

ANTHONY SEQUEIRA, CCIE® NO. 15626



Cert Guide

Learn, prepare, and practice for exam success



CompTIA®

Network+

N10-007

CompTIA Network+ logo

PEARSON IT CERTIFICATION

Save 10% on Exam Voucher
See Inside

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



CompTIA Network+ N10-007 Cert Guide

Anthony Sequeira, CCIE No. 15626

PEARSON

Pearson IT Certification
800 East 96th Street
Indianapolis, Indiana 46240 USA

CompTIA Network+ N10-007 Cert Guide

Anthony Sequeira

Copyright © 2018 Pearson IT Certification

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-7897-5981-8

ISBN-10: 0-7897-5981-0

Library of Congress Control Number: 2017957346

Printed in the United States of America

01 18

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification 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.

Warning and Disclaimer

This book is designed to provide information about IT networking in the scope of the CompTIA Network+ exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The author 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 author and are not necessarily those of Pearson.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Editor-in-Chief

Mark Taub

Product Line Manager

Brett Bartow

Managing Editor

Sandra Schroeder

Development Editor

Marianne Bartow

Project Editor

Mandie Frank

Copy Editor

Bart Reed

Technical Editor

Robert Fleming

Editorial Assistant

Vanessa Evans

Designer

Chuti Prasertsith

Composition

Studio Galou

Indexer

Heather McNeill

Proofreader

Paula Lowell

Contents at a Glance

	Introduction	xxviii
CHAPTER 1	Computer Network Fundamentals	3
CHAPTER 2	The OSI Reference Model	31
CHAPTER 3	Network Components	63
CHAPTER 4	Ethernet Technology	117
CHAPTER 5	IPv4 and IPv6 Addresses	153
CHAPTER 6	Routing IP Packets	205
CHAPTER 7	Wide Area Networks (WANs)	239
CHAPTER 8	Wireless Technologies	275
CHAPTER 9	Network Optimization	305
CHAPTER 10	Command-Line Tools	337
CHAPTER 11	Network Management	379
CHAPTER 12	Network Security	409
CHAPTER 13	Network Policies and Best Practices	467
CHAPTER 14	Network Troubleshooting	481
CHAPTER 15	Final Preparation	529
APPENDIX A	Answers to Review Questions	537
APPENDIX B	CompTIA Network+ N10-07 Cert Guide Exam Updates	547
	Glossary	551
	Index	585

ONLINE ELEMENTS:

APPENDIX C	Memory Tables
APPENDIX D	Memory Tables Answer Key
APPENDIX E	Study Planner
	Exam Essentials Interactive Study Guide
	Key Terms Flash Cards Application
	Instructional Videos
	Performance-Based Exercises
	CompTIA Network+ N10-007 Hands-on Lab Simulator Lite Software

Table of Contents

Introduction	xxviii
Chapter 1 Computer Network Fundamentals	3
Foundation Topics	4
Defining a Network	4
The Purpose of Networks	4
Overview of Network Components	5
Networks Defined by Geography	7
LAN	7
WAN	8
WLAN	8
SAN	9
Other Categories of Networks	9
CAN	9
MAN	9
PAN	9
Networks Defined by Topology	10
Physical Versus Logical Topology	10
Bus Topology	11
Ring Topology	13
Star Topology	15
Hub-and-Spoke Topology	16
Full-Mesh Topology	17
Partial-Mesh Topology	18
Wireless Topologies	20
Ad Hoc	20
Infrastructure	20
Mesh	20
Networks Defined by Resource Location	21
Client/Server Networks	21
Peer-to-Peer Networks	22
Real-World Case Study	24
Summary	25
Exam Preparation Tasks	25

Review All the Key Topics 25

Complete Tables and Lists from Memory 26

Define Key Terms 26

Complete Chapter 1 Hands-On Lab in Network+ Simulator Lite 26

Additional Resources 26

Review Questions 26

Chapter 2 The OSI Reference Model 31

Foundation Topics 32

The Purpose of Reference Models 32

The OSI Model 33

Layer 1: The Physical Layer 35

Layer 2: The Data Link Layer 38

Media Access Control 39

Logical Link Control 40

Layer 3: The Network Layer 41

Layer 4: The Transport Layer 44

Layer 5: The Session Layer 46

Layer 6: The Presentation Layer 47

Layer 7: The Application Layer 48

The TCP/IP Stack 49

Layers of the TCP/IP Stack 49

Common Application Protocols in the TCP/IP Stack 53

Real-World Case Study 56

Summary 57

Exam Preparation Tasks 58

Review All the Key Topics 58

Complete Tables and Lists from Memory 59

Define Key Terms 59

Complete Chapter 2 Hands-On Labs in Network+ Simulator Lite 59

Additional Resources 59

Review Questions 60

Chapter 3 Network Components 63

Foundation Topics 64

Media 64

Coaxial Cable	64
Twisted-Pair Cable	66
Shielded Twisted Pair	66
Unshielded Twisted Pair	67
Plenum Versus Nonplenum Cable	70
Fiber-Optic Cable	70
Multimode Fiber	70
Single-Mode Fiber	72
Fiber Connector Polishing Styles	74
Media Converters	75
Cable Distribution	75
Wireless Technologies	77
Technologies for the Internet of Things	78
Network Infrastructure Devices	79
Hubs	80
Bridges	81
Switches	82
Multilayer Switches	89
Routers	90
Infrastructure Device Summary	91
Specialized Network Devices	91
VPN Concentrators	91
Firewalls	92
DNS Servers	93
DHCP Servers	96
Proxy Servers	98
Content Engines	99
Content Switches	100
Other Specialized Devices	101
Virtual Network Devices	101
Virtual Servers	101
Virtual Routers and Firewalls	103
Virtual Switches	103
Virtual Desktops	104

Other Virtualization Solutions	105
Cloud Computing	105
Software-Defined Networking (SDN)	107
Voice over IP Protocols and Components	107
Real-World Case Study	108
Summary	110
Exam Preparation Tasks	110
Review All the Key Topics	110
Complete Tables and Lists from Memory	111
Define Key Terms	112
Complete Chapter 3 Hands-On Labs in Network+ Simulator Lite	112
Additional Resources	112
Review Questions	113
Chapter 4	
Ethernet Technology	117
Foundation Topics	118
Principles of Ethernet	118
Ethernet Origins	118
Carrier-Sense Multiple Access/Collision Detect	120
Distance and Speed Limitations	123
Ethernet Switch Features	126
Virtual LANs	126
Switch Configuration for an Access Port	128
Trunks	129
Switch Configuration for a Trunk Port	130
Spanning Tree Protocol	130
Corruption of a Switch's MAC Address Table	131
Broadcast Storms	132
STP Operation	133
Link Aggregation	136
LACP Configuration	137
Power over Ethernet	138
Port Monitoring	139
Port Mirroring Configuration	141
User Authentication	141

Management Access and Authentication	142
First-Hop Redundancy	144
Other Switch Features	145
Real-World Case Study	145
Summary	146
Exam Preparation Tasks	146
Review All the Key Topics	146
Complete Tables and Lists from Memory	147
Define Key Terms	147
Complete Chapter 4 Hands-On Labs in Network+ Simulator Lite	147
Additional Resources	148
Review Questions	148
Chapter 5 IPv4 and IPv6 Addresses	153
Foundation Topics	154
Binary Numbering	154
Principles of Binary Numbering	154
Converting a Binary Number to a Decimal Number	155
Converting a Decimal Number to a Binary Number	155
Binary Numbering Practice	157
Binary Conversion Exercise 1	157
Binary Conversion Exercise 1: Solution	158
Binary Conversion Exercise 2	158
Binary Conversion Exercise 2: Solution	158
Binary Conversion Exercise 3	159
Binary Conversion Exercise 3: Solution	159
Binary Conversion Exercise 4	160
Binary Conversion Exercise 4: Solution	160
IPv4 Addressing	161
IPv4 Address Structure	161
Classes of Addresses	163
Types of Addresses	165
<i>Unicast</i>	165
<i>Broadcast</i>	165
<i>Multicast</i>	166

Assigning IPv4 Addresses	166
IP Addressing Components	167
Static Configuration	168
Dynamic Configuration	172
BOOTP	173
DHCP	173
Automatic Private IP Addressing	174
Subnetting	176
Purpose of Subnetting	176
Subnet Mask Notation	177
Subnet Notation: Practice Exercise 1	178
Subnet Notation: Practice Exercise 1 Solution	178
Subnet Notation: Practice Exercise 2	179
Subnet Notation: Practice Exercise 2 Solution	179
Extending a Classful Mask	179
Borrowed Bits	179
Calculating the Number of Created Subnets	180
Calculating the Number of Available Hosts	180
Basic Subnetting Practice: Exercise 1	181
Basic Subnetting Practice: Exercise 1 Solution	181
Basic Subnetting Practice: Exercise 2	182
Basic Subnetting Practice: Exercise 2 Solution	182
Calculating New IP Address Ranges	183
Advanced Subnetting Practice: Exercise 1	186
Advanced Subnetting Practice: Exercise 1 Solution	186
Advanced Subnetting Practice: Exercise 2	187
Advanced Subnetting Practice: Exercise 2 Solution	188
Additional Practice	189
Classless Interdomain Routing	190
IP Version 6	191
Need for IPv6	191
IPv6 Address Structure	192
IPv6 Address Types	193
IPv6 Data Flows	194

<i>Unicast</i>	194
<i>Multicast</i>	195
<i>Anycast</i>	195
Real-World Case Study	196
Summary	197
Exam Preparation Tasks	197
Review All the Key Topics	197
Complete Tables and Lists from Memory	198
Define Key Terms	199
Complete Chapter 5 Hands-On Labs in Network+ Simulator Lite	199
Additional Resources	199
Review Questions	200
Chapter 6 Routing IP Packets	205
Foundation Topics	206
Basic Routing Processes	206
Sources of Routing Information	209
Directly Connected Routes	209
Static Routes	210
Dynamic Routing Protocols	211
Routing Protocol Characteristics	213
Believability of a Route	214
Metrics	214
Interior Versus Exterior Gateway Protocols	215
Route Advertisement Method	215
Distance Vector	216
Link State	218
Routing Protocol Examples	218
Address Translation	220
NAT	220
PAT	222
Multicast Routing	224
IGMP	224
PIM	226

PIM-DM	227
PIM-SM	229
Real-World Case Study	230
Summary	231
Exam Preparation Tasks	232
Review All the Key Topics	232
Complete Tables and Lists from Memory	233
Define Key Terms	233
Complete Chapter 6 Hands-On Lab in Network+ Simulator Lite	233
Additional Resources	233
Review Questions	234
Chapter 7	
Wide Area Networks (WANs)	239
Foundation Topics	240
WAN Properties	240
WAN Connection Types	240
WAN Data Rates	242
WAN Media Types	243
Physical Media	243
Wireless Media	244
WAN Technologies	245
Dedicated Leased Line	246
T1	246
E1	247
T3	247
E3	247
CSU/DSU	248
Metro Ethernet	248
Point-to-Point Protocol	249
<i>Point-to-Point Protocol over Ethernet</i>	250
Microsoft RRAS	251
Digital Subscriber Line	252
Cable Modem	254
Synchronous Optical Network	255

Satellite	257
Plain Old Telephone Service	258
Integrated Services Digital Network	260
Frame Relay	262
SIP Trunk	264
Asynchronous Transfer Mode	264
Multiprotocol Label Switching	266
Overlay Networks	268
Real-World Case Study	268
Summary	269
Exam Preparation Tasks	270
Review All the Key Topics	270
Complete Tables and Lists from Memory	270
Define Key Terms	271
Complete Chapter 7 Hands-On Lab in Network+ Simulator Lite	271
Additional Resources	271
Review Questions	271
Chapter 8	Wireless Technologies
Foundation Topics	276
Introducing Wireless LANs	276
WLAN Concepts and Components	276
Wireless Routers	276
Wireless Access Point	277
Antennas	278
Frequencies and Channels	281
CSMA/CA	283
Transmission Methods	284
WLAN Standards	285
<i>802.11a</i>	285
<i>802.11b</i>	285
<i>802.11g</i>	285
<i>802.11n</i>	285
<i>802.11ac</i>	286
<i>802.11x Standard Summary</i>	286

Deploying Wireless LANs	287
Types of WLANs	287
IBSS	287
BSS	288
ESS	288
<i>Mesh Topology</i>	289
Sources of Interference	289
Wireless AP Placement	291
Securing Wireless LANs	292
Security Issues	292
Approaches to WLAN Security	294
Security Standards	295
WEP	296
WPA	296
WPA2	297
Additional Wireless Options	297
Real-World Case Study	298
Summary	298
Exam Preparation Tasks	299
Review All the Key Topics	299
Complete Tables and Lists from Memory	299
Define Key Terms	300
Complete Chapter 8 Hands-On Lab in Network+ Simulator Lite	300
Additional Resources	300
Review Questions	300
Chapter 9	Network Optimization 305
Foundation Topics	306
High Availability	306
High-Availability Measurement	306
Fault-Tolerant Network Design	307
Hardware Redundancy	308
Layer 3 Redundancy	309
Design Considerations for High-Availability Networks	310
High-Availability Best Practices	311

Content Caching	312
Load Balancing	312
Hardware Redundancy	313
QoS Technologies	313
Introduction to QoS	314
QoS Configuration Steps	315
QoS Components	316
QoS Mechanisms	317
<i>Classification</i>	318
<i>Marking</i>	318
<i>Congestion Management</i>	319
<i>Congestion Avoidance</i>	319
<i>Policing and Shaping</i>	320
<i>Link Efficiency</i>	322
Case Study: SOHO Network Design	323
Case Study Scenario	323
Suggested Solution	325
IP Addressing	325
Layer 1 Media	326
Layer 2 Devices	327
Layer 3 Devices	327
Wireless Design	328
Environmental Factors	329
Cost Savings Versus Performance	329
Topology	329
Real-World Case Study	330
Summary	331
Exam Preparation Tasks	331
Review All the Key Topics	331
Complete Tables and Lists from Memory	332
Define Key Terms	332
Complete Chapter 9 Hands-On Lab in Network+ Simulator Lite	332
Additional Resources	333
Review Questions	333

Chapter 10 Command-Line Tools 337

Foundation Topics 338

Windows Commands 338

arp 338

ipconfig 340

nbtstat 343

netstat 346

nslookup 348

ping 350

ping with IPv6 352

route 352

tracert 356

tracert with IPv6 358

PathPing 358

UNIX Commands 358

arp 360

dig and nslookup 362

host 363

ifconfig 363

iptables 364

nmap 365

tcpdump 365

traceroute 365

traceroute for IPv6 366

netstat 366

ping 368

Real-World Case Study 371

Summary 371

Exam Preparation Tasks 371

Review All the Key Topics 371

Complete Tables and Lists from Memory 372

Define Key Terms 373

Complete Chapter 10 Hands-On Lab in Network+ Simulator Lite 373

Additional Resources	373
Review Questions	374
Chapter 11 Network Management 379	
Foundation Topics	380
Maintenance Tools	380
Bit-Error Rate Tester	380
Butt Set	381
Cable Certifier	381
Cable Tester	382
Connectivity Software	382
Crimper	383
Electrostatic Discharge Wrist Strap	383
Environmental Monitor	384
Loopback Plug	385
Multimeter	385
Protocol Analyzer	386
Wi-Fi Analyzer	387
Looking-Glass Sites	387
Speed Test Sites	388
Punch-Down Tool	388
Throughput Tester	388
Time Domain Reflectometer and Optical Time Domain Reflectometer	389
Toner Probe	390
Spectrum Analyzer	390
Network Documentation	391
Monitoring Resources and Reports	392
SNMP	392
Syslog	395
Logs	398
Application Logs	398
Security Logs	399
System Logs	399
Remote Access Methods	400
Real-World Case Study	401

Summary	402
Exam Preparation Tasks	402
Review All the Key Topics	402
Complete Tables and Lists from Memory	403
Define Key Terms	403
Complete Chapter 11 Hands-On Lab in Network+ Simulator Lite	403
Additional Resources	404
Review Questions	404
Chapter 12 Network Security	409
Foundation Topics	410
Security Fundamentals	410
Network Security Goals	410
Confidentiality	410
<i>Symmetric Encryption</i>	411
<i>Asymmetric Encryption</i>	412
Integrity	414
Availability	415
Categories of Network Attacks	415
Confidentiality Attacks	415
Integrity Attacks	419
Availability Attacks	422
<i>Logic Bomb</i>	422
<i>Wireless Attacks</i>	422
<i>Denial of Service</i>	422
<i>Distributed Denial of Service</i>	423
<i>TCP SYN Flood</i>	423
<i>Buffer Overflow</i>	424
<i>ICMP Attacks</i>	424
<i>Electrical Disturbances</i>	425
<i>Attacks on a System's Physical Environment</i>	426
Defending Against Attacks	427
User Training	427
Patching	428
Security Policies	429

Governing Policy	430
Technical Policies	431
End-User Policies	431
More Detailed Documents	431
Incident Response	432
Vulnerability Scanners	433
Nessus	434
Nmap	434
Honey Pots and Honey Nets	435
Access Control Lists	436
Physical Security Devices	437
Network Device Hardening	438
Layer 2 Protections	439
Remote-Access Security	439
Firewalls	442
Firewall Types	442
Firewall Inspection Types	443
Packet-Filtering Firewall	443
Stateful Firewall	444
Firewall Zones	445
Unified Threat Management Firewalls	446
Virtual Private Networks	447
Overview of IPSec with IKEv1	449
IKE Modes and Phases	449
Authentication Header and Encapsulating Security Payload	451
The Five Steps in Setting Up and Tearing Down an IPSec Site-to-Site VPN Using IKEv1	452
Other VPN Technologies	454
Intrusion Detection and Prevention	454
IDS Versus IPS	455
IDS and IPS Device Categories	456
Detection Methods	456
Signature-Based Detection	456
Policy-Based Detection	457
Anomaly-Based Detection	457

Deploying Network-Based and Host-Based Solutions	458
Real-World Case Study	459
Summary	460
Exam Preparation Tasks	461
Review All the Key Topics	461
Complete Tables and Lists from Memory	462
Define Key Terms	462
Complete Chapter 12 Hands-On Lab in Network+ Simulator Lite	463
Additional Resources	463
Review Questions	463
Chapter 13 Network Policies and Best Practices	467
Foundation Topics	468
Policies	468
Password Policy	468
Data Loss Prevention	469
Remote-Access Policies	470
Incident Response Policies	470
Bring Your Own Device (BYOD)	471
Acceptable Use Policy (AUP)	471
Safety Procedures	472
Best Practices	472
Privileged User Agreement (PUA)	472
On-boarding/Off-boarding Procedures	473
Licensing Restrictions	473
International Export Controls	474
Non-Disclosure Agreement (NDA)	474
System Life Cycle	474
Real-World Case Study	475
Summary	475
Exam Preparation Tasks	476
Review All the Key Topics	476
Complete Tables and Lists from Memory	476
Define Key Terms	476

Complete Chapter 13 Hands-On Lab in Network+ Simulator Lite	477
Additional Resources	477
Review Questions	477
Chapter 14 Network Troubleshooting	481
Foundation Topics	482
Troubleshooting Basics	482
Troubleshooting Fundamentals	482
Structured Troubleshooting Methodology	484
Physical Layer Troubleshooting	487
Physical Layer Troubleshooting: Scenario	488
Physical Layer Troubleshooting: Solution	489
Data Link Layer Troubleshooting	490
Data Link Layer Troubleshooting: Scenario	491
Data Link Layer Troubleshooting: Solution	491
Network Layer Troubleshooting	492
Layer 3 Data Structures	492
Common Layer 3 Troubleshooting Issues	494
Network Layer Troubleshooting: Scenario	496
Network Layer Troubleshooting: Solution	496
Wireless Troubleshooting	497
Wireless Network Troubleshooting: Scenario	499
Wireless Network Troubleshooting: Solution	500
Specialized Networks	500
Real-World Case Study	501
Troubleshooting Scenarios	501
Summary	522
Exam Preparation Tasks	523
Review All the Key Topics	523
Complete Tables and Lists from Memory	523
Define Key Terms	524
Complete Chapter 14 Hands-On Lab in Network+ Simulator Lite	524
Additional Resources	524
Review Questions	524

Chapter 15 Final Preparation 529

Tools for Final Preparation	529
Video Training	530
Memory Tables	530
Simulations and Performance-Based Exercises	531
End-of-Chapter Review Tools	531
Suggested Plan for Final Review and Study	531
Strategies for Taking the Exam	533
Summary	535

Appendix A Answers to Review Questions 537

Appendix B CompTIA Network+ N10-007 Cert Guide Exam Updates 547

Always Get the Latest at the Book's Product Page	547
Technical Content	548

Glossary 551

Index 585

ONLINE ELEMENTS:

Appendix C Memory Tables

Appendix D Memory Tables Answer Key

Appendix E Study Planner

 Exam Essentials Interactive Study Guide

 Key Terms Flash Cards Application

 Instructional Videos

 Performance-Based Exercises

 CompTIA Network+ N10-007 Hands-on Lab Simulator Lite Software

About the Author

Anthony Sequeira began his IT career in 1994 with IBM in Tampa, Florida. He quickly formed his own computer consultancy, Computer Solutions, and then discovered his true passion—teaching and writing about networking technologies. Anthony has lectured to massive audiences around the world while working for Mastering Computers. Anthony has never been happier in his career than he is now as a trainer for CBT Nuggets. He is an avid tennis player, a private pilot, a semi-professional poker player, and loves anything at all to do with technology.

About the Technical Reviewers

Rob Fleming is a Cisco Certified Systems Instructor (CCSI #35229) and is a trainer for Boson, Nterone, and other learning partners. He has been an IT enthusiast since the mid-1980s, has more than 10 years of experience as a network administrator, and has a bachelor's degree in Management Information Systems. Rob has worked for all sizes of companies, from small IT startups to Fortune 100 companies. He has written lab guides and built environments for several networking courses, but his true passion is in instruction, where he enjoys transferring knowledge to students. When not training or studying for new certifications in security and wireless, Rob can be found attending IT meet-ups and conferences, programming on Raspberry Pis, or nerding out with fellow IT enthusiasts on a variety of new technologies.

Dedication

This book is dedicated to the amazing Keith Barker. Keith is a true inspiration and an incredible friend.

Acknowledgments

It is rare for it to go well when you work with your friends, especially in what could be a stressful environment of constant deadlines. Fortunately, I work with my friends Brett and Marianne Bartow. Thank you so much for your friendship—and PATIENCE!

Thanks also to my dear friend Kevin Wallace. He is a wonderful friend, and crazy talented.

Check out all of his great training products at <https://kwallaceccie.mykajabi.com>.

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in Cisco's Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets [] indicate optional elements.
- Braces { } indicate a required choice.
- Braces within brackets [{ }] indicate a required choice within an optional element.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Register your copy of *CompTIA Network+ N10-007 Cert Guide* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780789759818 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

The CompTIA Network+ certification is a popular certification for those entering the computer networking field. Although many vendor-specific networking certifications are popular in the industry, the CompTIA Network+ certification is unique in that it is vendor neutral. The CompTIA Network+ certification often acts as a stepping-stone to more specialized and vendor-specific certifications, such as those offered by Cisco Systems.

In CompTIA Network+, the topics are mostly generic in that they can apply to networking equipment regardless of vendor. Although the CompTIA Network+ is vendor neutral, network software and systems are implemented by multiple independent vendors. In that light, several of the exercises, examples, and simulations in this book include using a vendor's configuration and technology, such as Microsoft Windows operating systems or Cisco Systems routers and switches. More detailed training for a specific vendor's software and hardware can be found in books and training specific to that vendor.

Who Should Read This Book?

This book was written with two audiences in mind—those who want to learn all they can about networking technology, and those who want to pass the CompTIA Network+ exam. I think that both groups are going to be very impressed with the breadth of technologies this book details. Although it would be impossible to cover every topic found in networking today, this book manages to cover all the massive areas that make networking the exciting field so many want to learn.

Readers will range from people who are attempting to attain a position in the IT field to people who want to keep their skills sharp or perhaps retain their job because of a company policy that mandates they take the new exams. This book is also for the reader who wants to acquire additional certifications beyond the Network+ certification (for example, the Cisco Certified Network Associate [CCNA] certification and beyond). The book is designed in such a way to offer easy transition to future certification studies.

Resources

This book comes with a wealth of digital resources to help you review, practice, and assess your knowledge. The end of each chapter contains a review section that references several of these tools, and you should be sure to use them as you complete each chapter to help reinforce the knowledge you are learning. You can use them again after you finish the book to help you review and make sure you are fully prepared for the exam.

Here's a list of resources available on the companion website:

- Interactive glossary flash card application
- Interactive exam essentials appendix
- Performance-based exercises
- CompTIA Network+ Hands-on Lab Simulator Lite Software for exam N10-007
- The Pearson Test Prep practice test software
- Video training on key exam topics
- Memory Table review exercises and answer keys
- A study planner tool
- Instructions to redeem your Network+ certification exam voucher, providing a 10% discount on the exam

To access the companion website, follow these steps:

- Step 1.** Go to <http://www.pearsonitcertification.com/register>.
- Step 2.** Either log in to your account (if you have an existing account already) or create a new account.
- Step 3.** Enter the ISBN of your book (9780789759818) and click Submit.
- Step 4.** Answer the challenge questions to validate your purchase.
- Step 5.** In your account page, click the **Registered Products** tab and then click the **Access Bonus Content** link.

