CISCO

Cisco Networking Simplified

Second Edition

- Master today's world of Cisco networking with this book's completely updated, fully illustrated visual approach
- Easy enough for novices, substantive enough for networking professionals
- Covers the latest networking topics—from security to wireless, availability to virtualization

In Full Color

ciscopress.com

Jim Doherty • Neil Anderson • Paul Della Maggiora

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Cisco Networking Simplified

Second Edition

Jim Doherty

Neil Anderson

Paul Della Maggiora

Illustrations by Nathan Clement

Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Cisco Networking Simplified, Second Edition

Jim Doherty, Neil Anderson, Paul Della Maggiora

Copyright© 2008 Cisco Systems, Inc.

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

Sixth Printing May 2013

Library of Congress Cataloging-in-Publication Data:

Doherty, Jim.
Cisco networking simplified / Jim Doherty, Neil Anderson, Paul Della Maggiora. -- 2nd ed.
p. cm.
ISBN 978-1-58720-199-8 (pbk.)
1. Computer networks. I. Anderson, Neil. II. Della Maggiora, Paul L.
III. Title.
TK5105.8.C57D44 2007
004.6—dc22
2007046376

ISBN-13: 978-1-58720-199-8

ISBN-10: 1-58720-199-2

Warning and Disclaimer

This book is designed to provide information about Cisco networking. Every effort has been made to make this book as complete and accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

Publisher

Paul Boger

Associate Publisher

Dave Dusthimer

Cisco Representative

Anthony Wolfenden

Cisco Press Program Manager

Jeff Brady

Executive Editor

Karen Gettman

Managing Editor

Patrick Kanouse

Development Editor

Sheri Cain

Senior Project Editor

Tonya Simpson

Copy Editor

Gayle Johnson

Technical Editors

Bradley Mitchell, Matthew Stein

Editorial Assistant

Vanessa Evans

Cover Designer

Louisa Adair

Interior Design and Composition

Mark Shirar

Proofreader

Paula Lowell

Indexer

Heather McNeil

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside the United States, please contact:

International Sales
international@pearsoned.com

About the Technical Reviewers

Bradley Mitchell is a freelance writer covering technology topics, specializing in computer networking. Online, he has produced the About.com Wireless/Networking site since 2000. He also is a senior engineer at Intel Corporation. Over the past 14 years at Intel he has served in various capacities for research and development of software and network systems. He obtained a master's degree in computer science from the University of Illinois and a bachelor's degree from MIT.

Matthew Stein is a marketing manager for Enterprise Solutions Marketing (ESM) at Cisco. In his role, he defines and develops network service solutions for the enterprise market, which spans multiple networking technologies and drives business growth, performance, and IT efficiencies. He previously worked in the Wireless Business Unit of Cisco, where he was responsible for leading the development and marketing integration of Enterprise networking solutions for the Cisco Aironet Wireless product line. Before joining Cisco in May 2000, Stein served as a database design system engineer for GE Lighting. He also was a system engineer for the Center for Brain Imaging at the Medical College of Wisconsin. He received his bachelor of science degree in electrical engineering from Case Western Reserve University.

Dedications

This book is dedicated to Bradley Mitchell.

Bradley was introduced to us by our publisher as a technical reviewer when we wrote our first book together back in 2004 (*Home Networking Simplified*).

We were so happy with his effort, his insightful comments, and his technical expertise that we asked him to be a reviewer on the next book. And on the one after that. And so on and so on until we look back and realize that over five titles, the entire set of the *Networking Simplified* series, Bradley has been a critical part of our writing team, and our books are better for it.

This is not to say that our other reviewers along the way have not been great. They have. But Bradley catches errors that no one else catches (writers, reviewers, publishing team). He is constantly making sure that we have our audience in mind and advises us to rewrite sections when have gone off the deep end. And when we refer to a 128-digit number (and then feel compelled to give an example of one), Bradley actually counts the digits, lets us know that we left off two 0s at the beginning, and then reminds us that you probably don't care about seeing the actual number anyway.

It's nearly impossible to attain perfection in a book like this, but Bradley gets us much, much closer than we would have otherwise. This book, and all our books, are better than they would have been, because Bradley took the time to help us make them better.

We've never had a chance to meet him in person. When we do, we'll shake his hand and buy him a beer (or maybe five—one for each book). In the meantime, we hope this is enough.

Acknowledgments

Jim and Neil would like to thank the following people:

Our families, whom we lied to after the last book, when we said we would not do this again, and who put up with our working late nights and weekends. This time, we mean it.

Our publisher and the fine team at Cisco Press and Pearson Education. We would especially like to thank our editor, Sheri Cain, who bravely agreed to join us on another project; our production manager, Patrick Kanouse; Chris Cleveland; Karen Gettman; Tonya Simpson; Jennifer Gallant; Gayle Johnson; and the rest of the Cisco Press team working behind the scenes.

As always, we want to thank our illustrator, Nathan Clement at Stickman Studios (http://www.stickman-studio.com/), who never fails to deliver a great product.

A special thanks to our technical reviewers, Bradley Mitchell and Matthew Stein, who worked hard on our readers' behalf to keep us honest and accurate.

We would also like to thank the following people at Cisco who helped with content and questions: Tim Szigeti, Brian Cox, Ron Maxam, John Strika, Mike Herbert, Jason Frazier, Max Ardica, Stephenie Chastain, Joel King, May Konfong, Damon Li, Martin Pueblas, Chris O'Brien, and Roland Dobbins.

Contents

Introduction xiii

Part I: Networking Fundamentals 3

How Computers Communicate 4

The OSI Model 5

Open Versus Proprietary Systems 5

Seven Layers 5

At-a-Glance: OSI Model 7–9

Internet Infrastructure: How It All Connects 10–11

TCP/IP and IP Addressing 12

Computers Speaking the Same Language 13

What Is an Address? 13

Dynamically Allocated IP Addresses 14

Domain Names and Relationship to IP Addresses 14

Matching Domain Names to IP Addresses 15

At-a-Glance: TCP/IP 16–18

At-a-Glance: IP Addressing 19–21

At-a-Glance: IPv6 22–24

NAT and PAT 25

Internet Applications 26

The Internet and Its Applications 27

E-Mail 27

Web Browsing 28

E-Mail 30

Peer-to-Peer Sharing 31

Part II: Networking Infrastructure 33

Ethernet 34

History of Ethernet 35

What Is Ethernet? 35

Evolution of Ethernet 36

At-a-Glance: Ethernet 37–39

Reducing Collisions on Ethernet 40

LAN Switching 42

Fast Computers Need Faster Networks 43

Switching Basics: It's a Bridge 43

Switching Ethernets 44

Switches Take Over the World 44

At-a-Glance: Switching 45–47

Spanning Tree 48

Network Loops 49

Sometimes, the Earth Is Flat 49

Preventing Network Loops 49

Spanning-Tree Fundamentals 49

At-a-Glance: Spanning Tree 51–53

Routing 54

Routers 55

Routers Talk Among Themselves to Find Routes 55

Routers Route Packets 55

Routers Bridge and Switches Route 56

At-a-Glance: Routing 57–59

Routing and Switching 60–61

Part III: Network Design 63

Campus Networks and Hierarchical Design 64

Building Networks for Ease of Use 65

At-a-Glance: Hierarchical Campus Design 66–69

WAN Network Design 70

Moving Traffic Across the Street and the World 71

WAN Services 71

Integrated Services Digital Network 71

Frame Relay 72

ATM 72

MPLS 73

Broadband 73

Virtual Private Networks (VPN) 73

WAN Devices 73

At-a-Glance: Frame Relay 74–75

At-a-Glance: Asynchronous Transfer Mode (ATM) 76–77

Multiprotocol Label Switching (MPLS) Services 78

At-a-Glance: MPLS 79–81

MPLS Traffic Separation 82

Broadband Technologies 84

Always-on Access 85

Broadband Technology Evolution 85

At-a-Glance: ISDN 87–88

At-a-Glance: Broadband 89–91

Virtual Private Networks 92

Secure Networking Over the Internet 93

At-a-Glance: VPNs 95–97

Establishing a VPN Connection 98–99

At-a-Glance: Encryption 100–102

Client Authentication 103–104

Optical Technologies 106

LANs, WANs—and Now MANs 107

SONET, DWDM, and DPT 107

At-a-Glance: Metro Optical 109–111

Branch Office Network Designs 112

Distributed Workforce 113

Distributed Office Challenges 113

At-a-Glance: Branch Office Design 114–117

Part IV: Network Availability 119

High Availability 120

At-a-Glance: High Availability 124–126

Control Plane 128

When Good Networks Go Bad 129

Control Plane Protection 129

At-a-Glance: Control Plane Protection 130–131

Quality of Service and Network Availability 132

Quality of Service as Network Protection? 133

Scavenger QoS 133

At-a-Glance: QoS for Network Resiliency 134–136

Disaster Recovery 138

What Happens When the Network Stops Working 139

DR Planning 139

Resiliency and Backup Services 140

Preparedness Testing 140

At-a-Glance: Disaster Recovery: Business Continuance 141–143

Disaster Recovery 144

Network Management 146
Keeping the Network Alive from Afar 147
Network Documentation: A Must-Have 148
Network-Management Protocols 148
Troubleshooting Tools 149
At-a-Glance: Network Management 150–151
Network Management 152

Part V: Securing the Network 155

Network Security 156
Identity 157
Perimeter Security 157
Data Privacy 157
Security Monitoring 158
Policy Enforcement 158
At-a-Glance: Network Security 159–160
At-a-Glance: Hacking 161–163
DoS Attacks 164–165
Snooping and Spoofing 166

Firewalls 168
Protecting the Perimeter 169
Get Off the Net! 169
Firewall for Your Protection 169
Personal Firewalls 170
At-a-Glance: Firewalls and IDS 171–172
Firewalls and IDS 173
Access and Content Security 174

Intrusion Prevention Systems 176
Intrusion Detection Systems 177
Intrusion Prevention Systems 177
The Problem with False Positives 177
At-a-Glance: Intrusion Detection 178–179

Port-Based Security 180
Combating Access-Based Attacks 181
At-a-Glance: Port-Based Security 182–184

Identity-Based Networking 186
Network Access Conundrum 187
Identity-Based Networking 187
802.1x 187
At-a-Glance: Identity 188–190
Authentication 191

Network Admission Control 192
Combating Virus Outbreaks 193
Assessing Device "Health" 193
Network Admission Control 194
At-a-Glance: NAC 195–197

URL Filtering: Eliminating Unwanted Web Page Access 198
Internet Access and Liability Issues 199
Enforcing Corporate Internet Usage Policies 199
At-a-Glance: URL Filtering 200–201
URL Filtering and Firewalls 202

Deep Packet Inspection: Controlling Unwanted Applications 204
How Do You Catch a Criminal When Everyone Wears a Mask? 205
Deep Packet Inspection 205
At-a-Glance: Deep Packet Inspection 206–208
Packet Inspection 209

