



Save 10%  
on Exam  
Voucher

See Inside

# 31 Days Before Your CompTIA® Network+ Certification Exam



A Day-By-Day Review Guide  
for the N10-006 Certification Exam

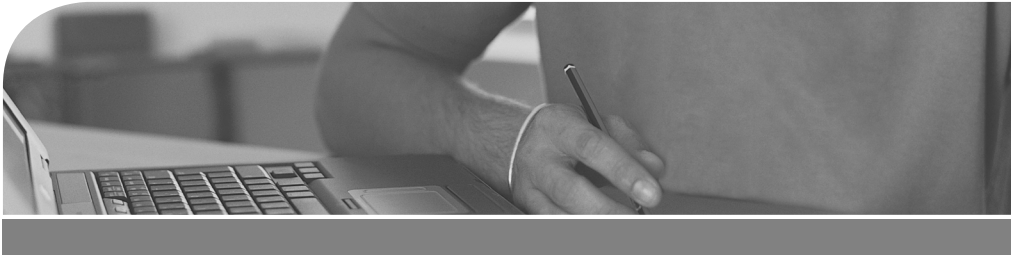
PEARSON IT  
CERTIFICATION

ALLAN JOHNSON

FREE SAMPLE CHAPTER



SHARE WITH OTHERS



# **31 Days Before Your** CompTIA Network+ Certification Exam

Allan Johnson

# 31 Days Before Your CompTIA Network+ Certification Exam

Copyright © 2016 by Pearson Education, Inc.

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: 978-0-7897-5647-3

ISBN-10: 0-7897-5647-1

Library of Congress Control Number: 2015957629

Printed in the United States of America

First Printing: February 2016

## 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

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 provided is on an “as is” basis. The author and the publisher 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.

## 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](mailto:corpsales@pearsoned.com) or (800) 382-3419.

For government sales inquiries, please contact [governmentsales@pearsoned.com](mailto:governmentsales@pearsoned.com).

For questions about sales outside the U.S., please contact [intlcs@pearson.com](mailto:intlcs@pearson.com).

<b>Associate Publisher</b>	Dave Dusthimer
<b>Executive Editor</b>	Mary Beth Ray
<b>Development Editor</b>	Andrew Cupp
<b>Managing Editor</b>	Sandra Schroeder
<b>Senior Project Editor</b>	Tonya Simpson
<b>Copy Editor</b>	Bart Reed
<b>Indexer</b>	Lisa Stumpf
<b>Proofreader</b>	Laura Hernandez
<b>Technical Editor</b>	Chris Crayton
<b>Publishing Coordinator</b>	Vanessa Evans
<b>Cover Designer</b>	Mark Shirar
<b>Compositor</b>	Studio Galou

# Contents at a Glance

<b>Introduction</b>	<b>xx</b>
<b>Day 31: Network Devices</b>	<b>1</b>
<b>Day 30: Network Services and Applications</b>	<b>9</b>
<b>Day 29: WAN Technologies</b>	<b>23</b>
<b>Day 28: Cable Installation</b>	<b>37</b>
<b>Day 27: Network Topologies and Infrastructure</b>	<b>49</b>
<b>Day 26: Implement IPv4 Addressing</b>	<b>63</b>
<b>Day 25: Implement IPv6 Addressing</b>	<b>75</b>
<b>Day 24: Routing Concepts</b>	<b>87</b>
<b>Day 23: Unified Communications, Virtualization, and Cloud</b>	<b>101</b>
<b>Day 22: Network Design and Documentation</b>	<b>117</b>
<b>Day 21: Network Monitoring and Metrics</b>	<b>125</b>
<b>Day 20: Network Segmentation, Patches, and Updates</b>	<b>137</b>
<b>Day 19: Switch Configuration</b>	<b>141</b>
<b>Day 18: STP, VLANs, Trunking, and VTP</b>	<b>151</b>
<b>Day 17: WLAN Implementation</b>	<b>163</b>
<b>Day 16: Risks, Threats, and Vulnerabilities</b>	<b>177</b>
<b>Day 15: Hardening Devices</b>	<b>185</b>
<b>Day 14: Physical Security, Firewalls, Access Control, and Forensics</b>	<b>193</b>
<b>Day 13: Network Models</b>	<b>201</b>
<b>Day 12: Network Theory</b>	<b>207</b>
<b>Day 11: Wired and Wireless Standards</b>	<b>213</b>
<b>Day 10: Implement Policies, Procedures, and Safety Practices</b>	<b>219</b>
<b>Day 9: Best Practices and Change Management</b>	<b>223</b>
<b>Day 8: Implement Ports and Protocols</b>	<b>227</b>
<b>Day 7: Troubleshooting Methodology</b>	<b>235</b>
<b>Day 6: Troubleshooting Tools</b>	<b>239</b>
<b>Day 5: Troubleshoot Wireless Issues</b>	<b>255</b>
<b>Day 4: Troubleshoot Copper and Fiber Cabling Issues</b>	<b>259</b>
<b>Day 3: Troubleshoot Network Issues</b>	<b>263</b>
<b>Day 2: Troubleshoot Security Issues</b>	<b>267</b>
<b>Day 1: Troubleshoot WAN Issues</b>	<b>271</b>
<b>Exam Day</b>	<b>275</b>
<b>Post-Exam Information</b>	<b>277</b>
<b>Index</b>	<b>279</b>

---

# Contents

Introduction xx

## **Day 31: Network Devices 1**

CompTIA Network+ N10-006 Exam Topics 1

Key Topics 1

Common Network Devices 1

Specialty Devices 2

Firewalls 2

IDS and IPS 3

Proxy Server 5

Load Balancer 5

Packet Shaper 6

VPN Concentrator 6

Study Resources 7

## **Day 30: Network Services and Applications 9**

CompTIA Network+ N10-006 Exam Topics 9

Key Topics 9

VPN 9

Types 9

IPsec and IKE 11

Other VPN Technologies 12

Remote Access Services 12

AAA Services 13

Microsoft's RAS 14

Other Remote Access Services 14

Unified Communications 14

DHCP 15

DNS 17

NAT 18

Study Resources 20

## **Day 29: WAN Technologies 23**

CompTIA Network+ N10-006 Exam Topics 23

Key Topics 23

Packet Switching and Circuit Switching 23

WAN Link Options 24

Home and Small Office 25

Wireless 29

- SONET 30
- Dedicated Leased Lines 31
- Enterprise WANs 32

- Study Resources 35

**Day 28: Cable Installation 37**

- CompTIA Network+ N10-006 Exam Topics 37

- Key Topics 37

- Copper 37

- Copper Cables 37

- Copper Connectors 40

- Fiber 42

- Fiber-Optic Cables 43

- Fiber Connectors 44

- Media Converters 45

- Tools 45

- Study Resources 48

**Day 27: Network Topologies and Infrastructure 49**

- CompTIA Network+ N10-006 Exam Topics 49

- Key Topics 49

- Network Topologies 49

- Bus 49

- Ring 50

- Star, Extended Star, and Hub-and-Spoke 51

- Full and Partial Mesh 53

- Client-Server and Peer-to-Peer 55

- Network Infrastructures 57

- PANs 57

- LANs and WLANs 57

- CANs 58

- MANs 59

- WANs 59

- Other Network Infrastructures 59

- Industrial Networks 59

- Medianets 60

- Study Resources 61

**Day 26: Implement IPv4 Addressing 63**

- CompTIA Network+ N10-006 Exam Topics 63

- Key Topics 63

---

Local Addressing	63
MAC Addresses	63
Collision and Broadcast Domains	63
IPv4 Addressing	64
IPv4 Address Structure	64
Private and Public IP Addressing	66
IPv4 Address Types	66
Subnetting in Four Steps	68
Determine How Many Bits to Borrow	68
Determine the New Subnet Mask	69
Determine the Subnet Multiplier	69
List the Subnets, Host Ranges, and Broadcast Addresses	69
Subnetting Example 1	70
Subnetting Example 2	70
Subnetting Example 3	71
VLSM and Classless Addressing	71
Study Resources	74

### **Day 25: Implement IPv6 Addressing 75**

CompTIA Network+ N10-006 Exam Topics	75
Key Topics	75
IPv6 Addressing Overview	75
Representing the IPv6 Address	76
Conventions for Writing IPv6 Addresses	76
Conventions for Writing IPv6 Prefixes	77
IPv6 Address Types	78
Global Unicast Addresses	79
Link-Local Addresses	79
Configuring IPv6 Addressing	80
EUI-64 Concept	81
Stateless Address Autoconfiguration	82
Migration to IPv6	83
Dual-Stack	83
Tunneling	83
Study Resources	86

### **Day 24: Routing Concepts 87**

CompTIA Network+ N10-006 Exam Topics	87
Key Topics	87
Static and Default Routing Overview	87
Dynamic Routing Protocols	88
Route Redistribution	90
IGP and EGP Routing Protocols	90



- Distance Vector Routing Protocols 90
- Link-State Routing Protocols 91
- Classful Routing Protocols 91
- Classless Routing Protocols 91
- Dynamic Routing Metrics 92
- Administrative Distance 93
- Routing Loop Prevention 94
- Link-State Routing Protocol Features 94
  - Building the LSDB 95
  - Calculating the Dijkstra Algorithm 95
  - Convergence with Link-State Protocols 96
- Route Aggregation 97
- High Availability 98
- Study Resources 99

**Day 23: Unified Communications, Virtualization, and Cloud 101**

- CompTIA Network+ N10-006 Exam Topics 101
- Key Topics 101
- Unified Communications 101
- Quality of Service 105
- Virtualization 107
  - Server Virtualization 108
  - Networking Device Virtualization 109
  - Software-Defined Networking 110
- Cloud Concepts 111
- Storage Area Networks 112
  - Directly Attached Storage 112
  - Network-Attached Storage 112
  - Fibre Channel 113
  - Fibre Channel over Ethernet 113
  - iSCSI 114
- Study Resources 115

**Day 22: Network Design and Documentation 117**

- CompTIA Network+ N10-006 Exam Topics 117
- Key Topics 117
- Network Design 117
  - Sample Design Approach 117
  - Design Considerations for Layers 1, 2, and 3 118
  - Wireless Design Considerations 119

Documentation	119
IP Addressing Scheme	119
Network Diagrams	120
Baselines	122
Asset Management	122
Policies and Procedures	122
Study Resources	123

## **Day 21: Network Monitoring and Metrics 125**

CompTIA Network+ N10-006 Exam Topics	125
Key Topics	125
Types of Metrics	125
SNMP	127
SNMP Message Types	127
SNMP Versions	128
The Management Information Base	128
Syslog	130
Syslog Operation	130
Severity Levels	130
Syslog Message Format	131
Port Scanners	132
Packet Sniffers	133
Packet Flow Monitors (NetFlow)	133
Study Resources	136

## **Day 20: Network Segmentation, Patches, and Updates 137**

CompTIA Network+ N10-006 Exam Topics	137
Key Topics	137
Network Segmentation	137
Patches and Updates	139
Study Resources	140

## **Day 19: Switch Configuration 141**

CompTIA Network+ N10-006 Exam Topics	141
Key Topics	141
Evolution to Switching	141
From Bridges to Switches	141
Switch Types	142
Switching Logic	142
Basic Switch Configuration	143
AAA Configuration	145

- Link Aggregation Configuration 146
  - LACP Modes 146
  - Configuring EtherChannel 147
- Port Mirroring Configuration 148
- Study Resources 148

**Day 18: STP, VLANs, Trunking, and VTP 151**

- CompTIA Network+ N10-006 Exam Topics 151
- Key Topics 151
- STP and RSTP Concepts and Operation 151
  - STP Algorithm 152
  - STP Convergence 153
  - Port Costs 154
  - RSTP Operation 155
  - RSTP Port Roles 155
- VLAN Concepts 156
  - Reasons for and Benefit of Using VLANs 156
  - Types of VLANs 157
  - Trunking VLANs 158
- VTP Concepts 159
  - VTP Modes 160
  - VTP Operation 160
  - VTP Pruning 161
- Study Resources 162

**Day 17: WLAN Implementation 163**

- CompTIA Network+ N10-006 Exam Topics 163
- Key Topics 163
- WLAN Features 163
  - Frequencies 163
  - Transmission Methods 164
  - Channels 165
  - Antennas 166
- WLAN Topologies 167
- WLAN Devices 167
  - Wireless Routers 167
  - Wireless Access Points 168
  - Wireless LAN Controllers 169
  - Wireless Bridge 170

- Wireless Installation 170
  - Channels and Frequency Bands 171
  - Wireless Site Surveys 172
  - Wireless Router Configuration 172
- Study Resources 175

### **Day 16: Risks, Threats, and Vulnerabilities 177**

- CompTIA Network+ N10-006 Exam Topics 177
- Key Topics 177
- Denial of Service 177
  - Distributed DoS 178
  - Reflected and Amplified Attacks 178
- Other Attack and Threat Terminology 179
- Wireless Attacks 180
- Vulnerabilities 181
- Risk Management 182
- Study Resources 183

### **Day 15: Hardening Devices 185**

- CompTIA Network+ N10-006 Exam Topics 185
- Key Topics 185
- Anti-malware Software 185
- Device Hardening 185
  - Disable Unused Network Services 186
  - Use Secure Protocols 186
  - Configure Switch Port Security 186
- User Authentication 188
- Data Integrity and Hashing 189
- Wireless Security 190
- Study Resources 190

### **Day 14: Physical Security, Firewalls, Access Control, and Forensics 193**

- CompTIA Network+ N10-006 Exam Topics 193
- Key Topics 193
- Physical Security 193
- Firewalls 194
- Firewall Placement and Configuration 196
- Access Control Models 197
- Forensic Concepts 198
- Study Resources 199