Pearson Test Prep Practice Test Software

The companion website that accompanies this book includes the Pearson Test Prep practice test engine (software that displays and grades a set of exam-realistic practice test questions). Using the Pearson Test Prep practice test engine, you can either

study by going through the questions in study mode or take a simulated CompTIA Network+ exam that mimics real exam conditions. The software also has a flash card mode that allows you to challenge yourself to answer the questions without seeing the multiple-choice answers.

The Pearson Test Prep software is available both online and as a Windows desktop application that you can run offline. The online version can be accessed at www.pearsontestprep.com. This version can be used on any device that has an Internet connection, including desktop computers, laptop computers, tablets, and smartphones. It is optimized for viewing on screens as small as a standard iPhone screen. The desktop application can be downloaded and installed from the companion website.

NOTE The desktop application is a Windows-based application, so it is only designed to run on Windows. Although it can be run on other operating systems using a Windows emulator, other operating systems are not officially supported on the desktop version. If you are using an OS other than Windows, you may want to consider using the online version instead.

Accessing the test engine is a two-step process. The first step is to either install the software on your desktop or access the online version website. However, the practice exam (that is, the database of CompTIA Network+ exam questions) is not available to you until you register the unique access code that accompanies your book.

NOTE The cardboard sleeve in the back of the physical book includes a piece of paper. The paper lists the *access code* for the practice exam associated with this book. Make sure you keep the access code even after you have registered your exam, as you may need to refer to it later. Also, on the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the *CompTIA Network+ Cert Guide, Premium Edition eBook and Practice Test* product, a \$40 value!

Installing the Pearson Test Prep Software

If you choose to use the Windows desktop version of the practice test software, you will need to download the installers from the companion website.

The software-installation process is similar to other wizard-based installation processes. If you have already installed the Pearson Test Prep practice test software from another Pearson product, you do not need to reinstall the software. Just launch

the software on your desktop and proceed to activate the practice exam from this book by using the activation code included in sleeve in the back of the book. The following steps outline the installation process:

- Step 1.** Download the software to your computer from the companion website.
- Step 2.** Extract all files from the .zip file you downloaded.
- Step 3.** Launch the installer from the extracted files folder.
- Step 4.** Respond to the wizard-based prompts.

The installation process gives you the option to activate your exam with the activation code supplied on the paper in the back of book sleeve. This process requires that you establish a Pearson website login. You need this login to activate the exam, so please register when prompted. If you already have a Pearson website login, you do not need to register again; just use your existing login.

Activating and Downloading the Practice Exam

The second step to accessing your practice exam product is to activate the product using the unique access code found in the back of book sleeve. You must follow this step regardless of which version of the product you are using—the online version or the Windows desktop version. The following steps walk you through how to activate your exam on each platform.

Windows Desktop Version:

1. Start the Pearson Test Prep Practice Test software from the Windows Start menu or from your desktop shortcut icon.
2. To activate and download the exam associated with this book, from the My Products or Tools tab, click the **Activate** button.
3. At the next screen, enter the *access code* from the paper inside the cardboard sleeve in the back of the book. Once this is entered, click the **Activate** button.
4. The activation process will download the practice exam. Click **Next** and then click **Finish**.

Online Version:

1. From a device with an active Internet connection, open your browser of choice and go to the website www.pearsontestprep.com.
2. Select Pearson IT Certification under product group.

3. Enter the email address and password associated with your account and click **Login**.
4. In the middle of the screen, click the **Activate New Product** button.
5. Enter the access code from the paper inside the cardboard sleeve in the back of the book and click the **Activate** button.

After the activation process is complete, the My Products tab should list your new exam. If you do not see the exam, make sure that you selected the My Products tab on the menu. At this point, the software and practice exam are ready to use. Simply select the exam and click the **Exams** button.

To update an exam that you have already activated and downloaded, simply select the **Tools** tab and click the **Update Products** button. Updating your exams ensures that you have the latest changes and updates to the exam data.

If you want to check for updates to the Pearson Cert Practice Test exam engine software, simply select the **Tools** tab and click the **Update Application** button. This ensures that you are running the latest version of the exam engine.

NOTE The online version always contains the latest updates to the exam questions, so there is never a need to update when you're using that version.

Activating Other Exams

The exam-software installation process and the registration process both only occur once. Then, for each new exam, only a few steps are required. For example, if you buy another new Pearson IT Certification Cert Guide, extract the activation code from the sleeve in the back of that book. From there, all you have to do is start the exam engine (if it's not still up and running) and perform the activation steps from the previous list.

Premium Edition

In addition to the free practice exam provided with the book, you can purchase additional exams with expanded functionality directly from Pearson IT Certification. The Premium Edition eBook and Practice Test for this title contains an additional two full practice exams and an eBook (in PDF, EPUB, and Kindle formats). Also, the Premium Edition title has remediation for each question that links to the specific part of the eBook that relates to that question.

For those who purchased the print version of this title, you can purchase the Premium Edition at a deep discount. You'll find a coupon code in the back of book sleeve that contains a one-time-use code and instructions for where you can purchase the Premium Edition.

To view the Premium Edition product page, go to the following website: <http://www.pearsonitcertification.com/title/9780134861012>.

Goals and Methods

The goal of this book is to assist you in learning and understanding the technologies covered in the Network+ N10-007 blueprint from CompTIA. This also allows you to demonstrate that knowledge by passing the N10-007 version of the CompTIA Network+ exam.

To aid you in mastering and understanding the Network+ certification objectives, this book uses the following methods:

- **Opening topics list:** This defines the topics that are covered in the chapter.
- **Foundation topics:** At the heart of a chapter, this section explains the topics from a hands-on and a theory-based standpoint. This includes in-depth descriptions, tables, and figures that build your knowledge so that you can pass the N10-007 exam. The chapters are each broken into multiple sections.
- **Key topics:** This section indicates important figures, tables, and lists of information that you need to know for the exam. They are sprinkled throughout each chapter and are summarized in table format at the end of each chapter.
- **Memory tables:** You can find these on the book's companion website within Appendixes C and D. Use them to help you memorize important information.
- **Key terms:** Key terms without definitions are listed at the end of each chapter. Write down the definition of each term, and check your work against the complete key terms in the Glossary. On the companion website, you will find a flash card application with all the glossary terms separated by chapter, so feel free to use that to study key terms as well.
- **Exercises:** This book comes with 40 performance-based practice exercises that are designed to help you prepare for the hands-on portion of the Network+ exam. These exercises are available on the companion website. Make sure you do the exercises as you complete each chapter and again when you have completed the book and are doing your final preparation.

- **Hands-on Labs:** These include matching, drag and drop, and simulations. These hands-on exercises are an important part of this book. In addition to reading this book, you should go through all the exercises included with the book. These interactive hands-on exercises provide examples, additional information, and insight about a vendor’s implementation of the technologies. To perform the labs, simply install the CompTIA Network+ N10-007 Hands-on Lab Simulator Lite software. This software is a Windows and Mac desktop application. You should be sure to install the software prior to reading the book, as each chapter will indicate what labs you should perform. To install the software, follow these steps:
 - Step 1.** Go to the companion website for the book (see the “Resources” section for how to access the companion website).
 - Step 2.** Click the link to download the CompTIA Network+ N10-007 Hands-on Lab Simulator Lite software.
 - Step 3.** Once you have downloaded the software to your computer, extract all the files from the .zip file.
 - Step 4.** Launch the installer from the extracted files.
 - Step 5.** Respond to the wizard-based prompts.
- **Practice Exams:** This book comes complete with several full-length practice exams available to you in the Pearson Test Prep practice test software, which you can download and install from the companion website. The Pearson Test Prep software is also available to you online at www.PearsonTestPrep.com. You can access both the online and desktop versions using the access code printed on the card in the sleeve in the back of this book. Be sure to run through the questions in Exam Bank 1 as you complete each chapter in study mode. When you have completed the book, take a full practice test using Exam Bank 2 questions in practice exam mode to test your exam readiness.
- **Exam Essentials:** This book includes an Exam Essentials appendix that summarizes the key points from every chapter. This review tool is available in print and as an interactive PDF on the companion website. Review these essential exam facts after each chapter and again when you have completed the book. This makes a great review summary that you can mark up as you review and master each concept.

For current information about the CompTIA Network+ certification exam, visit <https://certification.comptia.org/certifications/network>.

Strategies for Exam Preparation

This book comes with a study planner tool on the companion website. This spreadsheet helps you keep track of the activities you need to perform in each chapter and helps you organize your exam preparation tasks. As you read the chapters in this book, jot down notes with key concepts or configurations in the study planner. Each chapter ends with a summary and series of exam preparation tasks to help you reinforce what you learned. These tasks include review exercises such as reviewing key topics, completing memory tables, defining key terms, answering review questions, performing hands-on labs and exercises, and so on. Make sure you perform these tasks as you complete each chapter to improve your retention of the material and record your progress in the study planner.

The book concludes with a “Final Preparation” chapter that offers you guidance on your final exam preparation and provides you with some helpful exam advice. Make sure you read over that chapter to help you assess your exam readiness and identify areas where you need to focus your review.

Make sure you complete all the performance-based question exercises and hands-on labs associated with this book. The exercises and labs are organized by chapter, making it easy to perform them after you complete each section. These exercises will reinforce what you have learned, offer examples of some popular vendors’ methods for implementing networking technologies, and provide additional information to assist you in building real-world skills and preparing you for the certification exam.

Download the current exam objectives by submitting a form on the following web page: <http://certification.comptia.org/training/testingcenters/examobjectives.aspx>.

Use the practice exam, which is included on this book’s companion website. As you work through the practice exam, use the practice test software reporting features to note the areas where you lack confidence and then review those concepts. After you review these areas, work through the practice exam a second time and rate your skills. Keep in mind that the more you work through the practice exam, the more familiar the questions become, and the practice exam becomes a less-accurate judge of your skills.

After you work through the practice exam a second time and feel confident with your skills, schedule the real CompTIA Network+ exam (N10-007).

CompTIA Network+ Exam Topics

Table I-1 lists general exam topics (*objectives*) and specific topics under each general topic (*subobjectives*) for the CompTIA Network+ N10-007 exam. This table lists the primary chapter in which each exam topic is covered. Note that many objectives

and subobjectives are interrelated and are addressed in multiple chapters within the book itself.

Table I-1 CompTIA Network+ Exam Topics

Chapter	N10-007 Exam Objective	N10-007 Exam Subobjective
1 Computer Network Fundamentals	1.0 Networking Concepts	1.5 Compare and contrast the characteristics of network topologies, types, and technologies
2 The OSI Reference Model	1.0 Networking Concepts	1.1 Explain the purposes and uses of ports and protocols 1.2 Explain devices, applications, protocols, and services at their appropriate OSI layers
3 Network Components	1.0 Networking Concepts 2.0 Infrastructure	1.7 Summarize cloud concepts and their purposes 1.8 Explain the functions of network services 2.1 Given a scenario, deploy the appropriate cabling solution 2.2 Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them 2.3 Explain the purposes and use cases for advanced networking devices 2.4 Explain the purposes of virtualization and network storage technologies
4 Ethernet Technology	1.0 Networking Concepts	1.3 Explain the concepts and characteristics of routing and switching
5 IPv4 and IPv6 Addresses	1.0 Networking Concepts	1.4 Given a scenario, configure the appropriate IP addressing components
6 Routing IP Packets	1.0 Networking Concepts	1.3 Explain the concepts and characteristics of routing and switching
7 Wide Area Networks (WANs)	2.0 Infrastructure	2.5 Compare and contrast WAN technologies

Chapter	N10-007 Exam Objective	N10-007 Exam Subobjective
8 Wireless Technologies	1.0 Networking Concepts	1.6 Given a scenario, implement the appropriate wireless technologies and configurations
	4.0 Network Security	4.3 Given a scenario, secure a basic wireless network
9 Network Optimization	3.0 Network Operations	3.2 Compare and contrast business continuity and disaster recovery concepts
10 Command-Line Tools	5.0 Network Troubleshooting	5.2 Given a scenario, use the appropriate tool
11 Network Management	3.0 Network Operations	3.1 Given a scenario, use appropriate documentation and diagrams to manage the network
		3.3 Explain common scanning, monitoring, and patching processes and summarize their expected outputs
		3.4 Given a scenario, use remote access methods
	4.0 Network Security	4.1 Summarize the purposes of physical security devices
12 Network Security		4.2 Explain authentication and access controls
		4.4 Summarize common networking attacks
		4.5 Given a scenario, implement network device hardening
		4.6 Explain common mitigation techniques and their purposes
	3.0 Network Operations	3.5 Identify policies and best practices
13 Network Policies and Best Practices	5.0 Network Troubleshooting and Tools	5.1 Explain the network troubleshooting methodology
		5.3 Given a scenario, troubleshoot common wired connectivity and performance issues
		5.4 Given a scenario, troubleshoot common wireless connectivity and performance issues
		5.5 Given a scenario, troubleshoot common network service issues

How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with. However, if you do intend to read all the chapters, the order in the book is an excellent sequence to use:

- **Chapter 1: Computer Network Fundamentals**—This chapter covers what a network does, what components tend to make up a network, and how we like to define different networks.
- **Chapter 2: The OSI Reference Model**—The OSI model is an extremely powerful guide we can use as we design, implement, and troubleshoot networks.
- **Chapter 3: Network Components**—This chapter drills deep into the different devices we find in the network today as well as the media that connect these devices.
- **Chapter 4: Ethernet Technology**—Speaking of media in the network, this chapter expands on one of the most popular categories of network media—Ethernet.
- **Chapter 5: IPv4 and IPv6 Addresses**—Addressing of systems is critical in networks, and this chapter covers the addressing used in IPv4 and IPv6.
- **Chapter 6: Routing IP Packets**—Moving packets from one network to another is the job of the router. This chapter ensures you are well versed in the many technologies that operate in this category.
- **Chapter 7: Wide Area Networks (WANs)**—Moving packets across large geographic distances is the job of the WAN, and this chapter breaks down the technologies found in this area.
- **Chapter 8: Wireless Technologies**—Wires, who needs wires? Wireless networking is here to stay. This chapter provides you with the details and even includes such important topics as security and emerging technologies.
- **Chapter 9: Network Optimization**—Making the network more reliable is the focus of this chapter.
- **Chapter 10: Command-Line Tools**—Fortunately, a tremendous number of valuable tools can assist you in network troubleshooting. Some of these tools are not graphical in nature and you use them at a command line.
- **Chapter 11: Network Management**—This chapter covers network management in general and includes a look at more valuable tools.

- **Chapter 12: Network Security**—Now more than ever, our networks are under attack. This chapter prepares you for the many challenges ahead in this area.
- **Chapter 13: Network Policies and Best Practices**—Many excellent policies and plenty of best practices can assist you in your networking career. This chapter covers some of the most important ones.
- **Chapter 14: Network Troubleshooting**—Whereas other chapters just touch on network troubleshooting, this chapter makes it the focus. Here, you get a nice overall methodology you can use, as well as specifics on tools and techniques.
- **Chapter 15: Final Preparation**—This chapter provides guidance on how to make sure you are as prepared as possible for the big exam (should you choose to take it on).

The OSI Reference Model

Way back in 1977, the International Organization for Standardization (ISO) developed a subcommittee to focus on the interoperability of multivendor communications systems. This is fancy language for getting network “thingies” to communicate with each other, even if different companies made those network “thingies.” What sprang from this subcommittee was the Open Systems Interconnection (OSI) reference model (referred to as the *OSI model* or the *OSI stack*). With this model, you can talk about any networking technology and categorize that technology as residing at one or more of the seven layers of the model.

This chapter defines those seven layers and offers examples of what you might find at each layer. It also contrasts the OSI model with another model—the TCP/IP stack, also known as the Department of Defense (DoD) model—that focuses on Internet Protocol (IP) communications.

Foundation Topics

The Purpose of Reference Models

Throughout this book, various protocols and devices that play a role in your network (and your networking career) are introduced. To better understand how a technology fits in, it helps to have a common point of reference against which various technologies from different vendors can be compared. Understanding the OSI model is useful in troubleshooting networks.

One of the most common ways of categorizing the function of a network technology is to say at what layer (or layers) of the OSI model that technology runs. Based on how that technology performs a certain function at a certain layer of the OSI model allows you to better decide whether one device is going to be able to communicate with another device, which might or might not be using a similar technology at that layer of the OSI reference model.

For example, when your laptop connects to a web server on the Internet, your service provider assigns your laptop an IP address. Similarly, the web server to which you are communicating has an IP address. As you see in this chapter, an IP address lives at Layer 3 (the network layer) of the OSI model. Because both your laptop and the web server use a common protocol (that is, IP) at Layer 3, they are capable of communicating with one another.

Personally, I have been in the computer-networking industry since 1989, and I have had the OSI model explained in many classes I have attended and books I have read. From this, I have taken away a collection of metaphors to help describe the operation of the different layers of the OSI model. Some of the metaphors involve sending a letter from one location to another or placing a message in a series of envelopes. However, my favorite (and a more correct) way to describe the OSI model is to simply think of it as being analogous to a bookshelf, such as the one shown in Figure 2-1.



Figure 2-1 A Bookshelf Is Analogous to the OSI Model

If you were to look at a bookshelf in my home, you would see that I organized diverse types of books on different shelves. One shelf has my collection of *Star Wars* books, another shelf holds the books I wrote for Pearson, another shelf holds my old-school audio books, and so on. I grouped similar books together on a shelf, just as the OSI model groups similar protocols and functions together in a layer.

A common pitfall my readers meet when studying the OSI model is to try to neatly fit all the devices and protocols in their network into one of the OSI model's seven layers. However, not every technology is a perfect fit into these layers. In fact, some networks might not have any technologies running at one or more of these layers. This reminds me of my favorite statement about the OSI model. It comes from Rich Seifert's book *The Switch Book*. In that book, Rich reminds us that the OSI model is a *reference* model, not a *reverence* model. That is, no cosmic law states that all technologies must cleanly plug into the model. So, as you discover the characteristics of the OSI model layers throughout this chapter, remember that these layers are like shelves for organizing similar protocols and functions, not immutable laws.

The OSI Model

As previously described, the OSI model consists of seven layers:

- **Layer 1:** The physical layer
- **Layer 2:** The data link layer
- **Layer 3:** The network layer
- **Layer 4:** The transport layer

Key Topic

- **Layer 5:** The session layer
- **Layer 6:** The presentation layer
- **Layer 7:** The application layer

Graphically, we depict these layers with Layer 1 at the bottom of the stack, as shown in Figure 2-2.

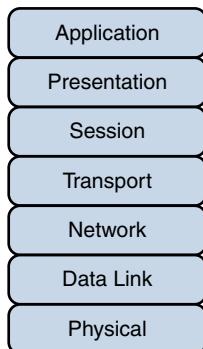


Figure 2-2 OSI “Stack”

Various mnemonics are available to help memorize these layers in their proper order. A top-down (that is, starting at the top of the stack with Layer 7 and working your way down to Layer 1) acrostic is *All People Seem To Need Data Processing*. As a couple of examples, using this acrostic, the *A* in *All* reminds us of the *A* in *Application*, and the *P* in *People* reminds us of the *P* in *Presentation*. Another common memory aid is *Please Do Not Throw Sausage Pizza Away*, which begins at Layer 1 and works its way up to Layer 7.

At the physical layer, binary expressions (that is, a series of 1s and 0s) represent data. A binary expression is created using bits, where a bit is a single 1 or a single 0. At upper layers, however, bits are grouped together, into what is known as a *protocol data unit* (PDU) or a *data service unit*.

Engineers tend to use the term *packet* generically to refer to these PDUs. However, PDUs might have an added name, depending on their OSI layer. Figure 2-3 illustrates these PDU names. A common memory aid for these PDUs is *Some People Fear Birthdays*, where the *S* in *Some* reminds us of the *S* in *Segments*. The *P* in *People* reminds us of the *P* in *Packets*, and the *F* in *Fear* reflects the *F* in *Frames*. Finally, the *B* in *Birthdays* reminds us of the *B* in *Bits*.

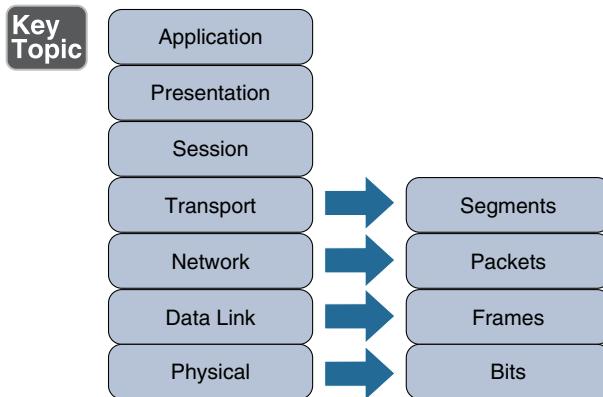


Figure 2-3 PDU Names

Layer 1: The Physical Layer

The concern of the physical layer, as shown in Figure 2-4, is the transmission of bits on the network along with the physical and electrical characteristics of the network.

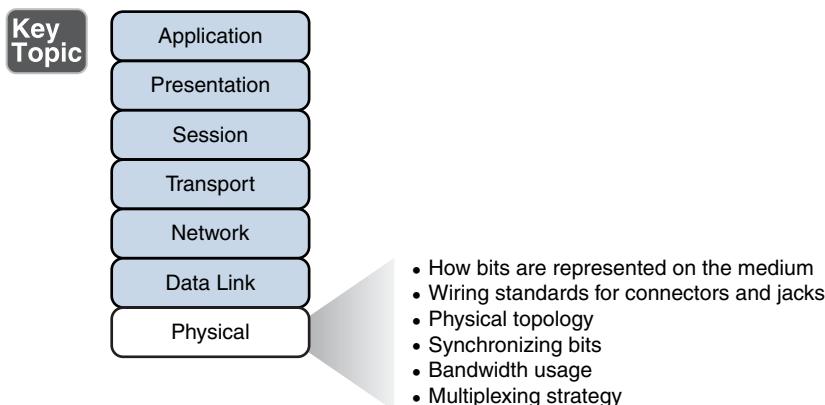


Figure 2-4 Layer 1: The Physical Layer

The physical layer defines the following:

- **How to represent bits on the medium:** Data on a computer network is represented as a binary expression. Chapter 5, “IPv4 and IPv6 Addresses,” discusses binary in much more detail. Electrical voltage (on copper wiring) or light (carried via fiber-optic cabling) can represent these 1s and 0s.

For example, the presence or the absence of voltage on a wire portrays a binary 1 or a binary 0, respectively, as illustrated in Figure 2-5. Similarly, the presence or absence of light on a fiber-optic cable renders a 1 or 0 in binary. This type of approach is called *current state modulation*.

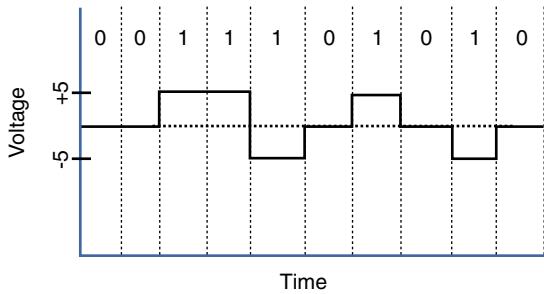


Figure 2-5 Current State Modulation

An alternate approach to portraying binary data is *state transition modulation*, as shown in Figure 2-6, where the transition between voltages or the presence of light shows a binary value.

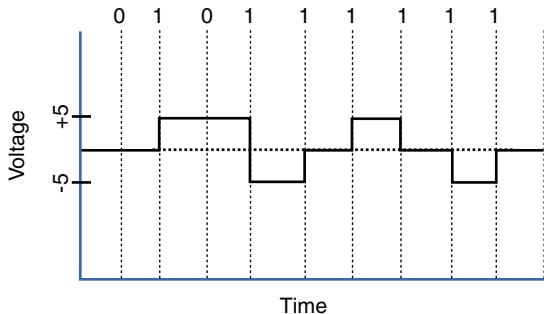


Figure 2-6 Transition Modulation

NOTE Other modulation types you might be familiar with from radio include amplitude modulation (AM) and frequency modulation (FM). AM uses a variation in a waveform's amplitude (that is, signal strength) to portray the original signal. However, FM uses a variation in frequency to stand for the original signal.

- **Wiring standards for connectors and jacks:** Chapter 3, “Network Components,” describes several standards for network connectors. For example, the TIA/EIA-568-B standard describes how to wire an RJ-45 connector for use on a 100BASE-TX Ethernet network, as shown in Figure 2-7.

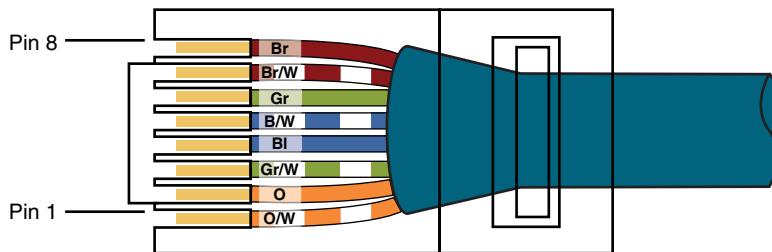


Figure 2-7 TIA/EIA-568-B Wiring Standard for an RJ-45 Connector

- **Physical topology:** Layer 1 devices view a network as a physical topology (as opposed to a logical topology). Examples of a physical topology include bus, ring, and star topologies, as described in Chapter 1, “Computer Network Fundamentals.”
- **Synchronizing bits:** For two networked devices to successfully communicate at the physical layer, they must agree on when one bit stops and another bit starts. Specifically, the devices need a method to synchronize the bits. Two basic approaches to bit synchronization include *asynchronous* and *synchronous* synchronization:
 - **Asynchronous:** With this approach, a sender states that it is about to start transmitting by sending a start bit to the receiver. When the receiver sees this, it starts its own internal clock to measure the next bits. After the sender transmits its data, it sends a stop bit to say that it has finished its transmission.
 - **Synchronous:** This approach synchronizes the internal clocks of both the sender and the receiver to ensure that they agree on when bits begin and end. A common approach to make this synchronization happen is to use an external clock (for example, a clock given by a service provider). The sender and receiver then reference this external clock.
- **Bandwidth usage:** The two fundamental approaches to bandwidth usage on a network are *broadband* and *baseband*:
 - **Broadband:** Broadband technologies divide the bandwidth available on a medium (for example, copper or fiber-optic cabling) into different channels. A sender can then transmit different communication streams over the various channels. For example, consider frequency-division multiplexing (FDM) used by a cable modem. Specifically, a cable modem uses certain ranges of frequencies on the cable coming into your home from the local cable company to carry incoming data, another range of frequencies for outgoing data, and several other frequency ranges for various TV stations.