Telemetry: Identifying and Isolating Attack Sources 210

Normal or Abnormal 211

Using Telemetry to Combat Attacks 211

At-a-Glance: Telemetry 212–213

Physical Security: IP Video Surveillance 214

Locks on the Doors 215

Video Surveillance 215

At-a-Glance: Physical Security 216–217

Physical and Logical Security 218

Part VI: Data Centers and Application Networking 221

Moving Data Efficiently 221

Data Centers 222

Store Once, Use Often 223

n-Tier Model 223

Functions and Requirements 223

At-a-Glance: Data Centers 225–227

Data Center Application: Corporate Expense System 228

Storage Area Networks 230

Efficient Deployment of Critical Data 231

Fiber Channel and IP 231

Infiniband 232

At-a-Glance: Storage Networking 233–235

Server-Centric Storage 236

Caching 238

Moving Content Close to the User 239

How Caching Works 239

Caching More Than Web Pages 239

Storage Caching: From Disk to Memory 240

Issues Affecting Caching 240

Caching 241

Wide Area File Services 242

Branch Offices Rule 243

Centralizing Storage 243

Enter Wide Area File Services (WAFS) 243

At-a-Glance: Wide Area File Services 244–246

Wide Area Application Services 248

Centralizing Applications 249

Enter Wide Area Application Services (WAAS) 249

At-a-Glance: Wide Area Application Services 250–252

Part VII: Unified Communications 255

Voice over IP 256

Making Calls over the Web 257

Unifying Communications 257

Client Layer 258

Infrastructure Layer 258

Call-Processing Layer 258

Application Layer 259

Deployment Models 259

At-a-Glance: Voice over IP 261–263

Voice over IP 264

At-a-Glance: Unified Communications 265–266

Voice over IP: Toll Bypass 267

Quality of Service .268

Converged Networks and QoS .269

What Is QoS? .269

QoS and Unified Communications .269

At-a-Glance: QoS .271–272

How Packets Are Prioritized .273

Unified Personal Communications .274

Too Many Communications, Too Little Time .275

Unify Me .275

Cisco Unified Personal Communicator (CUPC) .275

At-a-Glance: Unified Communications .276–277

Meeting Collaboration Spaces .278

Meetings, Meetings, Meetings .279

Meetings Are an Activity, Not a Place .279

At-a-Glance: Meeting Collaboration .280–281

Traditional Videoconferencing .282

I See You .283

Video over IP Networks .283

At-a-Glance: IP Videoconferencing .284–285

Videoconferencing .286

Videoconferencing Application E-Learning .287

Telepresence .288

Conferencing Gets Simple .289

Video Killed the Radio Star .289

The Next-Best Thing to Being There .289

At-a-Glance: Telepresence .290–291

Presence and Location-Aware Services .292

I Sense a Presence .293

The Importance of Location .293

At-a-Glance: Presence and Location-Aware Services .294–295

IP Call Center .296

Why Can't I Talk to a Real Person? .297

Anatomy of a Contact Center .297

From the Caller to the Agent, and Back Again .297

Managing Caller and Contact Agent Efficiency .298

New Methods for Customer Interaction .298

At-a-Glance: IP Contact Center .299–300

Call-Center Tech Support .301

Call-Center Telemarketing .302

Multicast and IPTV Broadcasts .304

Watching Movies Without Flooding the World .305

At-a-Glance: IP Multicast .307–308

Multicast .309

Part VIII: Mobility .311

Wireless World .311

Mobility and Wireless Networks .312

Throwing Away the Ties That Bind .313

At-a-Glance: Wireless LANs .314–315

Wired LANs .316

Wireless LANs .317

Selecting and Building Wireless Networks .318

Designing a Wireless Network .319

At-a-Glance: Designing Wi-Fi Networks .320–323

Securing Wireless Networks .324

Locking Down Wireless .325

Balancing Security and Access .325

At-a-Glance: Securing Wi-Fi .326–328

Outdoor and Municipal Wireless Networks 330

It's Just Like a Building, Only Way Bigger 331

At-a-Glance: Municipal Wi-Fi 332–334

VoIP over Wireless Networks 336

Wireless VoIP 337

At-a-Glance: Wireless VoIP 338–339

Wireless VoIP 340

Wireless Guest Access 342

Mi Casa Es Su Casa 343

At-a-Glance: Wireless Guest Access 344–345

RFID and Location-Based Services 346

Finding Your Stuff 347

Wireless LANS: They're Not Just for Checking E-Mail on the Toilet Anymore! .347

At-a-Glance: Location-Based Services 348–350

Wireless Location Services 351

Part IX: Virtualized Networks 353

Virtualizing Data Centers 354

Growth of the Data Center 355

Data Center Virtualization 355

At-a-Glance: Virtual Data Centers 356–358

Virtualizing Network Infrastructure 360

Leveraging Network Investment 361

A Network Is a Network 361

Virtualizing Network Infrastructure 361

At-a-Glance: Virtual Network Infrastructure 362–365

Applications of Virtualized Networks 366

What Can You Do with Virtualized Networks? 367

Corporate Employee "Clean" and "Dirty" Networks 367

Guest and Partner Networks 367

Isolating Specialized Devices and Applications 367

Load Balancing 367

Providing Hosted Networks to Entities Within Entities 367

Departmental Virtual Networks 368

Challenges with Virtual Networks 368

At-a-Glance: Virtualized Network Applications 369–372

Evolution of Virtual Networks 373–374

Index 376

Introduction

Welcome, and thank you for taking a look at this book! Unlike the vast array of networking books written by geeks for geeks, this book was written for you and for anyone who wants to understand the computer networking phenomenon that has taken the world by storm. (In other words, it's by geeks for nongeeks.) We understand that the vast majority of people working in this industry are not networking experts and that it is difficult to understand complex technical and business issues before knowing the answers to such questions as "How does the web work?," "What is a router?," and "What is an IP address?"

Whether you are a home computer user who has just purchased a broadband Internet connection or a company executive who wants to understand what your IT staff is talking about, this book is for you.

If you've decided that you want to make a career change, or if you are in school pursuing a Cisco certification, we believe that this book will serve both as a good primer, introducing the concepts of networking in clear and simple terms, and as a useful reference book as you grow in your career.

What's New in This Edition?

Five years ago, when Paul Della Maggiora and Jim Doherty wrote the first edition, we were trying to fill a gap in the market with a book that explained a broad selection of networking technologies and concepts for the beginner or nontechnical person. Upon sharing our early work, we realized we might be on to something. More talks with college interns, Cisco Academy students, and nontechnical executives at Cisco customers indicated demand for a show-me-what-it-is type of book. This book provides at-a-glance text and illustrations that explain a particular concept or technology in plain and simple language. The material illustrates how these concepts relate to our everyday lives.

We are pleased with the reception the book has received since it was first published. We have received a great deal of positive feedback both from our intended audience and, much to our surprise, from very technical people as well. In fact, the book has had enough interest that we were approached to write a second edition to cover all the new technologies that have come about in the last five years. After all was said and done, about half of this book ended up being new.

Among the biggest additions to this version are the topics covering security, communication tools, and wireless technologies. Security has become one of the biggest areas of investment for networking as companies attempt to protect their network and data from ever-increasing threats and attacks. Communication tools have also changed quite a bit in five years, as both voice and video tools have become more integrated and more sophisticated. Finally, wireless is everywhere now, and users expect all the networking tools on the wired network to be on the wireless network as well.

Another change in this book is that Neil Anderson has joined the writing team. Neil is the coauthor of four other *Networking Simplified* books that we have written since the original release of *Cisco Networking Simplified*. Neil is a great addition to the team and brings a wealth of expertise and insight to this edition.

So How Do I Use This Thing?

The book is divided into nine theme-based parts, each with several chapters covering a network concept or technology. Each chapter contains some or all of the following: a part summary, topic at-a-glance pages, and whiteboard illustrations of relevant concepts. The part summary provides a quick and easy introduction to the topic, so you should generally read it first. Useful for future reference are the topic at-a-glance pages, which illustrate core concepts. And the whiteboard illustrations demonstrate important concepts simply and graphically.

The flow of this book is a bit different from the first time around. In this edition, we took a building-block approach:

- Part I: Networking Fundamentals
- Part II: Networking Infrastructure
- Part III: Network Design
- Part IV: Network Availability
- Part V: Securing the Network
- Part VI: Data Center and Application Networking
- Part VII: Unified Communications
- Part VIII: Mobility
- Part IX: Virtualized Networks

We believe that this approach helps you get from the basics to the more advanced topics more easily. This approach also makes it easier to jump directly into a single topic of interest and understand the big picture.

The illustrations and descriptions of the topics serve to answer the primary questions "What is it?", "Why should I care?", and "What problems need to be solved?". We use "big animal" pictures to explain many of the concepts and avoid the temptation to dive into nitty-gritty details. If you are reading this book, you need to know, for example, what a router does, but not how to actually program one.

The second time around, we had as much fun as the first time through writing and illustrating this book. We also had the benefit of experience and are hopeful that we put it to good use. We hope you find this book both useful and entertaining. If it ends up being your primary reference for networking, so much the better.

This page intentionally left blank

Securing Wireless Networks

Locking Down Wireless

For every networking innovation, there is a hacker looking to exploit it. The advent of wireless networking was no different; in fact, the hackers had a field day with this one early on. The reason is that before wireless, hackers had only two ways to get into a network: They could either penetrate it from the Internet or could get physical access to a live switch port inside the network.

Despite all the news about hacking, breaching a corporate network from the Internet is extremely difficult. This method provides a lot of anonymity (always a plus when breaking the law). If someone can get access to the switch port, the technical stuff is easy. There is, of course, the matter of being caught and detained, though.

When wireless came about, it was a dream for hackers, because they could sit in a car in the parking lot, or even on a bench outside, protecting their anonymity while taking advantage of what was a live port on the network.

You may be wondering why those clever IT guys didn't see this coming. The truth is, they did. In fact, wireless was viewed as such a problem that many companies refused to implement it because of the security risks. However, wireless became accessible and affordable on the consumer side. Corporate employees instantly understood the productivity gains of being able to remain connected while away from their desks. As soon as the prices of wireless routers began to drop, they did what made sense to them. They plugged their own wireless access points—literally, their own personal hotspots—into the ports in their offices so that they could roam around and check e-mail.

Now IT had a huge problem. Not only was wireless a known security risk, but they had open wireless APs that they did not control all over their networks. This was the birth of the "rogue" AP, and it made their security look like Swiss cheese. This is when something really interesting happened. IT realized that the wireless cat could not be stuffed back in the bag. Wireless was here to stay. The people had mandated that they have wireless access, and IT departments realized it was better to "own" wireless so that they could properly secure it.

Balancing Security and Access

Most people in networking believe that balancing security and access is a zero-sum game: give to one, and you must take from the other. Wireless security was no different in the beginning, because users were forced to enter 26-digit hexadecimal codes to gain secure wireless access. It was a pain, but that was the price you paid for checking your e-mail when meetings started to get boring.

Wireless security has come a long way from the "easily" breached Wired Equivalent Privacy (WEP) security keys to the more secure Wi-Fi Protected Access (WPA) and WPA2 security standards. Ease of use has also been improved. Laptops are usually preconfigured by IT so that users can securely connect without a lot of additional steps.

At-a-Glance: Securing Wi-Fi

Why Should I Care About Wireless Security?

With wired networks, intruders need to gain physical access to a building to gain access to the network via a port. With wireless networks, security is a concern because intruders only need to be in the proximity of the building to "see" the wireless signal. In addition, with wired networks intruders need access to your wire to eavesdrop, but for wireless networks they only need to be in the proximity of your client to potentially conduct eavesdropping.

Additional security measures need to be employed on wireless networks to give them the same security confidence level as with wired networks.

An additional security threat presented by wireless networks is someone plugging in a "rogue" access point, essentially an unauthorized wireless network that can put a huge hole in a business's network security policies.

What Problems Need to Be Solved?

For WLANs to be secure, the first challenge is how to secure the process of associating a client to the wireless network to prevent unauthorized wireless access.

Next, there needs to be a way to secure the communications between a client and the wireless network to prevent eavesdropping, balancing security measures with the ease of use still required for clients to access the network.

As mentioned earlier, a secure WLAN implementation needs to be able to mitigate the threat of "rogue" or unauthorized wireless access points.

Wireless security is not a trivial thing. Early attempts at so-called "wired equivalence" (WEP, for example) gave/give a false sense of security in this regard. That is, WEP made people think that they were secure when it was actually a pretty easy thing to crack.

Securing Wireless Networks

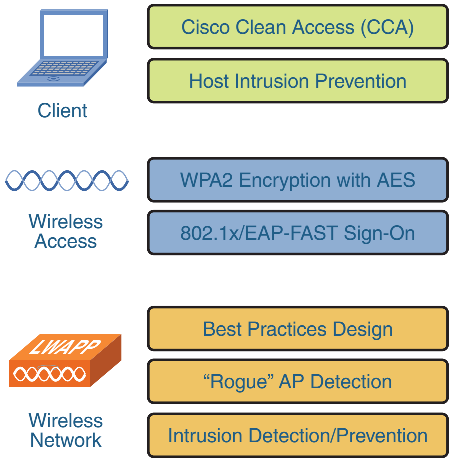
The Cisco Secure Wireless solution provides an integrated approach for deploying secure wireless and mobility services.

Clients are secured via a device "health check" and admission control with Cisco Clean Access (CCA).

Host intrusion prevention is assured with Cisco Secure Agent (CSA).

The wireless access interface is secured via 802.1x/EAP-FAST sign-on authentication, WPA and WPA2 Wi-Fi encryption, and best-practices wireless network.