### **Day 13: Network Models 201**

- CompTIA Network+ N10-006 Exam Topics 201

- Key Points 201
- The OSI and TCP/IP Models 201
  - OSI Layers 202
  - TCP/IP Layers and Protocols 203
- Data Flow Through the Layers 203
- Study Resources 204

**Day 12: Network Theory 207**

- CompTIA Network+ N10-006 Exam Topics 207
- Key Topics 207
- The TCP/IP Application Layer 207
- The TCP/IP Transport Layer 207
- The TCP/IP Internet Layer 208
- The TCP/IP Network Access Layer 208
  - Collisions 209
  - Transmission Techniques 209
  - End-to-End Communication 210
- Numbering Systems 211
- Study Resources 212

**Day 11: Wired and Wireless Standards 213**

- CompTIA Network+ N10-006 Exam Topics 213
- Key Topics 213
- Ethernet Standards 213
  - Wired Standards 213
  - TIA/EIA 568A and 568B Standards 214
- Wireless Standards 215
- Study Resources 217

**Day 10: Implement Policies, Procedures, and Safety Practices 219**

- CompTIA Network+ N10-006 Exam Topics 219
- Key Topics 219
- Policies and Procedures 219
- Safety Policies 220
- Study Resources 222

**Day 9: Best Practices and Change Management 223**

- CompTIA Network+ N10-006 Exam Topics 223
- Key Topics 223
- Best Practices 223
- Change Management 224
- Study Resources 226

**Day 8: Implement Ports and Protocols 227**

- CompTIA Network+ N10-006 Exam Topics 227
- Key Topics 227
- Transport Protocols: TCP and UDP 227
  - TCP and UDP Headers 228
  - Error Recovery 228
  - Flow Control 229
  - Connection Establishment and Termination 230
  - UDP 231
- Port Numbers 231
- Study Resources 234

**Day 7: Troubleshooting Methodology 235**

- CompTIA Network+ N10-006 Exam Topics 235
- Key Topics 235
- Identify the Problem 235
- Establish a Theory 236
- Test the Theory 236
- Establish a Plan of Action 236
- Implement the Solution or Escalate 237
- Verify the Solution and Implement Preventative Measures 237
- Document Findings, Actions, and Outcomes 237
- Study Resources 237

**Day 6: Troubleshooting Tools 239**

- CompTIA Network+ N10-006 Exam Topics 239
- Key Topics 239
- Command-Line Tools 239
  - The **ipconfig** Command 240
  - The **tracert** Command 241
  - The **ping** Command 242
  - Windows **pathping** Command 244
  - The **arp** Command 245
  - The **netstat** Command 247
  - The **nbtstat** Command 250
  - The **nslookup** Command 250
  - The Cisco **show mac-address-table** Command 252
- Hardware and Software Tools 252
- Study Resources 253

**Day 5: Troubleshoot Wireless Issues 255**

- CompTIA Network+ N10-006 Exam Topics 255

- Key Topics 255
- Wireless Transmission Issues 255
- Wireless Configuration Issues 257
- Study Resources 258

**Day 4: Troubleshoot Copper and Fiber Cabling Issues 259**

- CompTIA Network+ N10-006 Exam Topics 259
- Key Topics 259
- Common Copper Cable Issues 259
- Common Fiber Cable Issues 260
- Study Resources 261

**Day 3: Troubleshoot Network Issues 263**

- CompTIA Network+ N10-006 Exam Topics 263
- Key Topics 263
- Physical Layer Issues 263
- Data Link Layer Issues 264
- Network Layer Issues 265
- Study Resources 266

**Day 2: Troubleshoot Security Issues 267**

- CompTIA Network+ N10-006 Exam Topics 267
- Key Topics 267
- Security Configuration Issues 267
- Other Security Issues 268
- Study Resources 269

**Day 1: Troubleshoot WAN Issues 271**

- CompTIA Network+ N10-006 Exam Topics 271
- Key Topics 271
- Common WAN Issues 271
- Study Resources 273

**Exam Day 275**

- What You Need for the Exam 275
- What You Should Receive After Completion 275
- Summary 276

**Post-Exam Information 277**

- Receiving Your Certificate 277
- Examining Certification Options 277
- If You Failed the Exam 278
- Summary 278

**Index 279**

## About the Author

**Allan Johnson** entered the academic world in 1999 after 10 years as a business owner/operator to dedicate his efforts to his passion for teaching. He holds both an MBA and an M.Ed in Occupational Training and Development. He taught CCNA courses at the high school level for 7 years and has taught both CCNA and CCNP courses at Del Mar College in Corpus Christi, Texas. In 2003, Allan began to commit much of his time and energy to the CCNA Instructional Support Team, providing services to Networking Academy instructors worldwide and creating training materials. He now works full time for Cisco Networking Academy as a Learning Systems Developer.

## About the Technical Reviewer

**Chris Crayton** (MCSE) is an author, technical consultant, and trainer. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He holds numerous industry certifications, has been recognized with many professional teaching awards, and has served as a state-level SkillsUSA competition judge.



## **Dedication**

*For my wife, Becky. You continue to travel with me through those “thin times” when projects like these need to be nurtured. Without your constant vigilance and loving support, this work would not have come to fruition.*

---

# Acknowledgments

This book is a concise summary of networking concepts and draws upon the work of several Pearson authors. Thank you to Keith Barker, Emmett Dulaney, Anthony Sequeira, and Kevin Wallace for blazing a trail in the Network+ domain by authoring some outstanding resources for the reader.

Thank you to my technical editor, Chris Crayton, who is a tough task master and excellent subject matter expert. This book was made much better by his attentive guidance.

The Digital Study Guide version of this book includes activities, videos, and quizzes for each day.

I am grateful to Dan Alberghetti for agreeing to do the videos. Students of Cisco Network Academy will be familiar with his work. But you can also find Dan's work at his website, <http://danscourses.com>, and his YouTube channel, <http://youtube.com/danscourses>.

For writing outstanding quiz items to challenge our readers, we called on Troy McMillan. Thank you, Troy, for your attention to detail and assessment-authoring skill.

Lisa Matthews took my activity designs and Troy's quiz questions and made them interactive—a task that requires creativity, talent, and skill. Thank you, Lisa, for taking the final steps to make activities and quizzes available on PCs, tablets, and mobile devices.

Thank you to Drew Cupp, development editor, and Tonya Simpson, project editor, for juggling all the many pieces that must be managed to bring this product to our students, both in a book format and as a digital study guide.

A project like this goes through many review cycles. One of the very last reviews is for grammar and style. It always amazes me how much of an impact a copy editor can have on the final readability of a product. Thank you, Bart Reed, for making me look good.

And, finally, thank you to my editor, Mary Beth Ray, for bringing me this project when I said, "Okay, what's next?" You continue to challenge me to grow and expand my horizons.

## Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS 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).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- 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](mailto:feedback@pearsonitcertification.com)

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

## Reader Services

Register your copy of *31 Days Before Your CompTIA Network+ Certification Exam* at [www.pearsonitcertification.com](http://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](http://www.pearsonitcertification.com/register) and log in or create an account\*. Enter the product ISBN 9780789756473 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

You are almost there! If you're reading this Introduction, you've probably already spent a considerable amount of time and energy pursuing your CompTIA Network+ certification. Regardless of how you got to this point in your travels through your networking studies, *31 Days Before Your CompTIA Network+ Certification Exam* most likely represents the last leg of your journey on your way to the destination: to become Network+ certified.

However, if you're like me, you might be reading this book at the *beginning* of your studies. If such is the case, then this book provides you with an excellent overview of the material you must now spend a great deal of time studying and practicing. However, I must warn you: unless you are extremely well-versed in networking technologies and have considerable experience as a network technician or administrator, this book will not serve you well as the sole resource for Network+ exam preparation. I know this first hand. I recently took the Network+ exam and was impressed with both the breadth and depth of knowledge required to pass. I have been teaching, writing about, and implementing networks for more than a decade, and yet there was a moment during the Network+ exam where I thought, "Wow, this is really a tough exam!"

You see, CompTIA states that the Network+ exam "covers the configuration, management, and troubleshooting of common wired and wireless network devices." You simply cannot just study this content. You must practice it. Although I have a solid understanding of networking concepts and technologies, I also have extensive experience implementing and troubleshooting networks. That's why I was able to easily pass the exam. There really is no other way to correctly answer the many scenario-based questions a candidate will receive during the exam than to have experienced the same or similar scenarios in the real-world or a lab simulation.

Now that I've sufficiently challenged you, let me spend some time discussing my recommendations for study resources.

## Study Resources

Pearson IT Certification offers an abundance of books and resources to serve you well as you learn how to configure, manage, and troubleshoot wired and wireless networks. Most of the resources can be purchased in book form or as e-books for your tablet reader by visiting [www.pearsonitcertification.com](http://www.pearsonitcertification.com).

## Safari Books Online

All the resources I reference in the book are available with a subscription to Safari Books Online (<https://www.safaribooksonline.com>). If you don't have an account, you can try it free for 10 days.

## Primary Resources

First on the list must be Keith Barker and Kevin Wallace's book *CompTIA Network+ N10-006 Cert Guide* (ISBN: 9780789754080). These two Cisco Certified Internetwork Experts (CCIE) do an outstanding job of gathering together and organizing all the material you need to study for the Network+ certification exam. If you get the premium edition bundle, you'll also receive an e-book version, more practice exams, a free copy of the CompTIA Network+ Simulator Lite software, and more than 60 minutes of video mentoring from the author. The practice exams and study materials

---

on the DVD in the back of the book are worth the price of the book. There is no better resource on the market for a Network+ candidate.

Kevin Wallace also recorded more than 17 hours of video in his *CompTIA Network+ N10-006 Complete Video Course* (ISBN: 9780789754721), which is available free with your Safari Books Online account. You can also purchase it separately at [pearsonitcertification.com](http://pearsonitcertification.com). Kevin walks you through the full range of topics on the CompTIA Network+ exam using a variety of presentation styles, including live instructor whiteboarding, real-world demonstrations, animations of network activity, dynamic KeyNote presentations, and doodle videos. He also demonstrates hands-on router and switch CLI configuration and troubleshooting in real lab environments, enabling you to learn both the concepts and the hands-on application.

Next on the list must be Emmett Dulaney and Mike Harwood's *CompTIA Network+ N10-006 Exam Cram, Fifth Edition* (ISBN: 9780789754103). This dense Exam Cram book is jam packed with essential content for the Network+ exam. It also includes a handy, pullout exam cram sheet and a CD with practice exams.

At the end of each day in *31 Days Before Your CompTIA Network+ Certification Exam*, you will find a handy reference of what topics to look at in these three resources. They are referred to as "Certification Guide," "Video Course," and "Exam Cram," respectively.

## Supplemental Resources

In addition to the book you hold in your hands, there are two more supplemental resources I recommend to augment your final 31 days of review and preparation.

Michael Taylor's *CompTIA Network+ N10-006 Hands-on Lab Simulator* (ISBN: 9780789755179) helps you gain hands-on experience with the concepts presented on the Network+ exam. Using the labs in this software, you will be able to experience realistic operating system and network device configuration and troubleshooting. The three types of labs in the software present you with progressively more difficult real-world challenges. Drag-and-drop labs demonstrate network design concepts and allow you to manipulate physical network cables. Matching labs help reinforce key networking concepts. Operating system and Cisco router and switch command-line interface (CLI) simulator labs present real-world configuration and troubleshooting scenarios for you to solve.

Anthony Sequeira is a CCIE and well-respected networking technologies author. His *CompTIA Network+ N10-006 Flash Cards and Exam Practice Pack* (ISBN: 9780789754646) is a compilation of more than 700 flash cards, practice questions, and quick reference sheets to help you prepare for the Network+ exam. Go through the printed flash cards or install the flash card software on your computer. The CD also includes the practice test software as well as 40 performance-based question exercises, including drag-and-drop and command-line interface questions that mimic the kinds of hands-on questions you will face on the actual exam.

So which resources should you buy? That question is largely up to how deep your pockets are or how much you like books. If you're like me, you want it all—online access for mobile and tablet reading, as well as hard copies for intensive study sessions with a pencil in hand. I admit it: My bookcase is a testament to my "geekness." However, that's not practical for most students. So if you are on a budget, then choose one of the primary study resources and one of the supplemental resources, such as the Cert Guide and the Lab Simulator. Whatever you choose, you will be in good hands. Any or all of these authors will serve you well.

## Digital Study Guide

Pearson offers this book in an online digital format that includes enhancements such as video, activities, and Check Your Understanding questions:

- Read the complete text of the book on any web browser that supports HTML5, including mobile.
- Watch dozens of unique embedded videos that demonstrate configurations, explain important topics, and visually describe key Network+ exam objectives.
- Reinforce key network concepts with more than 30 dynamic and interactive hands-on exercises, and see the results with the click of a button.
- Test your understanding of the material at the end of each day with more than 300 fully interactive online quiz questions.

*31 Days Before Your CompTIA Network+ Certification Exam Digital Study Guide* is available at a discount for anyone who purchases this book. You can find details about redeeming this offer in the back of the book.

Throughout this book you'll see references to the Digital Study Guide enhancements that look like this:



### **Video: Data Encapsulation Summary**

Refer to the Digital Study Guide to view this video.



### **Activity: Identify the Encapsulation Layer**

Refer to the Digital Study Guide to complete this activity.



### **Check Your Understanding**

Refer to the Digital Study Guide to take a 10-question quiz covering the content of this day.

When you are at these points in the Digital Study Guide, you can start the enhancement.