- **Baseband:** Baseband technologies, in contrast, use all the available frequencies on a medium to send data. Ethernet is an example of a networking technology that uses baseband.
- **Multiplexing strategy:** Multiplexing allows multiple communications sessions to share the same physical medium. Cable TV, as previously mentioned, allows you to receive multiple channels over a single physical medium (for example, a coaxial cable plugged into the back of your television). Here are some of the more common approaches to multiplexing:
 - **Time-division multiplexing (TDM):** TDM supports different communication sessions (for example, different telephone conversations in a telephony network) on the same physical medium by causing the sessions to take turns. For a brief period, defined as a *time slot*, data from the first session is sent, followed by data from the second session. This continues until all sessions have had a turn, and the process repeats itself.
 - **Statistical time-division multiplexing (StatTDM):** A downside to TDM is that each communication session receives its own time slot, even if one of the sessions does not have any data to send at the moment. To make a more efficient use of available bandwidth, StatTDM dynamically assigns time slots to communications sessions on an as-needed basis.
 - **Frequency-division multiplexing (FDM):** FDM divides a medium's frequency range into channels, and different communication sessions send their data over different channels. As previously described, this approach to bandwidth usage is called *broadband*.

Examples of devices defined by physical layer standards include hubs, wireless access points, and network cabling.

NOTE A hub interconnects PCs in a LAN. However, it is considered a physical layer device because a hub takes bits coming in on one port and retransmits those bits out all other ports. At no point does the hub interrogate any addressing information in the data.

Layer 2: The Data Link Layer

The data link layer is concerned with the following:

- Packaging data into frames and transmitting those frames on the network
- Performing error detection/correction
- Uniquely finding network devices with an address
- Handling flow control

These processes are referred to collectively as *data link control* (DLC) and are illustrated in Figure 2-8.

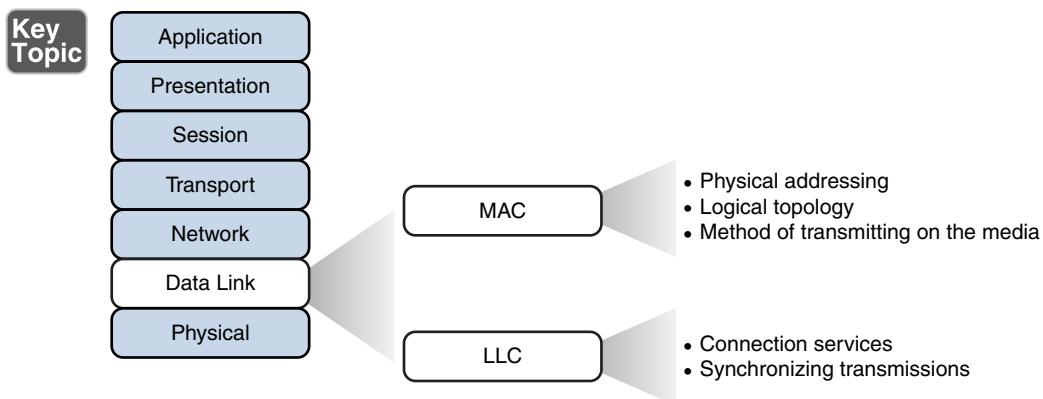


Figure 2-8 Layer 2: The Data Link Layer

In fact, the data link layer is unique from the other layers in that it has two sublayers of its own: MAC and LLC.

Media Access Control

Characteristics of the Media Access Control (MAC) sublayer include the following:

- **Physical addressing:** A common example of a Layer 2 address is a MAC address, which is a 48-bit address assigned to a device's network interface card (NIC). MAC addresses are written in hexadecimal notation (for example, 58:55:ca:eb:27:83). The first 24 bits of the 48-bit address is the *vendor code*. The IEEE Registration Authority assigns a manufacturer one or more unique vendor codes. You can use the list of vendor codes at <http://standards.ieee.org/develop/regauth/oui/oui.txt> to identify the manufacturer of a networking device, based on the first half of the device's MAC address. The last 24 bits of a MAC address are assigned by the manufacturer, and they act as a serial number for the device. No two MAC addresses in the world should have the same value.
- **Logical topology:** Layer 2 devices view a network as a logical topology. Examples of a logical topology include bus and ring topologies, as described in Chapter 1.
- **Method of transmitting on the media:** With several devices connected to a network, there needs to be some strategy for deciding when a device sends on the media. Otherwise, multiple devices might send at the same time and thus interfere with one another's transmissions.

Logical Link Control

Characteristics of the Logical Link Control (LLC) sublayer include the following:

- **Connection services:** When a device on a network receives a message from another device on the network, that recipient device can give feedback to the sender in the form of an acknowledgment message. The two main functions provided by these acknowledgment messages are as follows:
 - **Flow control:** Limits the amount of data a sender can send at one time; this prevents the sender from overwhelming the receiver with too much information.
 - **Error control:** Allows the recipient of data to let the sender know whether the expected data frame was not received or whether it was received but is corrupted. The recipient figures out whether the data frame is corrupt by mathematically calculating a checksum of the data received. If the calculated checksum does not match the checksum received with the data frame, the recipient of the data draws the conclusion that the data frame is corrupted and can then notify the sender via an acknowledgment message.
- **Synchronizing transmissions:** Senders and receivers of data frames need to coordinate when a data frame is being transmitted and should be received. The three methods of performing this synchronization are detailed here:
 - **Isochronous:** With isochronous transmission, network devices look to a common device in the network as a clock source, which creates fixed-length time slots. Network devices can determine how much free space, if any, is available within a time slot and then insert data into an available time slot. A time slot can accommodate more than one data frame. Isochronous transmission does not need to provide clocking at the beginning of a data string (as does synchronous transmission) or for every data frame (as does asynchronous transmission). As a result, isochronous transmission uses little overhead when compared to asynchronous or synchronous transmission methods.
 - **Asynchronous:** With asynchronous transmission, network devices reference their own internal clocks, and network devices do not need to synchronize their clocks. Instead, the sender places a start bit at the beginning of each data frame and a stop bit at the end of each data frame. These start and stop bits tell the receiver when to monitor the medium for the presence of bits.

An additional bit, called the *parity bit*, might also be added to the end of each byte in a frame to detect an error in the frame. For example, if even parity error detection (as opposed to odd parity error detection) is used, the parity bit (with a value of either 0 or 1) would be added to the end of a byte, causing the total number of 1s in the data frame to be an even number. If the receiver of a byte is configured for even parity error detection and receives a byte where the total number of bits (including the parity bit) is even, the receiver can conclude that the byte was not corrupted during transmission.

NOTE Using a parity bit to detect errors might not be effective if a byte has more than one error (that is, more than one bit that has been changed from its original value).

- **Synchronous:** With synchronous transmission, two network devices that want to communicate between themselves must agree on a clocking method to show the beginning and ending of data frames. One approach to providing this clocking is to use a separate communications channel over which a clock signal is sent. Another approach relies on specific bit combinations or control characters to indicate the beginning of a frame or a byte of data.

Like asynchronous transmissions, synchronous transmissions can perform error detection. However, rather than using parity bits, synchronous communication runs a mathematical algorithm on the data to create a cyclic redundancy check (CRC). If both the sender and the receiver calculate the same CRC value for the same chunk of data, the receiver can conclude that the data was not corrupted during transmission.

Examples of devices defined by data link layer standards include switches, bridges, and NICs.

NOTE NICs are not entirely defined at the data link layer because they are partially based on physical layer standards, such as a NIC's network connector.

Layer 3: The Network Layer

The network layer, as shown in Figure 2-9, is primarily concerned with forwarding data based on logical addresses.

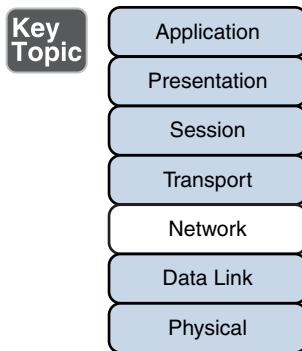


Figure 2-9 Layer 3: The Network Layer

Although many network administrators think of routing and IP addressing when they hear about the network layer, this layer is actually responsible for a variety of tasks:

- **Logical addressing:** Whereas the data link layer uses physical addresses to make forwarding decisions, the network layer uses logical addressing to make forwarding decisions. A variety of routed protocols (for example, AppleTalk and IPX) have their own logical addressing schemes, but by far, the most widely deployed routed protocol is Internet Protocol (IP). Chapter 5 discusses IP addressing in detail.
- **Switching:** Engineers often associate the term *switching* with Layer 2 technologies; however, the concept of switching also exists at Layer 3. Switching, at its essence, is making decisions about how data should be forwarded. At Layer 3, three common switching techniques exist:
 - **Packet switching:** With packet switching, a data stream is divided into packets. Each packet has a Layer 3 header that includes a source and destination Layer 3 address. Another term for packet switching is *routing*, which is discussed in more detail in Chapter 6, “Routing IP Packets.”
 - **Circuit switching:** Circuit switching dynamically brings up a dedicated communication link between two parties for those parties to communicate.

As a simple example of circuit switching, think of making a phone call from your home to a business. Assuming you have a traditional landline servicing your phone, the telephone company’s switching equipment interconnects your home phone with the phone system of the business you are calling. This interconnection (that is, *circuit*) only exists for the duration of the phone call.

- **Message switching:** Unlike packet switching and circuit switching technologies, message switching is usually not well suited for real-time applications because of the delay involved. Specifically, with message switching, a data stream is divided into messages. Each message is tagged with a destination address, and the messages travel from one network device to another network device on the way to their destination. Because these devices might briefly store the messages before forwarding them, a network using message switching is sometimes called a *store-and-forward* network. Metaphorically, you could visualize message switching like routing an email message, where the email message might be briefly stored on an email server before being forwarded to the recipient.
- **Route discovery and selection:** Because Layer 3 devices make forwarding decisions based on logical network addresses, a Layer 3 device might need to know how to reach various network addresses. For example, a common Layer 3 device is a router. A router can maintain a routing table indicating how to forward a packet based on the packet's destination network address.

A router can have its routing table populated via manual configuration (that is, by entering static routes), via a dynamic routing protocol (for example, RIP, OSPF, or EIGRP), or simply by the fact that the router is directly connected to certain networks.

NOTE Routing protocols are discussed in Chapter 6.

- **Connection services:** Just as the data link layer offers connection services for flow control and error control, connection services also exist at the network layer. Connection services at the network layer can improve the communication reliability, if the data link's LLC sublayer is not performing connection services.

The following functions are performed by connection services at the network layer:

- **Flow control (also known as congestion control):** Helps prevent a sender from sending data more rapidly than the receiver is capable of receiving it.
- **Packet reordering:** Allows packets to be placed in the proper sequence as they are sent to the receiver. This might be necessary because some networks support load balancing, where multiple links are used to send packets between two devices. Because multiple links exist, packets might arrive out of order.

Examples of devices found at the network layer include routers and multilayer switches. The most common Layer 3 protocol in use, and the protocol on which the Internet is based, is IPv4. However, IPv6 is beginning to be more common on networks today.

NOTE Routers and multilayer switches are discussed in Chapter 3.

Layer 4: The Transport Layer

The transport layer, as shown in Figure 2-10, acts as a dividing line between the upper layers and lower layers of the OSI model. Specifically, messages are taken from upper layers (Layers 5–7) and are encapsulated into segments for transmission to the lower layers (Layers 1–3). Similarly, data streams coming from lower layers are de-encapsulated and sent to Layer 5 (the session layer), or some other upper layer, depending on the protocol.

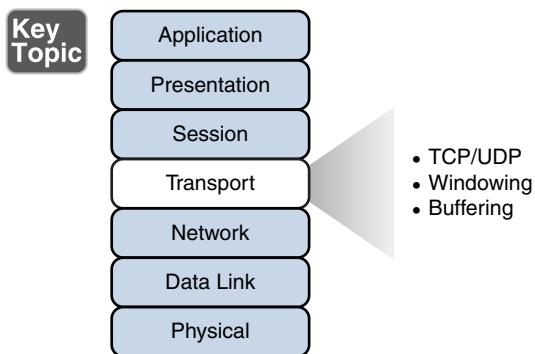


Figure 2-10 Layer 4: The Transport Layer

Two common transport layer protocols are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP):

- **Transmission Control Protocol (TCP):** A connection-oriented transport protocol. Connection-oriented transport protocols offer reliable transport, in that if a segment is dropped, the sender can detect that drop and retransmit the dropped segment. Specifically, a receiver acknowledges segments that it receives. Based on those acknowledgments, a sender can decide which segments were successfully received and which segments need to be transmitted again.
- **User Datagram Protocol (UDP):** A connectionless transport protocol. Connectionless transport protocols offer unreliable transport, in that if a segment is dropped, the sender is unaware of the drop, and no retransmission occurs.

Just as Layer 2 and Layer 3 offer flow control services, flow control services also exist at Layer 4. Two common flow control approaches at Layer 4 are windowing and buffering:

- **Windowing:** TCP communication uses windowing, in that one or more segments are sent at one time, and a receiver can attest to the receipt of all the segments in a window with a single acknowledgment. In some cases, as illustrated in Figure 2-11, TCP uses a sliding window, where the window size begins with one segment. If there is a successful acknowledgment of that one segment (that is, the receiver sends an acknowledgment asking for the next segment), the window size doubles to two segments. Upon successful receipt of those two segments, the next window holds four segments. This exponential increase in window size continues until the receiver does not acknowledge successful receipt of all segments within a certain amount of time—known as the *round-trip time* (RTT), which is sometimes called *real transfer time*—or until a configured maximum window size is reached.

Key Topic

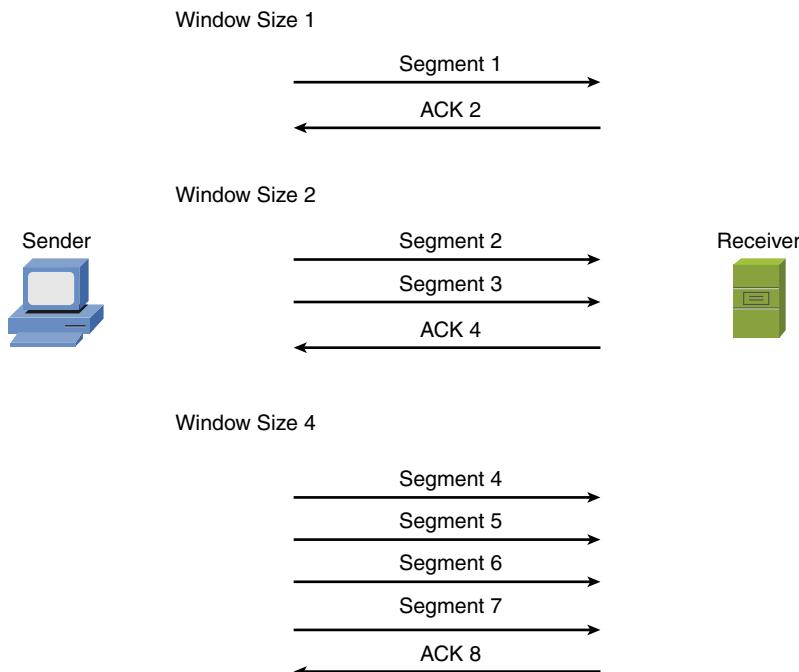


Figure 2-11 TCP Sliding Window

- **Buffering:** With buffering, a device (for example, a router) uses a chunk of memory (sometimes called a *buffer* or a *queue*) to store segments if bandwidth is not available to send those segments. A queue has a finite capacity, however, and can overflow (that is, drop segments) in case of sustained network congestion.

In addition to TCP and UDP, Internet Control Message Protocol (ICMP) is another transport layer protocol you are likely to meet. ICMP is used by utilities such as ping and traceroute, which are discussed in Chapter 10, “Command-Line Tools.”

Layer 5: The Session Layer

The session layer, as shown in Figure 2-12, is responsible for setting up, maintaining, and tearing down sessions. You can think of a session as a conversation that needs to be treated separately from other sessions to avoid the intermingling of data from different conversations.



Figure 2-12 Layer 5: The Session Layer

Here is a detailed look at the functions of the session layer:

- **Setting up a session:** Examples of the procedures involved in setting up a session include the following:
 - Checking user credentials (for example, username and password)
 - Assigning numbers to a session’s communication flows to uniquely find each one
 - Negotiating services needed during the session
 - Negotiating which device begins sending data
- **Maintaining a session:** Examples of the procedures involved in supporting a session include the following:
 - Transferring data
 - Reestablishing a disconnected session
 - Acknowledging receipt of data

- **Tearing down a session:** A session can be disconnected based on agreement of the devices in the session. Alternatively, a session might be torn down because one party disconnects (either intentionally or because of an error condition). If one party disconnects, the other party can detect a loss of communication with that party and tear down its side of the session.

H.323 is an example of a session layer protocol, which can help set up, support, and tear down a voice or video connection. Keep in mind, however, that not every network application neatly maps directly to all seven layers of the OSI model. The session layer is one of those layers where it might not be possible to name what protocol in each scenario is running in it. Network Basic Input/Output System (NetBIOS) is one example of a session layer protocol.

NOTE NetBIOS is an application programming interface (API) developed in the early 1980s to allow computer-to-computer communication on a small LAN (specifically, PC-Network, which was IBM's LAN technology at the time). Later, IBM needed to support computer-to-computer communication over larger Token Ring networks. As a result, IBM enhanced the scalability and features of NetBIOS with a NetBIOS emulator named NetBIOS Extended User Interface (NetBEUI).

Layer 6: The Presentation Layer

The presentation layer, as shown in Figure 2-13, handles formatting the data being exchanged and securing that data with encryption.

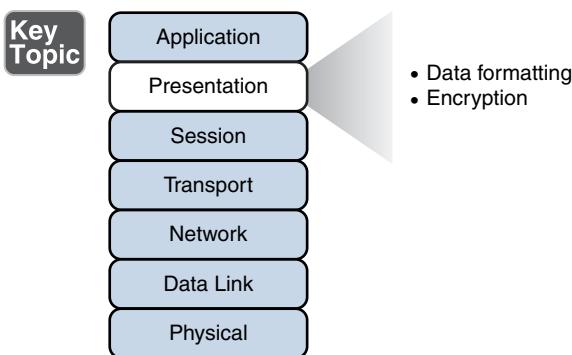


Figure 2-13 Layer 6: The Presentation Layer

The following list describes the function of data formatting and encryption in more detail:

- **Data formatting:** As an example of how the presentation layer handles data formatting, consider how text is formatted. Some applications might format text using American Standard Code for Information Interchange (ASCII), while other applications might format text using Extended Binary Coded Decimal Interchange Code (EBCDIC). The presentation layer handles formatting the text (or other types of data, such as multimedia or graphics files) in a format that allows compatibility between the communicating devices.
- **Encryption:** Imagine that you are sending sensitive information over a network (for example, your credit card number or bank password). If a malicious user were to intercept your transmission, they might be able to obtain this sensitive information. To add a layer of security for such transmissions, encryption can be used to scramble up (encrypt) the data in such a way that if the data were intercepted, a third party would not be able to unscramble it (decrypt). However, the intended recipient would be able to decrypt the transmission.

Encryption is discussed in detail in Chapter 12, “Network Security.”

Layer 7: The Application Layer

The application layer, as shown in Figure 2-14, gives application services to a network. An important (and often-misunderstood) concept is that end-user applications (such as Microsoft Word) live at the application layer. Instead, the application layer supports services used by end-user applications. For example, email is an application layer service that does exist at the application layer, whereas Microsoft Outlook (an example of an email client) is an end-user application that does not live at the application layer. Another function of the application layer is advertising available services.

Key Topic

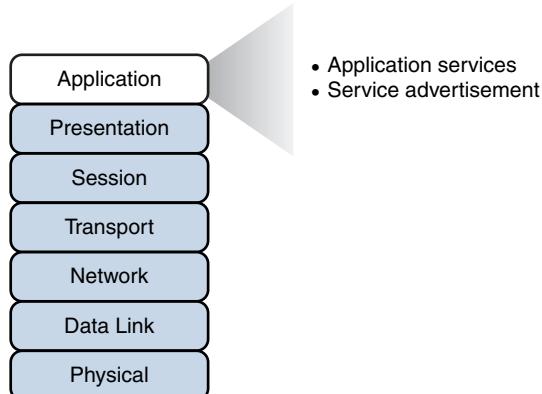


Figure 2-14 Layer 7: The Application Layer

The following describes the functions of the application layer in more detail:

- **Application services:** Examples of the application services living at the application layer include file sharing and email.
- **Service advertisement:** Some applications' services (for example, some networked printers) periodically send out advertisements, making their availability known to other devices on the network. Other services, however, register themselves and their services with a centralized directory (for example, Microsoft Active Directory), which can be queried by other network devices seeking such services.

Recall that even though the application layer is numbered as Layer 7, it is at the top of the OSI stack because its networking functions are closest to the end user.

The TCP/IP Stack

The ISO developed the OSI reference model to be generic, in terms of what protocols and technologies could be categorized by the model. However, most of the traffic on the Internet (and traffic on corporate networks) is based on the TCP/IP protocol suite. Therefore, a more relevant model for many network designers and administrators to reference is a model developed by the United States Department of Defense (DoD). This model is known as the *DoD model* or the *TCP/IP stack*.

NOTE An older protocol known as the Network Control Protocol (NCP) was similar to the TCP/IP protocol. NCP was used on ARPANET (the predecessor to the Internet), and it provided features like those offered by the TCP/IP suite of protocols on the Internet, although they were not as robust.

Layers of the TCP/IP Stack

The TCP/IP stack has only four defined layers, as opposed to the seven layers of the OSI model. Figure 2-15 contrasts these two models for an illustrative understanding.

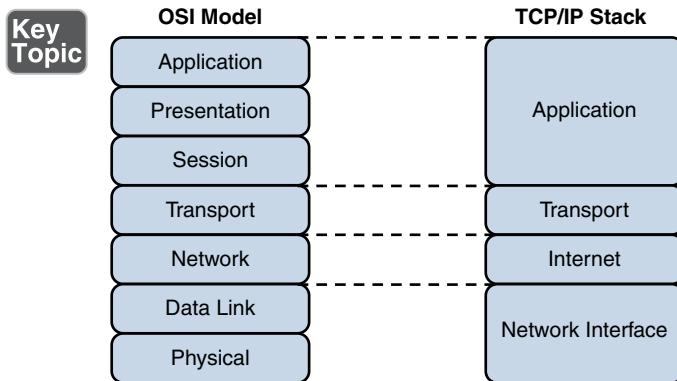


Figure 2-15 TCP/IP Stack

The TCP/IP stack is composed of the following layers:

- **Network interface:** The TCP/IP stack's network interface layer encompasses the technologies offered by Layers 1 and 2 (the physical and data link layers) of the OSI model.

NOTE Some literature refers to the network interface layer as the *network access layer*.

- **Internet:** The Internet layer of the TCP/IP stack maps to Layer 3 (the network layer) of the OSI model. Although multiple routed protocols (for example, IP, IPX, and AppleTalk) live at the OSI model's network layer, the Internet layer of the TCP/IP stack focuses on IP as the protocol to be routed through a network. Figure 2-16 shows the format of an IP Version 4 packet.

Key Topic

Version	Header Length	Type of Service	Total Length			
Identification		IP Flags	Fragment Offset			
TTL	Protocol		Header Checksum			
Source Address						
Destination Address						
IP Option (Variable Length)						

Figure 2-16 IP Version 4 Packet Format

Notice that there are fields in the IP packet header for both a source and a destination IP address. The Protocol field shows the transport layer protocol from which the packet was sent or to which the packet should be sent. Also of note is the Time-to-Live (TTL) field. The value in this field is decremented by 1 every time this packet is routed from one IP network to another (that is, passes through a router). If the TTL value ever reaches 0, the packet is discarded from the network. This behavior helps prevent routing loops. As a common practice, the OSI layer numbers of 1, 2, and 3 are still used when referring to physical, data link, and network layers of the TCP/IP stack, even though the TCP/IP stack does not explicitly separate the physical and data link layers.

- **Transport:** The transport layer of the TCP/IP stack maps to Layer 4 (the transport layer) of the OSI model. The two primary protocols found at the TCP/IP stack's transport layer are TCP and UDP.

Figure 2-17 details the structure of a TCP segment. Notice the fields for source and destination ports. As described later in this chapter, these ports identify to which upper-layer protocol data should be forwarded, or from which upper-layer protocol the data is being sent.