Finally, the wireless network is secured via an integrated Intrusion Detection System (IDS) and "rogue" (unauthorized) wireless AP detection and mitigation. This is a unified approach to wired and wireless security because many of the features just discussed are also deployed in the wired network.

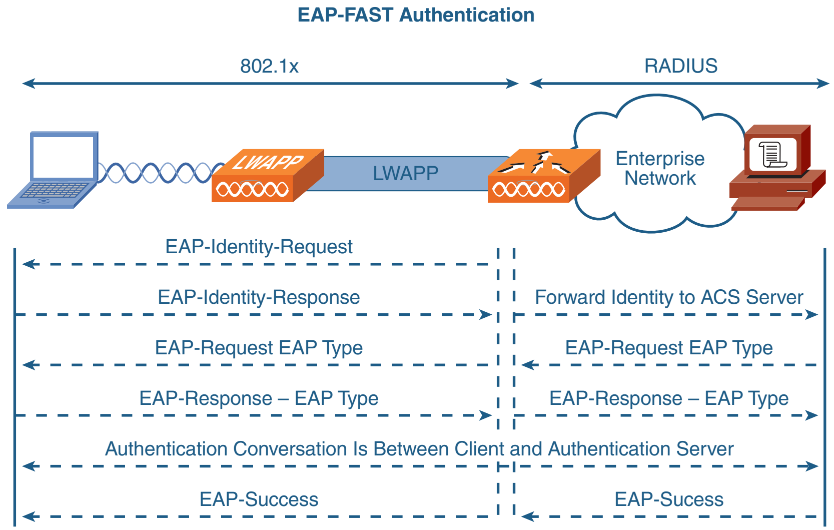


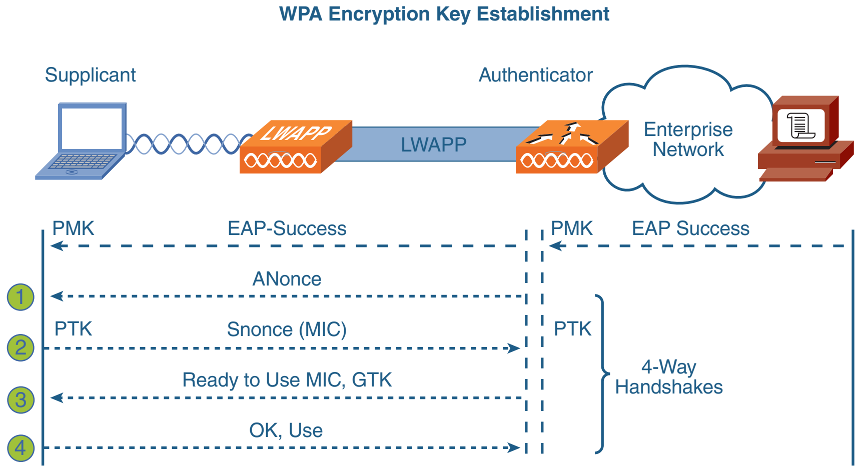
Wireless Encryption

The first important step in securing wireless is to follow best practices for client authentication and encryption. By using Extensible Authentication Protocol (EAP) and Flexible Authentication via Secure Tunnel (FAST) to authenticate wireless clients, only authorized clients are given access to the network. After they are connected, WPA or WPA2 (preferred) is used for encryption key establishment. After EAP-FAST is successful, a pairwise master key (PMK) is created.

WPA and WPA2 use a four-way handshake process to generate a pairwise temporal key (PTK) that is kept secret. WPA2 uses the Advanced Encryption Standard (AES) algorithm, adding security above WPA.

At-a-Glance: Securing Wi-Fi

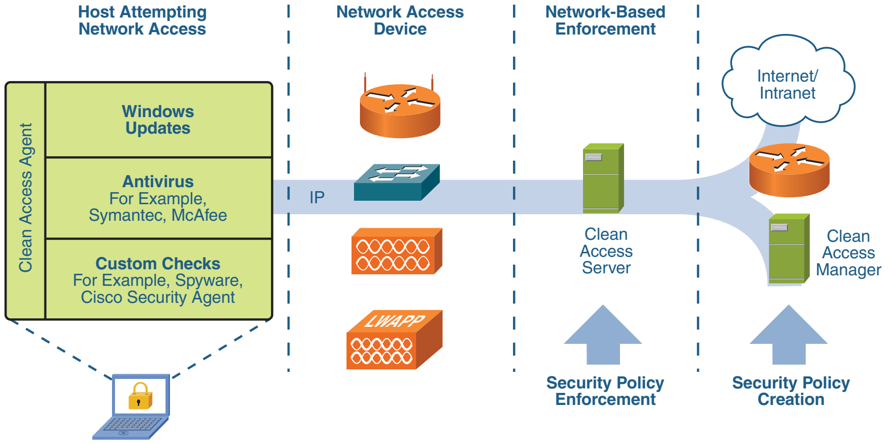




Health Checks

By their nature, laptops and other mobile devices inherently get exposed to more opportunities for infections by viruses, malware, spyware, and so on. Given that, it is a good wireless security practice to add a "posture check" to the authentication process to ensure that the client is healthy before gaining access. Cisco Network Admission Control (NAC) using Cisco Clean Access (CCA) performs an additional challenge to client devices to "prove their health" before being allowed to access the wireless network. The definition of a "healthy" device is determined by the IT staff. It can include the following:

- Free of viruses and other malware
- Correct antivirus software and signature files are loaded
- Operating system updates are current
- Custom policy checks added by IT staff



Unhealthy devices are placed in a "quarantine" wired or wireless network for remediation and are not permitted to access the rest of the production network.

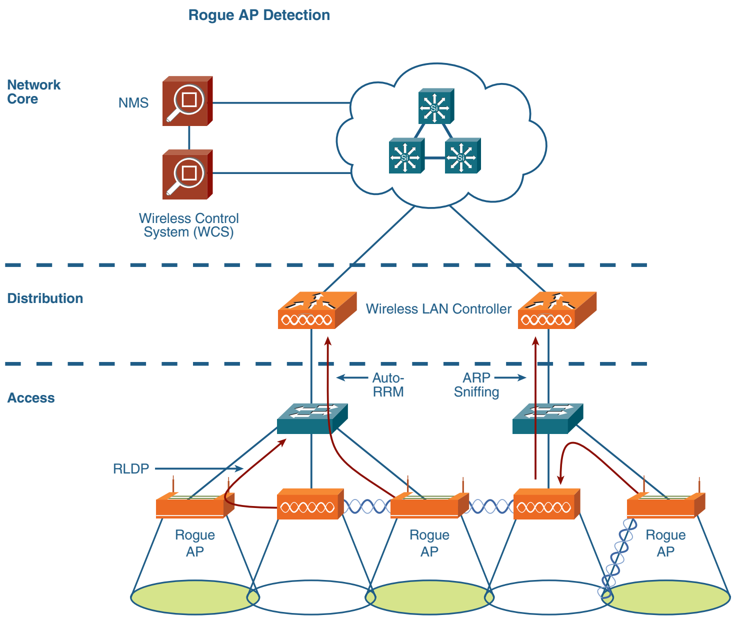
See Part V, "Securing the Network," for a more in-depth discussion of NAC and CCA.

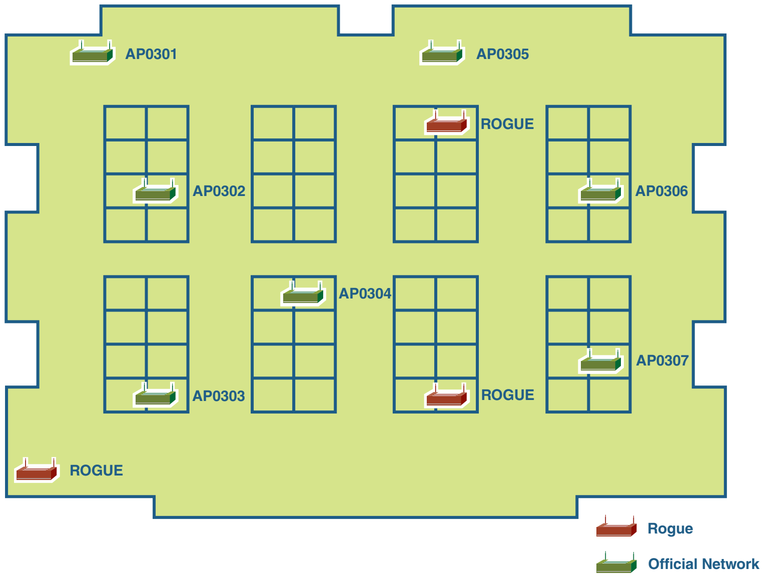
Rogue Access Points

"Rogue" or unauthorized wireless access points provide a serious security threat to a network. Locating and shutting down such unauthorized APs can be difficult without automated detection and location systems. The Cisco

At-a-Glance: Securing Wi-Fi

Unified Wireless solution uses authorized wireless access points to scan the environment for “rogue” access points. Detection information is provided to the WLCs, which can then assist in correlation and isolation and provide the information to the WCS. Wireless topology information can be married with building layout diagrams to provide visual indications of “rogue” AP locations so that IT staff can take appropriate actions to shut them down.





This page intentionally left blank

Index

Symbols

3DES (Triple Data Encryption Standard), 100

24/7/365 availability, 121

99.999 percent availability, 124

802.11b/802.11g/802.11n, 321

802.1x, 187–188

@ (at symbol), 27

A

AAA (Authentication, Authorization, and Accounting), 227

access

- attacks, combating, 181
- control, WLANs, 315
- guest, 343
  - *configuring, 345*
  - *importance, 344*
  - *problems, 344*
  - *SSID, 344*
  - *Unified Wireless solution, 344*
  - *virtualized networks, 371*
- Internet
  - *broadband, 85–90*
  - *ISDN, 87*
- limiting, 189
- methods, 231–232
- remote, 93–95
- unwanted, preventing, 189
- wireless networks, 325

access control lists. *See* ACLs

access layer (campus networks), 65

access points. *See* APs

ACD (automatic call distribution), 297

ACELP (Algebraic Code-Excited Linear Prediction), 263

ACLs (access control lists)

- data centers, 227
- perimeter security, 160

active attacks, 161

active monitoring, 179

Address Resolution Protocol (ARP), 16, 182–183

addresses

- e-mail, 27
- IP, 13
  - *classes, 19–20*
  - *diminishing availability, 22*
  - *domain names, 14*
  - *dotted-decimal notation, 13–14, 19*
  - *dynamic, 14*
  - *hosts/networks, 19*
  - *importance, 19*
  - *problems, 19*
  - *spoofing, 182–183*
  - *subnet addresses, 21*
  - *subnet masks, 20–21*
  - *subnets, 20*
- IPv4, 22
- IPv6, 22
  - *advantages, 22*
  - *autoconfiguration, 23*
  - *migration, 24*
  - *mobile devices, 23*
  - *notation, 22*
  - *security, 23*
- logical, 19
- MAC, 13
  - *flooding, 182–183*
  - *instability, 51*
- physical, 19
- subnet, 21
- switches, learning, 46

administration, 147

- documentation, 148
- importance, 150
- mobility, 151
- problems, 150
- process frameworks, 147–148
- protocols, 148–149
- troubleshooting tools, 149

ADSL (Asymmetric DSL), 86

Advanced Encryption Standard (AES), 100

advantages

- broadband, 85
- cable modems, 91
- DSL, 90
- IPv6, 22
- Layer 3 routed networks, 49
- OSI, 7
- unified communications, 277
- videoconferencing, 289
- virtualized data centers, 355
- VPNs, 95
- wireless networking, 313