## Goals and Methods

The main goal of this book is to provide you with a clear and succinct review of the Network+ exam objectives. Each day's exam topics are grouped into a common conceptual framework and uses the following format:

- A title for the day that concisely states the overall topic
- A list of one or more CompTIA Network+ N10-006 exam topics to be reviewed
- A "Key Topics" section to introduce the review material and quickly orient you to the day's focus

- An extensive review section consisting of short paragraphs, lists, tables, examples, and graphics
- A “Study Resources” section to provide you a quick reference for locating more in-depth treatment of the day’s topics

The book counts down starting with Day 31 and continues through the exam day to provide post-test information. You will also find a calendar and checklist that you can tear out and use during your exam preparation inside the book.

Use the calendar to enter each actual date beside the countdown day and the exact day, time, and location of your Network+ exam. The calendar provides a visual for the time that you can dedicate to each Network+ exam topic.

The checklist highlights important tasks and deadlines leading up to your exam. Use it to help you map out your studies.

## Who Should Read This?

The audience for this guide is anyone finishing his or her preparation for taking the CompTIA Network+ N10-006 exam. A secondary audience is anyone needing a refresher review of Network+ exam topics—possibly before attempting to recertify.

## Getting to Know the CompTIA Network+ N10-006 Exam

CompTIA launched the newest version of the Network+ exam, numbered N10-006, in February 2015. The exam covers the configuration, management, and troubleshooting of common wired and wireless network devices. Also included are emerging technologies such as unified communications, mobile, cloud, and virtualization technologies. CompTIA recommends that you are A+ certified and have at least 9 months of networking experience.

Currently for the Network+ exam, you are allowed 90 minutes to answer a maximum of 90 questions. A passing score is 720 on a scale of 100 to 900. If you’ve never taken a certification exam before with Pearson VUE, there is a 2-minute 45-second video titled “What to expect in a Pearson VUE test center” that nicely summarizes the experience. You will find it under “Related Links” at <http://www.pearsonvue.com/comptia>, or you can search for it on YouTube.

When you get to the testing center and check in, the proctor verifies your identity, gives you some general instructions, and then takes you into a quiet room containing a PC. When you’re at the PC, you have a few things to do before the timer starts on your exam. For instance, you can take the tutorial to get accustomed to the PC and the testing engine. Every time I sit for an exam, I go through the tutorial even though I know how the test engine works. It helps me settle my nerves and get focused. Anyone who has user-level skills in getting around a PC should have no problems with the testing environment.



## What Topics Are Covered on the Network+ Exam

Table I-1 summarizes the five domains of the Network+ exam.

**Table I-1 Network+ Domains and Weightings**

<b>Domain</b>	<b>% of Examination</b>
1.0 Network architecture	22%
2.0 Network operations	20%
3.0 Network security	18%
4.0 Troubleshooting	24%
5.0 Industry standards, practices, and network theory	16%
Total	100%

## Registering for the Network+ N10-006 Exam

If you are starting your *31 Days Before Your CompTIA Network+ Certification Exam* today, register for the exam right now. In my testing experience, there is no better motivator than a scheduled test date staring me in the face. I'm willing to bet it's the same for you. Don't worry about unforeseen circumstances. You can cancel your exam registration for a full refund up to 24 hours before taking the exam. So if you're ready, then you should gather the following information and register right now:

- Legal name
- Social Security or passport number
- Company name
- Valid email address
- Method of payment

You can schedule your exam at any time by visiting <http://www.pearsonvue.com/comptia/>. I recommend you schedule it for 31 days from now. The process and available test times will vary based on the local testing center you choose.

*This page intentionally left blank*

## WAN Technologies

### CompTIA Network+ N10-006 Exam Topics

- 1.4 Explain the characteristics and benefits of various WAN technologies

### Key Topics

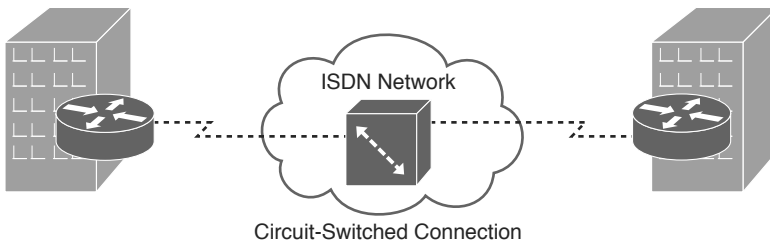
First today, we review packet switching and circuit switching. Then we review all the various ways networks are connected together through WAN technologies.

### Packet Switching and Circuit Switching

The switching function provides communication pathways between two endpoints and manages how data flows between them. The two most common switching methods are circuit switching and packet switching.

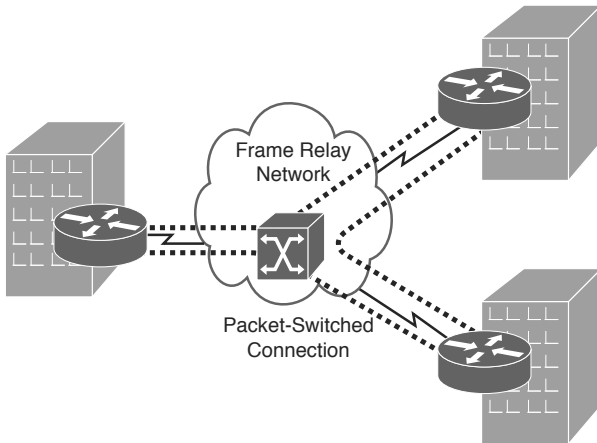
Integrated Service Digital Network (ISDN), shown in Figure 29-1, is an example of a circuit-switched network.

**Figure 29-1** Circuit Switching ISDN Topology



Circuit switching requires a dedicated physical connection between the sending and receiving devices. For example, parties involved in a phone call have a dedicated link between them for the duration of the conversation. When either party disconnects, the circuit is broken, and the data path is lost. This is an accurate representation of how circuit switching works with network and data transmissions. The sending system establishes a physical connection, and the data is transmitted between the two. When the transmission is complete, the channel is closed.

A Frame Relay network, shown in Figure 29-2, is an example of a packet-switched network.

**Figure 29-2 Packet Switching Frame Relay Topology**

In packet switching, messages are broken into smaller pieces called packets. Each packet is assigned source and destination addresses. Packets are required to have this information because they do not always use the same path or route to get to their intended destination. Packets can take an alternative route if a particular route is unavailable for some reason.

Table 29-1 compares circuit switching and packet switching.

**Table 29-1 Circuit Switching and Packet Switching Comparison**

Switching Method	Pros	Cons	Key Features
Circuit switching	Offers a dedicated transmission channel that is reserved until it is disconnected.	Dedicated channels can cause delays because a channel is unavailable until one side disconnects. Uses a dedicated physical link between the sending and receiving devices.	Offers the capability of storing messages temporarily to reduce network congestion.
Packet switching	Packets can be routed around network congestion. Packet switching makes efficient use of network bandwidth.	Packets can become lost while taking alternative routes to the destination. Messages are divided into packets that contain source and destination information.	The two types of packet switching are datagram and virtual circuit. Datagram packets are independently sent and can take different paths throughout the network. Virtual circuit uses a logical connection between the source and destination device.

## WAN Link Options

A variety of different methods can be used to link networks together. To select an appropriate WAN technology, you need the ability to compare one WAN technology to another.

## Home and Small Office

Home and small office networks can connect to other networks and the Internet through a variety of methods.

### Dialup

Dialup connectivity is done through the Public Switched Telephone Network (PSTN), which is composed of multiple telephone carriers from around the world. Although the bandwidth available on the PSTN is limited, it is more likely to be available in a given location than other wired WAN solutions. A dialup connection can be used to access the Internet by connecting a computer to a modem, connecting the modem to an analog phone line, and dialing in to a service provider. The service provider can then connect to the Internet, as shown in Figure 29-3. Modems in the United States and Canada are limited to 53.3Kbps download and 48.0Kbps upload.

**Figure 29-3 PSTN Dialup Topology**

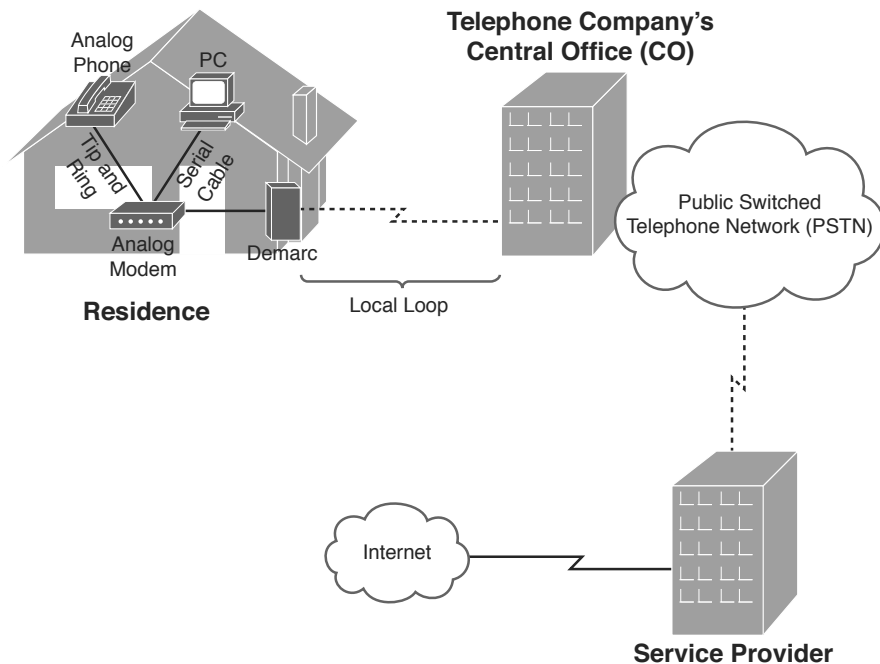


Table 29-2 describes some of the common terminology used to describe PSTNs.

**Table 29-2 Common PSTN Terms**

Term	Definition
Telco	Abbreviation for telephone company.
Local loop	A local loop is a connection between a customer's premises and his local telephone central office (CO).

Term	Definition
Central office (CO)	A building containing a telephone company's telephone switching equipment is referred to a central office (CO).
Tip and ring	The tip and ring wires are the red and green wires found in an RJ-11 wall jack, which carry voice, ringing voltage, and signaling information between an analog device and a telephone's wall jack.
Demarc	A demarc, short for demarcation point, is the point in a telephone network where the maintenance responsibility passes from a telephone company to the subscriber.
Smart jack	A smart jack is a type of network interface device that adds features such as converting between framing formats on digital circuits, supporting remote diagnostics, and regenerating a digital signal.

## ISDN

ISDN connections are considerably faster than regular modem connections. ISDN is a digital technology that supports multiple 64Kbps channels on a single connection. ISDN circuits are classified as either a basic rate interface (BRI) circuit or a primary rate interface (PRI) circuit:

- **BRI**—A BRI circuit consists of two 64Kbps bearer (B) channels and one 16Kbps delta (D) channel. The B channels carry voice, video, and data. They can carry two separate voice conversations or they can be combined using PPP multilink. The D channel carries Layer 2 (Q.921) and Layer 3 (Q.931) signaling.
- **PRI**—A PRI circuit is equivalent to a 1.544Mbps T1 circuit. Therefore, it consists of 23 B channels and one 64Kbps D channel.

The components of an ISDN network are shown in Figure 29-4.

**Figure 29-4 ISDN Topology**

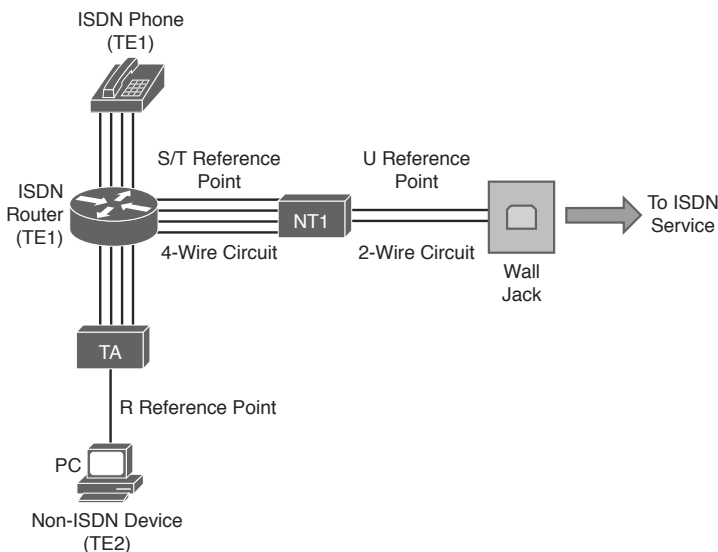


Table 29-3 lists a brief description of the ISDN components shown in Figure 29-4.

**Table 29-3 ISDN Components**

<b>Term</b>	<b>Definition</b>
R reference point	The R reference point resides between a non-ISDN device and a terminal adapter (TA).
S/T reference point	The S/T reference point resides between a network termination 1 (NT1) and a terminal endpoint 1 (TE1).
U reference point	The U reference point resides between a network termination 1 (NT1) and the wall jack connecting back to an ISDN service provider.
Terminal adapter (TA)	A TA performs protocol conversion between a non-ISDN device and a terminal endpoint 1 (TE1) device.
Terminal endpoint 1 (TE1)	A TE1 is a device (such as an ISDN phone) that natively supports ISDN.
Terminal endpoint 2 (TE2)	A TE2 is a device (such as a PC) that does not natively support ISDN.
Network termination 1 (NT1)	An NT1 is a device that interconnects a four-wire ISDN circuit and a two-wire ISDN circuit.

## DSL

Digital Subscriber Line (DSL) is a group of technologies that provide high-speed data transmission over existing telephone wiring. There are many different varieties of DSL. Together, all these variations are referred to as xDSL. Popular variants include the following:

- **Asymmetric DSL (ADSL)**—ADSL is the most popular variant. It include a channel for analog voice conversations, a channel for uploads, and a channel for downloads. It is called asymmetrical because the download channel is faster than the upload channel.
- **Symmetric DSL (SDSL)**—SDSL is more suited to business applications because it offers the same speeds for uploads and downloads.
- **Very High Bit-Rate DSL (VDSL)**—VDSL is a variant of ADSL that provides data speeds of up to 13Mbps.