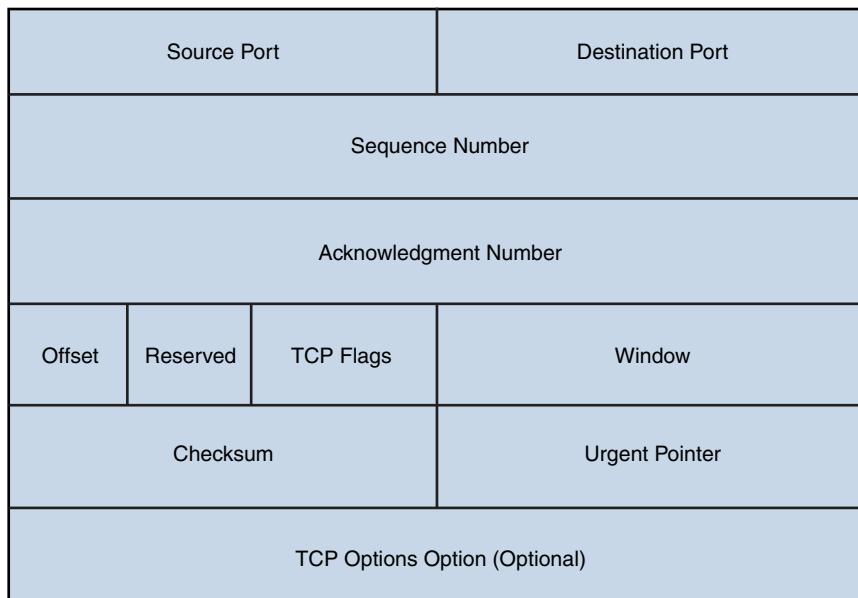
Key Topic

Figure 2-17 TCP Segment Format

Also notice the field for window size. The value in this field determines how many bytes a device can receive before expecting an acknowledgment. As previously described, this feature offers flow control.

The header of a TCP segment also contains sequence numbers for segments. With sequence numbering, if segments arrive out of order, the recipient can put them back in the proper order based on these sequence numbers.

The acknowledgment number in the header shows the next sequence number the receiver expects to receive. This is a way for the receiver to let the sender know that all segments up to and including that point have been received. Due to the sequencing and acknowledgements, TCP is considered to be a *connection-oriented* transport layer protocol.

Figure 2-18 presents the structure of a UDP segment. UDP is a connectionless, unreliable protocol. UDP lacks the sequence numbering, window size, and acknowledgment numbering present in the header of a TCP segment. The UDP segment's header simply contains source and destination port numbers, a UDP checksum (which is an optional field used to detect transmission errors), and the segment length (measured in bytes).

Key Topic

Source Port	Destination Port
UDP Length	UDP Checksum

Figure 2-18 UDP Segment Format

Because a UDP header is so much smaller than a TCP header, UDP becomes a good candidate for the transport layer protocol for applications that need to maximize bandwidth and do not require acknowledgments (for example, audio or video streams).

- **Application:** The biggest difference between the TCP/IP stack and the OSI model is found at the TCP/IP stack’s application layer. This layer addresses concepts described by Layers 5, 6, and 7 (the session, presentation, and application layers) of the OSI model.

With the reduced complexity of a four-layer model like the TCP/IP stack, network designers and administrators can more easily categorize a given networking technology into a specific layer. For example, although H.323 was shown earlier as a session layer protocol within the OSI model, you would have to know more about the behavior of H.323 to properly categorize it. However, with the TCP/IP stack, you could quickly figure out that H.323 is a higher-level protocol that gets encapsulated inside of TCP, and thus classify H.323 in the application layer of the TCP/IP stack.

Common Application Protocols in the TCP/IP Stack

Application layer protocols in the TCP/IP stack are identifiable by unique port numbers. For example, when you enter a web address in an Internet browser, you are (by default) communicating with that remote web address using TCP port 80. Specifically, Hypertext Transfer Protocol (HTTP), which is the protocol used by web servers, uses TCP port 80. Therefore, the data you send to that remote web server has a destination port number of 80. That data is then encapsulated into a TCP segment at the transport layer. That segment is then further encapsulated into a packet at the Internet layer and sent out on the network using an underlying network interface layer technology such as Ethernet.

Continuing with the example depicted in Figure 2-19, when you send traffic to that remote website, the packet you send out to the network needs not only the destination IP address (172.16.1.2 in this example) of the web server and the destination port number for HTTP (that is, 80), it also needs the source IP address of your computer (10.1.1.1 in this example). Because your computer is not acting as a

web server, its port is not 80. Instead, your computer selects a source port number greater than 1023. In this example, let's imagine that the client PC selects the source port 1248.

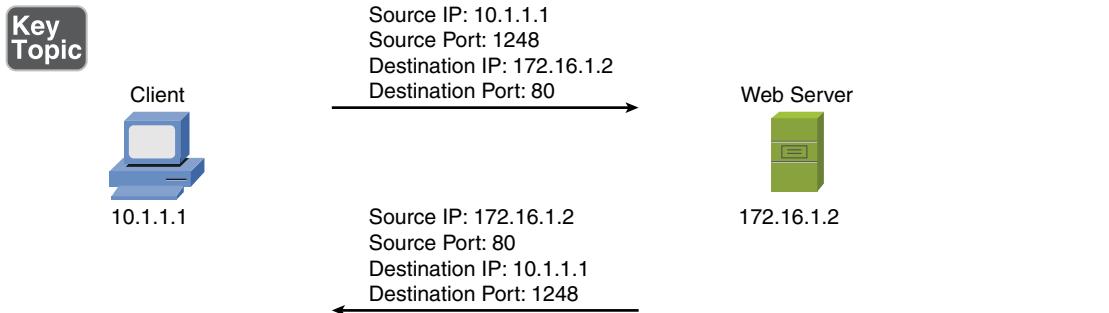


Figure 2-19 Example: Port Numbers and IP Addresses

Notice that when the web server sends content back, the IP addresses and port numbers have now switched, with the web server as the source and your PC as the destination. With both source and destination port numbers, along with source and destination IP addresses, two-way communication becomes possible.

NOTE Ports numbered 1023 and below are called *well-known* ports, and ports numbered above 1023 are called *ephemeral* ports. The maximum value of a port is 65,535. Well-known port number assignments are found at <http://www.iana.org/assignments/port-numbers>.

Table 2-1 serves as a reference for some of the more popular application layer protocols and applications found in the TCP/IP stack. Some protocols or applications (such as DNS) may use TCP or UDP for their transport protocol, depending on the specific function being performed.

Table 2-1 Application Layer Protocols/Applications

Protocol	Description	TCP Port	UDP Port
DHCP	Dynamic Host Configuration Protocol: Dynamically assigns IP address information (for example, IP address, subnet mask, DNS server's IP address, and default gateway's IP address) to a network device		67, 68
DNS	Domain Name System: Resolves domain names to corresponding IP addresses	53	53

Protocol	Description	TCP Port	UDP Port
FTP	File Transfer Protocol: Transfers files with a remote host (typically requires authentication of user credentials)	20 and 21	
H.323	A signaling protocol that provides multimedia communications over a network	1720	
HTTP	Hypertext Transfer Protocol: Retrieves content from a web server	80	
HTTPS	Hypertext Transfer Protocol Secure: Used to securely retrieve content from a web server	443	
IMAP	Internet Message Access Protocol: Retrieves email from an email server	143	
IMAP4	Internet Message Access Protocol Version 4: Retrieves email from an email server	143	
LDAP	Lightweight Directory Access Protocol: Provides directory services (for example, a user directory that includes username, password, email, and phone number information) to network clients	389	
LDAPS	Lightweight Directory Access Protocol over SSH: A secured version of LDAP	636	
MGCP	Media Gateway Control Protocol: Used as a call control and communication protocol for Voice over IP networks		2427, 2727
NetBIOS	Network Basic Input/Output System: Provides network communication services for LANs that use NetBIOS	139	137, 138
NNTP	Network News Transport Protocol: Supports the posting and reading of articles on Usenet news servers	119	
NTP	Network Time Protocol: Used by a network device to synchronize its clock with a time server (NTP server)		123
POP3	Post Office Protocol Version 3: Retrieves email from an email server	110	
RDP	Remote Desktop Protocol: A Microsoft protocol that allows a user to view and control the desktop of a remote computer	3389	
rsh	Remote Shell: Allows commands to be executed on a computer from a remote user	514	
RTP	Real-time Transport Protocol: Used for delivering media-based data (such as Voice over IP) through the network	5004, 5005	5004, 5005

Protocol	Description	TCP Port	UDP Port
RTSP	Real-Time Streaming Protocol: Communicates with a media server (for example, a video server) and controls the playback of the server's media files	554	554
SCP	Secure Copy: Provides a secure file-transfer service over an SSH connection and offers a file's original date and time information, which is not available with FTP	22	
SFTP	Secure FTP: Provides FTP file-transfer service over an SSH connection	22	
SIP	Session Initiation Protocol: Used to create and end sessions for one or more media connections, including Voice over IP calls	5061	5060
SMB	Server Message Block: Used to share files, printers, and other network resources	445	
SMTP	Simple Mail Transfer Protocol: Used for sending email	25	
SNMP	Simple Network Management Protocol: Used to monitor and manage network devices		161
SNMP Trap	Simple Network Management Protocol Trap: A notification sent from an SNMP agent to an SNMP manager	162	162
SNTP	Simple Network Time Protocol: Supports time synchronization among network devices, similar to Network Time Protocol (NTP), although SNTP uses a less complex algorithm in its calculation and is slightly less accurate than NTP		123
SSH	Secure Shell: Used to securely connect to a remote host (typically via a terminal emulator)	22	
Telnet	Telnet: Used to connect to a remote host (typically via a terminal emulator)	23	
TFTP	Trivial File Transfer Protocol: Transfers files with a remote host (does not require authentication of user credentials)		69

Real-World Case Study

Bob, a manager of the networking team at Acme, Inc., is paying extra attention to the specific words he uses as he talks to his team in preparation for the implementation of the network. When referring to transport protocols such as the connection-oriented TCP and the connectionless UDP, the word Bob uses to describe those protocol data units is *segment*.

In discussing the applications that the company will be using over its network, Bob notes that many of these applications will be using TCP at the transport layer. This includes HTTP for web browsing, HTTPS for secure web traffic, and SMTP and IMAP for email services.

The SSH protocol, which also uses TCP at the transport layer, is a secure method that the company will use to remotely connect to and manage its network devices. A common connectionless UDP protocol is DNS, which will be used thousands of times a day to translate a friendly name like <http://www.pearson.com> to an IP address that is reachable over the network. Another protocol based on UDP that will be used often is Dynamic Control Host Protocol (DHCP), which assigns client computers on the network an IP address that is required for sending and receiving Layer 3 packets.

For the traffic on the LAN, the Ethernet cables and electronic signals being sent as bits going over those cables represent Layer 1 from an OSI perspective. On the LAN, they will be using Ethernet technology, and as a result the Layer 2 frames that are sent on the LAN will be encapsulated and sent as Ethernet Layer 2 frames.

For datagrams being sent across the serial WAN connections provided by the service provider, it is likely that either PPP or HDLC encapsulation will be used for the Layer 2 frames. On both the LAN and the WAN, at Layer 3 (the network layer), IPv4 will be used for host addressing and defining networks. The same Layer 1, Layer 2, and Layer 3 infrastructure is also capable of transporting IPv6, if desired.

Inside the Layer 3 IP headers, each packet contains the source and destination address, in addition to the information to tell the receiving network device about which Layer 4 transport protocol is encapsulated or carried inside of the Layer 3 packet. When a network device receives the packet and opens it up to look at the contents, this process is called *de-encapsulation*. As the recipient de-encapsulates and looks at the Layer 4 information, it identifies the application layer protocol or service being used. A segment going to a web server is likely to have a TCP destination port of 80 or 443, depending on whether encryption is being used for a secure connection. A DNS request uses a UDP destination port of 53.

Summary

Here are the main topics covered in this chapter:

- The ISO's OSI reference model consists of seven layers: physical (Layer 1), data link (Layer 2), network (Layer 3), transport (Layer 4), session (Layer 5), presentation (Layer 6), and application (Layer 7). The purpose of each layer was presented, along with examples of technologies living at the individual layers, as it pertains to networking.

- The TCP/IP stack was presented as an alternative model to the OSI reference model. The TCP/IP stack consists of four layers: network interface, Internet, transport, and application. These layers were compared with the seven layers of the OSI model.
- This chapter discussed how port numbers are used to associate data at the transport layer with a proper application layer protocol. Examples of common application layer protocols in the TCP/IP suite were presented, along with their port numbers.

Exam Preparation Tasks

Review All the Key Topics

Review the most important topics from inside the chapter, noted with the Key Topic icon in the outer margin of the page. Table 2-2 lists these key topics and the page numbers where each is found.



Table 2-2 Key Topics for Chapter 2

Key Topic Element	Description	Page Number
List	Layers of the OSI model	33
Figure 2-3	Protocol data unit names	35
Figure 2-4	Layer 1: The physical layer	35
Figure 2-8	Layer 2: The data link layer	39
Figure 2-9	Layer 3: The network layer	42
Figure 2-10	Layer 4: The transport layer	44
Figure 2-11	TCP sliding window	45
Figure 2-12	Layer 5: The session layer	46
Figure 2-13	Layer 6: The presentation layer	47
Figure 2-14	Layer 7: The application layer	48
Figure 2-15	TCP/IP stack	50
Figure 2-16	IP Version 4 packet format	51
Figure 2-17	TCP segment format	52
Figure 2-18	UDP segment format	53
Figure 2-19	Example: Port numbers and IP addresses	54
Table 2-1	Application layer protocols/applications	54

Complete Tables and Lists from Memory

Print a copy of Appendix C, “Memory Tables,” or at least the section for this chapter, and complete as many of the tables as possible from memory. Appendix D, “Memory Tables Answer Key,” includes the completed tables and lists so you can check your work.

Define Key Terms

Define the following key terms from this chapter, and check your answers in the Glossary:

Open Systems Interconnection (OSI) reference model, protocol data unit (PDU), current state modulation, state transition modulation, cyclic redundancy check (CRC), physical layer, data link layer, network layer, transport layer (OSI model), session layer, presentation layer, application layer (OSI model), network interface layer, Internet layer, transport layer (TCP/IP stack), application layer (TCP/IP stack), time-division multiplexing (TDM), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), TCP/IP stack

Complete Chapter 2 Hands-On Labs in Network+ Simulator Lite

- Matching Well-Known Port Numbers
- TCP/IP Protocols and Their Functions
- Network Application Protocols
- OSI Model Layer Functions

Additional Resources

Bring the OSI Model to Life: <http://www.ajsnetworking.com/osi-life>

The OSI Reference Model: <https://youtu.be/OHpzuPvQygU>

The OSI Model Challenge: <http://ajsnetworking.com/osiquiz1>

Review Questions

The answers to these review questions appear in Appendix A, “Answers to Review Questions.”

1. Which layer of the OSI reference model contains the MAC and LLC sublayers?
 - a. Network layer
 - b. Transport layer
 - c. Physical layer
 - d. Data link layer

2. Which approach to bandwidth usage consumes all the available frequencies on a medium to transmit data?
 - a. Broadband
 - b. Baseband
 - c. Time-division multiplexing
 - d. Simplex

3. Windowing is provided at what layer of the OSI reference model?
 - a. Data link layer
 - b. Network layer
 - c. Transport layer
 - d. Physical layer

4. IP addresses reside at which layer of the OSI reference model?
 - a. Network layer
 - b. Session layer
 - c. Data link layer
 - d. Transport layer

5. Which of the following is a connectionless transport layer protocol?
 - a. IP
 - b. TCP
 - c. UDP
 - d. H.323

- 6.** Identify the four layers of the TCP/IP stack. (Choose four.)
 - a.** Session layer
 - b.** Transport layer
 - c.** Internet layer
 - d.** Data link layer
 - e.** Network layer
 - f.** Application layer
 - g.** Network interface layer
- 7.** What is the range of well-known TCP and UDP ports?
 - a.** Below 2048
 - b.** Below 1024
 - c.** 16,384–32,768
 - d.** Above 8192
- 8.** Which protocol supports a secure connection to a remote host via terminal emulation software?
 - a.** Telnet
 - b.** SSH
 - c.** FTP
 - d.** SFTP
- 9.** Identify the well-known UDP port number for NTP.
 - a.** 53
 - b.** 69
 - c.** 123
 - d.** 143
- 10.** Identify three e-mail protocols. (Choose three.)
 - a.** SNMP
 - b.** SMTP
 - c.** POP3
 - d.** IMAP4



After completion of this chapter, you will be able to answer the following questions:

- What are the characteristics of various media types?
- What is the role of a given network infrastructure component?
- Specialized network devices offer what features?
- How are virtualization technologies changing traditional corporate data center designs?
- What are some of the primary protocols and hardware components found in a Voice over IP (VoIP) network?

Index

Symbols

2.4GHz band channel frequencies, 281-282
3DES (Triple DES) algorithm, 411
4 parameter (PathPing command), 358
5GHz band channel frequencies, 281-283
6 parameter (PathPing command), 358
8-bit subnet masks, 162
9-pin D-subminiature (DB-9) connectors, 69
10BASE2 Ethernet standard, 118, 125
10BASE5 Ethernet standard, 118, 125
10BASE-T Ethernet standard, 119, 125
10GBASE-ER Ethernet standard, 125
10GBASE-EW Ethernet standard, 125
10GBASE-LR Ethernet standard, 125
10GBASE-LW Ethernet standard, 125
10GBASE-SR Ethernet standard, 125
10GBASE-SW Ethernet standard, 125
10GBASE-T Ethernet standard, 125
10-Gigabit Ethernet, 124
40MHz mode, 286
66 blocks, 76
80-20 rule, 239
100BASE-FX Ethernet standard, 125

100BASE-T Ethernet standard, 125
100BASE-TX Ethernet standard, 125
100GBASE-ER4 Ethernet standard, 125
100GBASE-LR4 Ethernet standard, 125
100GBASE-SR10 Ethernet standard, 125
100-gigabit Ethernet, 124
110 blocks, 76
802.1aq protocol, 131
802.1D. *See* STP
802.1w protocol, 131
802.11 wireless signals, 79
802.11a WLAN standard, 285
802.11ac WLAN standard, 286
802.11b WLAN standard, 285
802.11g WLAN standard, 285
802.11n WLAN standard, 285-286
1000BASE-LH Ethernet standard, 125
1000BASE-LX Ethernet standard, 125
1000BASE-T Ethernet standard, 125
1000BASE-TX Ethernet standard, 125
1000BASE-ZX Ethernet standard, 125

A

A (address) records, 95
a parameter
arp command, 338, 360-361
nbtstat command, 344
netstat command, 346, 367

A parameter (nbtstat command), 344
AAA (authentication, authorization, and accounting), 440
AAAA records, 95
acceptable use policies (AUPs), 429, 471
access
ACLs
 attacks, preventing, 436-437
 packet-filtering firewalls, 443
CLI, 511
control lists (ACLs), 436-437
Ethernet devices, 122
Internet, 521-522
points (APs), 77
ports, switch configuration, 128
remote, 400-401, 439-442
slow Internet, troubleshooting, 501-504
WAN services technologies, 521-522
acknowledgment messages, 40
ACLs (access control lists)
 attacks, preventing, 436-437
 packet-filtering firewalls, 443
active-active mode (NICs), 308
active hubs, 80
active IPS devices, 455
active routers, 144, 310
active-standby mode (NICs), 308
AD (administrative distance), 214
ad hoc wireless networks, 20, 276
add parameter (route command), 355, 370
address (A) records, 95
Address Resolution Protocol.
 See ARP

addresses

APIPA, 502
 dotted-decimal notation, 161
 IP
assignable in subnets, 176
configuration parameters, displaying, 340
DHCP server, 97
DNS records pointing to, 95
duplicate, 495
expired, 495
FQDNs, resolving, 362-363
host, 180-181
interfaces, configuring, 364
leases, 98
listing, 347
loopback, 163
management (IPAM), 96
NAT classifications, 221
NAT names, 221
next-hop, 211
parameters, displaying, 340
ranges, calculating, 183-186
scopes, 98
target, specifying, 356
 IPv4, 161
APIPA, 174-176
assignment, 164
available hosts, number of, 180-181
bits, 154
BOOTP protocol, 173
borrowed bits, 179
broadcast, 165
CIDR, 190-191
classes, 163
classful masks, extending, 179
components, 167-168
DHCP, 173-174
dotted-decimal notation, 161
dynamic configuration, 172
FQDN translation, 167
multicast, 166
network address calculation, 162
network/host address divisions, 162
private addressing, 164
ranges, calculating, 183-186
static configuration, 168-172
structure, 161-163

subnet masks, 161
subnet notation, 177-178
subnet octet values, 178
subnets created, number of, 180
transitioning to IPv6, 192
unicast, 165
 IPv6, 191
anycast, 195-196
bits, 154
features, 192
IPv4 transitions, 192
multicast, 195
NDP, 193
ping command, 352
records, 95
structure, 192-193
traceroute command, 366
tracert command, 358
types, 193
unicast, 194
link-local IP, assigning, 175
logical, 42
MAC
duplicate, 495
filtering, 145, 294
table corruption, 131-132
network, 126
physical, 39
prefix notation, 162
private, 222
public, 222
translation
NAT, 220-222
PAT, 222-224
adjacencies, 494
administrative distance (AD), 214
ADSL (Asymmetric DSL), 252-254
advanced distance-vector routing protocols, 219
Advanced Encryption Standard (AES), 297, 411
advertisements
link-state (LSAs), 218
neighbor, 194
routing, 194, 216-218
services, 49
AES (Advanced Encryption Standard), 297, 411

agents
call, 108
relay, 98
SNMP, 392
aggressive mode (IKE), 450
AHs (Authentication Headers), 451-452
AirDrop, 20
algorithms
3DES, 411
AES, 411
DES, 411
Dijkstra's shortest path first, 218
DUAL, 219
GPG, 411
hashing, 414
MD5, 414
PGP, 411
queuing, 319
RSA, 412
SHA-1, 414
symmetric encryption, 411
all parameter (ipconfig command), 340-341
AM (amplitude modulation), 36
Amazon Web Services (AWS), 106
American Registry for Internet Numbers (ARIN), 164
American Standard Code for Information Interchange (ASCII), 48
amplified DoS attacks, 423
amplitude modulation (AM), 36
analog phones, 108
analysis (traffic), 386
analyzers
protocols, 386
Wi-Fi, 387
anomaly-based detection, 457
Ant+, 78
antennas (WLANs), 278-281
gain, 279
omnidirectional, 279
orientation, 281
selecting, 279
throughput, increasing, 510
unidirectional, 280

- anycast IPv6 addresses, 195-196
- APIPA (Automatic Private IP Addressing), 174-176, 502**
- Apple AirDrop, 20**
- application layer
 - OSI model, 48-49
 - TCP/IP stack, 53-56
- application-specific integrated circuits (ASICs), 82**
- applications**
 - logs, 398
 - open connections, 347
 - services, 49
- appropriate use policies, 429, 471**
- APs (access points), 77**
 - evil twins, 422
 - fat configurations, 511
 - incorrect placement, 499
 - rogue, 293, 422
 - updates, troubleshooting, 516
 - wireless, 277-278, 291
- arc four, 296**
- arguments. *See* parameters**
- ARIN (American Registry for Internet Numbers), 164**
- ARP (Address Resolution Protocol), 361**
 - cache, 338
 - replies, 85-86
 - requests, 83-84
- arp command**
 - UNIX, 360-361
 - Windows, 338-340
- ASCII (American Standard Code for Information Interchange), 48**
- ASICs (application-specific integrated circuits), 82**
- asset tracking tags, 437**
- assigning**
 - IP addresses, 164, 176
 - IPv4 addresses
 - APIPA*, 174-176
 - BOOTP protocol*, 173
 - components*, 167-168
 - DHCP*, 173-174
 - dynamic configuration*, 172
 - FQDN translation*, 167
 - static configuration*, 168-172
 - associations, 277
 - Asymmetric DSL (ADSL), 252-254**
 - asymmetric encryption, 412-413
 - asynchronous bit synchronization, 37**
 - asynchronous transmissions, 40**
 - ATM (Asynchronous Transfer Mode), 8, 242, 264-265**
 - attacks**
 - availability, 422
 - buffer overflow*, 424
 - DDoS*, 423
 - DoS*, 422-423
 - electrical disturbances*, 425-426
 - ICMP*, 424
 - logic bombs*, 422
 - physical environment*, 426-427
 - TCP SYN floods*, 423
 - wireless attacks*, 422
 - banner-grabbing, 515
 - Bluetooth, 431
 - confidentiality, 415-419
 - covert channels*, 418
 - dumpster diving*, 417
 - EMI interceptions*, 417
 - FTP bounce*, 418
 - insider*, 419
 - malware*, 418
 - MitM*, 417
 - overt channels*, 418
 - packet captures*, 417
 - phishing*, 419
 - ping sweeps*, 417
 - port scans*, 417
 - social engineering*, 418
 - wiretapping*, 417
 - integrity, 419-422
 - botnets*, 421
 - brute force*, 421
 - data diddling*, 420
 - dictionary attacks*, 421
 - bijacking sessions*, 422
 - keyloggers*, 421
 - MitM*, 420
 - packet captures*, 421
 - password*, 421
 - salami*, 420
 - Trojan horses*, 421
 - trust relationship exploitation*, 420
 - means, 432
 - motives, 432
 - opportunities, 433
 - preventing
 - ACLs*, 436-437
 - detailed documentation*, 431-432
 - end-user policies*, 431
 - governing policies*, 430
 - honey pots*, 435
 - incident response*, 432-433
 - Layer 2 protections*, 439
 - network device hardening*, 438
 - patching*, 428
 - physical devices*, 437-438
 - security policies*, 429
 - technical policies*, 431
 - user training*, 427-428
 - vulnerability scanners*, 433-435
 - auditing infrastructure, 514-518**
 - AUPs (acceptable use policies), 429, 471**
 - authentication**
 - certificates, 413
 - CHAP, 250
 - headers, 451-452
 - HMACs, 414
 - LCP, 249
 - local, 441
 - multifactor, 441
 - passwords, 249
 - servers, 142, 440
 - SNMP messages, 395
 - SSO, 441
 - switches, 142-143
 - two-factor, 441
 - users, 141-142
 - VPN traffic, 449
 - WLANs, 294
 - authentication, authorization, and accounting (AAA), 440**
 - authenticators, 141, 440**
 - authNoPriv security level, 394**
 - authPriv security level, 394**
 - Automatic Private IP Addressing (APIPA), 174-176, 502**
 - availability, 415**
 - attacks, 422
 - buffer overflow*, 424
 - DDoS*, 423