AES (Advanced Encryption Standard), 100

aggregation (data centers), 223

aging out, 46

Algebraic Code-Excited Linear Prediction (ACELP), 263

analog-to-digital conversions, 261–262

anarchists, 162

anomalies, detecting, 213

ANSI (American National Standards Institute), 231

Any Transport over MPLS (AToM), 81

appliance-based clean access, 196

- **application layers**
  - encryption, 102
  - OSI, 6–7
  - unified communications, 258–259, 266
- **application servers, centralizing, 249**
- **applications.** ***See also*** **software**
  - data centers, 223
  - Internet
    - *e-mail, 27–28*
    - *web browsing, 28–29*
  - virtualized networks, 367
    - *challenges, 368*
    - *clean/dirty endpoints, 367*
    - *departmental regulation compliance, 368*
    - *device isolation, 372*
    - *framework solution, 369–370*
    - *guest/partner access, 367, 371*
    - *importance, 369*
    - *load balancing, 367*
    - *network admission control, 370*
    - *private entities, hosting, 367*
    - *problems, 369*
    - *specialized devices, isolating, 367*
- **APs (access points), 313**
  - municipal wireless, 333
  - roaming WLANs, 315
  - rogue, 162, 320, 325–328
- **architecture**
  - branch offices, 114
  - MPLS, 80
  - VPNs, 95–96
- **ARP (Address Resolution Protocol), 16, 182–183**
- **assets (wireless), finding, 347**
  - location-based services, 348–349
  - monitoring, 350
  - planning, 350
  - RFID, 347
- **Asymmetric DSL (ADSL), 86**
- **asynchronous transmission (ATM networks), 76**
- **at symbol (@), 27**
- **ATM networks, 72**
  - asynchronous transmission, 76
  - connections, 77
  - endpoints, 72, 76
  - fixed cell size, 77
  - importance, 76
  - interfaces, 76
  - LANE, 77
  - problems, 76
  - switches, 72, 76
  - virtual connections, 77
- **AToM (Any Transport over MPLS), 81**
- **attacks**
  - access, combating, 181
  - active, 161
  - blocked by firewalls, 169
  - DoS, 162
  - false positives, 177
  - hit-and-run, 161
  - internal, 162
  - man-in-the-middle, 161
  - passive, 161
  - remote, 161
  - rogue access points, 162
  - sneak, 179
  - sources, 211–213
- **attenuation, 109**
- **audioconferencing, 280**
- **authentication**
  - network infrastructure virtualization, 364
  - servers, 190
- **Authentication, Authorization, and Accounting (AAA), 227**
- **auto-configuration (IPv6), 23**
- **automatic call distribution (ACD), 297**
- **availability.** ***See*** **high availability**

B

- **back doors, 162**
- **back-end congestion notification (BECN), 72**
- **back end functions (data centers), 223**
- **backbone, 65**
- **backups**
  - availability, 122–123
  - data centers, 223
  - dial, 71
  - disaster recovery, 143
- **Backward Explicit Congestion Notification (BECN), 75**
- **bad packets, 171**
- **bandwidth**
  - conservation for VoIP, 262–263
  - Ethernet, 38
  - low-bandwidth tools, 272
  - videoconferencing, 284
- **baselining, 213**
- **basic bridging, 43**
- **Basic Rate Interface (BRI), 85–87**
- **BECN (back-end congestion notification), 72**
- **BGP (Border Gateway Protocol), 55**
- **botnets, 163**

BPDU (bridge protocol data units), 49

branch office designs, 113–115, 243

- architecture, 114
- communications, 116–117
- distributed offices, 113
- distributed workforce, 113
- importance, 114
- problems, 114
- scaling, 114
- security, 115–116
- storage centralization, 243
- WAFS, 243
  - *caching, 245–246*
  - *file engine, 244–245*
  - *importance, 244*
  - *problems, 244*
  - *transparency, 245*

BRI (Basic Rate Interface), 85–87

bridge protocol data units (BPDU), 49

bridges

- basic, 43
- Ethernet, 36–38
- as firewalls, 43
- LANs, 43
- routers as, 56
- switches, compared, 43–44
- transparent, 43
- types, 43
- wireless, 313

broadband

- advantages over dialup, 85
- cable, 85–86, 90–91
- choosing, 86
- DSL, 85, 89–90
- importance, 89
- overview, 85
- problems, 89
- speed, 89
- technology evolution, 85
- WANs, 73

broadcast domains, 45

broadcast storms, 51

browsing (web), 28–29

building WLANs, 314–315

building-to-building bridge systems, 314

C

Cable Modem Termination System (CMTS), 91

cable modems, 85, 90

- advantages, 91
- DSL, compared, 86
- equipment, 91
- limitations, 91

cables

- availability, 122, 125
- Ethernet, 35

CAC (Call Admission Control), 339

caching, 28, 221, 239

- content freshness, 240
- disk to memory, 240
- load limits, 240
- overview, 239
- problems, 240
- video/audio files, 239
- WAFS, 245–246

call processing layer, 258–259, 266

CallManager (CM), 258–259, 299

CAM (Clean Access Manager), 196

campus networks, 65

- hierarchical, 65
- high availability, 67
- importance, 66
- oversubscription, 67
- redundancy, 67
- services, 69
- size, 67–69

carrier sense multiple access/collision detect (CSMA/CD) protocol, 35

CAS (Clean Access Server), 196

causes

- disaster recovery, 141
- network unavailability, 121–124

CCA (Cisco Clean Access), 326

CCTV (closed-circuit TV), 215

CDPD (Cellular Digital Packet Data), 332

centralizing

- applications, 249
- storage, 243

CGMP (Cisco Group Management Protocol), 308

change control management, 122, 126

choosing

- broadband connections, 86
- e-mail addresses, 27

chromatic distortion, 109

CIPS (Cisco Intrusion Prevention System), 178

circuit switching, 71

Cisco Clean Access (CCA), 326

Cisco Group Management Protocol (CGMP), 308

Cisco Intrusion Prevention System (CIPS), 178

Cisco Secure Agent (CSA), 326

Cisco Unified Personal Communicator (CUPC), 275

- **citywide wireless, 331–334**
  - access points, 333
  - importance, 332
  - legacy wide-area wireless data networks, 332
  - Outdoor Wireless Mesh, 332
  - portable devices, 332
  - problems, 332
  - security, 334
  - wireless backhauls, 333
- **classes (IP addresses), 19–20**
- **Clean Access Manager (CAM), 196**
- **Clean Access Server (CAS), 196**
- **clean implementations, 122–125**
- **clean nets, 171**
- **client layer, 257–258, 266**
- **client/server models, 226**
- **closed-circuit TV (CCTV), 215**
- **CM (CallManager), 299**
- **CMTS (Cable Modem Termination System), 91**
- **coarse wavelength division multiplexing (CWDM), 110**
- **collisions, 20, 37**
- **comfort noise (VoIP), 263**
- **communications**
  - audioconferencing, 280
  - branch offices, 116–117
  - IP call centers, 297
    - *anatomy, 297*
    - *call flow examples, 299–300*
    - *components, 297*
    - *customer interaction methods, 298*
    - *equipment, 299*
    - *importance, 299*
    - *inbound calls, 297–298*
    - *managing, 298*
    - *migrating from east to west, 300*
    - *outbound calls, 298*
    - *problems, 299*
    - *remote workers, 300*
    - *routing to specialized agents, 300*
  - location services, 294
  - managing
    - *location services. See location services*
    - *presence, 293*
  - meeting collaboration
    - *importance, 280*
    - *instant messaging integration, 281*
    - *MeetingPlace solution, 280*
    - *meetings as activities, 279*
    - *problems, 280*
    - *scheduling application integration, 280*
    - *spaces, 279*
    - *Telepresence, 289–291*
    - *videoconferencing, 281–285, 289*
  - models
    - *open-source, 5*
    - *OSI, 5–9*
    - *proprietary, 5*
  - Presence, 295
  - QoS, 269
    - *classification, 272*
    - *importance, 271*
    - *jitter, 271*
    - *latency, 271*
    - *loss, 271*
    - *low-bandwidth tools, 272*
    - *MOS, 270*
    - *provisioning, 271*
    - *scheduling, 272*
  - unified, 257
    - *advantages, 277*
    - *application layer, 258-259, 266*
    - *call processing layer, 258-259, 266*
    - *client layer, 257–258, 266*
    - *convergence, 257, 275*
    - *CUPC, 275*
    - *deployment, 259–260*
    - *device convergence, 275*
    - *importance, 265, 276*
    - *infrastructure layer, 258, 266*
    - *IP phone calls, placing, 265*
    - *jitter, 270*
    - *latency, 270*
    - *layers, 257*
    - *loss, 269*
    - *management capabilities, 277*
    - *overview, 266*
    - *problems, 265, 276*
    - *productivity, increasing, 277*
    - *QoS, 269–270*
    - *solution, 276*
    - *toll bypass, 265*
    - *types of communication, 275*
  - VoIP
    - *analog-to-digital conversions, 261–262*
    - *bandwidth conservation, 262–263*
    - *codecs, 263*
    - *comfort noise, 263*
    - *importance, 261*
    - *packet transportation, 261*
- **complexity, reducing, 125**
- **compressing voice, 262–263**
- **computer health**
  - assessing, 193
  - NAC, 194–196

- **computer telephony integration (CTI), 297–299**
- **configuring wireless guest access, 345**
- **congestion notification, 75**
- **connections**
  - ATM networks, 77
  - Internet. *See* broadband
  - MPLS, 78
  - multipoint, 291
  - TCP, 16
  - VPNs, 93
  - WANs, 71
    - *ATM. See ATM networks*
    - *broadband, 73, 85*
    - *circuit switching, 71*
    - *Frame Relay, 72–74*
    - *ISDN, 71, 87*
    - *MPLS, 73, 78*
    - *packet switching, 71*
    - *point-to-point, 71*
    - *virtual circuits, 71*
    - *VPNs, 73, 93*
- **consistent uptime (availability), 123**
- **console messages, 148**
- **contact centers, 297**
  - anatomy, 297
  - call flow examples, 299–300
  - components, 297
  - customer interaction methods, 298
  - equipment, 299
  - importance, 299
  - inbound calls, 297–298
  - managing, 298
  - migrating from east to west, 300
  - outbound calls, 298
  - problems, 299
  - remote workers, 300
  - routing to specialized agents, 300
- **content freshness (caching), 240**
- **control plane, 129–131**
- **Control Plane Protection Policing (CoPP), 129–131**
- **convergence**
  - QoS, 269
  - unified communications, 275
- **CoPP (Control Plane Protection Policing), 129**
  - dedicated processors, 131
  - implementing, 130
  - importance, 130
  - overview, 130
  - problems, 130
- **core layer, 65**
- **corporate Internet usage policies, 199**
- **corporate WLANs. *See* WLANs**
- **costs**
  - downtime, 124
  - routers, 57
  - videoconferencing, 283
- **CPE (Customer Premises Equipment), 73, 79**
- **crackers, 162**
- **CRM (customer resource management), 223**
- **CSA (Cisco Secure Agent), 326**
- **CSMA/CD (carrier sense multiple access/collision detect) protocol, 35**
- **CTI (computer telephony integration), 297–299**
- **CUPC (Cisco Unified Personal Communicator), 275**
- **cut-through switching mode, 46**
- **CWDM (coarse wavelength division multiplexing), 110**