Table 29-4 summarizes the maximum speeds for all the DSL variants.

**Table 29-4 DSL Speeds**

<b>DSL Variation</b>	<b>Upload Speed</b>	<b>Download Speed</b>
ADSL	1Mbps	3Mbps
ADSL2	1.3Mbps	12Mbps
ADSL2+	1.4Mbps	24Mbps
SDSL	1.5Mbps	1.5Mbps
IDSL (ISDN DSL)	144Kbps	144Kbps
RADSL (Rate-adaptive DSL)	1Mbps	7Mbps

DSL Variation	Upload Speed	Download Speed
VHDSL	1.6Mbps	13Mbps
HDSL (High bit rate DSL)	768Kbps	768Kbps

## PPP

Point-to-Point Protocol (PPP) is a common Layer 2 protocol used on dedicated leased lines. It can carry multiple Layer 3 protocols, such as IPv4 and IPv6. IP uses PPP's IP control protocol (IPCP). When a link is configured with IP and PPP, IPCP initiates the Link Control Protocol (LCP), which can provide any or all of the following features:

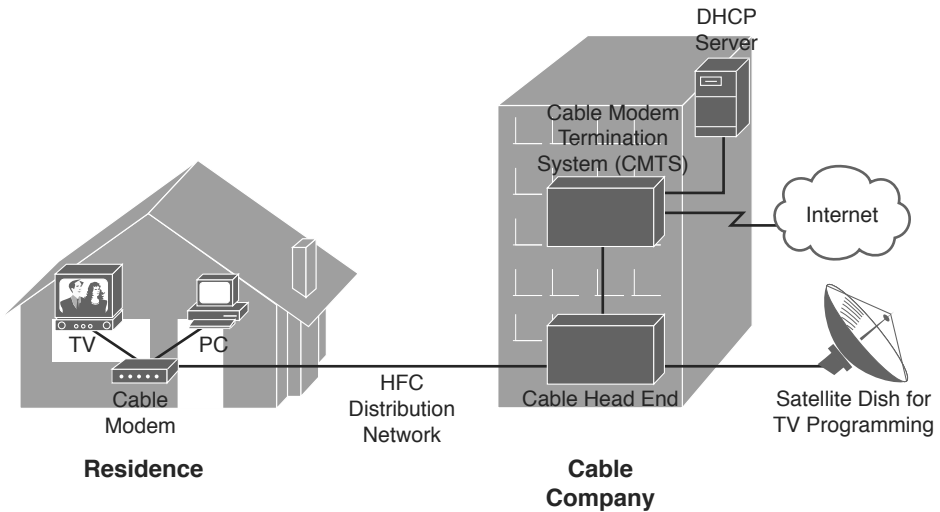
- **Multilink interface**—PPP multilink allows multiple interfaces to be combined into one logical interface.
- **Looped link detection**—A Layer 2 loop (of PPP links) can be detected and prevented.
- **Error detection**—Frames containing errors can be detected and discarded by PPP.
- **Authentication**—PPP provides three methods of authentication methods:
  - **Password Authentication Protocol (PAP)**—PAP performs one-way authentication. Passwords are sent in clear text.
  - **Challenge Handshake Authentication Protocol (CHAP)**—CHAP performs one-way authentication using a three-way handshake (challenge, response, and acceptance). Passwords are not sent across the link.
  - **Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)**—MS-CHAP is a Microsoft-enhanced version of CHAP, offering a collection of additional features, including two-way authentication.

## Broadband Cable

Broadband cable is an always-on Internet access method available in areas that have digital cable television. Connectivity is achieved by using a device called a cable modem. It has a coaxial connection for connecting to the provider's outlet and an unshielded twisted-pair (UTP) connection for connecting directly to a system or to a hub, switch, or router.

The provider's infrastructure probably has a mix of coaxial and fiber cabling called hybrid fiber-coax (HFC). A broadband cable network is shown in Figure 29-5.



**Figure 29-5 Broadband Cable Topology**

## Wireless

Wireless WAN connection options include satellite, Worldwide Interoperability for Microwave Access (WiMAX), and several varieties of cellular technologies.

### Satellite

Some locations do not have the WAN connectivity options, such as DSL connections or cable modems, commonly available in urban areas. However, these locations might be able to connect to the Internet or to a remote office using satellite communications, where a transmission is bounced off of a satellite, received by a satellite ground station, and then sent to its destination using either another satellite hop or a wired WAN connection.

Two different types of broadband Internet satellite services are deployed:

- **One-way satellite system**—A one-way satellite system requires a satellite card and a satellite dish installed at the end user's site. Outgoing requests are sent using a phone line. Inbound traffic returns on the satellite link.
- **Two-way satellite system**—A two-way satellite system, in contrast, provides data paths for both upstream and downstream data. Bidirectional communication occurs directly between the end user's site and the satellite.

## WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) provides wireless Internet broadband access to fixed locations (as an alternative to technologies such as DSL or cable). Depending on the WiMAX service provider, WiMAX coverage areas could encompass entire cities or small countries. Based on the IEEE 802.16 standard, WiMAX can provide data rates up to 1Gbps. Although WiMAX can send data up to 31 miles (50 km), it is most effective within one mile. WiMAX is a popular choice for connecting cell towers in cellular networks.

## Cellular Technologies

Some cellular phone technologies (for example, Long-Term Evolution [LTE], which supports a 100Mbps data rate to mobile devices and a 1Gbps data rate for stationary devices) can be used to connect a mobile device (such as a smartphone) to the Internet. Other technologies for cellular phones include the older 2G edge, which provides slow data rates. 2G edge was improved upon with 3G, in addition to the newer 4G, LTE, and Evolved High-Speed Packet Access (HSPA+). Code division multiple access (CDMA) and Global System for Mobile Communications (GSM) are the two major radio systems used in cell phones.

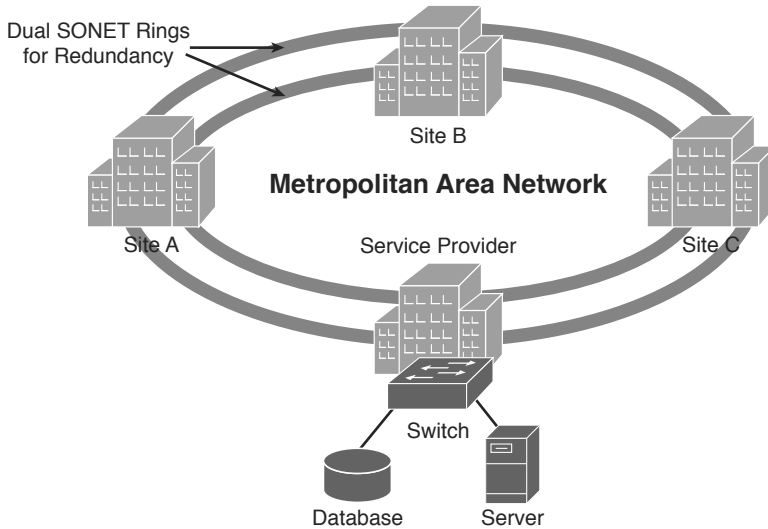
## SONET

Synchronous Optical Network (SONET) is a fiber-optic WAN technology that delivers voice, data, and video at speeds starting at 51.84Mbps. SONET uses dense wavelength-division multiplexing (DWDM), which uses erbium-doped fiber amplifiers (EDFA) to amplify the signal and allow it to travel greater distances. An alternative to DWDM is CWDM (coarse wavelength-division multiplexing), which is commonly used with television cable networks. SONET is classified into various Optical Carrier (OCx) levels, as shown in Table 29-5.

**Table 29-5 Optical Carrier Data Rates**

OCx Level	Data Rate
OC-1	51.84Mbps
OC-3	155.52Mbps
OC-12	622.08Mbps
OC-24	1.244Gbps
OC-48	2.488Gbps
OC-96	4.976Gbps
OC-192	9.953Gbps
OC-768	39.813Gbps

SONET can connect as many as 16 other devices in a linear fashion (similar to a bus topology) or in a ring topology. A metropolitan area network (MAN), as depicted in Figure 29-6, often uses SONET in a ring topology.

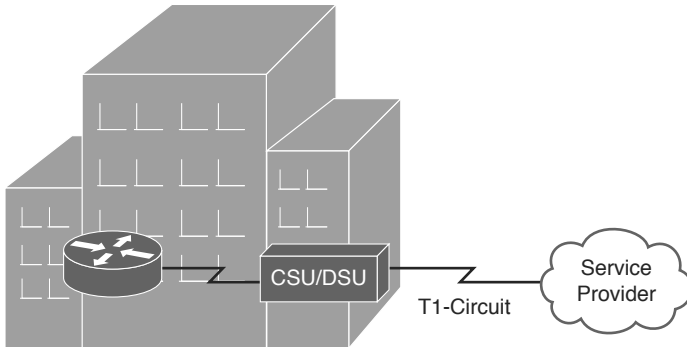
**Figure 29-6 SONET Ring Topology**

## Dedicated Leased Lines

A dedicated leased line is typically a point-to-point digital circuit interconnecting two sites. All the bandwidth on that circuit is available to those sites. These circuits can use multiplexing technology to simultaneously carry multiple conversations in different 64Kbps channels. A single 64Kbps channel is called a Digital Signal 0 (DS0). WAN technologies commonly used with dedicated leased lines include the following:

- **T1**—T1 circuits were originally used in telephony networks, with the intent of one voice conversation being carried in a single channel. A T1 circuit is composed of 24 DS0s, which is called a Digital Signal 1 (DS1). The bandwidth of a T1 circuit is 1.544Mbps.
- **T3**—T3 circuits combine 672 DS0s into a single physical connection, which is called a Digital Signal 3 (DS3). A T3 circuit has a bandwidth capacity of 44.7Mbps.
- **E1**—E1 circuits are popular outside of North America and Japan. They contain 32 channels, in contrast to the 24 channels on a T1 circuit, for a bandwidth capacity of 2.048Mbps.
- **E3**—E3 circuits have a bandwidth capacity of 34.4Mbps, which is less than a T3 circuit.

Dedicated leased lines are terminated at the customer's premises with a channel service unit/data service unit (CSU/DSU), as shown in Figure 29-7.

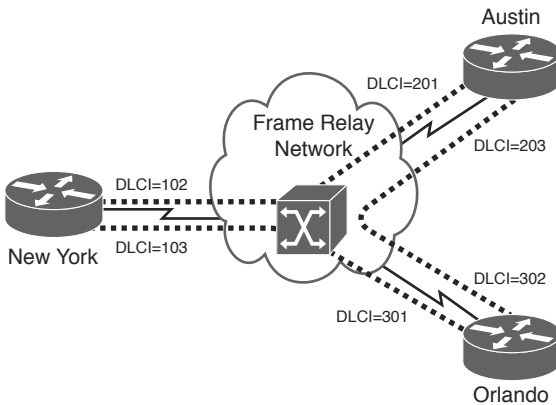
**Figure 29-7 Terminating a Leased Line**

## Enterprise WANs

Initially, dedicated leased lines were used by enterprises to connect various sites. However, as network traffic and the number of required WAN connections grew, leased lines became cost prohibitive. Several technologies emerged to answer the need, including Frame Relay, Asynchronous Transfer Mode (ATM), Multiprotocol Label Switching (MPLS), and Metro Ethernet.

### Frame Relay

Frame Relay sites are interconnected using virtual circuits (VCs). Frame Relay is a Layer 2 technology that uses locally significant identifiers called data-link connection identifiers (DLCI). DLCIs identify the VC. A single router interface can have multiple VCs, as shown in Figure 29-8.

**Figure 29-8 Frame Relay Topology**

Unlike a dedicated leased line, Frame Relay shares a service provider's bandwidth with other customers of its service provider. Therefore, subscribers might purchase a service level agreement (SLA) to guarantee a minimum level of service. Part of the Frame Relay SLA would be a minimum bandwidth guarantee called a committed information rate (CIR).

During times of congestion, the service provider manages transmission rates using the backward explicit congestion notification (BECN) and forward explicit congestion notification (FECN) bits in the frame relay header. The BECN and FECN bits inform the customers to slow down the transmission rates.

If the service is not congested, a customer might have an SLA that allows transmission rates higher than the CIR. In such cases, the discard eligibility (DE) bit is set in each frame. If the service becomes congested, these frames can be discarded by the Frame Relay service provider.

## ATM

ATM is a Layer 2 technology that uses VCs. However, ATM uses a fixed-length frame, called a cell, which includes 48 bytes of data and a 5-byte header, as shown in Figure 29-9.

**Figure 29-9 ATM Cell Format**

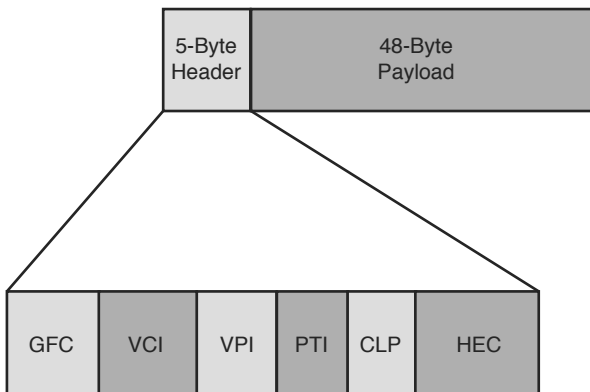


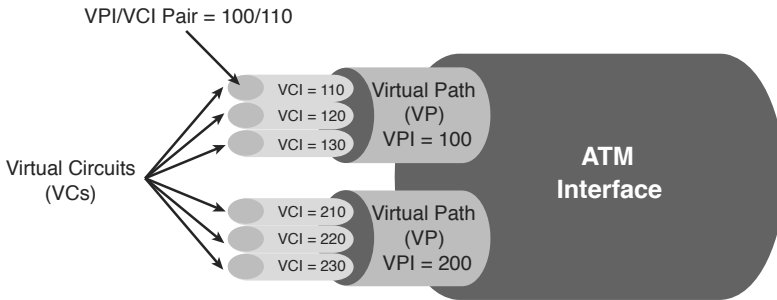
Table 29-6 details the fields of the ATM cell header.