DoS, 422-423
electrical disturbances, 425-426
ICMP, 424
logic bombs, 422
physical environment, 426-427
TCP SYN floods, 423
wireless attacks, 422

five nines, 130, 415
 high, 514
best practices, 311
designing, 310-311
measuring, 306

host IP addresses, calculating, 180-181
 network faults, 306
 reliability, compared, 306

avoiding congestion, 319

AWS (Amazon Web Services), 106

B

B channels, 260

b parameter (netstat command), 346-347, 367

back-off timers, 121

back-out plans, 486

backups, 311

backward explicit congestion notification (BECN), 263

bad cables, 487

bad modules, 490

bad ports, 487

badges, 437

bands (frequency), 281

bandwidth
 CIR, 320
 Ethernet, 124
 Frame Relay, 263
 measuring, 123
 QoS issues, 314-315
 usage, 37
 WANs, 243

banking bits/bytes, 321

banner-grabbing, 515

baseband technologies, 38

basic rate interface circuits (BRI), 261

basic routing process, 206-208

basic service set (BSS) WLANs, 288

bayonet connectors, 73

BC (business continuity) plans, 427

Bc (committed burst), 321

Be (excess burst) parameter, 321

bearer channels, 260

BECN (backward explicit congestion notification), 263

behavior-based detection, 457

believability (routes), 214

benefits
 bus topology, 12
 client/server networks, 21
 content switches, 101
 full-mesh topology, 17
 hub-and-spoke topology, 16
 partial-mesh topology, 19
 peer-to-peer networks, 23
 proxy servers, 99
 ring topology, 14
 star topology, 15
 UNXI, 359

BER (bit error rate), 380

BERT (bit-error rate tester), 380

best-effort treatment, 316

best practices
 international export controls, 474
 licensing restrictions, 473
 non-disclosure agreements, 474
 on-boarding/off-boarding, 473
 privileged user agreements (PUAs), 472-473
 system life cycle, 474

BGP (Border Gateway Protocol), 219, 387, 503

bidirectional Telnet sessions, 88

binary data, displaying, 36

binary numbering, 154
 converting to decimal numbers, 155-158
 decimal to binary conversions, 155-160

biometrics, 437

bit error rate (BER), 380

bit-error rate tester (BERT), 380

bits
 banking, 321
 Bc, 321
 borrowed, 179

DE, 263
 defined, 123
 error detectors, 380
 errors, 380
 goodput, 290
 IPv4/IPv6 addresses, 154
 marking, 318
 octets, 161
 parity, 41
 pattern generators, 380
 rates, 521
 splitters, 80
 synchronization, 37

blackhole parameter (arp command), 360

black-hole routers, 494

blackouts, 425

block sizes, 184

blocked TCP/UDP ports, 495

blocking state, 135

bluebugging, 431

bluejacking, 431

bluesnarfing, 431

Bluetooth, 79, 431

bonding
 channels, 286
 NICs, 308
 ports, 137

BOOTP protocol, 173

BOOTPS (BOOTP server), 173

Border Gateway Protocol (BGP), 219, 387, 503

borrowed bits, 179

botnets, 421

bots, 421

BPDUs (bridge protocol data units), 135

BRI (basic rate interface) circuits, 261

bridges, 81-82

bring-your-own-device (BYOD) policies, 471, 506

broadband technologies, 37

broadcasts
 domains
network addresses, 126
switches, 88

IPv4 addresses, 165
 SSID, disabling, 294
 storms, 132-133
brownouts, 426
brute force attacks, 421, 513
BSS (basic service set) WLANs, 288
buffer overflow attacks, 424
buffering, 45
bus topology, 11-12
business continuity (BC) plans, 427
butt sets, 381
BYOD (bring-your-own-device) policies, 471, 506
bytes, 321

C

c parameter
 nbtstat command, 344
 ping command, 368
cable modems, 254-255
cables
 10BASE2, 118
 10BASE-T, 119
 bad, 487
 breaks, identifying, 389
 certifiers, 381
 coaxial, 64-65, 244
 crossover, 68
 distance limitations exceeded, 488
 distribution, 75-77
 fiber-optic, 70
 MMF, 70-72
 mode of propagation, 71
 polishing styles, 74
 SMF, 72-74
 WANs, 244
 locations, documenting, 391
 multimeters, 385-386
 placement, 488
 plenum/nonplenum, 70
 recrimping, 515
 rollover, 68
 splitting pairs, 487
 testers, 382
 tip and ring, 260
 troubleshooting, 515
 twisted-pair, 66-69

UTP, 15, 243
 wires connecting back to end-user location, 390
caching, 99, 312
calculating
 IP address ranges, 183-186
 network addresses, 162
 number of host IP addresses available, 180-181
 number of subnets created, 180
call agents, 108
canonical name (CNAME) records, 95
CANs (campus area networks), 9
captive portals, 441
capturing packets
 network sniffers, 139
 port mirroring, 140
CARP (Common Address Redundancy Protocol), 310
carrier sense, 121
carrier-sense multiple access/collision avoidance. *See CSMA/CA*
carrier-sense multiple access/collision detection. *See CSMA/CD*
Cat 3 cables, 67
Cat 5 cables, 68
Cat 5e cables, 68
Cat 6 cables, 68
Cat 6a cables, 68
CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), 297
CDMA (Code Division Multiple Access), 244
CE (customer edge) routers, 267
cells (WLANs), 291
cellular phones, 244
cellular technologies, 287
center frequencies, 284
central offices (COs), 260
certificates
 authentication, 413
 authorities, 413
 untrusted SSL, 495
chain of custody, 433
challenge-handshake authentication protocol (CHAP), 250, 441
Challenge-Response Authentication Mechanism Message Digest 5 (CRAM-MD5), 414
change management documentation, 391
channel service unit/data service unit (CSU/DSU), 246
channels
 2.4GHz band frequencies, 282
 5GHz band frequencies, 283
 bonding, 286
 center frequencies, 284
 covert, 418
 nonoverlapping, 282-283
 overt, 418
 sources of interference, 289-291
 transmission methods, 284
 WLANs, 281
CHAP (challenge-handshake authentication protocol), 250, 441
characteristics
 802.11x standards, 286
 bus topology, 12
 client/server networks, 21
 full-mesh topology, 17
 hub-and-spoke topology, 16
 infrastructure devices, 91
 partial-mesh topology, 19
 peer-to-peer networks, 23
 ring topology, 14
 routing protocols
 believability, 214
 distance-vector, 216-218
 interior versus exterior, 215
 link-state, 218
 metrics, 214
 star topology, 15
cheapernet, 118
child tunnels, 454
CIDR (classless interdomain routing), 190-191
CIR (committed information rate), 263, 320
circuit-switched connections, 241
circuits
 CSU/DSU, 248
 E1, 247

- E3, 247
- ISDN, 261
- switching, 42
- T1, 246-247
- T3, 247
 - virtual. *See* VCs
- CIRs (committed information rates), 263**
- Class A addresses, 163**
- Class B addresses, 163**
- Class C addresses, 163**
- Class D addresses, 163**
- Class E addresses, 163**
- class of service (CoS), 504**
- classes**
 - addresses, 163-164
 - traffic, 316
- classful masks, 163, 179**
- classifying**
 - NAT IP addresses, 221
 - networks
 - geographic dispersion* 7-9
 - resource location*, 21-23
 - QoS, 318
 - STP switches, 133
- classless interdomain routing (CIDR), 190-191**
- CLI (command-line interface), 511**
- clients**
 - defined, 5
 - syslog, 396
- client/server networks, 21-22**
- client-to-site VPNs, 400, 448**
- cloud computing, 105-106**
- clustering computers, 309**
- CNAME (canonical name) records, 95**
- coarse wavelength-division multiplexing (CWDM), 256**
- coaxial cables, 64-65**
 - common, 64
 - connectors, 65
 - WANs, 243
- Code Division Multiple Access (CDMA), 244**
- cold sites, 313**
- collisions**
 - bus, 12
 - detection, 122
- domains, 80, 122
- Ethernet, 120-121
- command-line interface (CLI), 511**
- command parameter (route command), 352**
- Command Prompt (Windows), accessing, 338**
- commands**
 - UNIX, 358
 - arp*, 360-361
 - dig*, 362
 - host*, 363
 - ifconfig*, 363-364
 - iptables*, 364
 - man*, 359
 - netstat*, 366
 - nmap*, 365
 - nslookup*, 362
 - ping*, 368-369
 - route*, 369-370
 - tcpdump*, 365
 - traceroute*, 365-366
 - Windows, 338
 - arp*, 338-340
 - ipconfig*, 340-343
 - nbtstat*, 343-345
 - netstat*, 346-347
 - nslookup*, 348-349
 - PathPing*, 358
 - ping*, 350-352
 - route*, 352-355
 - tracert*, 356-358
- committed burst (Bo), 321**
- committed information rate (CIR), 263, 320**
- Common Address Redundancy Protocol (CARP), 310**
- community cloud, 106**
- community strings, 393**
- companion website, 529, 530-531**
- components. *See also* devices**
 - environmental monitors, 384
 - IPv4 addresses, 167-168
 - media, 64
 - cable distribution*, 75-77
 - coaxial cables*, 64-65
 - converters*, 75
 - fiber-optic cables*, 70-74
 - plenum/nonplenum cables*, 70
- twisted-pair cables, 66-69**
 - wireless*, 77
- networks, 5-7**
- QoS, 316-317**
- SNMP, 392**
- compressing headers, 322**
- computers**
 - clustering, 309
 - forensics, 433
 - names, resolving, 175
- concentrators (VPN), 449**
- confidentiality, 410-411**
 - attacks, 415-419
 - covert channels*, 418
 - dumpster diving*, 417
 - EMI interceptions*, 417
 - FTP bounce*, 418
 - insider*, 419
 - malware*, 418
 - MitM*, 417
 - overt channels*, 418
 - packet captures*, 417
 - phishing*, 419
 - ping sweeps*, 417
 - port scans*, 417
 - social engineering*, 418
 - wiretapping*, 417
 - encryption
 - asymmetric*, 412-413
 - defined*, 411
 - keys*, 411
 - PKI*, 412
 - session keys*, 411
 - symmetric*, 411
 - VPN traffic, 449
- configuring**
 - APs, 511
 - baselines, documenting, 391
 - DNS, 495
 - interface IP addresses, 364
 - IPv4 addresses, 168-172
 - LACP, 137
 - ports, 141, 490
 - QoS, 315-316
 - sessions, 46
 - switch access ports, 128
 - time, 495
 - trunk ports, 130
 - VLANs, 490

conforming traffic, 321

congestion

- avoidance, 319
- backward explicit congestion notification, 263
- flow control, 40, 43
- management, 319
- uplink, 136

connections

- application open, 347
- bad, 487
- cable modems, 254-255
- CSU/DSU, 248
- dedicated leased line, 246
- DSL, 252-254
- E1, 247
- E3, 247
- Internet access technologies, 521-522
- LLC sublayer, 40
- networks, 4
- outages, troubleshooting, 505-507
- point-to-point, 246
- POTS, 258-260
- remote desktop, 382
- satellite, 257-258
- services, 43
- T1, 246-247
- T3, 247
- testing with ping command, 350
- third-party networks, troubleshooting, 516
- trunks, 129-130
- WANs

 - circuit-switched*, 241
 - dedicated leased line*, 240
 - packet-switched*, 241
 - RDP applications*, troubleshooting, 518-521
 - services*, 521-522
 - troubleshooting*, 517

connectivity software, 382

connectors

- coaxial cables, 65
- crimpers, 383
- Ethernet, 124
- fiber-optic cables, 74
- SMF cables, 73-74
- UTP cables, 69

consultant infrastructure audits, 514-518

contact blades, 388

content engines, 99, 312

content switches, 100-101, 312

control protocols (CPs), 249

convergence, 4, 213, 216

converters (media), 75

converting

- binary numbers to decimal numbers, 155-158
- decimal numbers to binary numbers, 155-160

cordless phone interference, 290

corruption, MAC address tables, 131-132

COs (central offices), 260

CoS (class of service), 504

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), 297

counter-rotating rings, 14

covert channels, 418

CPE (customer premises equipment) devices, 267

CPs (control protocols), 249

cracking WLANs, 293

CRAM-MD5 (Challenge-Response Authentication Mechanism Message Digest 5), 414

CRC (cyclic redundancy check), 41

credentials, changing, 438

cross-connect blocks, 76

crossover cables, 68

crosstalk, 488

cRTP (RTP header compression), 322

CSMA/CA (carrier-sense multiple access/collision avoidance)

- Ethernet, 122
- WLANs, 283

CSMA/CD (carrier-sense multiple access/collision detection), 121-123

CSU/DSU (channel service unit/data service unit), 246-248

current state modulation, 36

customer edge (CE) routers, 267

customer premises equipment (CPE) devices, 267

CWDM (coarse wavelength-division multiplexing), 256

cyclic redundancy check (CRC), 41

D

D channels, 260

d parameter (arp command), 338, 360-361

D parameter (ping command), 368

data

- authentication, 449
- availability
 - attacks*, 422-427
 - five nines*, 415
- binary, 36
- confidentiality, 410
 - attacks*, 415-419
 - encryption*, 411-413
 - VPN traffic*, 449
- diddling, 420
- encapsulation/decapsulation, 521
- formatting, 48
- fragility, 433
- integrity, 414
 - attacks*, 419-422
 - hash digests*, 414
 - hashing*, 414
 - hashing algorithms*, 414
 - violations*, 414
 - VPN traffic*, 449
- loss prevention (DLP), 469-470
- rates, 242-243
- service units, 34

Data Encryption Standard (DES) algorithm, 411

data link layer (OSI model), 38-41

- sublayers
 - LLC*, 40-41
 - MAC*, 39
- troubleshooting, 490
 - bad modules*, 490
 - example*, 491
 - loops*, 490
 - port configuration*, 490
 - power failure*, 490
 - VLAN configuration*, 490

data-link connection identifiers (DLCIs), 263

Data-Over-Cable Service Interface Specification (DOCSIS), 255

Datagram Transport Layer Security (DTLS), 400

dB (decibels), 279, 488

DB-9 (9-pin D-subminiature) connectors, 69

DCSs (distributed control systems), troubleshooting, 500

DDNS (dynamic DNS), 95

DDoS (distributed denial-of-service) attacks, 423

DE (discard eligible) bits, 263

deauthentication attacks, 422

decapsulation, 521

decibels (dB), 279, 488

decimals

binary number conversions, 155-158

converting to binary, 155-160

decryption keys, 411

dedicated leased lines, 240, 246

default gateways, 144, 167

default static routes, 210

default subnet masks, 176

delay, 314

satellite transmissions, 257

serialization, 322

delete parameter (route command), 354, 370

deleting routing table entries, 354

delta channels, 260

demarc, 260

DEMILITARIZED (DMZ) zone (firewalls), 446

demultiplexing, 521

denial-of-service (DoS attacks), 422-423

dense wavelength-division multiplexing (DWDM), 256

deploying

NIPS/HIPS, 458

WLANs

BSS, 288

ESS, 288

IBSS, 287

mesh topology, 289

DES (Data Encryption Standard algorithm), 411

design

fault-tolerant, 307-308

high-availability networks, 310-311

designated ports, 134

desktops (virtual), 104

destination parameter

route command, 352

tracert command, 356

detailed documentation, preventing attacks, 431-432

detection devices, 437

devices. *See also components*

CPE, 267

credentials, changing, 438

full-duplex/half-duplex mode, 123

hardening, 438

IDS/IPS

active, 455

anomaly-based, 457

passive, 455

policy-based, 457

signature-based, 456

infrastructure, 79

bridges, 81-82

characteristics, 91

hubs, 80

multilayer switches, 89-90

routers, 90

switches, 85-89

switches. *See switches*

ISDNs, 262

NAS storage, 22

physical security, 437-438

placement, 384

sources of WLAN interference, 289

specialized, 91

content engines, 99

content switches, 100-101

DHCP servers, 96-98

DNS servers, 93-96

firewalls, 92-93

next-generation firewall, 101

proxy servers, 98-99

software-defined networking, 101

VPN concentrators, 91-92

wireless range extenders, 101

switches

forwarding Telnet segments, 87

Layer 3, 89

virtual, 101

cloud computing, 105-106

desktops, 104

firewalls, 103

off-site, 105

routers, 103

SDN, 107

servers, 101-103

switches, 103

DHCP (Dynamic Host Configuration Protocol), 54, 96

exhaustion, 495

IPv4 address assignment, 173-174

leases, releasing/renewing, 342

servers, 96-98

IP addressing, 97

relay agents, 98

reservations, 98

rogue, 495

snooping, 439

DHCPv6 (DHCP for IPv6), 193

diagnosing problems, 482-483

diagraming, 390-391

dictionary attacks, 421

differential backups, 311

differentiated service code point (DSCP), 318

DiffServ (differentiated services), 317

diffusing update algorithm (DUAL), 219

dig command, 362

Digital Signal 1 (DS1), 246

Digital Signal 3 (DS3), 247

digital subscriber line (DSL), 250

Dijkstra's shortest path first algorithm, 218

directly connected routes, 209-210

direct-sequence spread spectrum (DSSS), 284

disabling SSID broadcasts, 294

disaster recovery (DR) plans, 427

discard eligible (DE) bits, 263

discovery (routes), 43

displaying binary data, 36
 distance-vector routing protocols, 216-218
 distributed control systems (DCSs), troubleshooting, 500
 distributed denial-of-service (DDoS) attacks, 423
 distribution, cables, 75-77
 distribution trees
 multicast, 226
 shared, 229
 source, 227
 SPT switchover, 230
 DLCIs (data-link connection identifiers), 263
 DLP (data loss prevention), 469-470
 DMVPN (Dynamic Multipoint VPN), 268
DMZ (DEMILITARIZED) zone (firewalls), 446
 DNAT (dynamic NAT), 222
 DNS (Domain Name System), 54
 advanced TCP/IP settings, 171
 FQDN translation, 167
 incorrect configuration, 495
 servers, 93-96
 dynamic, 95
 extension mechanisms, 96
 FQDNs, 94
 hierarchy, 94
 IP addresses, 95-96
 record types, 94-95
 DNS-SD (DNS-based Service Discovery), 175
 DNS DOCSIS (Data-Over-Cable Service Interface Specification), 255
 documentation, 390, 391
 chain of custody, 433
 preventing attacks, 431-432
 DoD model. *See* TCP/IP stack
 Domain Name System. *See* DNS
 DoS (denial-of-service) attacks, 422-423
 dotted-decimal notation, 161, 177-178
 downstream data frequencies, 255
 DR (disaster recovery) plans, 427

drawbacks
 bus topology, 12
 client/server networks, 21
 distance-vector protocols, 216
 full-mesh topology, 17
 hub-and-spoke topology, 16
 hubs, 80
 partial-mesh topology, 19
 peer-to-peer networks, 23
 ring topology, 14
 star topology, 15
 drops, 314
DS1 (Digital Signal 1), 246
DS3 (Digital Signal 3), 247
DSCP (differentiated service code point), 318
DSL (digital subscriber line), 250-254
 asymmetric, 252-254
 dial tone, confirming, 381
 symmetric, 254
 very high bit-rate, 254
DSSS (direct-sequence spread spectrum), 284
DTLS (Datagram Transport Layer Security), 400
DUAL (diffusing update algorithm), 219
dual stack (IPv6 addresses), 192
duplex mismatches, troubleshooting, 488
duplicate IP addresses, 495
duplicate MAC addresses, 495
duplicating problems, 483
DWDM (dense wavelength-division multiplexing), 256
dynamic configuration (IPv4 addresses), 172
dynamic DNS (DDNS), 95
Dynamic Host Configuration Protocol *See* DHCP
Dynamic Multipoint VPN (DMVPN), 268
dynamic NAT (DNAT), 222
dynamic routes, 211-213
dynamic routing protocols, 503

E

e parameter (netstat command), 346
E1 circuits WANs, 247
E3 circuits WANs, 247
EAP (Extensible Authentication Protocol)
 IEEE 802.1X security, 295
 remote-access security, 441
EAP-FAST (EAP-Flexible Authentication via Secure Tunneling), 295
EAP-TLS (EAP-Transport Layer Security), 295
EAP-TTLS (EAP-Tunneled Transport Layer Security), 295
EBCDIC (Extended Binary Coded Decimal Interchange Code), 48
edge label switch routers (ELSRs), 267
EDNS (Extension Mechanisms for DNS), 96
EGPs (Exterior Gateway Protocols), 215
EIGRP (Enhanced Interior Gateway Routing Protocol), 219, 503
electric power lines, 244
electrical disturbance attacks, 425-426
electrical surges, 425
electromagnetic interference (EMI) interceptions, 417
electrostatic discharge (ESD) wrist straps, 383-384
ELSRs (edge label switch routers), 267
emanations, 417
EMI (electromagnetic interference), 417
 coaxial cables, 64
 fiber-optic cables, 70
Encapsulating Security Payload (ESP), 451-452
encapsulation, 521
encryption
 AH versus ESP, 451
 asymmetric, 412-413
 defined, 411
 keys, 411-412
 presentation layer, 48

SNMP messages, 395
 symmetric, 411
 VPN concentrators, 92

end-of-chapter reviews, 531

end-user policies, preventing attacks, 431

endpoints, sending Telnet segments, 86

Enhanced Interior Gateway Routing Protocol (EIGRP), 219, 503

enterprise-class WLANs, 276

Enterprise mode (WLANs), 297

environmental monitors, 384-385

ephemeral ports, 54

errors

- bits, 380
- collisions, 12
- controlling, 40
- detection, 249, 380

ESD (electrostatic discharge) wrist straps, 383-384

ESF (extended super frame), 247

ESP (Encapsulating Security Payload), 451-452

ESS (extended service set) WLANs, 288

ESSID (extended service set identifier), 293

eth_addr parameter (arp command), 339, 360

EtherChannel, 137

Ethernet

- 10BASE2, 118
- 10BASE5, 118
- 10BASE-T, 119
- bandwidth, 124
- collisions, 120-122
- connectors, 124
- CSMA/CA, 122
- CSMA/CD, 121-123
- development, 118
- frames, 118
- hubs, 80
- origins, 118-119
- shared bus topology, 120
- standards, 124-125
- switches, 126
- access port configuration, 128
- broadcast storms, 132-133

diagnostics, 145
 first-hop redundancy, 144
LACP configuration, 137
link aggregation, 136-137
MAC address filtering, 145
MAC address table corruption, 131-132
management access, 142-143
PoE, 138-139
port mirroring, 141
port monitoring, 139-140
ports on same subnet, 126
QoS, 145
STP, 130-135
trunking, 129-130
trunk port configuration, 130
user authentication, 141-142
VLANs, 127
 VLANs, 127-128
 WANs, 248

EUI-64 (Extended Unique Identifier), 193

Euro-DOCSIS, 255

evil twins, 422

exam preparation tools

- companion website, 529-530
- end-of-chapter reviews, 531
- exam taking strategies, 533-535
- memory tables, 530
- performance-based questions, 531
- suggested study plan, 531-533
- training videos, 530

exam taking strategies, 533-535

exceeding traffic, 321

excess burst (Be) parameter, 321

exhausted DHCP scope, 495

expired IP addresses, 495

export controls, 474

Extended Authentication (XAUTH) protocol, 451

Extended Binary Coded Decimal Interchange Code (EBCDIC), 48

extended service set (ESS) WLANs, 288

extended service set identifier (ESSID), 293

extended super frame (ESF), 247

Extended Unique Identifier (EUI-64), 193

extending classful masks, 179

Extension Mechanisms for DNS (EDNS), 96

Extensive Authentication Protocol.
See EAP

Exterior Gateway Protocols (EGPs), 215

external routing protocols, 503

F

f parameter

- arp command, 360
- netstat command, 346
- ping command, 350
- route command, 352

failures

- fault-tolerant design, 307-308
- logins on vty lines, troubleshooting, 511-514

MTBF, 306

single points, 307

fair use policies

fast Ethernet

fat configurations (APs)

fault-tolerant design

FCC (Federal Communications Commission)

FCoE (Fibre Channel over Ethernet)

FDDI (Fiber Distributed Data Interface)

FDM (frequency-division multiplexing)

FEP (fluorinated ethylene polymer)

