather than developing the expertise needed for the complex server technologies the company needed, Netflix decided to outsource server operation to a company that could meet Netflix’s high requirements for capacity, reliability, and agility in responding to sudden demand changes.