**Table 29-6 ATM Header Fields**

Field	Description
GFC (4 bits)	The Generic Flow Control (GFC) field is used to indicate congestion.
VCI (16 bits)	The Virtual Circuit Identifier (VCI) field indicates a VC.
VPI (8 bits)	The Virtual Path Identifier (VPI) indicates the virtual path, which could contain multiple VCs.
PTI (3 bits)	The Payload Type Indicator (PTI) indicates the type of payload (for example, user data versus ATM management data).
HEC (8 bits)	The Header Error Control (HEC) field is used to detect and correct errors in the header.

ATM VCs are identified with a VPI/VCI pair, as shown in Figure 29-10.

**Figure 29-10 Identifying ATM VCs**



## MPLS

Multiprotocol Label Switching (MPLS) can accommodate both Frame Relay and ATM on the same backbone. It does this by inserting a 32-bit header between the Layer 2 and Layer 3 headers. The 32-bit header contains a 20-bit label. This label is used to make forwarding decisions within an MPLS cloud. Therefore, the process of routing MPLS frames through an MPLS cloud is commonly referred to as label switching. Figure 29-11 shows an MPLS topology.

**Figure 29-11 MPLS Topology**

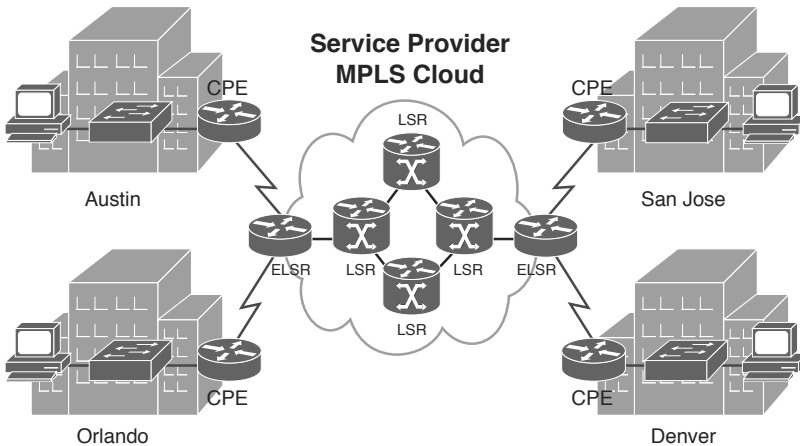


Table 29-7 lists the definitions for the components of the MPLS topology shown in Figure 29-11.

**Table 29-7 MPLS Components**

Component	Description
CPE	A customer premises equipment (CPE) device resides at a customer site.
ELSR	An edge label switch router (ELSR) resides at the edge of an MPLS service provider's cloud and interconnects a service provider to one or more customers.
LSR	A label switch router (LSR) resides as part of a service provider's MPLS cloud and makes frame-forwarding decisions based on labels applied to frames.

## Metro Ethernet

Metro Ethernet is simply Ethernet technology extended into the metropolitan area network (MAN). The customer connects to the service provider through an Ethernet connection (using an RJ-45 connector). This effectively extends the LAN into the MAN. The service provider is responsible for configuring the logical connections between the customer sites. The technologies used with the service provider network are hidden from the customer.



### **Video: WAN Links (Circuit Switched)**

Refer to the Digital Study Guide to view this video.



### **Video: WAN Links (Packet Switched)**

Refer to the Digital Study Guide to view this video.



### **Activity: Identify the WAN Technology**

Refer to the Digital Study Guide to complete this activity.

## Study Resources

For today's exam topics, refer to the following resources for more study.

Resource	Location	Topic
<b>Primary Resources</b>		
Certification Guide	7	All
Video Course	5	All
Exam Cram	6	WAN Technologies Internet Access Technologies
<b>Supplemental Resources</b>		
Lab Simulator	7	Configuring a VPN Client
Flash Cards	3	WAN Technologies
Quick Reference	3	WAN Technologies



### **Check Your Understanding**

Refer to the Digital Study Guide to take a 10-question quiz covering the content of this day.

*This page intentionally left blank*



## Symbols

- 2.4GHz band, 165
- 5GHz band, 165
- 6to4 tunneling, IPv6, 84
- 10BASE2, 214
- 10BASE5, 214
- 10BASE-T, 214
  - limitations of, 141
- 10GBASE-ER, 214
- 10GBASE-EW, 214
- 10GBASE-LR, 214
- 10GBASE-LW, 214
- 10GBASE-SR, 214
- 10GBASE-SW, 214
- 10GBASE-T, 214
- 100BASE-FX, 214
- 100BASE-TX, 214
- 100GBASE-ER4, 214
- 100GBASE-LR4, 214
- 100GBASE-SR10, 214
- 802.1Q, 159
- 802.1Q tag inside an Ethernet frame, 159
- 802.11, 215
  - characteristics of, 216
- 802.11a, 215
- 802.11ac, 216
- 802.11a-ht, 165
- 802.11b, 216
- 802.11g, 216
- 802.11g-ht, 165
- 802.11n, 216
- 1000BASE-LH, 214
- 1000BASE-LX, 214
- 1000BASE-T, 214
- 1000BASE-TX, 214
- 1000BASE-ZX, 214

## A

- AAA (authentication, authorization, and accounting), 13
- AAA configuration, 145-146
- AAA server, 268
- acceptable use policies (AUP), 219
- access control entries (ACEs), 196
- access control lists (ACLs), 188, 196
- access control models, 197-198
- access points (APs), 2, 165
- ACEs (access control entries), 196
- ACLs (access control lists), 188, 196
  - misconfigured, 267
- active mode, LACP, 146
- AD (administrative distance), routing, 93
- ad hoc WLAN topologies, 167
- Address Resolution Protocol (ARP), 245
- address types
  - IPv4 addressing, 66-67
  - IPv6, 78
    - global unicast addresses, 79
    - link-local unicast addresses, 79-80
- addressing
  - classless addressing, 71-73
  - IPv4 addressing, 64
    - address types, 66-67
    - private, 66
    - public, 66
    - structure, 64-65
  - IPv6 addressing. *See* IPv6 addressing
  - local addressing, 63
    - collision and broadcast domains, 63-64
    - MAC addresses, 63
  - VLSM, 71-73
- administrative distance (AD), routing, 93
- ADSL (asymmetric DSL), 27

**Advanced Encryption Standard (AES),**  
190

**advertisement request message, 161**

**AES (Advanced Encryption Standard),**  
190

**AH (Authentication Header), 11**

**algorithms**

Dijkstra Shortest Path First (SPF)  
algorithm, 95–96

STP, 152–153

**amplified attacks, 178**

**amplitude, 163**

**analog modems, 1**

**analog phone, 15, 102**

**ANDing process, 65**

**antennas, WLANs, 166**

**anti-malware software, 185**

**AP placement, wireless configuration  
issues, 258**

**APs (access points), 2, 165**

wireless access points, 168

**application-aware firewalls, 195**

**application layer**

OSI model, 202

TCP/IP, 203, 207

**applications, misconfigured, 267**

**ARP (Address Resolution Protocol),**  
245

**arp, 239, 245–247**

**arp -a, 245**

**ARP inspection, 187**

**AS (autonomous system), 90**

**asset management, documentation, 122**

**asymmetric DSL (ADSL), 27**

**Asynchronous Transfer Mode (ATM),**  
59

enterprise WANs, 33

**ATM (Asynchronous Transfer Mode),**  
59

enterprise WANs, 33

header fields, 33

VCs (virtual circuits), 33–34

**attacks, 180. See also threats**

brute force, 179

DoS (denial of service) attack, 177–178

man-in-the-middle, 179

packet abuse, 179

session hijacking, 179

smurf attacks, 178

social engineering, 180

spoofing, 179

VLAN hopping, 180

wireless attacks, 180

zero-day attacks, 180

**AUP (acceptable use policies), 219**

**authentication**

multifactor authentication, 189

PPP, 28

two-factor authentication, 189

**authentication, authorization, and  
accounting (AAA), 13**

**Authentication Header (AH), 11**

**authentication issues, 268**

**authentication port-control auto  
command, 188**

**autonomous APs, wireless configura-  
tion issues, 258**

**autonomous system (AS), 90**

## **B**

**backdoor access, 268**

**backup procedures, 123**

**backward explicit congestion notifica-  
tion (BECN), 33**

**bad connections, copper cable, 260**

**bad wiring, copper, 259**

**bandwidth, 125**

metrics, 92

**bandwidth saturation, wireless trans-  
missions, 256**

**banner grabbing, 269**

**base10 numbering, 211**

**baseband, 210**

**baselines, documentation, 122**

**basic rate interface (BRI), 26**  
**baud rate, 210**  
**Bayonet Neill-Concelman (BNC)**  
   connectors, 41  
**BECN (backward explicit congestion notification), 33**  
**behavior-based IDSs, 4**  
**Bellman-Ford algorithm, 90**  
**best-effort, QoS, 106**  
**best practices, 223**  
   cable management, 223  
   labeling, 224  
   power management, 224  
   rack systems, 224  
   wiring closets, 223  
**BGP (Border Gateway Protocol), 89**  
**BID (bridge ID), 152-153**  
**binary, 211**  
**biometrics, 194**  
**bit boundaries, 65**  
**bit rate, 210**  
**black hole VLAN, 157**  
**blocking, STP, 153**  
**Bluejacking, 180**  
**Bluesnarfing, 180**  
**Bluetooth, 57**  
**BNC (Bayonet Neill-Concelman) connectors, 41**  
**Border Gateway Protocol (BGP), 89**  
**bottom-up approach, 236**  
**bounce, wireless configuration issues, 257**  
**BPDU (bridge protocol data unit), 152**  
**BRI (basic rate interface), 26**  
**bridge ID (BID), 152-153**  
**bridge protocol data unit (BPDU), 152**  
**bridges**  
   evolving to switches, 141-142  
   wireless bridges, 170  
**bring-your-own-device (BYOD), 219**

**broadband, 210**  
**broadband cable, 28-29**  
**broadband modems, 2**  
**broadcast addresses, subnetting, 69-70**  
**broadcast domains, 63-64**  
**broadcast storms, 152, 264**  
**broadcast transmission, 67**  
**brute force attacks, 179**  
**buffer overflow, 178**  
**bus topologies, 49-50**  
**business continuity, 183**  
**BYOD (bring-your-own-device), 219**

## C

**cable crimpers, 46**  
**cable management, best practices, 223**  
**cable placement**  
   copper cable, 260  
   physical layer issues, 263  
**cable testers, 253**  
**cables**  
   coaxial cables, 39-40  
   copper, 37  
     *coaxial cables, 39-40*  
     *plenum, 39*  
     *PVC cables, 39*  
     *twisted-pair, 37-39*  
   copper cable issues, 259-260  
   fiber cable issues, 260-261  
   fiber-optic cables, 43  
   tools for installing, 45-47  
   twisted-pair cables, 38-39  
**cabling properties, Ethernet, 214**  
**calculating network addresses, 65-66**  
**call agent, 15, 102**  
**CANs (campus area networks), 58**  
**CAPWAP (Control and Provisioning of Wireless Access Points), 169**  
**Carrier Sense Multiple Access with Collision Detection (CSMA/CD), 209**

- catalyst switch configuration commands, 144-145
- CCMP, 190
- CCTVs (closed-circuit TVs), 194
- CDP (Cisco Discovery Protocol), 264
- cells, ATM, 33
- cellular technologies, 30
- central office (CO), 26
- certificates, receiving after exam, 277
- certification options, 277-278
- certified examination score report, 275
- chain of custody, 198
- Challenge Handshake Authentication Protocol (CHAP), 28, 189
- change management, 224-225
- channel service unit/data service unit (CSU/DSU), 272
- channels, WLANs, 165-166
  - wireless installation, 171-172
- CHAP (Challenge Handshake Authentication Protocol), 28, 189
- characteristics of 802.11, 216
- CIDR (classless interdomain routing), route aggregation, 97
- CIR (committed information rate), 32
- circuit switching, 23
  - versus packet switching, 24
- Cisco catalyst switch configuration commands, 144
- Cisco Discovery Protocol (CDP), 264
- Cisco Systems, 277
- Cisco Unified Communications, 102
- Cisco Unified Communications Manager (CUCM), 102
- Cisco Unified Communications Manager Express (CME), 102
- Cisco Unified Communications Manager IM and Presence, 102
- Cisco Unity Connection, 102, 104
- Cisco wireless control system heat map, 172
- class of service (CoS), 106
- classful routing protocols, 91
- classification, DiffServ QoS, 106
- classless addressing, 71-73
- classless interdomain routing (CIDR)
  - route aggregation, 97
- classless routing protocols, 91
- client mode, VTP (VLAN Trunking Protocol), 160
- client-server network, 55
- client-to-site VPNs, 10
- clients, network devices, 1
- closed-circuit TVs (CCTVs), 194
- cloud computing, 101, 111-112
- cloud/server-based anti-malware, 185
- CME (Cisco Unified Communications Manager Express), 102
- CNAME, 18
- CO (central office), 26
- coarse wavelength-division multiplexing (CSDM), 30
- coaxial cables, copper, 39-40
- coaxial connectors, 41-42
- collision domains, 63-64
- collisions, TCP/IP network access layer, 209
- command-line tools, 239-240
  - arp, 245-247
  - ifconfig, 240-241
  - nbtstat, 250
  - netstat, 247-250
  - nslookup, 250-251
  - pathping, 244-245
  - ping, 242-243
  - show mac-address-table, 252
  - tracert, 241-242
- command switches
  - arp, 246
  - netstat, 247
  - pathping, 245
  - ping, 243
  - tracert, 242