D

- **Daemen, Joan, 100**
- **DARPA (Defense Advanced Research Projects Agency), 13**
- **DAS (directly attached storage), 231**
- **data**
  - caching, 221
  - de-encapsulation, 9
  - encapsulation, 9
  - privacy, 157, 160
- **data centers**
  - aggregation, 223
  - application servers, centralizing, 249
  - applications, 223
  - back end, 223
  - backups, 223
  - branch offices, 243
  - caching, 221
    - *content freshness, 240*
    - *disk to memory, 240*
    - *load limits, 240*
    - *overview, 239*
    - *problems, 240*
    - *video/audio files, 239*
  - distribution, 226
  - facilities, 227
  - front end, 223
  - functions, 223
  - high availability, 224
  - importance, 225
  - layers, 225–226
  - managing, 227
  - n-tier models, 223
  - network transport, 223

overview, 223
problems, 225
requirements, 224
SANs, 221
scalability, 224
security, 224, 227
storage, 223, 227
importance, 233
NAS, 234–235
overview, 233
problems, 233
SANs. See SANs
technologies, 234
traditional server-centric storage methods, 233
traditional client/server model, 226
types, 225
virtualization, 224
advantages, 355
data center virtualization solution, 356
fixed data centers, compared, 357–358
importance, 356
migration, 358
overview, 355
problems, 356
WAAS, 249
data redundancy elimination, 252
importance, 250
overview, 250
problems, 250
TCP compatibility, 251
transparency, 250–251
data communications equipment (DCE), 74
Data Encryption Standard (DES), 100
data flow layers (OSI), 7
data link connection identifiers (DLCI), 72, 75
data link layers, 6, 102
data plane, 129
data read caching, 245
Data Redundancy Elimination (DRE), 252
data terminal equipment (DTE), 72–74
datagrams, 16
DCE (data communications equipment), 74
DDoS (Distributed DoS), 162
DDR (dial-on-demand routing), 71
dedicated processors, 131
de-encapsulation, 9
deep packet inspections, 205
catalyst example, 208
importance, 206
overview, 207
problems, 206
defects per million (DPM), 124
Defense Advanced Research Projects Agency (DARPA), 13
delays (routers), 57
demilitarized zone (DMZ), 169
Denial of Service (DoS), 162
dense wavelength division multiplexing (DWDM), 107–108, 111
deployment
IDSs, 178
unified communications, 259–260
VPNs, 95
DES (Data Encryption Standard), 100
designing
branch offices, 113–115
architecture, 114
communications, 116–117
distributed offices, 113
distributed workforce, 113
importance, 114
problems, 114
scaling, 114
security, 115–116
campus networks, 65
high availability, 67
importance, 66
oversubscription, 67
redundancy, 67
size, 67–69
high availability, 124
metro optical technologies, 109–110
wireless networks, 319
WLANs, 322
DHCP (Dynamic Host Configuration Protocol), 14
DHCP servers, 182–183
dial backups, 71
dial-on-demand routing (DDR), 71
dialup services, 71
Diffie-Hellman Key Exchange, 101
digital signal processing (DSP), 258
digital subscriber line (DSL), 85–86, 89–90
digital surveillance systems, 216
Direct Sequence Spread Spectrum (DSS), 315
directly attached storage (DAS), 231
dirty nets, 172
disaster recovery
backups, 143
business resiliency, 140
causes, 141
fires, 139
importance, 141
normal operations, 143
overview, 139
planning, 139, 142

preparedness testing, 140, 143
primary systems, restoring, 143
problems, 141
risk assessments, 142
discovery, 59
dispersion, 109
distance accumulation, 58
distance vector routing, 58–59
Distributed DoS (DDoS), 162
distributed offices, 113
distributed workforce, 113
distribution layer, 65
distribution trees, 307
DIX standard (Ethernet), 35
DLCIs (data link connection identifiers), 72, 75
DMVPNs (dynamic multipoint VPNs), 96–97
DMZ (demilitarized zone), 169
DNS (Domain Name System), 14
documentation, 148
Domain Name System (DNS), 14
domains
broadcast, 45
collision, 20, 37
names, 14, 27
DoS (Denial of Service), 162
dotted-decimal notation, 13–14, 19
downtime
costs, 124
measuring, 121
per year measurements, 121
DPI (deep packet inspection), 205
catalyst example, 208
importance, 206
overview, 207
problems, 206
DPM (defects per million), 124
DPT (dynamic packet transport), 107–108
DRE (Data Redundancy Elimination), 252
DSL (digital subscriber line), 85–86, 89–90
DSP (digital signal processing), 258
DSS (Direct Sequence Spread Spectrum), 315
DTE (data terminal equipment), 72–74
duplicate frames, 51
DWDM (dense wavelength division multiplexing), 107–108, 111
Dynamic Host Configuration Protocol (DHCP), 14
dynamic IP addresses, 14
dynamic multipoint VPNs (DMVPNs), 96–97
dynamic packet transport (DPT), 107–108
dynamic routes, 57

E

EAP (Extensible Authentication Protocol), 188, 326
EGP (Exterior Gateway Protocols), 58
EIGRP (Enhanced Interior Gateway Routing Protocol), 55
e-mail, 27
addresses, 27
clients, 27
domain names, 27
receiving, 28
recipients, 27
sending, 28
web-based, 27
encapsulation, 9, 78
encryption
export laws, 100
importance, 100
keys, 101
layers, 102
packets, 205
problems, 100
standards, 100
VPNs, 95
wireless, 326
endpoints, 72, 76
enforcing security policies, 158–160
engineering traffic, 272
Enhanced Interior Gateway Routing Protocol (EIGRP), 55
enterprise resource planning (ERP), 223
equipment. *See* hardware
ERP (enterprise resource planning), 223
Ethernet
bandwidth, increasing, 38
bridges, 36–38
cables, 35
collisions, 37
distance limitations, 36
DIX standard, 35
evolution, 36
full duplex, 36
history, 35
hubs, 36–38
importance, 37
LAN routers, 38
LAN switches, 38
naming, 35
optical, 110
overview, 35–36
problems, 37
repeaters, 38
segmenting, 37–38
switches, 36, 44
Token Ring, 35

Extensible Authentication Protocol (EAP), 188, 326

Exterior Gateway Protocols (EGP), 58

external security attacks, 159

extranets

- server farms, 225
- VPNs, 93

F

facilities (data centers), 227

factoring, 101

false positive attacks, 177

FAST (Flexible Authentication via Secure Tunnel), 326

fault tolerance, 231

FCAPS (Fault, Configuration, Accounting, Performance, and Security), 147–148

FCIP (Fiber Channel over IP), 232

FEC (Forwarding Equivalence Classes), 80

FECN (front-end congestion notification), 72, 75

fiber-based MANs, 107

fiber channel, 231–232, 234

Fiber Channel over IP (FCIP), 232

Fiber-Optic Transmission Systems (FOTS), 107

file engine, 244–245

filters

- inside, 171
- outside, 172
- server-side, 28
- SRTBH, 213
- switches, 45
- URL filtering, 199
  - *black/white lists, 201*
  - *importance, 200*
  - *overview, 200*
  - *problems, 200*
  - *third-party servers, 201*

finding wireless assets, 347

- location-based services, 348–349
- monitoring, 350
- planning, 350
- RFID, 347

firewalls, 169

- bad packets, 171
- clean nets, 171
- dirty nets, 172
- DMZ, 169
- function, 171
- good packets, 171
- hackers, 172
- importance, 171
- inside filters, 171
- isolation LANs, 171
- outside filters, 172
- personal, 170
- problems, 171
- protection provided, 169

first-order traffic anomalies, 135

five nines availability, 124

flat Earth popularity, 49

flat networks, 57

Flexible Authentication via Secure Tunnel (FAST), 326

flooding, 44–46, 182–183

Forward Explicit Congestion Notification (FECN), 75

forwarding

- multicast, 308
- packets, 55
- ports, 50
- switches, 46

Forwarding Equivalence Classes (FEC), 80

FOTS (Fiber-Optic Transmission Systems), 107

fragment-free switching mode, 46

Frame Relay, 72

- congestion, 72, 75
- DLCIs, 75
- equipment, 74
- importance, 74
- LMIs, 75
- performance, 75
- problems, 74
- virtual circuits, 74–75

frames

- duplicate, 51
- switching modes, 46

front-end congestion notification (FECN), 72

front end functions, 223

full duplex, 36

functions

- control plane, 130
- data centers, 223
- firewalls, 171
- identities, 188
- NAC, 195–196
- telemetry, 212

G

gateways, 258

GRE (generic routing encapsulation), 96

guest access

- virtualized networks, 371
- wireless, 343
  - *configuring, 345*
  - *importance, 344*
  - *problems, 344*
  - *SSID, 344*
  - *Unified Wireless solution, 344*

H

- **H.323 protocol, 283–284**
- **hacking, 161**
  - active attacks, 161
  - anarchists, 162
  - back doors, 162
  - botnets, 163
  - breaking in, 161
  - breaking stuff, 161
  - calling cards, 161
  - crackers, 162
  - DoS, 162
  - firewalls, 172
  - hit-and-run attacks, 161
  - internal attacks, 162
  - man-in-the-middle attacks, 161
  - passive attacks, 161
  - remote attacks, 161
  - rogue access points, 162
  - script kiddies, 162
  - sniffing/spoofing, 163
  - stealing stuff, 161
  - Trojan horses, 162
  - viruses/worms, 162
- **half duplex, 36**
- **hardware**
  - availability, 125
  - cable modems, 91
  - contact centers, 299
  - DSL, 90
  - errors, 124
  - Frame Relay, 74
  - health
    - *assessing, 193*
    - *NAC, 194–196*
  - ISDN, 88
  - MPLS, 79
  - redundancy, 122
  - videoconferencing, 284
- **hashes, 101**
- **health (devices)**
  - assessing, 193
  - NAC, 194
    - *appliance-based clean access, 196*
    - *functions, 195–196*
    - *importance, 195*
    - *network-based clean access, 196*
    - *problems, 195*
  - WLANs, 327
- **hexadecimal numbers, 13**
- **hierarchy**
  - campus networks, 65–66
  - routers, 58
- **high availability, 121**
  - 24/7/365, 121
  - campus networks, 67
  - causes of failures, 124
  - change control management, 126
  - clean implementations, 125
  - complexity, reducing, 125
  - consistent uptime, 123
  - Control Plane Protection, 129
    - *dedicated processors, 131*
    - *implementing, 130*
    - *importance, 130*
    - *overview, 130*
    - *problems, 130*
  - data centers, 224
  - designing, 124
  - disaster recovery
    - *backups, 143*
    - *business resiliency, 140*
    - *causes, 141*
    - *fires, 139*
    - *importance, 141*
    - *normal operations, 143*
    - *overview, 139*
    - *planning, 139, 142*
    - *preparedness testing, 140, 143*
    - *primary systems, restoring, 143*
    - *problems, 141*
    - *risk assessments, 142*
  - downtime, 121, 124
  - five nines, 124
  - hardware, 125
  - importance, 124
  - increasing, 122–123
  - measuring, 121, 124
  - network monitoring, 125
  - QoS, 133
    - *first-order traffic anomalies, 135*
    - *normal traffic, 134–135*
    - *overview, 134*
    - *resiliency, 134*
    - *scavenger, 133*
    - *second-order traffic anomalies, 136*
    - *traffic management, 134*
  - redundancy, 126
  - security, 126
  - service providers, 125
  - software, 125
  - training for, 126
  - unavailability causes, 121–122
- **hit-and-run attacks, 161**

home WLANs, 314
hop counts, 57
hosts, isolating, 213
HSRP (Hot Standby Router Protocol), 65, 125
HTML (Hypertext Markup Language), 29
HTTP (Hypertext Transfer Protocol), 29
hub-and-spoke DMVPN, 97
hubs, 36–38

I

IBNS (Identity-Based Networking Services, 187
ICM (intelligent call management), 299
ICMP (Internet Control Message Protocol), 16
identities, 157
  802.1x, 188
  access limitations, 189
  authentication servers, 190
  EAP, 188
  establishing, 159–160
  function, 188
  importance, 188
  PKI, 190
  problems, 188
  RADIUS, 190
  unwanted access, preventing, 189
  user-based service provisioning, 190
Identity-Based Networking Services (IBNS), 187
IDS (Intrusion Detection System), 177, 227, 326
  data centers, 227
  deploying, 178
  false positive attacks, 177
  importance, 178
  IPS, 177
  passive monitoring, 179
  problems, 178
  sneak attacks, 179
IEEE (Institute of Electrical and Electronic Engineers), 5
IGMP (Internet Group Management Protocol), 305–308
IGP (Interior Gateway Protocol), 58
IKE (Internet Key Exchange), 94
IMAP (Internet Mail Access Protocol), 28
inbound calls (contact centers), 297–298
increasing
  availability, 122–123
  bandwidth, 38
Infiniband, 232
Information Technology Infrastructure Library (ITIL), 147–148
infrastructure layer, 258, 266
inside filters, 171
Institute of Electrical and Electronic Engineers (IEEE), 5
Integrated Services, 71
intelligent call management (ICM), 299
intelligent rerouting, 81
interactive voice response (IVR), 297
interdomain routing, 58
interfaces
  ATM networks, 76
  ISDN, 87
Interior Gateway Protocol (IGP), 58
internal attacks, 159, 162
International Organization for Standardization (ISO), 5
International Telecommunications Union (ITU), 283
Internet
  broadband
    advantages over dialup, 85
    cable modems, 85–86, 90–91
    choosing, 86
    DSL, 85, 89–90
    importance, 89
    overview, 85
    problems, 89
    speed, 89
    technologies, 85
    WANs, 73
  browsing, 28–29
  connection speeds, 89
  e-mail, 27
    addresses, 27
    clients, 27
    domain names, 27
    receiving, 28
    recipients, 27
    sending, 28
    web-based, 27
  ISDN, 87
  protocols, 16. *See also* TCP/IP
  security, 157, 199
  server farms, 225
Internet Control Message Protocol (ICMP), 16
Internet Group Management Protocol (IGMP), 305–308
Internet Key Exchange (IKE), 94
Internet Protocol. *See* IP
intradomain routing, 58
intranet server farms, 225
Intrusion Detection System. *See* IDS