FHSS (frequency-hopping spread spectrum)

fiber-optic cables

MMF, 70-72

mode of propagation, 71

polishing styles, 74

SMF, 72-74

WANs, 244

Fibre channel

Fibre Channel over Ethernet (FCoE)

files, remote access

File Transfer Protocol. *See FTP*

filtering
 MAC addresses, 145, 294
 packets, 364
 stateful, 515

firewalls, 92-93, 442
 hardware, 443
 incorrect host-based settings, 495
 packet-filtering, 443-444
 software, 442
 stateful, 93, 444, 515
 troubleshooting, 514
 UTM, 446-447, 515
 virtual, 103
 virtual wire, 514
 zones, 445-446

firing employees, 473

first-hop redundancy, 144

five nines of availability, 130, 415

flash card mode (Pearson Test Prep Practice Test engine), 532

flooding
 ARP requests, 84
 PIM-DM, 227

flow control, 40, 43

fluorinated ethylene polymer (FEP), 70

FM (frequency modulation), 36

forensics (computer), 433

formatting
 data, 48
 IPv4 addresses, 161-163
 IPv6 addresses, 193
 TCP segments, 51

forwarding
 ARP replies, 85-86
 ports, 220
 Telnet segments, 86-87

forwarding state, 135

fox and hound, 390

FQDNs (fully qualified domain names), 93-94
 DNS translation, 167
 resolving to IP addresses, 362-363

fragility (data), 433

Frame Relay, 262-263

Frame Relay Traffic Shaping (FRTS), 263

frames
 Ethernet, 118
 extended super, 247
 jumbo, 103
 MPLS labels, 268
 super, 247

frequencies
 2.4GHz band, 282
 5GHz band, 283
 bands, 281
 cable modems, 255
 center, 284
 channels, 281
 DOCSIS, 255
 modulation (FM), 36
 sources of interference, 289-291
 transmission methods, 284
 WLANs, 281

frequency-division multiplexing (FDM), 38

frequency-hopping spread spectrum (FHSS), 284

FRTS (Frame Relay Traffic Shaping), 263

FTP (File Transfer Protocol), 55
 bounce attacks, 418
 remote file access, 400

FTPS (FTP over SSL), 400

full backups, 311

full-duplex mode, 123

full-mesh topology, 17

fully qualified domain names. *See* FQDNs

G

g parameter
 arp command, 338
 PathPing command, 358

gain, 279

gas attacks, 426

Gateway Load Balancing Protocol (GLBP), 310

gateway parameter (route command), 352, 370

gateways
 default, 144, 167
 incorrect default, 495
 VoIP networks, 108

gathering information (troubleshooting), 483

GBICs (gigabit interface converters), 124

Generic Flow Control (GFC), 264

generic routing encapsulation (GRE), 451

geofencing, 297

geographic dispersion of networks, 7-9

get messages, 393

GFC (Generic Flow Control), 264

gigabit Ethernet, 124

gigabit interface converters (GBICs), 124

GLBP (Gateway Load Balancing Protocol), 310

global positioning system (GPS), 297

Global System for Mobiles (GSM), 244

GNU Privacy Guard (GPG), 411

goodput, 290

governing policies, preventing attacks, 430

PGP (GNU Privacy Guard), 411

GPS (global positioning system), 297

GRE (generic routing encapsulation), 451

GSM (Global System for Mobiles), 244

guidelines, preventing attacks, 432

H

h parameter (PathPing command), 358

H.323 protocol, 55

HA (high availability), 514

half-duplex mode, 123

hardening devices, 438

hardware
 firewalls, 443
 redundancy, 308-309, 313

hash-based message authentication codes (HMACs), 414

hashing, 395, 414

HDLC (High-Level Data Link Control), 246

Header Error Control (HEC), 264

headers

- ATM, 264-265
- authentication, 451-452
- compressing, 322
- IEEE 802.1Q, 129
- MPLS, 266
- TCP segments, 52
- UDP segments, 52

heat maps, 281

HEC (Header Error Control), 264

HFC (hybrid fiber-coax), 254

HIDS (host-based intrusion detection system), 455

high availability (HA), 514

- best practices, 311
- designing, 310-311
- measuring, 306

High-Level Data Link Control (HDLC), 246

High-Speed Packet Access (HSPA+), 245

high throughput (ht), 510

hijacking sessions, 422

HIPS (host-based intrusion prevention system), 455, 458

hiring employees, 473

HMACs (hash-based message authentication codes), 414

hold-down timers, 216

honeynets, 513

honeypots, 435, 513

hop counts, 212, 216

host addresses, 162, 180-181

host command, 363

host routing tables, viewing, 367

host-based firewalls, 442

host-based intrusion detection system (HIDS), 455

host-based intrusion prevention system (HIPS), 455, 458

hostname parameter (arp command), 360

hotspots, 276

HSPA+ (High-Speed Packet Access), 245

HSRP (Hot Standby Router Protocol), 144, 309

ht (high throughput), 510

HTTP (Hypertext Transfer Protocol), 53-55

HTTPS (Hypertext Transfer Protocol Secure), 55, 400

hub-and-spoke topology, 16

hubs, 6, 80

humidity attacks, 426

hybrid cloud services, 105

hybrid fiber-coax (HFC), 254

hybrid networks, 24

hybrid routing protocols, 219

Hypertext Transfer Protocol (HTTP), 53-55

Hypertext Transfer Protocol Secure (HTTPS), 55, 400

hypervisors, 102

I

i (isotropic), 279

i parameter

- arp command, 360
- PathPing command, 358
- ping command, 350

IaaS (infrastructure as a service), 105

IANA (Internet Assigned Numbers Authority), 164

IB (InfiniBand), 103

IBSS (independent basic service set) WLANs, 287

ICA (Independent Computing Architecture), 252, 440

ICANN (Internet Corporation for Assigned Names and Numbers), 164

ICMP (Internet Control Message Protocol), 46

- attacks, 424
- echo messages, 350-351

ICS (Internet connection sharing), 245

ICSS (industrial control systems), troubleshooting, 500

identifying problems, 485

IDF (independent distribution facility), 391

IDFs (intermediate distribution frames), 75-76

IDS (intrusion detection system), 454

- detection methods, 456-457
- devices, 455
- host-based, 458
- implementing, 517
- IPS, compared, 455-456
- network-based, 458

IEEE (Institute of Electrical and Electronics Engineers), 7

IEEE 802.1Q standard, 129

IEEE 802.1X standard, 141-142, 294, 440

IEEE 802.3. *See* Ethernet

IEEE 802.3af standard, 138

IEEE Registration Authority, 39

if parameter (route command), 352

if_addr parameter (arp command), 339

ifconfig command, 363-364

ifscope parameter (arp command), 360

IGMP (Internet Group Management Protocol), 224-226

IGMPv1, 224

IGMPv2, 224

IGMPv3, 225

IGPs (Interior Gateway Protocols), 215

IKE (Internet Key Exchange), 449-451

IKEv1, 450

IMAP (Internet Message Access Protocol), 55

IMAP4 (Internet Message Access Protocol Version 4), 55

implementing troubleshooting solutions, 486

in-band management, 509

incident response

- policies, 470-471
- preventing attacks, 432-433

incorrect AP placement, troubleshooting, 499

incorrect default gateways, 495

incorrect DNS configuration, 495

incorrect host-based firewall settings, 495

- incorrect subnet masks, 495
- incorrect time, 495
- incremental backups, 311
- independent basic service set (IBSS) WLANs, 287
- Independent Computing Architecture (ICA), 252, 440
- independent distribution facility (IDF), 391
- industrial control systems (ICSSs), troubleshooting, 500
- inet_addr parameter (arp command), 338
- InfiniBand (IB), 103
- infrared (IR), 79
- infrastructure as a service (IaaS), 105
- infrastructure audits by consultants, troubleshooting, 514-518
- infrastructure devices, 79
 - bridges, 81-82
 - characteristics, 91
 - hubs, 80
 - routers, 90
 - switches, 82-89
 - ARP replies sent from servers*, 85
 - bidirectional Telnet sessions*, 88
 - broadcast domains*, 88
 - endpoints sending ARP requests*, 83
 - endpoints sending Telnet segments*, 86
 - flooding ARP requests*, 84
 - forwarding ARP replies*, 85-86
 - forwarding Telnet segments*, 86
 - multilayer*, 89-90
- initiators
 - IPSec peers, 450
 - iSCSI, 103
- inside global addresses, 221
- inside local addresses, 221
- INSIDE zone (firewalls), 445
- insider attacks, 419
- inspecting traffic, 443-444
- Institute of Electrical and Electronics Engineers (IEEE), 7
- Integrated Services Digital Networks (ISDNs), 260
- integrated services (IntServ), 316
- integrity, 414
 - attacks, 419-422
 - botnets*, 421
 - brute force*, 421
 - data diddling*, 420
 - dictionary attacks*, 421
 - bijacking sessions*, 422
 - keyloggers*, 421
 - MitM*, 420
 - packet captures*, 421
 - password*, 421
 - salami*, 420
 - Trojan horses*, 421
 - trust relationship exploitation*, 420
 - hashing, 414
 - SNMP messages, 395
 - violations, 414
 - VPN traffic, 449
- interesting octets, 184, 325
- interfaces
 - functionality, confirming, 385
 - IP addresses, configuring, 364
- interference (WLANs), 289-291
- interior dynamic routing protocols, 503
 - Interior Gateway Protocols (IGPs), 215
- intermediate distribution frames (IDFs), 75-76
- Intermediate System-to-Intermediate System (IS-IS), 219
- international export controls, 474
- International Organization for Standardization (ISO), 31
- Internet access technologies, 521-522
- Internet Assigned Numbers Authority (IANA), 164
- Internet Connection Sharing (ICS), 245
- Internet Control Message Protocol. *See* ICMP
- Internet Corporation for Assigned Names and Numbers (ICANN), 164
- Internet Group Management Protocol (IGMP), 224-226
- Internet Key Exchange (IKE), 449-451
- Internet layer (TCP/IP stack), 50
- Internet Message Access Protocol (IMAP), 55
- Internet Message Access Protocol Version 4 (IMAP4), 55
- Internet of Things (IoT), 78-79
- Internet Protocol. *See* IP
- intranets, 167
- intrusion detection system. *See* IDS
- intrusion prevention system. *See* IPS
- IntServ (integrated services), 316
- inventory management, documenting, 391
- IoT (Internet of Things), 78-79
- IP (Internet Protocol)
 - helpers, 174
 - phones, 108
 - phone voice quality, troubleshooting, 501-504
 - precedence, 318
 - routing tables, 209
- IP addresses
 - assignable in subnets, 176
 - configuration parameters, displaying, 340
 - DHCP server, 97
 - DNS records pointing to, 95
 - duplicate, 495
 - expired, 495
 - FQDNs, resolving, 362-363
 - host, 180-181
 - interfaces, configuring, 364
 - leases, 98
 - listing, 347
 - loopback, 163
 - management (IPAM), 96
 - NAT classifications, 221
 - NAT names, 221
 - next-hop, 211
 - parameters, displaying, 340
 - ranges, calculating, 183-186
 - scopes, 98
 - target, specifying, 356
 - translation
 - NAT*, 220-222
 - PAT*, 222-224
- IP Address Manager subnet calculator, 189

IP small computer system interface (iSCSI), 103, 500, 504**IPAM (IP address management), 96****ipconfig command, 340-343****IPCP (IP control protocol), 249****IPS (intrusion prevention system), 454**

detection methods, 456-457

devices, 455

host-based, 458

IDS, compared, 455-456

implementing, 517

network-based, 458

IPSec (IP Security), 268

IKE modes/phases, 451

overlay networks, 268

remote access, 400

tunnels, 451

VPNs, 449

AH, 451-452 *ESP, 451-452* *IKE modes/phases, 449-451* *site-to-site example, 452-454***iptables command, 364****IPv4 (IP Version 4), 153, 161**

APIPA, 174-176

assignment, 164

available hosts, number of, 180-181

bits, 154

BOOTP protocol, 173

borrowed bits, 179

broadcast, 165

CIDR, 190-191

classes, 163

classful masks, extending, 179

components, 167-168

DHCP, 173-174

dotted-decimal notation, 161

dynamic configuration, 172

FQDN translation, 167

multicast, 166

network address calculation, 162

network/host address divisions, 162

private addressing, 164

ranges, calculating, 183-186

static configuration, 168-172

structure, 161-163

subnet masks, 161

subnet notation, 177-178

subnet octet values, 178

subnets created, number of, 180

transitioning to IPv6, 192

unicast, 165

IPv6 (IP Version 6), 153, 191

anycast, 195-196

bits, 154

features, 192

IPv4 transitions, 192

multicast, 195

NDP, 193

ping command, 352

records, 95

structure, 192-193

traceroute command, 366

tracert command, 358

types, 193

unicast, 194

IP Version 4. See IPv4**IP Version 6. See IPv6****IR (infrared), 79****iSCSI (IP small computer system interface), 103, 500, 504****ISDNs (Integrated Services Digital Networks), 260-262****IS-IS (Intermediate System-to-Intermediate System), 219****ISM bands, 281****isochronous transmissions, 40****ISO (International Organization for Standardization), 31****isotropic (i), 279****J-K****jitter, 314****jumbo frames, 103****Kerberos, 440****key fobs, 438****keyloggers, 421****keys**

encryption/decryption, 411

HMACs, 414

IKE, 449-451

PKI, 412

session, 411

L**L2F (Layer 2 Forwarding) protocol, 454****L2TP (Layer 2 Tunneling Protocol), 454****labels, 391**

MPLS frames, 268

switching, 266

label switch router (LSR), 267**LACP (Link Aggregation Control Protocol), 137****LAGs (link aggregation groups), 137****LANs (local area networks), 7**

virtual, 127-128

configuration, troubleshooting, 490 *native, 129* *segmentation, 439* *trunking, 129-130*

wireless, 8, 275

ad hoc, 276 *antennas, 278-281* *APs, 277-278* *attacks, 422* *BSS, 288* *cells, 291* *cellular technologies, 287* *channels, 281-283* *CSMA/CA, 283* *enterprise-class, 276* *ESS, 288* *frequencies, 281* *geofencing, 297* *hotspots, 276* *IBSS, 287* *mesh topology, 289* *networking issues, troubleshooting, 507-511* *personal mode, 294* *routers, 276-277* *security, 292-297* *sources of interference, 289-291* *standards, 285-286* *transmission methods, 284* *wireless AP placement, 291***latency, 313, 498****Layer 1, troubleshooting, 487-489**

bad cables/connections, 487

bad ports, 487

- cable placement, 488
- crosstalk, 488
- dB loss, 488
- distance limitations exceeded, 488
- example, 488-489
- opens/shorts, 487
- speed/duplex mismatches, 488
- splitting pairs in cables, 487
- transposed Tx/Rx leads, 488
- Layer 2**
 - Forwarding (L2F) protocol, 454
 - security protections, 439
 - troubleshooting, 490-491
 - Tunneling Protocol (L2TP), 454
- Layer 3**
 - Layer 2 mapping, 209
 - redundancy, 309-310
 - switches, 89
 - troubleshooting, 492-495
 - blocked TCP/UDP ports*, 495
 - data structures*, 492-494
 - duplicate IP address*, 495
 - duplicate MAC addresses*, 495
 - example*, 496-497
 - exhausted DHCP scope*, 495
 - expired IP addresses*, 495
 - incorrect ACL settings*, 495
 - incorrect default gateways*, 495
 - incorrect DNS configuration*, 495
 - incorrect host-based firewall settings*, 495
 - incorrect subnet masks*, 495
 - incorrect time*, 495
 - mismatched MTU*, 494
 - rogue DHCP servers*, 495
 - unresponsive services*, 495
 - untrusted SSL certificates*, 495
- layers**
 - OSI model, 32-33
 - application*, 48, 49
 - data link*, 38-41
 - listing of*, 33
 - network*, 41-43
 - order*, 34
 - physical*, 35-38
 - presentation*, 47-48
 - session*, 46-47
 - transport*, 44-46
- TCP/IP stack, 49-53
 - application*, 53
 - Internet*, 50
 - network interface*, 50
 - transport*, 51
- LC (Lucent connectors)**, 73
- LCP (Link Control Protocol)**, 249-250
- LDAP (Lightweight Directory Access Protocol)**, 55, 441
- LDAPS (Lightweight Directory Access Protocol over SSH)**, 55
- LEAP (Lightweight Extensible Authentication Protocol)**, 295
- learning state, 135
- leases, 98, 342
- LED (light emitting diodes), 70
- legal holds, 433
- LFI (link fragmentation and interleaving)**, 322
- licensing restrictions, 473
- light propagation, 72
- Lightweight Directory Access Protocol (LDAP)**, 55, 441
- Lightweight Directory Access Protocol over SSH (LDAPS)**, 55
- Lightweight Extensive Authentication Protocol (LEAP)**, 295
- Link Aggregation Control Protocol (LACP)**, 137
- link aggregation groups (LAGs), 137
- Link Control Protocol (LCP)**, 249-250
- link fragmentation and interleaving (LFI), 322
- Link Layer Discovery Protocol (LLDP)**, 520
- link-local IP addresses, assigning, 175
- link-state advertisements (LSAs), 218
- link-state routing protocols, 218
- links
 - aggregation, 136-137
 - efficiency, 322
 - high BER, 380
 - looped detection, 249
 - uplink congestion, 136
 - WANs, 7
- listening state, 135
- LLC (Logical Link Control sublayer)**, 40-41
- LLDP (Link Layer Discovery Protocol)**, 520
- LLQ (low-latency queuing)**, 319
- load balancing, 100, 312
- Local Area Connection properties**, 170
- Local Area Connection Status window**, 170
- local area networks. *See LANs*
- local authentication, 441
- local loops, 260
- locating network services, 175
- locks, 438
- logic bombs, 422
- logical addressing, 42
- logical diagrams, 391
- Logical Link Control (LLC sublayer)**, 40-41
- logical topologies**
 - MAC, 39
 - physical topology, compared, 10-11
- logins, failed attempts on vty lines, 511-514
- logs, 398-399
- long STP, 135
- Long-Term Evolution (LTE)**, 244
- looking-glass sites, 387
- loopback IP addresses, 163
- loopback plugs, 385
- looped link detection, 249
- loops
 - Layer 2, 490
 - local, 260
 - routing, 217-218
- Low Delay**, 316
- low-latency queuing (LLQ), 319
- Low Priority**, 316
- LSAs (link-state advertisements), 218
- LSR (label switch router), 267
- LTE (Long-Term Evolution)**, 244
- Lucent connectors (LC)**, 73

M**MAC (Media Access Control) addresses**

- duplicate, 495
- filtering, 145, 294
- table corruption, 131-132

MAC (Media Access Control) sublayer, 39

mail exchange (MX) records, 95

main distribution facility (MDF), 391

main distribution frames (MDFs), 77

main mode (IKE), 450

maintenance tools, 380

- BERT, 380
- butt sets, 381
- cable certifiers, 381
- cable testers, 382
- connectivity software, 382
- crimpers, 383
- electrostatic discharge wrist straps, 383-384
- environmental monitors, 384-385
- looking-glass sites, 387
- loopback plugs, 385
- multimeters, 385-386
- protocol analyzers, 386
- punch-down tool, 388
- speed testing, 388
- TDR, 389
- throughput tester, 388
- toner probes, 390
- Wi-Fi analyzer, 387

malicious intent, 511

malware, 418

management

- change, 391
- congestion, 319
- in-band, 509
- inventory, documenting, 391
- switches, 142-143

Management Information Base (MIB), 392

man command, 359

man-in-the-middle (MitM) attacks, 417, 420

MANs (metropolitan area networks), 9

marking (QoS), 318

mask netmask parameter (route command), 352

mask parameter (route command), 370

masks

- classful, 163
- subnet, 495

master service agreements (MSAs), 514

maximum transmission unit (MTU), 494

MD5 (message digest 5) algorithm, 414

MDF (main distribution facility) documentation, 391

MDFs (main distribution frames), 77

MDI (media-dependent interface ports), 69

MDIX (media-dependent interface crossover) ports, 69

mDNS (Multicast Domain Name Service), 175

means (attackers), 432

mean time between failures (MTBF), 306

measuring

- bandwidth, 123
- bit errors, 380
- gain, 279
- high-availability, 306

media, 64

cables

- coaxial*, 64-65
- distribution*, 75-77
- plenum/nonplenum*, 70
- twisted-pair*, 66-69

converters, 75

defined, 6

fiber-optic cables, 70

- MMF*, 70-72
- mode of propagation*, 71
- polishing styles*, 74
- SMF*, 72-74

WANs, 243

- physical*, 243-244
- wireless*, 244-245

wireless, 77

Media Access Control (MAC) sublayer, 39

media converters, 77

media-dependent interface (MDI) ports, 69

media-dependent interface crossover (MDIX) ports, 69

Media Gateway Control Protocol (MGCP), 55

media termination recommended jacks (MTRJs), 73

memorandum of understanding (MOU), 516

memory

- buffer overflow attacks, 424
- tables, 530

mesh cloud, 289

mesh topology, 289

mesh wireless topology, 20

message digest 5 (MD5) algorithm, 414

Message Integrity Check (MIC), 297

messages

- acknowledgment, 40
- ICMP echo, sending to target, 351
- PIM-DM pruning, 228
- SNMP, 393-394
- switching, 43
- syslog, 395-397

metric parameter (route command), 352

metro Ethernet, 248

metropolitan area networks (MANs), 9

MGCP (Media Gateway Control Protocol), 55

mGRE (multiple GRE) tunnels, 268

MIB (Management Information Base), 392

MIC (Message Integrity Check), 297

Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP), 250, 441

Microsoft RRAS (Routing and Remote Access Server), 251-252

microwave oven interference, 290

MIMO (multiple input, multiple output), 286, 510

Miredo, 192

mirroring ports, 140-141

misconfiguration of wireless parameters, 498

mismatched MTU, 494

MitM (man-in-the-middle) attacks, 417, 420

MMF (multimode fiber) cables, 70-72

mode of propagation, 71-72

mode selection (Pearson Test Prep Practice Test engine), 533

modulation, 36

modules, 490

monitoring

- environmental monitors, 384-385
- ports, 139-140
- switches, 145
- tools, 392
 - application logs*, 398
 - logs*, 398
 - security logs*, 399
 - SNMP, 392-395
 - syslog, 395-397
 - system logs*, 399

motion detection devices, 437

motives (attackers), 432

MOU (memorandum of understanding), 516

MPLS (Multiprotocol Label Switching), 8, 266-268

- elements, 266-267
- frame labels, 268
- headers, 266
- label switching, 266

MSAs (master service agreements), 514

MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol), 250, 441

MTBF (mean time between failures), 306

MTRJs (media-termination recommended jacks), 73

MTU (maximum transmission unit), mismatched, 494

multicast distribution trees, 226

Multicast Domain Name Service (mDNS), 175

multicast groups, 166, 224

multicast IPv4 addresses, 166

multicast IPv6 addresses, 195

multicast routing

- distribution trees, 226
- IGMP, 224-226
- PIM, 226
 - PIM-DM, 227-229
 - PIM-SM, 229-230

multifactor authentication, 441

multiframes, 247

multilayer switches, 89-90

multilink interfaces, 249

multimedia networks, troubleshooting, 500

multimeters, 385-386

multimode delay distortion, 72

multimode fiber cables (MMF cables), 70-72

multipath issues, 290

Multiprotocol label switching. *See* MPLS

multiple GRE (mGRE) tunnels, 268

multiple input, multiple output (MIMO), 286, 510

multiple paths of propagation, troubleshooting, 498

multiplexing, 38, 521

MUMIMO (multi-user MIMO), 510

MX (mail exchange) records, 95

N

n parameter

- arp command, 360
- nbtstat command, 344
- PathPing command, 358
 - ping command, 350

N parameter (arp command), 338

NaaS (network as a service), 105

NAC (Network Admission Control), 142, 440

names

- NAT IP addresses, 221
- NetBIOS
 - resolving*, 345
 - viewing*, 344
- PDUs, 34
- universal naming convention (UNC), 167

narrowband transmission, 284

NAS (network-attached storage devices), 22, 500

NAT (Network Address Translation), 220-222

native VLANs, 129

nbtstat command, 343-345

NCP (Network Control Protocol), 49

NDAs (non-disclosure agreements), 474

NDP (Neighbor Discovery Protocol), 193

near-end crosstalk (NEXT), 516

near field communication (NFC), 79

neighbor advertisements, 194

neighbor solicitations, 194

neighborships, 494

Nessus, 434

net parameter (route command), 370

NetBEUI (NetBIOS Extended User Interface), 47

NetBIOS (Network Basic Input/Output System), 47, 55

Extended User Interface (NetBEUI), 47

information, displaying, 343

names

- cache, viewing*, 344
- resolving*, 345

tables, viewing, 345

netstat command

- output, 347
- UNIX, 366-367
- Windows, 346-347

network addresses

- broadcast domains, 126
- calculating, 162
- IPv4 addresses, 162

Network Address Translation. *See* NAT

Network Admission Control (NAC), 142, 440

Network and Internet control panel, 168

Network as a Service (NaaS), 105

network-attached storage (NAS) devices, 22, 500

network-based firewalls, 442

network-based intrusion prevention system (NIPS), 455, 458

Network Basic Input/Output System. *See* **NetBIOS**

Network Connections window, 170

Network Control Protocol (NCP), 49

Network File System (NFS), 22, 500

Network Interface Cards (NICs), 308

network interface devices (NIDs), 260

network interface layer (TCP/IP stack), 50

network layer, 41-43, 492-495

- blocked TCP/UDP ports, 495
- data structures, 492-494
- duplicate IP address, 495
- duplicate MAC addresses, 495
- example, 496-497
- exhausted DHCP scope, 495
- expired IP addresses, 495
- incorrect ACL settings, 495
- incorrect default gateways, 495
- incorrect DNS configuration, 495
- incorrect host-based firewall settings, 495
- incorrect subnet masks, 495
- incorrect time, 495
- mismatched MTU, 494
- rogue DHCP servers, 495
- unresponsive services, 495
- untrusted SSL certificates, 495

network management system (NMS), 392

Network News Transport Protocol (NNTP), 55

network-node interfaces (NNIs), 265

network operating system (NOS), 22

network parameter (route command), 370

network termination 1s (NT1s), 262

Network Time Protocol (NTP), 55

networks, 7

- CANs, 9
- client/server, 21-22
- components, 5-7
- connections, 4

converged, 4

defined, 4

hybrid, 24

faults, 306

LANs. *See* **LANs**

MANs, 9

PANs, 9

peer-to-peer, 22-23

purpose, 4

resource locations, 21

SANs, 9

services, locating, 175

sniffers, 139, 386

topologies, 10

- bus*, 11
- characteristics/benefits/drawbacks*, 12
- full-mesh*, 17
- hub-and-spoke*, 16
- partial-mesh*, 18-19
- physical versus logical*, 10-11
- ring*, 11-14
- star*, 15
- wireless*, 20