**commands**

arp, 245-247  
 arp -a, 245  
 catalyst switch configuration commands, 144-145  
 nbtstat, 250  
 netstat, 247-250  
 netstat -a, 132  
 nslookup, 250-251  
 pathping, 244-245  
 ping, 242-243  
 show, 264, 271  
 show cdp neighbors detail, 264  
 show interface, 126  
 show interface gigabitethernet 0/0, 126  
 show mac-address-table, 252  
 traceroute, 271  
 tracert, 241-242

**committed information rate (CIR), 32****community cloud, 112****company security policies, WANs, 272****comparing**

circuit switching and packet switching, 24  
 RADIUS and TACACS+, 13  
 static and default routing, 87-88

**compliance, network segmentation, 138****components**

of ISDN, 27  
 of MPLS (Multiprotocol Label Switching), 34

**computer room security, 193****configuration, firewalls, 196-197****configurations**

AAA, 145-146  
 link aggregation, 146  
   *EtherChannel*, 147  
   *Link Aggregation Control Protocol (LACP) modes*, 146-147  
 port mirroring, 148  
 security configuration issues, 267-268  
 switch configurations, 143-145  
 wireless configuration issues, 257-258

**configuring**

EtherChannel, 147  
 IPv6 addressing, 80-81  
   *EUI-64*, 81  
   *SLAAC (stateless address autoconfiguration)*, 82  
 switch port security, 186-188

**congestion avoidance, QoS, 107****congestion management, DiffServ, 106****connection establishment, TCP, 230****connection termination, TCP, 230****connectionless protocol, 231****connectors**

copper, 40  
   *coaxial connectors*, 41-42  
   *registered jack connectors*, 40-41  
   *RS-232*, 41  
 fiber-optic, 44

**content caching, proxy servers, 5****content filters, proxy servers, 5****content virtualization, medianets, 60****context-aware firewalls, 195****Control and Provisioning of Wireless Access Points (CAPWAP), 169****controllers, wireless LAN controllers, 169****conventions for writing**

IPv6 addresses, 76-77  
 IPv6 prefixes, 77-78

**convergence**

link-state protocols, 96-97  
 STP, 153

**converters, media converters, 45****copper, 37**

cables, 37  
 coaxial cables, 39-40  
 connectors, 40  
   *coaxial connectors*, 41-42  
   *registered jack connectors*, 40-41  
   *RS-232*, 41  
 plenum, 39  
 PVC cables, 39  
 twisted-pair cabling, 37-39

copper cable issues, 259-260  
copper line drivers, 272  
CoS (class of service), 106  
cost, metrics, 92  
CPE (customer premises equipment), 34, 271  
    WANs, 272  
CPU usage, 125  
crosstalk, copper cable, 260  
cRTP (RTP header compression), 107  
CSMA/CD (Carrier Sense Multiple Access with Collision Detection), 209  
CSU/DSU (channel service unit/data service unit), 272  
CUCM (Cisco Unified Communications Manager), 102-105  
CUCUM, 103  
customer premises equipment (CPE), 34, 271  
    WANs, 272  
CWDM (coarse wavelength-division multiplexing), 30

## **D**

-d switch, 242  
DAS (directly attached storage), 112  
data encapsulation, 203-204  
    MAC sublayer, 213  
data flow through layers, 203-204  
data integrity, 189  
data-link connection identifiers (DLCI), 32  
data link layer, OSI model, 202  
data link layer issues, networks, 264  
Data Over Cable Service Interface Specification (DOCSIS), 215  
data rates, OCx (Optical Carrier), 30  
data transport, 198  
data VLAN, 157  
DCSs (distributed control systems), 59  
DDoS (distributed DoS), 178

DE (discard eligibility) bit, 33  
decimal, 211  
dedicated leased lines, 31  
    terminating, 32  
default VLAN, 157  
delay, 105  
    metrics, 92  
demarc, 26  
demarcation point, 272  
demilitarized zone (DMZ), 196  
denial of service (DoS), 268  
dense wavelength-division multiplexing (DWDM), 30  
density, APs (access points), 166  
description, syslog, 131  
design, network design. *See* network design  
design considerations for networks, layers 1, 2, and 3, 118-119  
destination NAT (DNAT), 19  
device hardening, 185  
    configuring switch port security, 186-188  
    data integrity, 189  
    disabling unused network services, 186  
    hashing, 189  
    secure protocols, 186  
    user authentication, 188-189  
    wireless security, 190  
device saturation, wireless transmission, 256  
devices, WLANs, 167  
    wireless access points, 168  
    wireless bridges, 170  
    wireless LAN controllers, 169  
    wireless routers, 167-168  
DHCP (Dynamic Host Configuration Protocol), 15-17  
    misconfigured, 265  
    port numbers, 233  
DHCP snooping, 187  
DHCPv6, 80-82  
dialup, home and small office networks, 25-26

differentiated service code point (DSCP), 106  
 differentiated services, QoS, 106-107  
 dig, 240  
 Digital Subscriber Line (DSL), 27-28  
 Dijkstra Shortest Path First (SPF) algorithm, 95-96  
 Direct Sequence Spread Spectrum (DSSS), 164  
 directly attached storage (DAS), 112  
 disabling unused network services, 186  
 disaster recovery, 183  
 discard eligibility (DE) bit, 33  
 discovering neighbors, 264  
 distance limitations, copper cable, 260  
 distance vector, routing protocols, 90  
 distributed control system (DCS), 59  
 distributed DoS (DDoS), 178  
 divide-and-conquer approach, 236  
 DLCI (data-link connection identifiers), 32  
 DMZ (demilitarized zone), 196  
 DMZ devices, 197  
 DNAT (destination NAT), 19  
 DNS (Domain Name System), 17-18  
   misconfigured, 265  
   port numbers, 232  
   record types, 18  
 DNS issues, WANs, 271  
 DOCSIS (Data Over Cable Service Interface Specification), 215  
 documentation  
   network design, 119  
     *asset management*, 122  
     *baselines*, 122  
     *IP addressing*, 119-120  
     *network diagrams*, 120-121  
     *policies*, 122  
     *procedures*, 123  
   standard business documents, 220  
 documenting troubleshooting actions, 237

domain configurations, troubleshooting, 267  
 Domain Name System (DNS), 17-18  
   misconfigured, 265  
   record types, 18  
 domains, 63-64  
 door access controls, 194  
 DORA (Discover, Offer, Request, and Acknowledge), 16  
 DoS (denial of service), 268  
 DoS (denial of service) attack, 177-178  
 downgrading, 139  
 driver updates, 139  
 drops, 105  
 DSCP (differentiated service code point), 106  
 DSL (Digital Subscriber Line)  
   home and small office networks, 27-28  
   speeds, 27  
 DSSS (Direct Sequence Spread Spectrum), 164  
 dual-stack, IPv6, 83  
 duplex mismatch, 264  
 DWDM (dense wavelength-division multiplexing), 30  
 Dynamic Host Configuration Protocol (DHCP), 15-17  
 dynamic NAT, 19  
 dynamic routing metrics, 92  
 dynamic routing versus static routing, 87-88  
 dynamic routing protocols, 90-91

## E

-e switch, 249  
 E1 circuits, 31  
 E3 circuits, 31  
 EAP (Extensible Authentication Protocol), 189  
 edge and access control, 198  
 edge label switch router (ELSR), 34

**ediscovery, 198**

**EGP (Exterior Gateway Protocol), 89-90**

**EIA (Electronics Industry Alliance), 215**

**EIGRP (Enhanced Interior Gateway Routing Protocol), 89**

**electrical safety, 220**

**electromagnetic interference (EMI), 263**

**Electronics Industry Alliance (EIA), 215**

**electrostatic discharge (ESD), 220**

**ELSR (edge label switch router), 34**

**email usage policy, 122**

**emergency procedures, 221**

**EMI (electromagnetic interference), 263**

**encapsulating FC frames, 114**

**Encapsulating Security Payload (ESP), 11**

**end-to-end communication, TCP/IP network access layer, 210-211**

**end-user awareness, 183**

**Enhanced Interior Gateway Routing Protocol (EIGRP), 89**

**enterprise WANs, 32**

ATM (Asynchronous Transfer Mode), 33

Frame Relay, 32-33

Metro Ethernet, 35

MPLS (Multiprotocol Label Switching), 34

**environmental factors, wireless transmissions, 256**

**environmental monitoring, 127**

**error detection, PPP, 28**

**error recovery, 227**

TCP, 228-229

**escalating issues, 237**

**ESD (electrostatic discharge), 220**

**ESP (Encapsulating Security Payload), 11**

**EtherChannel, 146**

configuring, 147

**Ethernet, standards, 213**

TIA/EIA 568A and 568B standards, 214-215

wired standards, 213-214

wireless standards, 215-216

**Ethernet cabling properties, 214**

**Ethernet frames, encapsulating, 114**

**Ethernet switches, 142**

**EUI-64, 80**

IPv6, 81

**evil twins, 180**

**exam day, 275**

**exams, re-taking, 278**

**extended star topologies, 51**

**Extensible Authentication Protocol (EAP), 189**

**Exterior Gateway Protocol (EGP), 89-90**

## **F**

**facility, syslog, 131**

**failed exams, retaking, 278**

**far-end crosstalk (FEXT), 260**

**fault detection, 125**

**FC frames, encapsulating, 114**

**FCoE (fibre channel over Ethernet), 101, 113-114**

**FDDI (Fiber Distributed Data Interface), 50**

**FDM (frequency-division multiplexing), 210**

**feature changes and updates, 139**

**FECN (forward explicit congestion notification), 33**

**FEXT (far-end crosstalk), 260**

**FHRPs (first-hop redundancy protocols), 98-99**

**FHSS (Frequency-Hopping Spread Spectrum), 164**

**fiber cable issues, 260-261**

**Fiber Distributed Data Interface (FDDI), 50**

**fiber-optic cables, 43**

**fiber-optic connectors, 44**

**fibre channel, 113**



fibre channel over Ethernet (FCoE),  
 101, 113-114  
 fire extinguishers, 221  
 fire suppression, 221  
 firewalls, 2-3, 194-195  
   misconfigured, 267  
   placement and configuration, 196-197  
 FireWire, 57  
 firmware updates, 139  
 first-hop redundancy protocol (FHRP),  
 98-99  
 first responders, security breaches, 198  
 fixed switches, 142  
 fixed systems, fire suppression, 221  
 Flexible NetFlow, 133  
 flow control, TCP, 229  
 forensics concepts, 198  
 forensics report, 198  
 forward explicit congestion notification  
 (FECN), 33  
 forwarding STP, 153  
 four-post racks, 224  
 FQDN (fully qualified domain name),  
 17  
 fraggle attacks, 178  
 Frame Relay, 59  
   enterprise WANs, 32-33  
   packet switching, 23  
 free-standing racks, 224  
 frequencies, WLANs, 163-164  
 frequency bands, WLANs (wireless  
 installation), 171-172  
 frequency-division multiplexing  
 (FDM), 210  
 Frequency-Hopping Spread Spectrum  
 (FHSS), 164  
 frequency-shift keying (FSK), 164  
 friendly DoS, 178  
 FSK (frequency-shift keying), 164  
 FTP, port numbers, 232  
 F-type connectors, 42  
 full-mesh topologies, 53-54

fully qualified domain name  
 (FQDN), 17

## G

gateway, 102  
   VoIP, 15  
 Gateway Load Balancing Protocol  
 (GLBP), 99  
 GBIC (gigabit interface converter), 260  
 Generic Routing Encapsulation  
 (GRE), 12  
   IPv6, 85  
 get-bulk-request, 128  
 get-next-request, 128  
 get-request, 128  
 get-response, 128  
 gigabit interface converter (GBIC), 260  
 GLBP (Gateway Load Balancing  
 Protocol), 99  
 global unicast addresses, IPv6, 79  
 global unicast configuration options, 80  
 Graziani's 3-1-4 rule for remembering  
 global unicast address structure, 79  
 GRE (Generic Routing Encapsulation),  
 12  
   IPv6, 85  
 guest networks, 198

## H

H.323, port numbers, 233  
 hardening devices, 185  
   configuring switch port security, 186-188  
   data integrity, 189  
   disabling unused network services, 186  
   hashing, 189  
   secure protocols, 186  
   user authentication, 188-189  
   wireless security, 190  
 hardware and software tools, 252-253  
 hardware failure  
   physical layer issues, 263