IP (Internet Protocol), 13
addresses, 13
classes, 19–20
diminishing availability, 22
domain names, 14
dotted-decimal notation, 13–14, 19
dynamic, 14
hosts/networks, 19
importance, 19
IPv4, 22
IPv6, 22–24
problems, 19
spoofing, 182–183
subnets, 20–21
call centers, 297
anatomy, 297
call flow examples, 299–300
components, 297
customer interaction methods, 298
equipment, 299
importance, 299
inbound calls, 297–298
managing, 298
migrating from east to west, 300
outbound calls, 298
problems, 299
remote workers, 300
routing to specialized agents, 300
enabled video, 217
multicast, 305–306
CGMP, 308
distribution trees, 307
forwarding, 308
IGMP, 307–308
importance, 307
Layer 2, 308
PIM, 308
problems, 307
networks
Telepresence over, 290–291
videoconferencing over, 283
phone calls, placing, 265
SANs access, 232
SCSI (iSCSI), 227, 234
telephony, 265
version 4 (IPv4), 22
version 6 (IPv6), 22
advantages, 22
autoconfiguration, 23
migration, 24
mobile devices, 23
notation, 22
security, 23
IPS (Intrusion Prevention Systems), 177
active monitoring, 179
false positive attacks, 177
IPsec, 23, 96
IPv4 (IP version 4), 22
IPv6 (IP version 6), 22
advantages, 22
autoconfiguration, 23
migration, 24
mobile devices, 23
notation, 22
security, 23
iSCSI (IP SCSI), 227, 234
ISDN (Integrated Services Digital Network), 71, 85
calls, initiating, 88
equipment, 88
importance, 87
interfaces, 87
Internet access, 87
problems, 87
WANs, 71
ISO (International Organization for Standardization), 5
isolation
hosts, 213
LANs, 171
network infrastructure virtualization, 364
specialized devices, 367, 372
ITIL (Information Technology Infrastructure Library), 147–148
ITU (International Telecommunications Union), 283
IVR (interactive voice response), 297

J – K

JBOD (just a bunch of disks), 231
jitter, 270–271

keys, 101

L

Label Distribution Protocol (LDP), 79
label switch routers (LSR), 79
labels, 79
LANE (LAN emulation), 77
LANs
bridges, 43
congestion, 43
emulation clients (LEC), 77
emulation servers (LES), 77
isolation, 171
repeaters, 43
routers, 38

switches, 38
aging out, 46
bridges, compared, 43–44
filtering, 45
forwarding, 46
importance, 45
overview, 43
problems, 45
VLANs, 47
wireless. *See* WLANs
large campus networks, 69
latency (communication), 270–271
Layer 2 bridged (flat) networks, 49
Layer 2 multicast IP, 308
Layer 3 routed networks, 49
Layer 8 (OSI), 9
layers
campus networks, 65
data centers, 225–226
encryption, 102
OSI, 7
communicating between, 8
data application, 7
data flow, 7
de-encapsulation, 9
encapsulation, 9
Layer 8, 9
problems, 7
unified communications, 257
application, 258–259, 266
call-processing, 258–259, 266
client, 257–258, 266
infrastructure, 258, 266
LDP (Label Distribution Protocol), 79
LEC (LAN emulation clients), 77
LES (LAN emulation servers), 77
limiting access, 189
link state routing, 59
LMIs (local management interfaces), 75
loads
balancing, 367
limits, 240
location services
importance, 293–294
problems, 294
solution, 294
wireless assets, 348
monitoring, 350
planning, 350
problems, 348–349
Unified Wireless solution, 349
locking down wireless networks, 325
logical addresses, 19
loops
overview, 49
preventing. *See* STP
problems, 51
loss
communication QoS, 271
unified communications, 269
low-bandwidth tools, 272
low-pass filters (LPF), 90
LPF (low-pass filters), 90
LSR (label switch routers), 79

M

MAC addresses, 13
flooding, 182–183
instability, 51
managing
cables, 125
change control, 122, 126
communications, 293
contact centers, 298
data centers, 224, 227
networks, 147
documentation, 148
FCAPS, 147–148
importance, 150
ITIL, 147–148
mobility, 151
problems, 150
protocols, 148–149
troubleshooting tools, 149
temperature, 122
traffic, 134
man-in-the-middle attacks, 161
man-made disasters, 141
MANs (metropolitan-area networks), 107, 232
maximum message length (MTU), 57
MBGP (Multiprotocol Border Gateway Protocol), 306
MCU (Multipoint Conferencing Unit), 291
Mean Opinion Score (MOS), 270
measuring
availability, 121, 124
downtime, 121
medium campus networks, 68
meeting collaboration
importance, 280
instant messaging integration, 281
MeetingPlace solution, 280
meetings as activities, 279
problems, 280
scheduling application integration, 280

spaces, 279
Telepresence, 289–291
videoconferencing, 281
advantages, 289
bandwidth, 284
costs, 283
equipment, 284
H.323 protocol, 284
importance, 284
legacy systems, 284
over IP networks, 283
overview, 283
problems, 284
QoS, 284
T.120 protocols, 284
traditional, 283
zones, 285
MeetingPlace solution, 280
Metcalfe, Robert, 35
metro optical technologies, 109
attenuation, 109
chromatic distortion, 109
CWDM, 110
designing, 109–110
dispersion/nonlinearities, 109
DWDM, 111
Ethernet, 110
fiber basics, 109
multiplexing, 110
polarization, 110
problems, 109
SONET, 111
metropolitan-area networks (MANs), 107, 232
migration
IPv6, 24
virtualized data centers, 358
MIPv6 (Mobile IPv6), 23
mobility
administration, 151
IPv6, 23
models of communication, 5–7
monitoring
active, 179
availability, 122, 125
passive, 179
security, 158–160
wireless asset location, 350
MOS (Mean Opinion Score), 270
MPLS (Multiprotocol Label Switching), 78
any-to-any connectivity, 78
architecture, 80
encapsulation, 78
equipment, 79
importance, 79
intelligent rerouting, 81
labels, 79
Layer 2 tunneling, 81
problems, 79
routers, 80
security, 80
services, 78
traffic engineering, 78, 81
VPNs, 78, 81, 97
WANs, 73
MSDP (Multicast Source Discovery Protocol), 305
MST (Multiple Spanning Tree), 49
MTU (maximum message length), 57
multicast protocols, 305
Multicast Source Discovery Protocol (MSDP), 305
multicasting (IP), 305–306
CGMP, 308
distribution trees, 307
forwarding, 308
IGMP, 307–308
importance, 307
Layer 2, 308
PIM, 308
problems, 307
multimode fiber, 109
Multiple Spanning Tree (MST), 49
multiple zones (videoconferencing), 285
multiplexing metro optical technologies, 110
Multipoint Conferencing Unit (MCU), 291
multipoint connections (Telepresence), 291
Multiprotocol Border Gateway Protocol (MBGP), 306
Multiprotocol Label Switching. *See* MPLS
multisite independent call processing deployment, 259
multisite with centralized call processing deployment, 259
multisite with distributed call processing deployment, 259
multitasking, 43
municipal wireless, 331
access points, 333
importance, 332
legacy wide-area wireless data networks, 332
Outdoor Wireless Mesh, 332
portable devices, 332
problems, 332
security, 334
wireless backhauls, 333

N

NAC (Network Admission Control), 194, 370
- appliance-based clean access, 196
- functions, 195–196
- importance, 195
- network-based clean access, 196
- problems, 195
- virtualization, 370

names
- domain names, 14, 27
- Ethernet, 35

NAS (Network Attached Storage), 227, 234–235

NAT (Network Address Translation), 22

natural disasters, 141

Network Admission Control. *See* NAC

network-based clean access, 196

network broadcast domains, 45

network discovery, 59

network infrastructures (virtualization)
- applications
  - *challenges, 368*
  - *clean/dirty endpoints, 367*
  - *departmental regulation compliance, 368*
  - *device isolation, 372*
  - *framework solution, 369–370*
  - *guest/partner access, 367, 371*
  - *importance, 369*
  - *load balancing, 367*
  - *network admission control, 370*
  - *private entities, hosting, 367*
  - *problems, 369*
  - *specialized devices, isolating, 367*
- authentication, 364
- implementing, 361
- importance, 362
- investing, 361
- isolation, 364
- network virtualization solution, 362–363
- partitions, 365
- problems, 362
- security, 361
- service levels, 361

network layers, 6, 102

next-hop associations, 55

nonlinearities, 109

normal traffic, 134–135

n-tier (data centers), 223, 226

number of nines, 124

Nyquist Rate, 262

O

Open Shortest Path First (OSPF) protocol, 55

Open Systems Interconnection seven-layer model. *See* OSI

open-source systems, 5

operational errors, 124

optical technologies
- DPT, 107–108
- DWDM, 107–108
- fiber-based MANs, 107
- metro, 109
  - *attenuation, 109*
  - *chromatic distortion, 109*
  - *CWDM, 110*
  - *designing, 109–110*
  - *dispersion/nonlinearities, 109*
  - *DWDM, 111*
  - *Ethernet, 110*
  - *fiber basics, 109*
  - *multiplexing, 110*
  - *polarization, 110*
  - *problems, 109*
  - *SONET, 111*
- SONET, 107–108

OSI (Open Systems Interconnection) seven-layer model, 5
- advantages, 7
- layers
  - *application, 7*
  - *communicating between, 8*
  - *data flow, 7*
  - *de-encapsulation, 9*
  - *encapsulation, 9*
  - *Layer 8, 9*
  - *problems, 7*
  - *seven layers, 5–6*
- overview, 5
- protocols, 6

OSPF (Open Shortest Path First) protocol, 55

out-of-band network, 129–131

outbound calls (contact centers), 298

outdoor wireless. *See* municipal wireless

Outdoor Wireless Mesh, 332

outside filters, 172

oversubscription, 67

P

packets
- analog-to-digital conversions, 261
- bad, 171
- deep inspections, 205
  - *catalyst example, 208*
  - *importance, 206*
  - *overview, 207*
  - *problems, 206*

encryption, 205
forwarding, 55
good, 171
loss, 339
switching, 55, 71
transporting, 261
pairwise master keys (PMK), 326
pairwise temporal keys (PTK), 326
PARC (Palo Alto Research Center), 35, 39
partitions
network infrastructure virtualization, 365
private entities, hosting, 367
passive monitoring (IDS), 179
PAT (Port Address Translation), 22
paths
recalculating, 53
routers, 55
spanning tree, 53
PBX (private branch exchange), 257, 297
PDUs (protocol data units), 8
PE (provider edge), 79
performance (Frame Relay), 75
perimeter security (firewalls), 157, 160, 169
bad packets, 171
clean nets, 171
dirty nets, 172
DMZ, 169
function, 171
good packets, 171
hackers, 172
importance, 171
inside filters, 171
isolation LANs, 171
outside filters, 172
personal, 170
problems, 171
protection provided, 169
permanent virtual circuits (PVC), 71
personal firewalls, 170
PG (peripheral gateway), 299
physical addresses, 19
physical layer (OSI), 5
physical security (video surveillance), 215
digital systems, 216
importance, 216
IP enabled, 217
problems, 216
PIM (Protocol-Independent Multicast), 305, 308
PKI (Public Key Infrastructure), 190
planning
disaster recovery, 139, 142
location-based services, 350
PMKs (pairwise master keys), 326
PoE (Power over Ethernet), 217
point-to-point connections (WANs), 71
Points of Presence (PoPs), 73
polarization, 110
policies
checking, 195
corporate Internet usage, 199
security, 158–160
POP3 (Post Office Protocol 3), 28
PoPs (Points of Presence), 73
ports
forwarding, 50
learning, 50
listening, 50
numbers, 17
roles, 52
security
access attacks, combating, 181
ARP poisoning, 183
importance, 182
IP addresses, spoofing, 183
MAC flooding, 183
malicious DHCP servers, 183
problems, 182
tools, 182
states, 52
transitions, 50
Post Office Protocol 3 (POP3), 28
Power over Ethernet (PoE), 217
preparedness testing, 140, 143
presence, 293–295
presentation layer (OSI), 6
preventing loops. *See* STP
PRI (primary rate interface), 87
primary systems, restoring, 143
privacy
data, 157, 160
WLANs, 315
private branch exchange (PBX), 257, 297
private keys, 101
problems
administration, 149–150
ATM networks, 76
branch offices, 114
broadband, 89
caching, 240
Control Plane Protection, 130
DAS, 231
data centers, 225
deep packet inspections, 206
disaster recovery, 141