WANs, 8

WLANs, 8

next-generation firewalls (NGFs), 447

next-hop IP addresses, 211

NEXT (near-end crosstalk), 516

NFC (near field communication), 79

NFS (Network File System), 22, 500

NGFs (next-generation firewalls), 447

NGFW (next-generation firewall), 101

NHRP (Next-Hop Resolution Protocol), 268

NICs (Network Interface Cards), 308

NIDs (network interface devices), 260

NIPS (network-based intrusion prevention system), 455, 458

Nmap utility, 365, 434

NMS (network management system), 392

NNIs (network-node interfaces), 265

NNTP (Network News Transport Protocol), 55

noAuthNo Priv security level, 394

nondesignated ports, 134-135

non-disclosure agreements (NDAs), 474

nonoverlapping channels, 282-283

nonplenum cables, 70

nonroot bridge switches, 133

nonstatistical anomaly detection, 457

no single points of failure, 307

NOS (network operating system), 22

notation

- dotted-decimal, 161
- prefix, 162
- subnet masks, 177-178

notifications

- backward explicit congestion, 263
- SNMP traps, 384

NS records, 95

nslookup command

- UNIX, 362
- Windows, 348-349

NT1s (network termination 1s), 262

NTP (Network Time Protocol), 55

numbering

- binary, 154
- converting
 - binary to decimal*, 155-158
 - decimal to binary*, 155-160
- dotted-decimal notation, 161
- prefix notation, 162

Nyquist theorem, 246

O

octets, 161

- interesting, 184, 325
- subnet mask values, 178

OFDM (orthogonal frequency-division multiplexing), 284

off-boarding best practices, 473

off-site virtual devices, 105

omnidirectional antennas, 279

on-boarding best practices, 473

on demand WANs, 240

OOB (out-of-band) management, 142, 401

open authentication, 294
Open Shortest Path First (OSPF), 212, 219, 503
Open Systems Interconnection. *See* **OSI model**
 opens, troubleshooting, 487
 opportunities (attackers), 433
 optical time domain reflectometer (OTDR), 389
optimization
 content caching, 312
 fault-tolerant design, 307–308
 hardware redundancy, 308–313
 high-availability
 best practices, 311
 design, 310–311
 measuring, 306
 Layer 3 redundancy, 309–310
 load balancing, 312
 QoS, 313
 classification, 318
 components, 316–317
 configuration, 315–316
 congestion, 319
 lack of bandwidth, 314–315
 link efficiency, 322
 marking, 318
 mechanisms, 317
 policing, 320
 shaping, 320–322
ordering OSI model layers, 34
organizationally unique identifiers (OUIs), 515
orthogonal frequency-division multiplexing (OFDM), 284
OSI (Open Systems Interconnection model), 31
 layers, 32–33
 application, 48–49
 data link, 38–41
 listing of, 33
 network, 41–43
 order, 34
 physical, 35–38
 presentation, 47–48
 session, 46–47
 transport, 44–46
 TCP/IP stack, 49
 application layer protocols, 53–56
 layers, 49–53

OSPF (Open Shortest Path First), 212, 219, 503
 ot sites, 313
OTDR (optical time domain reflectometer), 389
OUIs (organizationally unique identifiers), 515
outages (WANs), 505–507
out-of-band management (OOB), 142, 401
outside global addresses, 221
outside local addresses, 221
OUTSIDE zone (firewalls), 445
overlay networks, 268
overt channels, 418

P

P (provider) routers, 267
p parameter
 netstat command, 346
 PathPing command, 358
 route command, 352
PaaS (platform as service), 106
packets
 capturing
 attacks, 417, 421
 network sniffers, 139
 port mirroring, 140
 delay, 314
 drops, 314
 filtering
 firewalls, 443–444
 rules, 364
 GRE, 451
 ICMP echo, sending, 369
 jitter, 314
 LFI, 322
 loss, 358
 marking, 318
 reordering, 43
 shapers, 263
 sniffing, 417
 switched connections, 241
 switching. *See* **routing**
 tail dropped, 319
 transport mode, 452
 tunnel mode, 452
PANs (personal area networks), 9
PAP (Password Authentication Protocol), 249, 441
parameters
 arp command, 338, 360
 IP addresses, displaying, 340
 ipconfig command, 340
 nbtstat command, 344
 netstat command, 346, 366
 PathPing command, 358
 ping command, 350, 368
 route command, 352, 369
Pareto principal, 239
parity bits, 41
partial-mesh topology, 18–19
passive hubs, 80
passive IDS devices, 455
passive optical networks (PONs), 257
Password Authentication Protocol (PAP), 249, 441
passwords
 attacks, 421
 policies, 468–469
patches
 panels, 75
 preventing attacks, 428
 updates, compared, 429
path-vector routing protocols, 219
PathPing command, 358
PAT (Port Address Translation), 220–224
pattern generators, 380
Payload Type Indicator (PTI), 264
PBQs (performance-based questions), 531
PBX (private branch exchange), 106
 five nines of availability, 130
 VoIP networks, 108
PDUs (protocol data units), 34
PE (provider edge) routers, 267
PEAP-GTC (Protected EAP–Generic Token Card), 295
PEAP-MSCHAPv2 (Protected EAP–Microsoft Challenge Handshake Authentication Protocol version 2), 295

Pearson Test Prep Practice Test engine, 532

flash card mode, 532
mode selection, 533
practice exam mode, 532
study mode, 532

peer-to-peer networks, 22-23**performance-based questions (PBQs), 531****performance baselines, documenting, 391****permanent virtual circuits (PVCs), 263****personal area networks (PANs), 9****personal mode (WLANs), 294****PGP (Pretty Good Privacy) algorithm, 411****phishing, 419****physical addressing, 39****physical diagrams, 391****physical environment attacks, 426-427****physical layer, 35-38, 487-489****physical media (WANs), 243-244****physical obstacles (WLANs), 290****physical security devices, 437-438****physical topology, 10-11****PIM (Protocol Independent Multicast), 226****PIM-DM (PIM dense mode), 227-229****PIM-SM (PIM sparse mode), 229-230****ping command**

UNIX, 368-369
ICMP echo packets, sending, 369

parameters, 368

syntax, 368

Windows, 350-351
ICMP echo messages, sending to target, 351

IPv6, 352

parameters, 350

syntax, 350

unreachable destinations, 351

ping of death, 424**ping sweep attacks, 417****PKI (public key infrastructure), 412****placement**

APs, 499
cables, 488
devices, 384
wireless APs, 291

plain old telephone service (POTS), 258-260**plan of action (troubleshooting), 486****plans**

back-out, 486
incident response, 432-433

platform as a service (PaaS), 106**PLCs (programmable logic controllers), troubleshooting, 500****plenum cables, 70****PoE (Power over Ethernet), 138-139****pointer (PTR) records, 95****point-to-point connections, 246****Point-to-Point Protocol (PPP), 246, 249, 439****Point-to-Point Protocol over Ethernet (PPPoE), 250, 439****Point-to-Point Tunneling Protocol (PPTP), 454****poison reverse feature, 218****policies, 468**

acceptable use, 471
AUPs, 429
BYOD, 471, 506
DLP, 469-470
end-user, 431
governing, 430
incident-response, 470-471
passwords, 468-469
remote-access, 470
safety procedures, 472
security, 429
technical, 431

policing traffic, 320**policy-based detection, 457****polishing styles, 74****polyvinyl chloride (PVC), 70****PONs (passive optical networks), 257****POP3 (Post Office Protocol Version 3), 55****Port Address Translation (PAT), 220-224****portals, 441****ports**

access, 128
bad, 487
blocked TCP/UDP, 495
bonding, 137
configuration, 490
defined, 6
ephemeral, 54
forwarding, 220
locations, documenting, 391
MDI, 69
MDIX, 69
mirroring, 140-141
monitoring, 139-140
on switches on same subnet, 126
scans, 417
STP

costs, 134-135

states, 135

types, 133-134

switch port security, 517

trunk configuration, 130

well-known, 54

post-mortem reports, 486**Post Office Protocol Version 3 (POP3), 55****posture assessment, 440****POTS (plain old telephone service) connections, 258-260****power failures, 490****power faults, 425****Power over Ethernet (PoE), 138-139****power sags, 426****power spikes, 425****PPP (Point-to-Point Protocol), 246, 249, 439**

LCP, 249-250

Microsoft RRAS, 251

PPPoE (Point-to-Point Protocol over Ethernet), 250, 439**PPTP (Point-to-Point Tunneling Protocol), 454****practice exam mode (Pearson Test Prep Practice Test engine), 532****prefix notation, 162, 177-178****preparing for exam**

companion website, 529-530

end-of-chapter reviews, 531

- exam taking strategies, 533-535
- memory tables, 530
- performance-based questions, 531
- suggested study plan, 531-533
- training videos, 530
- presentation layer (OSI model), 47-48**
- preshared keys (PSKs), 293**
- Pretty Good Privacy (PGP) algorithm, 411**
- preventing**
 - attacks
 - ACLs*, 436-437
 - detailed documentation*, 431-432
 - end-user policies*, 431
 - governing policies*, 430
 - honey pots*, 435
 - incident response*, 432-433
 - Layer 2 protections*, 439
 - network device hardening*, 438
 - patching*, 428
 - physical devices*, 437-438
 - security policies*, 429
 - technical policies*, 431
 - user training*, 427-428
 - vulnerability scanners*, 433-435
 - data loss (DLP), 469-470
- prevention security devices, 437**
- print parameter (route command), 353**
- priority treatment, 316**
- PRI (primary rate interface) circuits, 261**
- private addresses, 222**
- private branch exchange (PBX), 106**
- private IP addressing, 164, 174**
- privileged user agreements (PUAs), 472-473**
- probable cause theory, 485**
- procedures, preventing attacks, 432**
- programmable logic controllers (PLCs), troubleshooting, 500**
- Protected EAP-Generic Token Card (PEAP-GTC), 295**
- Protected EAP-Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2), 295**
- protocol data units (PDUs), 34**
- Protocol Independent Multicast (PIM), 226**
- protocols**
 - AH, 451-452
 - analyzers, 386
 - Ant+, 78
 - application layer, 53-56
 - ARP, 83
 - BGP, 503
 - BOOTP, 173
 - CARP, 310
 - CCMP, 297
 - CHAP, 250, 441
 - DHCP, 54, 173-174
 - DHCPv6, 193
 - DNS, 54
 - dynamic routing, 503
 - EAP
 - IEEE 802.1X security*, 295
 - remote-access security*, 441
 - EGPs, 215
 - EIGRP, 503
 - ESP, 451-452
 - FTP, 55, 400
 - FTPS, 400
 - GLBP, 310
 - H.323, 55
 - HSRP, 144, 309
 - HTTP, 53-55
 - HTTPS, 55
 - ICMP, 46, 350, 424
 - IGMP, 224-226
 - IGPs, 215
 - IMAP, 55
 - IMAP4, 55
 - IPSec
 - AH, 451-452
 - ESP, 451-452
 - IKE modes/phases*, 449-451
 - site-to-site VPN example*, 452-454
 - VPNs, 449
 - Kerberos, 440
 - L2F, 454
 - L2TP, 454
 - LACP, 137
 - LCP, 249-250
 - LDAP, 55, 441
 - LDAPS, 55
 - LLDP, 520
- MGCP, 55
- MS-CHAP, 441
- NCP, 49
- NDP, 193
- NHRP, 268
- NNTP, 55
- NTP, 55
- OSPF, 503
- PAP, 249, 441
- PIM, 226
- PIM-DM, 227-229
- PIM-SM, 229-230
- POP3, 55
- PPP, 249, 439
 - LCP*, 249-250
 - Microsoft RRAS*, 251
- PPPoE, 250, 439
- PPTP, 454
- RADIUS, 440
- Rapid Spanning Tree, 131
- RARP, 174
- RDP, 55, 382, 439
- RIPv2, 503
- routing**
 - believability*, 214
 - BGP*, 219
 - distance-vector*, 216-218
 - EIGRP*, 219
 - interior versus exterior*, 215
 - IS-IS*, 219
 - link-state*, 218
 - metrics*, 214
 - OSPF*, 219
 - RIP*, 218
 - routed protocols, compared*, 213
 - route redistribution*, 220
- RTP, 55, 108
- RTSP, 56
- SCP, 56
- SFTP, 400
- SIP, 56, 108
- SLP, 175
- SMB, 56
- SMTP, 56
- SNMP, 56, 392-395
 - agents*, 392
 - components*, 392
 - managers*, 392
 - message types*, 393

MIB, 392
security enhancements, 394
trap, 56
walk, 393
SPB, 131
SSDP, 175
SSH, 400
SSL, 454
 statistics, displaying, 366
STP, 130-131
port costs, 134-135
port states, 135
port types, 133-134
switches, classifying, 133
TACACS+, 440
TCP, 44
Telnet, 400
TFTP, 56, 401
TKIP, 296
TLS, 454
 transport layer, 44
UDP, 44
VNC, 400
 VoIP networks, 107
VPNs, 454
VRRP, 310
VTP, 128
XAUTH, 451
Z-Wave, 78
provider (P) routers, 267
provider edge (PE) routers, 267
proxy servers, 98-99
pruning PIM-DM, 228
PSKs (preshared keys), 293-294
PSTN (Public Switched Telephone Network), 105, 258, 509
PTI (Payload Type Indicator), 265
PTR (pointer records), 95
PUAs (privileged user agreements), 472-473
 public addresses, 222
public key infrastructure (PKI), 412
Public Switched Telephone Network (PSTN), 105, 258, 509
punch down tools, 388
PVC (polyvinyl chloride), 70
PVCs (permanent virtual circuits), 263

Q

q parameter
PathPing command, 358
route command, 370
QoS (quality of service), 145, 313
 components, 316-317
configuration, 315-316
lack of bandwidth, 314-315
mechanisms, 317
classification, 318
congestion avoidance, 319
congestion management, 319
link efficiency, 322
marking, 318
policing, 320
shaping, 320-322
 switches, 145
 troubleshooting, 500
questioning users, 483
queue depth, 319
queuing, 319
quick mode (IKE), 450

R

r parameter
nbtstat command, 344
netstat command, 347, 367
R parameter (nbtstat command), 344
R reference points, 262
rack diagrams, 391
radio, 245
radio frequency identification (RFID), 79, 297
radio frequency interference. *See RFI*
RADIUS (Remote Authentication Dial-In User Service), 440
random early detection (RED), 319
ranges
 IP addresses, calculating, 183-186
 wireless extenders, 101
Rapid Spanning Tree, 131
RARP (Reverse Address Resolution Protocol), 174
RAS (Remote Access Server), 439
RC4 (Ron's Code), 296

RDP (Remote Desktop Protocol), 55, 382, 439
 access, troubleshooting, 518-521
 remote access, 400
Real-time Streaming Protocol (RTSP), 56
Real-time Transport Protocol (RTP), 55, 108
real transfer time, 45
receive (Rx) leads, 488
reconnaissance attacks, 417
records, 94-95
recrimping cables, 515
redirecting routers, 194
redistributing routes, 220
RED (random early detection), 319
redundancy
 hardware, 308-309, 313
 Layer 3, 309-310
 NICs, 308
reference points, 262
reflective DoS attacks, 423
refraction, 71
registries (IP addresses), 164
reject parameter (arp command), 360
relay agents, 98
release parameter (ipconfig command), 340-342
release6 parameter (ipconfig command), 340
releasing DHCP leases, 342
reliability
 availability, compared, 306
 hardware redundancy, 308-309
remote access, 400-401
 policies, 470
 RDP applications, troubleshooting, 518-521
 security, 439-442
 SQL Server database, troubleshooting, 504-505
 VPNs, 400, 448
Remote Access Server (RAS), 439
Remote Authentication Dial-In User Service (RADIUS), 440
remote desktop
 connections, 382
 control, 252

Remote Desktop Protocol (RDP), 55, 382, 439

remote shell (rsh), 55

rendezvous points (RPs), 229

renew6 parameter (ipconfig command), 340

renewing DHCP leases, 342

renew parameter (ipconfig command), 340, 343

reordering packets, 43

reporting problems, 482

reporting tools, 392

- logging, 398-399
- SNMP, 392-395
 - agents,* 392
 - components,* 392
 - managers,* 392
 - message types,* 393
 - MIB,* 392
 - security enhancements,* 394
 - walk,* 393
- syslog, 395-397

reservations (DHCP), 98

resolving problems, 482

resource locations, 21

- client/server, 21-22
- peer-to-peer, 22-23

Resource Reservation Protocol (RSVP), 316

resources (exam)

- companion website, 529-530
- end-of-chapter reviews, 531
- memory tables, 530
- performance-based questions, 531
- suggested study plan, 531-533
- training videos, 530

responders (IPSec peers), 450

responding to incidents

- policies, 470-471
- preventing attacks, 432-433

restricting licensing, 473

Reverse Address Resolution Protocol (RARP), 174

RFI (radio frequency interference), 64, 70

troubleshooting, 498

WLANs, 289-291

RFID (radio frequency identification), 79, 297

RG-6 cables, 65

RG-58 cables, 65

RG-59 cables, 64

ring topology, 11-14

RIP (Routing Information Protocol), 218

IPv2 (Routing Information Protocol version 2), 503

Rivest Cipher, 296

Rivest, Shamir, Adleman (RSA) algorithm, 412

RJ-11 (type 11 registered jack) connectors, 69

RJ-45 (type 45 registered jack) connectors, 69

rogue APs, 293, 422

rogue DHCP servers, 495

rollover cables, 68

Ron's Code (RC4), 296

root bridge switches, 133

root ports, 134

round-trip time (RTT), 45

route aggregation, 190-191

route command, 352-355

- add parameter, 355
- delete parameter, 354
- parameters, 352
- print parameter, 353
- syntax, 352
- UNIX, 369-370

routed protocols, 213

routers, 90

- active, 144, 310
- advertisements, 194
- black-hole, 494
- CE, 267
- defined, 6
- ELSRs, 267
- LSR, 267
- P, 267
- packet loss, 358
- PE, 267
- redirecting, 194
- solicitations, 193
- standby, 144, 310

virtual, 103, 310

wireless, 276-277

routing, 42

- address translation
 - NAT,* 220-222
 - PAT,* 222-224
- advertisements, 216-218
- basic process, 206-208
- convergence, 213
- directly connected routes, 209-210
- discovery, 43
- distribution trees, 226
 - shared,* 229
 - source,* 227
 - SPT switchover,* 230
- dynamic routes, 211-213
- IP routing tables, 209
- loops, 217-218
- multicast
 - IGMP,* 224-226
 - PIM,* 226
 - PIM-DM,* 227-229
 - PIM-SM,* 229, 230

protocols

- believability,* 214
- BGP,* 219
- distance-vector,* 216-218
- EIGRP,* 219
- interior versus exterior gateway,* 215
- IS-IS,* 219
- link-state,* 218
- metrics,* 214
- OSPF,* 219
- RIP,* 218
- routed protocols, compared,* 213
- route redistribution,* 220

route redistribution, 220

selection, 43

static routes, 210-211

tables

- contents, displaying,* 353
- directly connected routes,* 209-210
- dynamic routes,* 211-213
- entries, deleting,* 354
- routes, adding,* 355
- static routes,* 210-211
- UNIX host, viewing,* 367

Routing and Remote Access Server (RRAS), 439

Routing Information Protocol (RIP), 218

Routing Information Protocol version 2 (RIPv2), 503

RPs (rendezvous points), 229

RRAS (Routing and Remote Access Server), 251-252, 439

RSA (Rivest, Shamir, Adleman) algorithm, 412

rsh (remote shell), 55

RSVP (Resource Reservation Protocol), 316

RTP (Real-time Transport Protocol), 55, 108

RTP header compression (cRTP), 322

RTSP (Real-time Streaming Protocol), 56

RTT (round-trip time), 45

Rx (receive) leads, 488

S

s parameter

arp command, 339, 360
netstat command, 347, 367

S parameter

nbtstat command, 344
ping command, 351, 369

SaaS (software as a service), 105, 521-522

safety procedures policies, 472

salami attacks, 420

sanity checks (troubleshooting), 485

SANs (storage area networks), 9

SAs (security associations), 450

satellite connections, 257-258

satellites, 245, 258

SC (subscriber connector), 73

SCADA (supervisory control and data acquisition) networks, troubleshooting, 500, 505

scanner vulnerability, 433-435

scanning ports, 417

scope (DHCP), 173, 495

SCP (Secure Copy Protocol), 56

SDH (Synchronous Digital Hierarchy), 256

SDN (software-defined networking), 101, 107

SDSL (Symmetric DSL), 254

Secure Copy Protocol (SCP), 56

Secure Hash Algorithm 1 (SHA-1), 414

Secure Shell (SSH), 56, 400, 440

Secure Sockets Layer (SSL), 454

security

associations (SAs), 450

attacks

availability, 422-427

Bluetooth, 431

confidentiality, 415-419

integrity, 419-422

means, 432

motives, 432

opportunities, 433

availability

attacks, 422-427

five nines, 415

BC plans, 427

confidentiality, 410-411

attacks, 415-419

encryption, 411-413

DR plans, 427

encryption, 451

firewalls, 442

hardware, 443

packet-filtering, 443-444

software, 442

stateful, 444

UTM, 446-447

zones, 445-446

goals, 410

IDS/IPS

anomaly-based detection, 457

comparison, 455-456

host-based, 458

implementing, 517

network-based, 458

policy-based detection, 457

signature-based detection, 456

integrity, 414

attacks, 419-422

hash digests, 414

bashing, 414

bashing algorithms, 414

violations, 414

logs, 399

overlay networks, 268

policies, preventing attacks, 429

prevention

ACLs, 436-437

detailed documentation, 431-432

end-user policies, 431

governing policies, 430

honey pots, 435

incident response, 432-433

Layer 2 protections, 439

network device hardening, 438

patching, 428

physical devices, 437-438

security policies, 429

technical policies, 431

user training, 427-428

vulnerability scanners, 433-435

remote-access, 439-442

SNMP enhancements, 394

switch ports, 517

Trojan horses, 420

viruses, 420

VPNs, 447

authentication headers, 451-452

client-to-site, 448

concentrators, 449

encapsulating security payload, 451-452

IKE modes/phases, 449-451

IPSec, 449

IPSec site-to-site, 452-454

protocols, 454

site-to-site, 447

wiring closets, 516

WLANs, 292

MAC address filtering, 294

open authentication, 294

standards, 295

threats, 292-293

WEP, 296

WPA, 296-297

WPA2, 297

worms, 420

Security Event Management (SEM) software, 392

Security Information and Event Management (SIEM) software, 392

Security Information Management (SIM) software, 392

segments

- Ethernet, 122
- TCP, 51-52
- Telnet, 86-87
- UDP, 52
- VLANs, 439

Seifert, Rich, 33

SEM (Security Event Management) software, 392

sending

- ARP
 - replies from servers, 85*
 - requests, 83*
- Telnet segments, 86

sensitivity to weather conditions (satellites), 258

sequencing packets, 43

serialization delay, 322

Serial Line Internet Protocol (SLIP), 252

Server Message Block (SMB), 56

servers

- authentication, 142, 440
- BOOTPS, 173
- defined, 5
- DHCP, 96-98
 - IP address assignment, 97, 173-174*
 - relay agents, 98*
 - reservations, 98*
 - rogue, 495*
- DNS, 93-96
 - advanced TCP/IP settings, 171*
 - dynamic, 95*
 - extension mechanisms, 96*
 - FQDNs, 94*
 - hierarchy, 94*
 - IP addresses, pointing to, 95*
 - IP address management, 96*
 - record types, 94, 95*
- looking-glass sites, 387
- proxy, 98-99
- RAS, 439
- RRAS, 251-252, 439

 sending ARP replies, 85

 syslog, 396

 virtual, 101-103

 WINS, 167

service-level agreements (SLAs), 306

Service Location Protocol (SLP), 175

service location (SRV) records, 95

service set identifier (SSID), 293

services

- advertisements, 49
- Amazon Web Services (AWS), 106
- applications, 49
- cloud computing, 105-106
- connection, 43
- disruptions, troubleshooting, 516
- hybrid cloud, 105
- network, 175
- unresponsive, 495
- WAN, 521-522