- hardware firewalls, 195
  - hash-based message authentication code (HMAC), 190
  - hashing, 189
  - HBA (host bus adapter), 113
  - header fields, ATM (Asynchronous Transfer Mode), 33
  - headers, 228
  - hextets, 76
  - HFC (hybrid fiber and coaxial) network, 215
  - HIDS (host-based IDSs), 4
  - high availability, 98-99
  - HMAC (hash-based message authentication code), 190
  - hold-down timers, 94
  - home and small office networks, 25
    - broadband cable, 28-29
    - dialup, 25-26
    - DSL (Digital Subscriber Line), 27-28
    - ISDN, 26-27
    - PPP (Point-to-Point Protocol), 28
  - home networks, 58
  - honeynets, 138
  - honeypot, network segmentation, 138
  - hop count, 92
  - host-based anti-malware, 185
  - host-based firewalls, 195
  - host-based IDSs (HIDS), 4
  - host bus adapter (HBA), 113
  - host ranges, subnetting, 69-70
  - Hot Standby Router Protocol (HSRP), 99
  - HSRP (Hot Standby Router Protocol), 99
  - ht (high throughput), 165
  - HTTP, port numbers, 233
  - HTTP requests, 207
  - HTTP responses, 207
  - HTTPS (Hypertext Transfer Protocol Secure), 186
    - port numbers, 233
  - hub-and-spoke topologies, 52-53
  - hubs, network devices, 1
  - HVAC (heating, ventilation, and air-conditioning), procedures, 221
  - hybrid cloud, 112
  - hybrid topologies, 52
  - Hypertext Transfer Protocol Secure (HTTPS), 186
  - hypervisors, 108
    - identifying, 109
- I**
- IaaS (Infrastructure as a Service), 111
  - ICA (Independent Computing Architecture), 14
  - ICS (industrial control system), 59
  - identifying
    - hypervisors, 109
    - problems, 235-236
  - IDF (intermediate distribution frame), 223
  - IDS (intrusion detection systems), 3-4
  - IEEE 802.1X, 188, 197
  - IEEE 1901.5-2013, 214
  - ifconfig, 239-241
  - IGP (Interior Gateway Protocols), 90
  - IGRP (Interior Gateway Routing Protocol), 89
  - IKE (Internet Key Exchange), VPNs, 11-12
  - IMAP (Internet Message Access Protocol), port numbers, 233
  - IMP (Instant Messaging and Presence), 105
  - implementing
    - preventative measures, 237
    - solutions when troubleshooting, 237
  - incompatibilities, wireless configuration issues, 257
  - incorrect VLAN assignment, 264
  - Independent Computing Architecture (ICA), 14
  - industrial control system (ICS), 59

- industrial networks, 59
- Infrared (IR), 57
- Infrastructure as a Service (IaaS), 111
- infrastructure WLAN topologies, 167
- INID (intelligent network interface device), 272
- inside global, NAT, 19
- inside local, NAT, 19
- INSIDE zone devices, 197
- insider threats, 180
- instability, MAC database instability, 152
- installation safety, 220
- installing WLANs. *See* wireless installation
- Integrated Service Digital Network (ISDN), 23
- integrated services, QoS, 106
- intelligent network interface device (INID), 272
- interface errors
  - physical layer issues, 263
  - WANs, 271
- interface monitoring, 126
- interference
  - WANs, 272
  - wireless transmissions, 255
- interior environmental obstacles, wireless transmission issues, 256
- Interior Gateway Protocols (IGP), 90
- Interior Gateway Routing Protocol (IGRP), 89
- intermediate distribution frames (IDFs), 223
- Intermediate System-to-Intermediate System (IS-IS), 89
- Internet Key Exchange (IKE), VPNs, 11-12
- Internet layer, TCP/IP, 203, 208
- Internet Small Computer System Interface (iSCSI), 114-115
- Internet usage policies, 122
- Inter-Switch link (ISL), 159
- intrusion detection systems (IDS), 3-4
- intrusion prevention systems (IPS), 3-4
- IP addressing
  - documentation, 119-120
  - misconfigured IP addressing, 265
- ip arp inspection trust, 187
- ip dhcp snooping limit rate 5, 187
- IP phone, 15, 102
- IP routes, missing, 265
- ipconfig, 239
- IPS (intrusion prevention systems), 3-4
- IPsec (IP Security), 186
  - VPNs, 11-12
- IPv4 addressing, 64
  - address types, 66-67
  - private, 66
  - public, 66
  - structure, 64-65
- IPv6 addressing
  - address types, 78
    - global unicast addresses*, 79
    - link-local unicast addresses*, 79-80
  - configuring, 80-81
    - EUI-64*, 81
    - SLAAC (stateless address autoconfiguration)*, 82
  - conventions for writing, 76-77
    - prefixes*, 77-78
  - migrating
    - dual-stack*, 83
    - tunneling*, 83-85
  - overview, 75-76
- ipv6 unicast-routing, 82
- IPv6 Unnumbered, 80
- IR (Infrared), 57
- ISATAP, tunneling (IPv6), 85
- iSCSI (Internet Small Computer System Interface), 114-115
- ISDN (Integrated Service Digital Network), 23
  - components of, 27
  - home and small office networks, 26-27

**IS-IS (Intermediate System-to-Intermediate System)**, 89

**ISL (Inter-Switch link)**, 159

**ISM bands (industrial, scientific, and medical)**, 165

## **J**

**jamming**, 269

**jitter**, 105

## **K**

**Kerberos**, 189

**key fobs**, 194

**keypad/cipher locks**, 194

## **L**

**L2F (Layer 2 Forwarding)**, 12

**L2TP (Layer 2 Tunneling Protocol)**, 12

**label switch router (LSR)**, 34

**labeling, best practices**, 224

**LACP (Link Aggregation Control Protocol)**, 146

modes, 146-147

**LANs (local area networks)**, 57-58

**LAN switches**, 143

**latency**, 273

**Layer 2 Forwarding (L2F)**, 12

**Layer 2 Tunneling Protocol (L2TP)**, 12

**layers**

data flow through, 203-204

OSI model, 202-203

TCP/IP, 203

**LDAP (Lightweight Directory Access Protocol)**, port numbers, 233

**legacy systems, network segmentation**, 138

**LFI (link fragmentation and interleaving)**, 107

**light meter**, 253

**Lightweight Access Point Protocol (LWAPP)**, 169

**Lightweight Directory Access Protocol (LDAP)**, port numbers, 233

**limitations of 10BASE-T**, 141

**line of sight**, 273

**link aggregation**, 146

EtherChannel, configuring, 147

LACP (Link Aggregation Control Protocol) modes, 146-147

**Link Aggregation Control Protocol (LACP)**, 146

**link efficiency**, 107

**link fragmentation and interleaving (LFI)**, 107

**Link Layer Discovery Protocol (LLDP)**, 264

**link-local unicast addresses, IPv6**, 79-80

**link-state advertisements (LSA)**, 95

**link-state database (LSDB)**, 95

**link-state routing protocols**, 91, 94

convergence, 96-97

Dijkstra Shortest Path First (SPF) algorithm, 95-96

LSDB (link-state database), 95

**LLC (Logical Link Control) sublayer**, 213

**LLDP (Link Layer Discovery Protocol)**, 264

**load, metrics**, 92

**load balancers**, 5-6

**load balancing, network segmentation**, 138

**local AAA authentication**, 145

**local addressing**, 63

collision and broadcast domains, 63-64

MAC addresses, 63

**local area networks (LANs)**, 57-58

**local group configurations, troubleshooting**, 267

**local loop**, 25

**Logical Link Control (LLC) sublayer**, 213

**logical topology diagrams**, 120

**looking glass sites**, 253

loopbacks, 272  
 looped link detection, PPP, 28  
 loops, routing loop prevention, 94  
 loss of Internet connectivity,  
   WANs, 271  
 LSA (link-state advertisements), 95  
 LSDB (link-state database), 95  
 LSR (label switch router), 34  
 LWAPP (Lightweight Access Point  
   Protocol), 169

## M

MAC address filtering, 188  
 MAC address OUI, 269  
 MAC (Media Access Control)  
   addresses, 142  
   local addressing, 63  
   static, 188  
   switch forwarding, 143  
 MAC database instability, 152  
 MAC sublayer, 213  
 main distribution frames (MDF), 223  
 major updates, 139  
 malicious employees, 180  
 malicious users, 268  
 malware, 268  
   anti-malware software, 185  
 MAM (mobile application manage-  
   ment), 219  
 MAN (metropolitan area network),  
   35, 59  
 man-in-the-middle attacks, 179  
 managed switches, 142  
 management, medianets, 60  
 Management Information Base (MIB),  
   127-130  
 management VLANs, 157  
 managing change, 224-225  
 mantraps, 194  
 manual tunneling, IPv6, 84  
 marking DiffServ QoS, 106  
 master service agreement (MSA), 220  
 material safety data sheet (MSDS), 220  
 MDF (main distribution frames), 223  
 MDIX (medium dependent interface  
   crossover), 259  
 MDM (mobile device management),  
   219  
 media, network devices, 1  
 Media Access Control (MAC) sublayer,  
   213  
 media converters, 45  
 Media Gateway Control Protocol  
   (MGCP), port numbers, 233  
 medianets, 60  
 medium dependent interface crossover  
   (MDIX), 259  
 memorandum of understanding  
   (MOU), 220  
 memory usage, 125  
 mesh WLAN topologies, 167  
 message format, syslog, 131-132  
 message types, SNMP (Simple Net-  
   work Management Protocol), 127-128  
 metrics, dynamic routing metrics, 92  
 Metro Ethernet, 35  
 metropolitan area network (MAN),  
   35, 59  
 MGCP (Media Gateway Control  
   Protocol), port numbers, 233  
 MIB (Management Information Base),  
   127  
   SNMP (Simple Network Management),  
     128-130  
 Microsoft Challenge Handshake  
   Authentication Protocol (MS-CHAP),  
   28, 189  
 migrating IPv6  
   dual-stack, 83  
   tunneling, 83-85  
 MIMO (multiple-input and multiple-  
   output), 166  
   wireless configuration issues, 258  
 minor updates, 139  
 Miredo, 85  
 misconfigured ACLs/applications, 267

misconfigured DHCP, 265  
misconfigured DNS, 265  
misconfigured firewalls, 267  
misconfigured IP addressing, 265  
mismatched channels, wireless transmissions, 255  
missing IP routes, 265  
MMF (multimode fiber), 43  
MNEMONIC, syslog, 131  
mobile application management (MAM), 219  
mobile device management (MDM), 219  
mobile device policies, 122  
mobility, medianets, 60  
modems  
  analog modems, 1  
  broadband modems, 2  
modes  
  LACP (Link Aggregation Control Protocol), 146-147  
  VTP (VLAN Trunking Protocol), 160  
modular switches, 142  
modulation, 209  
MOU (memorandum of understanding), 220  
MPLS (Multiprotocol Label Switching), 34, 59  
MSA (master service agreement), 220  
MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), 28, 189  
MSDS (material safety data sheet), 220  
MTU (maximum transmission unit), 264  
  black hole, 264  
MU (multiuser), 166  
multicast transmission, IPv4, 67  
multifactor authentication, 189  
multilayer switches, network devices, 1  
multilink interface, PPP, 28  
multimeters, 252  
multimode fiber (MMF), 43

multiple frame transmission, 152  
multiple-input and multiple-output (MIMO), 166  
Multiprotocol Label Switching (MPLS), 34, 59  
multiuser, 166  
MUMIMO (multiuser multiple-input and multiple-output), 166  
MX (mail exchange), 18

## **N**

NAC (Network Access Control), 123  
NAS (network attached storage), 112-113  
NAT (Network Address Translation), 18-20, 66  
National Institute of Standards and Technology (NIST), 111  
native VLAN, 157  
nbtstat, 239, 250  
nbtstat -r, 250  
near-end crosstalk (NEXT), 260  
Near Field Communication (NFC), 57, 194  
Nessus Home Vulnerability Scanner, 182  
NetBIOS, port numbers, 232  
NetFlow, 133-135  
  collector functions, 134  
netstat, 239, 247-250  
netstat -a command, 132  
netstat -e, 249  
netstat -n, 248  
netstat -r, 249  
Network Access Control (NAC), 123  
network access layer, TCP/IP, 203, 208  
  collisions, 209  
  end-to-end communication, 210-211  
  transmission techniques, 209-210  
Network Address Translation (NAT), 18-20, 66  
network addresses, calculating, 65-66

**network admission procedures, 123**

**network attached storage (NAS), 112-113**

**network-based anti-malware, 185**

**network-based firewalls, 195**

**network-based IDSs (NIDS), 4**

**network closets, 193**

**network design, 117**

considerations for layers 1, 2, and 3, 118-119

documentation, 119

*asset management, 122*

*baselines, 122*

*IP addressing, 119-120*

*network diagrams, 120-121*

*policies, 122*

*procedures, 123*

sample approach to, 117-118

wireless considerations, 119

**network devices, 1**

analog modems, 1

AP (access point), 2

broadband modems, 2

clients, 1

firewalls, 2-3

hubs, 1

IDS (intrusion detection systems), 3-4

IPS (intrusion prevention systems), 3-4

load balancers, 5-6

media, 1

multilayer switches, 1

packet shapers, 6

proxy servers, 5

routers, 1

servers, 1

switches, 1

VPN concentrators, 6

**network diagrams, documentation, 120-121**

**network infrastructures, 57**

CANs (campus area networks), 58

industrial networks, 59

LANs (local area networks), 57-58

MANs (metropolitan area networks), 59

medianets, 60

PANs (personal area networks), 57

WANs (wide area networks), 59

**network interface unit (NIU), 272**

**network issues**

data link layer issues, 264

network layer issues, 265

physical layer issues, 263-264

**network layer, OSI model, 202**

**network layer issues, 265**

**network management system (NMS), 127**

**network models, 201-202**

data flow through layers, 203-204

OSI model, 201

*layers, 202-203*

TCP/IP model, 201

*layers and protocols, 203*

**network monitoring, 125-127**

port scanners, 132-133

*packet flow monitors, 133-135*

*packet sniffers, 133*

SNMP (Simple Network Management Protocol), 127

*message types, 127-128*

*MIB, 128-130*

*versions, 128*

syslog, 130

*message format, 131-132*

*operations, 130*

*security levels, 130-131*

**network monitoring procedures, 123**

**Network News Transport Protocol (NNTP), port numbers, 233**

**network operating system (NOS), 55**

**network policies, 219**

**network segmentation, 137-138**

**network termination 1 (NT1), 27**

**Network Time Protocol (NTP), 233**

**network topologies, 49**

bus, 49-50

client-server, 55

- extended star, 51
- full-mesh, 53-54
- hub-and-spoke, 52-53
- partial mesh, 54-55
- peer-to-peer networks, 56-57
- ring, 50-51
- star, 51