encryption, 100
Ethernet, 37
Frame Relay, 74
hacking, 161
identities, 188
IDSs, 178
IP
addresses, 19, 22
call centers, 299
multicast, 307
ISDN, 87
location services, 294, 348–349
loops, 51
meeting collaboration, 280
metro optical technologies, 109
MPLS, 79
municipal wireless, 332
NAC, 195
network infrastructure virtualization, 362
OSI layers, 7
port-based security, 182
redundancy, 51
routers, 57
security, 159
storage networking, 233
switches, 45
TCP protocol, 16
telemetry, 212
Telepresence, 290
unified communications, 265, 276
URL filtering, 200
videoconferencing, 284
video surveillance, 216
virtual network applications, 369
virtualized data centers, 356
VPNs, 95
WAAS, 250
WAFS, 244
wireless
guest access, 344
VoIP, 338
WLANs, 314, 320, 326
process frameworks, 147–148
processors (dedicated), 131
proprietary systems, 5
protecting, control plane, 129
dedicated processors, 131
implementing, 130
importance, 130
overview, 130
problems, 130
protocol data units (PDU), 8
Protocol-Independent Multicast (PIM), 305
protocols
802.1x, 187–188
administration, 148–149
ARP, 16, 182–183
CGMP, 308
CSMA/CD, 35
DHCP, 14
EAP, 188, 326
H.323, 283–284
HSRP, 65, 125
HTTP, 29
ICMP, 16
IGMP, 305–308
IMAP, 28
interdomain routing, 58
Internet protocol suite, 13
intradomain routing, 58
IP. *See* IP
IPsec, 23
LDP, 79
MBGP, 306
MSDP, 305
multicast, 305
OSI, 6
PIM, 305, 308
POP3, 28
routing, 55
SMTP, 28
SNMP, 148
STP, 5, 49
importance, 51
link health, 52
paths, recalculating, 53
port roles, 52
port states, 52
port transitions, 50
root, electing, 49
rules, 50
state, 49
T.120, 284
TCP, 13, 16
alternative, 16
compatibility, 251
connections, establishing, 16
Flow Optimization (TFO), 251
problems, 16
TCP/IP, 5, 16, 148
connections, establishing, 16
datagrams, 16
port numbers, 17
windowing, 17
UDP, 16–17

provider edge (PE), 79
provisioning QoS, 271
PSTN (Public Switched Telephone Network), 67, 121, 255
PTKs (pairwise temporal keys), 326
Public Key Infrastructure (PKI), 190
public keys, 101
Public Switched Telephone Network (PSTN), 67, 121, 255
PVCs (permanent virtual circuits), 71
ATM networks, 77
Frame Relay, 75

Q

QoS (Quality of Service), 133, 339
availability, 133
communications, 269
classification, 272
importance, 271
jitter, 271
latency, 271
loss, 271
low-bandwidth tools, 272
MOS, 270
provisioning, 271
scheduling, 272
converged networks, 269
overview, 134
resiliency, 134
scavenger, 133
Telepresence, 291
traffic
first-order anomalies, 135
management, 134
normal, 134–135
second-order anomalies, 136
unified communications, 269–270
videoconferencing, 284
wireless VoIP, 338–339

R

Radio Frequency Identification (RFID), 347
RADIUS (Remote Authentication Dial-In User Service), 190
RAID (Redundant Array of Inexpensive Disks), 231
Rapid Spanning Tree Protocol (RSTP), 49
RARP (Reverse Address Resolution Protocol), 16
receiving e-mails, 27–28
recovery
automatic, 123
disaster
backups, 143
business resiliency, 140
causes, 141
fires, 139
importance, 141
normal operations, 143
overview, 139
planning, 139, 142
preparedness testing, 140, 143
primary systems, restoring, 143
problems, 141
risk assessments, 142
reducing complexity, 125
redundancy
availability, 122, 126
campus networks, 67
problems, 51
Redundant Array of Inexpensive Disks (RAID), 231
remote access, 93–95
remote attacks, 161
Remote Authentication Dial-In User Service (RADIUS), 190
rendezvous points (RPs), 305
repeaters, 36
Ethernet, 38
LANs, 43
Requests for Comments (RFCs), 13
resiliency
disaster recovery, 140
QoS, 134
retrieving data, 234
Reverse Address Resolution Protocol (RARP), 16
Reverse Path Forwarding (RPF), 305
RFCs (Requests for Comments), 13
RFID (Radio Frequency Identification), 347
Rijmen, Vincent, 100
risk assessments, 142
roaming WLANs, 315, 323
rogue access points, 162, 320, 325–328
routers
as bridges, 56
costs, 57
delays, 57
distance vector routing, 58–59
dynamic, 57
flat networks, 57
hierarchical networks, 58
hop counts, 57
importance, 57
interdomain, 58
intradomain, 58
label switch (LSR), 79
LAN, 38

  - link-state routing, 59
  - maximum transmission unit, 57
  - metrics, 57
  - MPLS, 80
  - next-hop associations, 55
  - overview, 55
  - packets, 55
  - path determination, 55
  - problems, 57
  - protocols, 55
  - reliability, 57
  - routing, 55
  - static, 57
  - switches as, 56
  - updates, 55
  - WANs, 73
- **routing by rumor, 58**
- **RPF (Reverse Path Forwarding), 305**
- **RPs (rendezvous points), 305**
- **RSTP (Rapid Spanning Tree Protocol), 49**

S

- **sampling, 261**
- **SANs (Storage Area Networks), 221, 227, 235**
  - access methods, 231–232
  - DAS problems, 231
  - data centers, 227
  - fault tolerance, 231
  - Infiniband, 232
  - overview, 231
- **SATA (Serial Advanced Technology Attachment), 227, 234**
- **scalability (data centers), 224**
- **scavenger QoS, 133**
- **scheduling QoS, 272**
- **script kiddies, 162**
- **SCSI (Small Computer Systems Interface), 227, 234**
- **SDSL (Symmetric DSL), 86**
- **second-order traffic anomalies, 136**
- **Secure Wireless solution, 326**
- **security**
  - availability, 123, 126
  - branch offices, 115–116
  - data centers, 224, 227
  - data privacy, 157, 160
  - deep packet inspections, 205
    - *catalyst example, 208*
    - *importance, 206*
    - *overview, 207*
    - *problems, 206*
  - device health
    - *assessing, 193*
    - *NAC, 194–196*
  - external attacks, 159
  - firewalls, 169
    - *bad packets, 171*
    - *clean nets, 171*
    - *dirty nets, 172*
    - *DMZ, 169*
    - *function, 171*
    - *good packets, 171*
    - *hackers, 172*
    - *importance, 171*
    - *inside filters, 171*
    - *isolation LANs, 171*
    - *outside filters, 172*
    - *personal, 170*
    - *problems, 171*
    - *protection provided, 169*
  - hacking, 161
    - *active attacks, 161*
    - *anarchists, 162*
    - *back doors, 162*
    - *botnets, 163*
    - *breaking in, 161*
    - *breaking stuff, 161*
    - *calling cards, 161*
    - *crackers, 162*
    - *DoS, 162*
    - *firewalls, 172*
    - *hit-and-run attacks, 161*
    - *internal attacks, 162*
    - *man-in-the-middle attacks, 161*
    - *passive attacks, 161*
    - *remote attacks, 161*
    - *rogue access points, 162*
    - *script kiddies, 162*
    - *sniffing/spoofing, 163*
    - *stealing stuff, 161*
    - *Trojan horses, 162*
    - *viruses/worms, 162*
  - identities, 157, 187
    - *802.1x, 187–188*
    - *access limitations, 189*
    - *authentication servers, 190*
    - *EAP, 188*
    - *establishing, 159–160*
    - *function, 188*
    - *importance, 188*
    - *PKI, 190*
    - *problems, 188*
    - *RADIUS, 190*
    - *unwanted access, preventing, 189*
    - *user-based service provisioning, 190*

- IDSs, 177
  - *deploying, 178*
  - *false positive attacks, 177*
  - *importance, 178*
  - *IPS, 177*
  - *passive monitoring, 179*
  - *problems, 178*
  - *sneak attacks, 179*
- importance, 159
- internal attacks, 159
- Internet, 157, 199
- IPS, 179
- IPv6, 23
- monitoring, 158–160
- MPLS, 80
- municipal wireless, 334
- network infrastructure virtualization, 361
- networking, 311
- overview, 157
- perimeter, 157, 160
- physical, 215–217
- policies, 158–160
- ports
  - *access attacks, combating, 181*
  - *ARP poisoning, 183*
  - *importance, 182*
  - *IP addresses, spoofing, 183*
  - *MAC flooding, 183*
  - *malicious DHCP servers, 183*
  - *problems, 182*
  - *tools, 182*
- problems, 159
- telemetry, 211
  - *anomalies, detecting, 213*
  - *function, 212*
  - *host isolation, 213*
  - *importance, 212*
  - *problems, 212*
  - *source locations, 213*
- threats, 157
- trust, compared, 159
- URL filtering, 199
  - *black/white lists, 201*
  - *importance, 200*
  - *overview, 200*
  - *problems, 200*
  - *third-party servers, 201*
- VPNs, 93–94
- vulnerabilities, 160
- wireless networking, 157
- WLANs, 315
  - *access, 315, 325*
  - *encryption, 326*
  - *health checks, 327*
  - *importance, 326*
  - *locking down, 325*
  - *privacy, 315*
  - *problems, 326*
  - *rogue access points, 325–328*
  - *Secure Wireless solution, 326*

segmenting, Ethernet, 37–38

sending e-mails, 28

Serial Advanced Technology Attachment (SATA), 227, 234

servers
- application, 249
- authentication, 190
- CTI, 299
- DHCP, 182–183
- farms, 225
- filtering, 28
- IMAP, 28
- POP3, 28
- SMTP, 28
- storage, 233
- third-party filtering, 201

service providers
- availability, 122, 125
- identifiers, 88

Service Set IDs (SSIDs), 344

services
- campus, 69
- levels, 361
- location, 293–294
- MPLS, 78
- Unified Communications, 116–117
- WAN transport, 71
  - *ATM, 72, 76–77*
  - *broadband. See broadband*
  - *circuit switching, 71*
  - *Frame Relay, 72, 74–75*
  - *ISDN, 71, 85–87*
  - *MPLS, 78–81*
  - *packet switching, 71*
  - *point-to-point, 71*
  - *virtual circuits, 71*
  - *VPNs, 73, 93*

Session Initiation Protocol (SIP), 295

session layer (OSI), 6

seven layers (OSI model), 5–6

shortest path first, 59

SIMPLE (SIP for Instant Messaging and Presence Learning Extensions), 295

Simple Mail Transfer Protocol (SMTP), 28

Simple Network Management Protocol (SNMP), 148

single-mode fiber, 109
single site deployment, 259
single zones (videoconferencing), 285
SIP (Session Initiation Protocol), 295
SIP for Instant Messaging and Presence Learning Extensions (SIMPLE), 295
site-to-site VPN connections, 93
size
  branch offices, 114
  campus networks, 67–69
small campus networks, 67
Small Computer Systems Interface (SCSI), 227, 234
SMTP (Simple Mail Transfer Protocol), 28
sneak attacks, 179
sniffing, 163
SNMP (Simple Network Management Protocol), 148
softphones, 275
software. *See also* applications
  availability, 122–125
  failures, 124
SONET (Synchronous Optical Network), 107–108, 111
Source-Based Remote-Triggered Black Hole (SRTBH) filtering, 213
Spanning Tree Protocol. *See* STP
speed
  Internet connections, 89
  MANs, 107
  WLANs, 313
SPIDs (service provider identifiers), 88
spoke-to-spoke DMVPN, 97
spoofing, 163, 183
SRST (Survivable Remote-Site Telephony), 117
SRTBH (Source-Based Remote-Triggered Black Hole) filtering, 213
SSID (Service Set IDs), 344
stacks (OSI layers), 6
standards
  encryption, 100
  wireless, 321
states
  ports, 52
  spanning tree, 49
static routes, 57
storage
  centralizing, 243
  data centers, 221, 227, 235
    access methods, 231–232
    DAS problems, 231
    data centers, 227
    fault tolerance, 231
    Infiniband, 232
    overview, 231
  importance, 233
  NAS, 234–235
  overview, 233
  problems, 233
  SANs. *See* SANs
  technologies, 234
  traditional server-centric storage methods, 233
Storage Area Networks. *See* SANs
store-and-forward switching, 44–46
STP (Spanning Tree Protocol), 5, 49
  importance, 51
  link health, 52
  paths, recalculating, 53
  ports
    roles, 52
    states, 52
    transitions, 50
  root, electing, 49
  rules, 50
  state, 49
subnet addresses, 21
subnet masks, 20–21
Survivable Remote-Site Telephony (SRST), 117
SVCs (switched virtual circuits), 71
  ATM networks, 77
  Frame Relay, 74
switches
  addresses, learning, 46
  aging out, 46
  ATM, 72, 76–77
  bridges, compared, 43–44
  Ethernet, 36, 44
  filtering, 45
  flooding, 44
  forwarding, 46
  frame switching modes, 46
  functionality, increasing, 44
  importance, 45
  LAN, 38
  overview, 43
  problems, 45
  as routers, 56
  store-and-forward switching, 44
  STP rules, 50
  WANs, 73
switching packets, 55
Symmetric DSL (SDSL), 86
Synchronous Optical Network (SONET), 111
synchronous transmissions, 72