Session Initiation Protocol (SIP), 56, 108

session layer (OSI model), 46-47

sessions

- bidirectional Telnet, 88
- hijacking, 422
- keys, 411
- maintenance, 46
- setting up, 46
- stateful inspection, 444
- TCP SYN floods, 423
- tearing down, 47

set messages, 393

severity levels, 396

SF (super frame), 247

SFTP (SSH File Transfer Protocol), 400

SHA-1 (Secure Hash Algorithm 1), 414

shaping traffic, 320-322

shared bus topology, 120

shared distribution trees, 229

shielded twisted pair. *See* STP cables

shim headers, 266

Shortest Path Bridging (SPB) protocols, 131

shortest path tree (SPT) switchover, 230

shorts, troubleshooting, 487

SIEM (Security Information and Event Management) software, 392

signal strength

- troubleshooting, 498
- WLANs, 290

signature-based detection, 456

Simple Mail Transfer Protocol (SMTP), 56

Simple Network Management Protocol. *See* SNMP

Simple Network Management Protocol Trap (SNMP Trap), 56

Simple Network Time Protocol (SNTP), 56

Simple Service Discovery Protocol (SSDP), 175

SIM (Security Information Management) software, 392

single-mode fiber (SMF) cables, 72-74

single sign-on (SSO), 441

SIP (Session Initiation Protocol), 56, 108

site-to-site VPNs, 400, 447

slash notation, 162, 177-178

SLAs (service-level agreements), 306

SLIP (Serial Line Internet Protocol), 252

slow Internet access, troubleshooting, 501-504

SLP (Service Location Protocol), 175

small office/home office (SOHO), 252

smart cards, 438

smart hubs, 80

smart jacks, 260

smartphones, tethering, 244

SMB (Server Message Block), 56

SMF (single-mode fiber) cables, 72-74

SMTP (Simple Mail Transfer Protocol), 56

Smurf attacks, 424

snapshots, 311

SNAT (static NAT), 222

SNMP (Simple Network Management Protocol), 56, 392-395

- agents, 392
- components, 392
- managers, 392
- message types, 393
- MIB, 392
- security enhancements, 394
- traps, 56, 384
- walk, 393
- SNMP Trap (Simple Network Management Protocol Trap), 56**
- snooping, 225**
- SNTP (Simple Network Time Protocol), 56**
- SOA (start of authority) records, 95**
- social engineering attacks, 418**
- software**
 - connectivity, 382
 - firewalls, 442
 - software as a service (SaaS), 105**
 - software-defined networking (SDN), 101, 107**
 - SOHO (small office/home office), 252**
 - SOHO network design case study, 323**
 - cost savings versus performance, 329
 - design, 324
 - environmental factors, 329
 - IP addressing, 325-326
 - Layer 1 media, 326
 - Layer 2 devices, 327
 - Layer 3 devices, 327-328
 - scenario, 323
 - suggested solution, 325
 - topology, 323, 329
 - wireless design, 328
 - soliciting**
 - neighbors, 194
 - routers, 193
 - SONETs (Synchronous Optical Network), 255-257**
 - source distribution trees, 227**
 - source-specific multicast (SSM), 225**
 - SOW (statement of work), 514**
 - spanning tree protection, 439**
 - Spanning Tree Protocol (STP), 130-131**
 - spatial multiplexing, 286**
- SPB (Shortest Path Bridging) protocol, 131**
- special-purpose networks, troubleshooting, 500**
- specialized devices, 91**
 - content engines, 99
 - content switches, 100-101
 - DHCP servers, 96-98
 - IP addressing*, 97
 - relay agents*, 98
 - reservations*, 98
 - DNS servers, 93-96
 - dynamic*, 95
 - extension mechanisms*, 96
 - FQDNs*, 94
 - hierarchy*, 94
 - IP addresses, pointing to*, 95
 - IP address management*, 96
 - record types*, 94-95
 - firewalls, 92-93
 - next-generation firewall, 101
 - proxy servers, 98-99
 - software-defined networking, 101
 - VPN concentrators, 91-92
 - wireless range extenders, 101
- speed mismatches, troubleshooting, 488**
- speed testing, 388**
- split-horizon feature, 218**
- spread spectrum, 284**
- SPSs (standby power supplies), 426**
- SPT (shortest path tree) switchover, 230**
- SQL Server database remote-access, troubleshooting, 504-505**
- SRV (service location) records, 95**
- SSDP (Simple Service Discovery Protocol), 175**
- SSH File Transfer Protocol (SFTP), 400**
- SSH (Secure Shell), 56, 400, 440**
- SSIDs (service set identifiers), 293-294, 498**
- SSL (Secure Sockets Layer), 454**
 - remote access, 400
 - untrusted certificates, 495
- SSM (source-specific multicast), 225**
- SSO (single sign-on), 441**
- standard Ethernet, 124**
- standards**
 - Ethernet, 124-125
 - operating procedures, documenting, 391
 - preventing attacks, 432
 - WLANs, 285-286
 - WLAN security, 295-297
- ST (straight tip) connectors, 73**
- standby power supplies (SPSs), 426**
- standby routers, 144, 310**
- star topology, 15**
- start of authority (SOA) records, 95**
- stateful filtering, 515**
- stateful firewalls, 93, 444, 515**
- stateful inspection, 444**
- statement of work (SOW), 514**
- states**
 - modulation, 36
 - ports, transitioning through, 135
 - transition modulation, 36
- static ARP entries, 361**
- static IPv4 addresses, 168-172**
- static NAT (SNAT), 222**
- static routes, 210-211, 370**
- statistical anomaly detection, 457**
- StatTDM (statistical time-division multiplexing), 38**
- steganography, 418**
- storage**
 - NAS, 22
 - virtual servers, 102
- storage area networks (SANs), 9**
- store-and-forward networks, 43**
- STP (shielded twisted pair) cables, 66**
 - ports
 - costs*, 134-135
 - states*, 135
 - types*, 133-134
 - switches, classifying, 133
- STP (Spanning Tree Protocol), 130-131**
- straight-through UTP cables, 68**
- straight tip (ST) connectors, 73**
- strategies for taking the exam, 533-535**

S/T reference points, 262

structure

- IPv4 addresses, 161-163
- IPv6 addresses, 192-193
- syslog messages, 397

structured troubleshooting approach, 484-486

- identifying the problem, 485
- plan of action, 486
- post-mortem reports, 486
- probable cause theory, 485
- solution, implementing, 486
- testing theories, 485
- verifying system functionality, 486

study mode (Pearson Test Prep Practice Test engine), 532

study plan, 531-533

sublayers (data link layer), 39-41

subnets, 126

- assignable IP addresses, 176
- calculators, 189
- masks
 - available hosts, number of*, 180-181
 - borrowed bits*, 179
 - CIDR, 190-191
 - classful*, 179
 - default*, 176
 - incorrect*, 495
 - IP address ranges, calculating*, 183-186
 - IPv4 addresses*, 161
 - notation*, 177-178
 - octet values*, 178
 - subnets created, number of*, 180
 - VLSM, 176
 - number created, calculating, 180

subscriber connectors (SC), 73

suggested study plan, 531-533

super frame (SF), 247

supervisory control and data acquisition (SCADA) networks, troubleshooting, 500

suplicants, 141, 440

SVCs (switched virtual circuits), 263

The Switch Book (Seifert), 33

switched virtual circuits (SVCs), 263

switches, 82-89

ARP replies sent from servers, 85

- bidirectional Telnet sessions, 88
- broadcast domains, 88
- broadcast storms, 132-133
- content, 100-101
- defined, 6
- diagnostics, 145
- endpoints sending ARP requests, 83
- endpoints sending Telnet segments, 86
- Ethernet, 126, 132
- first-hop redundancy, 144
- flooding ARP requests, 84
- forwarding ARP replies, 85-86
- forwarding Telnet segments, 86-87
- LACP configuration, 137
- Layer 3, 89
- link aggregation, 136-137
- MAC address
 - filtering*, 145
 - table corruption*, 131
- management access, 142-143
- multilayer, 89-90
- PoE, 138-139
- ports
 - access port configuration*, 128
 - mirroring*, 141
 - monitoring*, 139-140
 - same subnet*, 126
 - security*, 517
 - trunk configuration*, 130
- QoS, 145
- STP, 130-131
 - classifying*, 133
 - port costs*, 134-135
 - port states*, 135
 - port types*, 133-134
 - switches, classifying*, 133
- troubleshooting, 516
- trunking, 129-130
- user authentication, 141-142
- virtual, 103
- VLANs, 127

switching

- circuits, 42
- messages, 43
- network layer, 42
- packets. *See routing*

switchovers, 230

symbols (diagrams), 390

Symmetric DSL (SDSL), 254

symmetric encryption, 411

symptoms (problems), 483

synchronizing

- bits, 37
- transmissions, 40

synchronous bit synchronization, 37

Synchronous Digital Hierarchy (SDH), 256

Synchronous Optical Networks (SONETs), 255-257

synchronous transmissions, 41

syntax

- arp command, 338, 360
- ipconfig command, 340
- nbtstat command, 343
- netstat command, 346, 366
- nmap command, 365
- ping command, 350, 368
- route command, 352, 369

syslog, 395-397

- clients, 396
- message structure, 397
- servers, 396
- severity levels, 396

system

- functionality, verifying, 486
- life cycle best practices, 474
- logs, 399

T

t parameter (ping command), 350

T1 circuits WANs, 246-247

T3 circuits WANs, 247

TACACS+ (Terminal Access Controller Access-Control System Plus), 440

tail dropped, 319

taking the exam strategies, 533-535

tamper detection devices, 437

target IP addresses, specifying, 356

target_name parameter (ping command), 351, 369

TAs (Terminal adapters), 262

Tc (timing interval), 321

tcpdump command, 365

TCP (Transmission Control Protocol), 44

- ports, blocked, 495
- segments, 51-52
- SYN floods, 423

TCP/IP stack, 49

- application layer protocols, 53-56
- layers, 49-53
 - application*, 53
 - Internet*, 50
 - network interface*, 50
 - transport*, 51

TDM (time-division multiplexing), 38, 256

TDMA (Time Division Multiple Access), 244

TDR (time domain reflectometer), 389

TE1s (Terminal endpoint 1s), 262

TE2s (Terminal endpoint 2s), 262

teaming (NICs), 308

tearing down sessions, 47

technical policies, preventing attacks, 431

telcos, 260

Telecommunications Industry Association/Electronic Industries Alliance (TIA/EIA), 66

Telnet, 56

- remote access, 400
- segments, 86-87
- sessions, bidirectional, 88

temperature attacks, 426

Tempest rooms, 417

Temporal Key Integrity Protocol (TKIP), 296

temp parameter (arp command), 360

Tenable Network Security, 434

Terminal Access Controller Access-Control System Plus (TACACS+), 440

Terminal adapters (TAs), 262

Terminal endpoint 1s (TE1s), 262

Terminal endpoint 2s (TE2s), 262

Test Prep Practice Test engine, 532

- flash card mode, 532
- mode selection, 533

practice exam mode, 532

study mode, 532

testing

- DSL dial tone, 381
- IP connectivity, 350

tethering smartphones, 244

text DNS records, 95

TFA (two-factor authentication), 441

TFTP (Trivial File Transfer Protocol), 56, 401

thick configurations (APs), 511

thinnet, 118

third-party network connections, troubleshooting, 516

threats (WLANs), 292-293

throughput, increasing, 510

throughput testers, 388

TIA/EIA (Telecommunications Industry Association/Electronic Industries Alliance), 66

TIA/EIA-568-A standard, 66

TIA/EIA-568-B standard, 66

time, incorrect configuration, 495

Time Division Multiple Access (TDMA), 244

time-division multiplexing (TDM), 38, 256

time domain reflectometer (TDR), 389

Time-to-Live (TTL) fields, 131

timers, hold-down, 216

timing interval (Tc), 321

tip and ring wires, 260

TKIP (Temporal Key Integrity Protocol), 296

TLS (Transport Layer Security), 400, 454

token ring networks, 120

toner probes, 390

tools, 380

- BERT, 380
- butt sets, 381
- cable certifiers, 381
- cable testers, 382
- connectivity software, 382
- crimpers, 383
- environmental monitors, 384-385
- ESD wrist straps, 383-384

looking-glass sites, 387

loopback plugs, 385

monitoring, 392

- application logs*, 398
- logs*, 398
- security logs*, 399
- SNMP*, 392-395
- syslog*, 395-397
- system logs*, 399

multimeters, 385-386

protocol analyzers, 386

punch down, 388

speed testing, 388

TDR, 389

toner probes, 390

troughput tester, 388

Wi-Fi analyzers, 387

topologies, 10

- ATM, 265
- basic routing, 206-208
- bus, 11-12
- Ethernet shared bus, 120
- Frame Relay, 262
- full-mesh, 17
- HSRP, 144
- hub-and-spoke, 16
- IGMP, 225
- ISDNs, 261
- logical, 39
- MPLS, 266
- NAT, 220
- partial-mesh, 18-19
- PAT, 223
- physical versus logical, 10-11
- PPPoE, 250
- ring, 11-14
- star, 15
- VoIP networks, 107
- wireless, 20
- WLANs, 276

ToS (type of service) bytes, 318

traceroute command, 365-366

tracert command, 356-358

- destination parameter, 356
- IPv6, 358
- successful trace, 356
- unsuccessful trace, 357

traffic

- analysis, 386

- classes, 316
- conditioners, 320-322
- conforming, 321
- congestion avoidance/management, 319
- exceeding, 321
- firewall inspection, 443-444
- flow control, 43
- in-band management, 509
- multicast
 - distribution trees*, 226
 - IGMP*, 224-226
 - PIM*, 226
 - PIM-DM*, 227-229
 - PIM-SM*, 229-230
- policing, 320
- QoS issues, 314-315
- shaping, 320-322
- uplink congestion, 136
- VPN, 449
- training videos**, 530
- translation addresses**
 - NAT, 220-222
 - PAT, 222-224
- Transmission Control Protocol.**
 - See TCP*
- transmissions**
 - delay, 257
 - sensitivity to weather conditions, 258
 - synchronizing, 40
 - WLANs
 - methods*, 284
 - sources of interference*, 289-291
- transmit (Tx) leads**, 488
- transport layer**
 - OSI model), 44-46
 - TCP/IP stack, 51
- Transport Layer Security (TLS)**, 454
- transport mode (AH/ESP)**, 452
- transposed Tx/Rx leads**, 488
- trap messages**, 393
- Triple DES (3DES) algorithm**, 411
- Trivial File Transfer Protocol (TFTP)**, 56, 401
- Trojan horses**, 420-421
- trouble tickets**, 482
- troubleshooting**
 - brute-force attacks, 513
 - cables, 515
 - data link layer, 490-491
 - diagnosing problems, 482, 483
 - firewalls, 514
 - honeypots/honeynets, 513
 - Internet access technologies, 521-522
 - network layer, 492-495
 - blocked TCP/UDP ports*, 495
 - data structures*, 492-494
 - duplicate IP address*, 495
 - duplicate MAC addresses*, 495
 - example*, 496-497
 - exhausted DHCP scope*, 495
 - expired IP addresses*, 495
 - incorrect ACL settings*, 495
 - incorrect default gateways*, 495
 - incorrect DNS configuration*, 495
 - incorrect host-based firewall settings*, 495
 - incorrect subnet masks*, 495
 - incorrect time*, 495
 - mismatched MTU*, 494
 - rogue DHCP servers*, 495
 - unresponsive services*, 495
 - untrusted SSL certificates*, 495
 - physical layer, 487-488
 - bad cables/connections*, 487
 - bad ports*, 487
 - cable placement*, 488
 - crosstalk*, 488
 - dB loss*, 488
 - distance limitations exceeded*, 488
 - example*, 488-489
 - opens/shorts*, 487
 - speed/duplex mismatches*, 488
 - splitting pairs in cables*, 487
 - transposed Tx/Rx leads*, 488
 - questioning users, 483
 - reporting problems, 482
 - resolving problems, 482
 - scenarios
 - failed logins on vty lines*, 511-514
 - infrastructure audit by consultants*, 514-518
 - slow Internet access*, 501-504
 - SQL Server database remote-access*, 504-505
 - unacceptable IP phone voice quality*, 501-504
 - WAN connectivity outages*, 505-507
 - wireless networking issues*, 507-511
 - service disruptions, 516
 - special-purpose networks, 500
 - structured approach, 484-486
 - identifying the problem*, 485
 - plan of action*, 486
 - post-mortem reports*, 486
 - probably cause theory*, 485
 - solution, implementing*, 486
 - testing theories*, 485
 - verifying system functionality*, 486
 - switches, 145, 516
 - third-party network connections, 516
 - tools
 - BERT*, 380
 - butt sets*, 381
 - cable certifiers*, 381
 - cable testers*, 382
 - connectivity software*, 382
 - crimpers*, 383
 - environmental monitors*, 384-385
 - ESD wrist straps*, 383-384
 - looking-glass sites*, 387
 - loopback plugs*, 385
 - multimeters*, 385-386
 - protocol analyzers*, 386
 - punch down*, 388
 - speed testing*, 388
 - TDR*, 389
 - throughput tester*, 388
 - toner probes*, 390
 - Wi-Fi analyzers*, 387
 - trouble tickets, 482
 - WANs
 - access technologies*, 521-522
 - connectivity*, 517
 - RDP application access*, 518-521
 - wireless, 497-499
 - example*, 499-500
 - incorrect AP placement*, 499
 - latency*, 498
 - misconfiguration of wireless parameters*, 498
 - multiple paths of propagation*, 499
 - RFI*, 498
 - signal strength*, 498

trunking, 129-130

trusted malicious users, 511

trust relationship exploitation, 420

TTL (Time-to-Live) fields, 131

tunneling

- IPv6/IPv4, 192
- mGRE, 268

tunnel mode (AH/ESP), 452

twisted-pair cables, 66

- shielded, 66
- TIA/EIA-568-A standard, 66
- TIA/EIA-568-B standard, 66
- unshielded, 67-69

two-factor authentication (TFA), 441

Tx (transmit) leads, 488

TXT records, 95

type 11 registered jack (RJ-11) connectors, 69

type 45 registered jack (RJ-45) connectors, 69

type of service (ToS) bytes, 318

U

U reference points, 262

UC (unified communications), 107

UDP (User Datagram Protocol), 44

- ports, blocked, 495
- segments, 52

UNC (universal naming convention), 167

unicast IPv4 addresses, 165

unicast IPv6 addresses, 194

unidirectional antennas, 280

unified communications (UC), 107

unified threat management (UTM) firewalls, 446-447, 515

uninterruptible power supplies (UPSs), 426

UNIs (user-network interfaces), 265

universal naming convention (UNC), 167

UNIX

- benefits, 359
- commands, 358
- arp*, 360-361
- dig*, 362
- host*, 363

ifconfig, 363-364

iptables, 364

man, 359

netstat, 366

nmap, 365

nslookup, 362

ping, 368-369

route, 369-370

tcpdump, 365

traceroute, 365-366

unreachable destinations, ping command, 351

unresponsive services, 495

unshielded twisted pair. *See* UTP cables

untrusted SSL certificates, 495

updates

- APs, 516
- patches, compared, 429

uplink congestion, 136

UPSs (uninterruptible power supplies), 426

upstream data frequencies, 255

uptime, 306

User Datagram Protocol. *See* UDP

users

- authentication, 141-142
- network interfaces (UNIs), 265
- questioning, 483
- training, preventing attacks, 427-428
- trusted malicious, 511

utilities. *See* commands

UTM (unified threat management) firewalls, 446-447, 515

UTP (unshielded twisted pair) cables, 15, 66-69

- categories, 67
- connectors, 69
- star topology, 15
- straight-through, 68

WANs, 243

V

v parameter

- arp* command, 338
- route* command, 370

Variable-Length Subnet Masking (VLSM), 176

VCI (Virtual Circuit Identifier), 264

VCs (virtual circuits), 262

- ATM, 265
- Frame Relay, 262
- permanent virtual (PVCs), 263

VDSL (Very High Bit-Rate DSL), 254

vendor codes, 39

verifying system functionality, 486

video surveillance devices, 437

video teleconference (VTC), troubleshooting, 500

Virtual Circuit Identifier (VCI), 264

virtual circuits. *See* VCs

virtual desktops, 104

virtual devices, 101

- cloud computing, 105-106
- desktops, 104
- firewalls, 103
- off-site, 105
- routers, 103
- SDN, 107
- servers, 101-103
- switches, 103

virtual firewalls, 103

virtual LANs. *See* VLANs

virtual network computing (VNC), 252

Virtual Path Identifier (VPI), 264

virtual PBX, 106

virtual private networks. *See* VPNs

Virtual Router Redundancy Protocol (VRRP), 310

virtual routers, 103, 310

virtual servers, 101-103

virtual switches, 103

Virtual Teletype (pty), 508

virtual wire firewalls, 514

viruses, 420

VLAN Trunking Protocol (VTP), 128

VLANs (virtual LANs), 127-128

- configuration, troubleshooting, 490
- native, 129
- segmentation, 439
- trunking, 129-130

VLSM (Variable-Length Subnet Masking), 176

VNC (virtual network computing), 252, 400

VoIP (Voice over IP), 106

devices/protocols, 107

topology, 107

troubleshooting, 500

VPI/VCI pairs, 265

VPI (Virtual Path Identifier), 264

VPNs (virtual private networks), 91, 268, 447

authentication headers, 451-452

client-to-site, 448

concentrators, 91-92, 449

encapsulating security payload, 451-452

IKE modes/phases, 449-451

IPSec site-to-site, 452-454

overlay networks, 268

protocols, 454

remote access, 400

security, 449

site-to-site, 447

VRRP (Virtual Router Redundancy Protocol), 310

VTC (video teleconference), troubleshooting, 500

VTP (VLAN Trunking Protocol), 128

vty (Virtual Teletype), 508, 511-514

vulnerability scanners, 433-435

W

Wallace, Kevin, 530

WANs (wide area networks), 7-8

access technologies, 521-522

ATM, 264-265

cable modems, 254-255

connections, 240-242

circuit-switched, 241

dedicated leased line, 240

outages, troubleshooting, 505-507

packet-switched, 241

troubleshooting, 517

CSU/DSU, 248

data rates, 242-243

dedicated leased line, 246

DSL, 252-254

E1 circuits, 247

E3 circuits, 247

Frame Relay, 262-263

full-mesh topology, 17

hub-and-spoke topology, 16

ISDNs, 260-262

links, 7

media, 243

physical, 243-244

wireless, 244-245

metro Ethernet, 248

MPLS, 266-268

elements, 266-267

frame labels, 268

headers, 266

label switching, 266

on demand, 240

overlay networks, 268

partial-mesh topology, 18-19

POTS, 258-260

PPP, 249-250

PPPoE, 250

RDP application access, troubleshooting, 518-521

RRAS, 251-252

satellites, 257-258

SONETs, 255-257

T1 circuits, 246-247

T3 circuits, 247

WAPs (wireless access points), 20, 277-278

war chalking, 292

war driving, 422

warm sites, 313

websites

companion, 529

accessing, 530

memory tables, 530

performance-based questions, 531

training videos, 530

IEEE Registration Authority vendor codes, 39

IP Address Manager, 189

Nessus, 434

Nmap utility, 434

Wireshark, 139, 387, 417

weighted fair queuing (WFQ), 319

weighted round-robin (WRR), 319

well-known ports, 54

WEP (Wired Equivalent Privacy), 293, 296

WFQ (weighted fair queuing), 319

wide area networks. *See WANs*

Wi-Fi analyzers, 387-388

Wi-Fi Protected Access (WPA), 293

WiMAX (Worldwide Interoperability for Microwave Access), 245

Windows

Command Prompt, accessing, 338

commands, 338

arp, 338-340

ipconfig, 340-343

nbtstat, 343-345

netstat, 346-347

nslookup, 348-349

PathPing, 358

ping, 350-352

route, 352-355

tracert, 356-358

control panel, 168

Internet Name Service (WINS) servers, 167

WINS (Windows Internet Name Service) servers, 167

Wired Equivalent Privacy (WEP), 293, 296

wireless

access points (WAPs), 20, 277-278, 291

attacks, 422

IoT technologies, 78-79

LAN controllers (WLCs), 506

local area networks. *See WLANs*

media, 244-245

PAN networks (WPANs), 9

range extenders, 101

routers, 276-277

security system devices interference, 290

service disruptions, troubleshooting, 516

technologies, 77

topologies, 20

troubleshooting, 497-499

example, 499-500

incorrect AP placement, 499

latency, 498

- misconfiguration of wireless parameters*, 498
- multiple paths of propagation*, 499
- networking issues*, 507-511
 - RFI*, 498
 - service disruptions*, 516
 - signal strength*, 498
- Wireshark**, 139, 387, 417
- wiretapping**, 417
- wiring closets**, 75, 516
- wiring locations**, documenting, 391
- WLANs (wireless LANs)**, 8, 275
 - ad hoc, 276
 - antennas, 278-281
 - gain*, 279
 - omnidirectional*, 279
 - orientation*, 281
 - selecting*, 279
 - unidirectional*, 280
 - APs, 277-278
 - attacks, 422
 - BSS, 288
 - cells, 291
 - cellular technologies, 287
 - channels, 281-283
 - CSMA/CA, 283
 - enterprise-class, 276
 - ESS, 288
 - frequencies, 281
 - geofencing, 297
 - hotspots, 276
 - IBSS, 287
 - mesh topology, 289
 - networking issues, troubleshooting, 507-511
 - personal mode, 294
 - routers, 276-277
 - security, 292
 - MAC address filtering*, 294
 - open authentication*, 294
 - standards*, 295
 - threats*, 292-293
 - WEP*, 296
 - WPA*, 296-297
 - WPA2*, 297
 - sources of interference, 289-291
 - standards, 285-286
 - transmission methods, 284
 - wireless AP placement, 291
- WLCs (wireless LAN controllers)**, 506
- work instructions**, documenting, 391
- Worldwide Interoperability for Microwave Access (WiMAX)**, 245
- worms**, 420
- WPA (Wi-Fi Protected Access)**, 293, 296-297
- WPA2 (WPA Version 2)**, 297
- WPAN (wireless PAN networks)**, 9
- w parameter (PathPing command)**, 358
- WRR (weighted round-robin)**, 319

X-Z

- XAUTH (Extended Authentication) protocol**, 451
- Z-Wave protocol**, 78
- Zero Configuration (Zeroconf)**, 175
- zombies**, 421
- zones (firewalls)**, 445-446