T

T.120 protocols, 284
tailgating, 181
TCP (Transmission Control Protocol), 13, 16
- alternative, 16
- compatibility, 251
- connections, establishing, 16
- Flow Optimization (TFO), 251
- problems, 16

TCP/IP (Transmission Control Protocol/Internet Protocol), 5, 148
- connections, establishing, 16
- datagrams, 16
- port numbers, 17
- windowing, 17

TDM (time-division multiplexing), 72, 76
technologies
- broadband, 85
- optical
  - *DPT, 107–108*
  - *DWDM, 107–108*
  - *fiber-based MANs, 107*
  - *metro, 109–111*
  - *SONET, 107–108*

telemetry, 211
- anomalies, detecting, 213
- function, 212
- host isolation, 213
- importance, 212
- problems, 212
- source locations, 213

telephony
- gateways, 258
- IP, 265
- VoIP, 257

Telepresence, 289. *See also* videoconferencing
- importance, 290
- meeting rooms, 290
- multipoint connections, 291
- over IP, 290–291
- problems, 290
- QoS, 291
- solution, 290

temperature management, 122
testing
- policies, 195
- preparedness, 140, 143

TFO (TCP Flow Optimization), 251
third-party filtering servers, 201
threats (security), 157
time-division multiplexing (TDM), 72, 76
Token Ring, 35
toll bypass, 265
tools
- low-bandwidth, 272
- port-based security, 182
- troubleshooting, 149
- VFrame, 356

traffic
- engineering, 78, 81, 272
- first-order anomalies, 135
- managing, 134
- normal, 134–135
- second-order anomalies, 136
- videoconferencing, 283

training for availability, 123, 126
translational bridging, 36
Transmission Control Protocol. *See* TCP
Transmission Control Protocol/Internet Protocol. *See* TCP/IP
transmissions
- asynchronous, 76
- synchronous, 72

transparency
- bridging, 43
- WAAS, 250–251
- WAFS, 245

transport layer (OSI), 6
triangularization, 347
Triple Data Encryption Standard (3DES), 100
Trojan horses, 162
troubleshooting tools, 149. *See also* problems
trunks, 257
trust, 159
tunneling VPNs, 95

U

UDP (User Datagram Protocol), 16–17
unavailability causes, 121, 124, 127
unified communications, 257
- advantages, 277
- branch networks, 116–117
- convergence, 257, 275
- CUPC, 275
- deployment, 259–260
- device convergence, 275
- importance, 265, 276
- IP phone calls, placing, 265
- jitter, 270
- latency, 270
- layers, 257
  - *application, 258–259, 266*
  - *call-processing, 258–259, 266*
  - *client, 257–258, 266*
  - *infrastructure, 258, 266*

loss, 269
management capabilities, 277
meeting collaboration
importance, 280
instant messaging integration, 281
MeetingPlace solution, 280
meetings as activities, 279
problems, 280
scheduling application integration, 280
spaces, 279
Telepresence, 289–291
videoconferencing. See videoconferencing
overview, 266
problems, 265, 276
productivity, increasing, 277
QoS, 269–270
solution, 276
toll bypass, 265
types of communication, 275
Unified Wireless solution, 321
location-based services, 349
wireless
guest access, 344
VoIP, 338
URL filtering, 199
black/white lists, 201
importance, 200
overview, 200
problems, 200
third-party servers, 201
URLs (Universal Resource Locator), 19
User Datagram Protocol (UDP), 16
users
Presence, 295
service provisioning, 190

V

VFrame, 356
video surveillance, 215
digital systems, 216
importance, 216
IP enabled, 217
problems, 216
videoconferencing, 281. *See also* Telepresence
advantages, 289
bandwidth, 284
costs, 283
equipment, 284
H.323 protocol, 284
importance, 284
legacy systems, 284
over IP networks, 283
overview, 283
problems, 284
QoS, 284
T.120 protocols, 284
traditional, 283
zones, 285
virtual circuits, 71, 74–75
virtual LANs (VLANs), 47
Virtual Private Networks. *See* VPNs
virtualization
applications, 367
challenges, 368
clean/dirty endpoints, 367
departmental regulation compliance, 368
device isolation, 372
framework solution, 369–370
guest/partner access, 367, 371
importance, 369
load balancing, 367
network admission control, 370
private entities, hosting, 367
problems, 369
specialized devices, isolating, 367
authentication, 364
data centers, 224
advantages, 355
data center virtualization solution, 356
fixed data centers, compared, 357–358
importance, 356
migration, 358
overview, 355
problems, 356
implementing, 361
importance, 362
investing, 361
isolation, 364
network virtualization solution, 362–363
overview, 353
partitions, 365
problems, 362
security, 361
service levels, 361
viruses, 162
VLANs (virtual LANs), 47
voice compression, 262–263
VoIP (Voice over IP), 257, 311
analog-to-digital conversions, 261–262
bandwidth conservation, 262–263
codecs, 263
comfort noise, 263
importance, 261
packet transportation, 261
total cost of ownership, 257

  - videoconferencing
    - *advantages, 289*
    - *bandwidth, 284*
    - *H.323 protocol, 284*
    - *hardware, 284*
    - *importance, 284*
    - *legacy systems, 284*
    - *problems, 284*
    - *QoS, 284*
    - *T.120 protocol, 284*
    - *zones, 285*
  - wireless, 337
    - *coverages, 338*
    - *importance, 338*
    - *packet loss, 339*
    - *problems, 338*
    - *QoS, 339*
    - *quality, 338*
    - *Unified Wireless solution, 338*
- **VPNs (Virtual Private Networks), 73**
  - advantages, 95
  - architecture, 95–96
  - connections, 93
  - deployment, 95
  - dynamic multipoint, 96–97
  - encryption, 95
  - GRE, 96
  - importance, 95
  - IPsec, 96
  - MPLS, 78, 81, 97
  - overview, 93
  - problems, 95
  - remote access, 95
  - security, 93–94
  - tunneling, 95
- **vulnerabilities (security), 160**

W

- **WAAS (Wide Area Application Services), 249**
  - data redundancy elimination, 252
  - importance, 250
  - overview, 250
  - problems, 250
  - TCP compatibility, 251
  - transparency, 250–251
- **WAE (Wide Area Engine), 250**
- **WAFS (Wide Area File Services), 243**
  - caching, 245–246
  - file engine, 244–245
  - importance, 244
  - problems, 244
  - transparency, 245
- **WANs (wide area networks)**
  - defined, 71
  - dialup services, 71
  - routers, 73
  - switches, 73
  - transport services, 71
    - *ATM, 72, 76–77*
    - *broadband, 73, 85*
    - *circuit switching, 71*
    - *Frame Relay. See Frame Relay*
    - *ISDN, 71, 85–88*
    - *MPLS, 73, 78–81*
    - *packet switching, 71*
    - *point-to-point, 71*
    - *virtual circuits, 71*
    - *VPNs, 73, 93*
- **WCS (Wireless Control System), 321**
- **WDM (wavelength division multiplexing), 107**
- **web-based e-mail tools, 27**
- **web browsing, 28–29**
- **WEP (Wired Equivalent Privacy), 325**
- **Wide Area Application. *See* WAAS**
- **Wide Area Engine (WAE), 250**
- **Wide Area File Services. *See* WAFS**
- **wide area networks. *See* WANs**
- **Wi-Fi Protected Access (WPA), 325**
- **windowing, 17**
- **Wired Equivalent Privacy (WEP), 325**
- **Wireless Control System (WCS), 321**
- **wireless networking**
  - access points, 313
  - advantages, 313
  - asset location, 347
    - *location-based services, 348–349*
    - *monitoring, 350*
    - *planning, 350*
    - *RFID, 347*
  - backhauls, 333
  - bridges, 313
  - building-to-building bridge systems, 314
  - in buildings, 314–315
  - corporate versus home, 314
  - designs, 319, 322
  - guest access, 343
    - *configuring, 345*
    - *importance, 344*
    - *problems, 344*
    - *SSID, 344*
    - *Unified Wireless solution, 344*
  - municipal, 331
    - *access points, 333*
    - *importance, 332*
    - *legacy wide-area wireless data networks, 332*

Outdoor Wireless Mesh, 332
portable devices, 332
problems, 332
security, 334
wireless backhauls, 333
overview, 314
problems, 314, 320
productivity, 320
roaming, 315, 323
rogue access points, 320
security, 157, 311
access, 315, 325
encryption, 326
health checks, 327
importance, 326
locking down, 325
privacy, 315
problems, 326
rogue access points, 325–328
Secure Wireless solution, 326
site planning, 319
speeds, 313
spontaneous system overloading, 319
standards, 321
Unified Wireless solution, 321
VoIP, 311, 337
coverages, 338
importance, 338
packet loss, 339
problems, 338
QoS, 339
quality, 338
Unified Wireless solution, 338
VPNs, 93
WLANs, 313

WLANs, 313
access points, 313
asset location, 347
location-based services, 348–349
monitoring, 350
planning, 350
RFID, 347
bridges, 313
building-to-building bridge systems, 314
in buildings, 314–315
corporate versus home, 314
designing, 319, 322
guest access, 343
configuring, 345
importance, 344
problems, 344
SSID, 344
Unified Wireless solution, 344
home WLANs, 314
municipal, 331
access points, 333
importance, 332
legacy wide-area wireless data networks, 332
Outdoor Wireless Mesh, 332
portable devices, 332
problems, 332
security, 334
wireless backhauls, 333
overview, 314
problems, 314, 320
productivity, 320
roaming, 315, 323
rogue access points, 320
security, 315
access, 315, 325
encryption, 326
health checks, 327
importance, 326
locking down, 325
privacy, 315
problems, 326
rogue access points, 325–328
Secure Wireless solution, 326
site planning, 319
speeds, 313
spontaneous system overloading, 319
standards, 321
Unified Wireless solution, 321
worms, 162
WPA (Wi-Fi Protected Access), 325

X – Z

Xerox PARC, 35, 39
zones (videoconferencing), 285

This page intentionally left blank

About the Authors

Jim Doherty is the Chief Marketing Officer at CipherOptics. Before joining the CipherOptics team, he held leadership positions with Symbol Technologies and Cisco Systems. He has more than 16 years of technical marketing and engineering experience and has led various marketing campaigns for IP telephony, routing and switching solutions, and network security solutions. He is the coauthor of the *Networking Simplified* series, published by Cisco Press. He is a former Marine Corps sergeant. He holds a B.S. in electrical engineering from North Carolina State University and an MBA from Duke University.

Neil Anderson is the Senior Manager of Technology Systems Engineering with Cisco Systems. He has more than 20 years of broad engineering experience, including public telephone systems, mobile phone systems, Internet, and home networking. At Cisco, his focus is on business networks in the areas of network architecture, wireless, security, unified communications, and emerging technologies. He is the coauthor of the *Networking Simplified* series, published by Cisco Press. He holds a B.S. in computer science.