**network usage policies, 122**

**networking device virtualization, 109-110**

**networks, WAN link options, 24**

- dedicated leased lines, 31
- enterprise WANs, 32-35
- home and small office networks, 25-29
- SONET (Synchronous Optical Network), 30
- wireless, 29-30

**NEXT (near-end crosstalk), 260**

**NFC (Near Field Communication), 57, 194**

**NIC teaming misconfiguration, 264**

**NIDS (network-based IDSs), 4**

**NIST (National Institute of Standards and Technology), 111**

**NIU (network interface unit), 272**

**NMS (network management system), 127**

**NNTP (Network News Transport Protocol), port numbers, 233**

**non-persistent agents, 197**

**NOS (network operating system), 55**

**nslookup, 240-251**

**nslookup tool, 265**

**NT1 (network termination 1), 27**

**NTP (Network Time Protocol), port numbers, 233**

**numbering systems, TCP/IP, 211**

## O

**octal numbering systems, 211**

**OCx (Optical Carrier), 30**

**OFDM (Orthogonal Frequency-division Multiplexing), 165**

**offboarding, 122**

**omnidirectional antenna, 166**

**on mode, LACP, 146**

**onboarding, 122**

**one-way satellite system, 29**

**open, copper cable, 259**

**open networks, wireless configuration issues, 257**

**open ports, 181**

**Open Shortest Path First (OSPF), 89**

**operating systems, unpatched, 268**

**operations**

- RSTP, 155
- syslog, 130
- VTP (VLAN Trunking Protocol), 160-161

**Optical Carrier (OCx), 30**

**optical time domain reflectometer (OTDR), 47**

**Organizationally Unique Identifier (OUI), 63, 269**

**Orthogonal Frequency-division Multiplexing (OFDM), 165**

**OS updates, 139**

**OSI model, 201**

- layers, 202-203

**OSPF (Open Shortest Path First), 89, 95**

**OUI (Organizationally Unique Identifier), 63, 269**

**outside global, NAT, 19**

**outside local, NAT, 19**

**OUTSIDE zone devices, 197**

**overlapping channels, wireless transmissions, 255**

**ownership policies, 122**

## P

**PaaS (Platform as a Service), 111**

**packet abuse, 179**

**packet flow monitors, 133-135**

**packet shapers, 6**



- packet sniffers, 133
- packet switching, 23-24
  - versus circuit switching, 24
- PAgP (Port Aggregation Protocol), 146
- PANs (personal area networks), 57
- PAP (Password Authentication Protocol), 28, 188
- partial mesh topologies, 54-55
- passive mode, LACP, 146
- Password Authentication Protocol (PAP), 28, 188
- PAT (Port Address Translation), 19-20
- patches, 139, 181
- pathping, 239, 244-245
- PBX (Private Branch Exchange), 15, 102
- peer-to-peer networks, 56-57
- penetration testing, 182
- performance optimization, network segmentation, 138
- perimeter security, 193
- permanent DoS, 178
- persistent agents, 197
- personal area networks (PANs), 57
- personal software policies, 122
- phase, 163
- phase-shift keying (PSK), 164
- physical layer, OSI model, 202
- physical layer issues, networks, 263-264
- physical security, 193-194
- physical topology diagrams, 120
- pin positions, 214
- ping, 239, 242-243
- ping -6, 239
- ping6, 239
- ping of death, 178
- placement of firewalls, 196-197
- plans of action, establishing, 236
- Platform as a Service (PaaS), 111
- PLCs (programmable logic controllers), 59
- plenum, 39
- POD (point of demarcation), 272
- PoE (Power over Ethernet), 142
- point of demarcation (POD), 272
- point-to-multipoint topologies, 53
- Point-to-Point Protocol (PPP), 28
- Point-to-Point Tunneling Protocol (PPTP), 12
- poison reverse, 94
- policies
  - AUP (acceptable use policies), 219
  - company security policies (WANs), 272
  - documentation, 122
  - network policies, 219
  - safety policies, 220-221
  - security policies, 219
- policing QoS, 107
- polyvinyl chloride (PVC), 39
- POP3, port numbers, 233
- Port Address Translation (PAT), 19-20
- Port Aggregation Protocol (PAgP), 146
- port costs, STP, 154
- port mirroring, configurations, 148
- port numbers, 231-232
  - protocols, 232-233
- port roles
  - RSTP, 155-156
  - STP, 155
- port scanners, 132-133
  - packet flow monitors, 133-135
  - packet sniffers, 133
- port states, 155
- ports
  - open ports, 181
  - source ports, 231
- positive acknowledgement, 229
- post-exam information, receiving your certificate, 277
- posture assessment, 197
- power anomalies, physical layer issues, 263
- power failures, physical layer issues, 263

**power levels, wireless configuration issues, 257**

**power management, 224**

**power monitoring, 127**

**Power over Ethernet (PoE), 142**

**powered ports, 142**

**PPP (Point-to-Point Protocol), home and small office networks, 28**

**PPTP (Point-to-Point Tunneling Protocol), 12**

**prefixes, writing for IPv6, 77**

**presentation layer, OSI model, 202**

**preventative measures, implementing, 237**

**preventing routing loops, 94**

**PRI (primary rate interface), 26**

**private, IPv4 addressing, 66**

**Private Branch Exchange (PBX), 15, 102**

**private cloud, 111**

**private networks, network segmentation, 138**

**problems, identifying, 235-236**

**procedures**

documentation, 123

emergency procedures, 221

fire suppression, 221

HVAC (heating, ventilation, and air-conditioning), 221

for security breaches, 198

**procedures for adding new users, 123**

**procedures for reporting violations, 123**

**programmable logic controllers (PLCs), 59**

**protocol analyzer, 253**

**protocol weaknesses, 179**

**protocols**

BGP (Border Gateway Protocol), 89

CHAP (Challenge Handshake Authentication Protocol), 28, 189

classful routing protocols, 91

classless routing protocols, 91

DHCP (Dynamic Host Configuration Protocol), 15-17

distance vector routing protocols, 90

EAP (Extensible Authentication Protocol), 189

EGP (Exterior Gateway Protocol), 89-90

EIGRP (Enhanced Interior Gateway Routing Protocol), 89

GLBP (Gateway Load Balancing Protocol), 99

GRE (Generic Routing Encapsulation), 12

HSRP (Hot Standby Router Protocol), 99

HTTPS (Hypertext Transfer Protocol Secure), 186

ICA (Independent Computing Architecture), 14

IGP (Interior Gateway Protocols), 90

IGRP (Interior Gateway Routing Protocol), 89

IPsec, 186

IS-IS (Intermediate System-to-Intermediate System), 89

Kerberos, 189

L2F (Layer 2 Forwarding), 12

L2TP (Layer 2 Tunneling Protocol), 12

link-state routing, 94

*convergence, 96-97*

*Dijkstra Shortest Path First (SPF) algorithm, 95-96*

*LSDB (link-state database), 95*

link-state routing protocols, 91

MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), 28, 189

OSPF (Open Shortest Path First), 89

PAP (Password Authentication Protocol), 28, 188

port numbers, 232-233

PPTP (Point-to-Point Tunneling Protocol), 12

RADIUS, 13

RDP (Remote Desktop Protocol), 14

RIP (Routing Information Protocol), 89

RIPng (Routing Information Protocol next generation), 89

RIPv2 (Routing Information Protocol version 2), 89

routing protocols, 88

RTP (Real-time Transport Protocol), 15

secure protocols, 186

SFTP (Secure File Transfer Protocol), 186

SIP (Session Initiation Protocol), 15

SNMPv3 (Simple Network Management Protocol version 3), 186

SSH (Secure Shell), 14, 186

SSL (Secure Sockets Layer), 12, 186

TACACS+, 13

TCP (Transmission Control Protocol), 227

- connection establishment, 230*
- connection termination, 230*
- error recovery, 228, 229*
- flow control, 229*
- headers, 228*

TCP/IP model, 203

Telnet, 14

TLS (Transport Layer Security), 12, 186

UDP (User Datagram Protocol), 227, 231

- headers, 228*

unsecure protocols, 181

VRRP (Virtual Router Redundancy Protocol), 99

**proximity readers, 194**

**proxy servers, 5**

**pruning, VTP (VLAN Trunking Protocol), 161-162**

**PSK (phase-shift keying), 164**

**PSTN (public switched telephone network), 25, 103**

**PTR records, 18**

**public cloud, 112**

**public IP addressing, IPv4 addressing, 66**

**public networks, network segmentation, 138**

**Public Switched Telephone Network (PSTN), 25, 103**

**punch down tool, 46**

**PVC (polyvinyl chloride), 39**

## Q

**QAM (quadrature amplitude modulation), 164**

**QoE (quality of experience), medianets, 60**

**QoS (Quality of Service), 101, 105-106**

- DiffServ, 106-107

**quadrature amplitude modulation (QAM), 164**

**quality of experience (QoE), medianets, 60**

**Quality of Service. *See* QoS**

**quarantine networks, 197**

## R

**R reference point, 27**

**-r switch, 249**

**rack systems, best practices, 224**

**radio frequency (RF), vulnerabilities, 181**

**radio frequency interference (RFI), 263**

**radio waves, 163**

**RADIUS (Remote Authentication Dial-In User Service), 13, 268**

**rain fade, 273**

**Rapid STP (RSTP), 151**

**RAS (remote access service), 14**

**RDP (Remote Desktop Protocol), 14**

- port numbers, 233

**read-only (ro), 128**

**read-write (rw), 128**

**Real-Time Streaming Protocol (RTSP), port numbers, 233**

**Real-time Transport Protocol (RTP), 15, 102**

**Recommended Standard 232 (RS-232), 41**

**record types, DNS (Domain Name System), 18**

**redundant switched topology, 152**

**reflected DoS (DDoS), 178**

**registered jack connectors, 40-41**

reliability, metrics, 92

remote access service (RAS), 14

remote access services, 12-14

AAA (authentication, authorization, and accounting), 13

Remote Authentication Dial-In User Service (RADIUS), 13, 268

Remote Desktop Protocol (RDP), 14  
port numbers, 233

remote terminal units (RTU), 59

re-taking exams, 278

reverse proxy, 5

RFI (radio frequency interference), 263

RF (radio frequency), vulnerabilities, 181

RG-6, 40

RG-58, 40

RG-59, 40

ring topologies, 50-51

SONET, 31

RIP (Routing Information Protocol), 89

metrics, 92

RIPng (Routing Information Protocol next generation), 89

RIPv2 (Routing Information Protocol version 2), 89

risk, DoS (denial of service) attack, 177-178

risk management, 182-183

RJ-11 (type 11 registered jack), 40

RJ-45 (type 45 registered jack), 40

RJ-48C (type 48C registered jack), 40

ro (read-only), 128

rogue access points, wireless configuration issues, 257

rogue AP, 180

rollover cables, 39

round trip timer (RTT), 241

route aggregation, 97-98

route poisoning, 94

route redistribution, 90

router configurations, WANs, 272

routers

network devices, 1

wireless routers, 167-168

routing, administrative distance (AD), 93

Routing Information Protocol (RIP), 89

Routing Information Protocol next generation (RIPng), 89

Routing Information Protocol version 2 (RIPv2), 89

routing loop prevention, 94

routing protocols, 88

AS (autonomous system), 90

classful routing protocols, 91

classless routing protocols, 91

distance vector, 90

link-state routing protocols, 91

route redistribution, 90

RS-232, 41

rsh (remote shell), port numbers, 232

RSTP (Rapid STP), 151

operations, 155

port roles, 155-156

port states, 155

RTP (Real-time Transport Protocol), 15, 102

port numbers, 233

RTP header compression (cRTP), 107

RTSP (Real-Time Streaming Protocol), port numbers, 233

RTT (round trip timer), 241

RTU (remote terminal units), 59

rw (read-write), 128

## S

SaaS (Software as a Service), 111

safety policies, 220-221

same service set identifier (SSID), 171

sampling size, 210

SAN (storage area network), 112

DAS (directly attached storage), 112

- fibres channel, 113
- fibres channel over Ethernet (FCoE), 113-114
- iSCSI (Internet Small Computer System Interface), 114-115
- NAS (network attached storage), 112-113
- satellites, 29**
  - WANs, 273
- SCADA (Supervisory Control and Data Acquisition), 59**
- SCADA systems, network segmentation, 138**
- SCCP (Skinny Client Control Protocol), 103**
- score report, 275**
- scores, certified score report, 275**
- SCP, port numbers, 232**
- SDN (software-defined networking), 110**
- SDSL (symmetric DSL), 27**
- Secure File Transfer Protocol (SFTP), 186**
- secure protocols, 186**
- Secure Shell (SSH), 14, 186**
- Secure Sockets Layer (SSL), 12, 186**
- security**
  - access control models, 197-198
  - firewalls, 194-195
    - placement and configuration, 196-197*
  - medianets, 60
  - network segmentation, 138
  - physical security, 193-194
  - risk management, 182-183
  - switch port security, configuring, 186-188
  - troubleshooting, 268-269
  - vulnerabilities, 181
  - wireless security, 190
- security breaches, procedures for, 198**
- security configuration issues, 267-268**
- security guards, 194**
- Security Information and Event Management (SIEM), 126**
- security levels, syslog, 130-131**
- security monitoring, 125**
- security policies, 219**
- security procedures, 123**
- seq no, syslong, 131**
- server mode, VTP (VLAN Trunking Protocol), 160**
- server rail racks, 224**
- server virtualization, 108-109**
- servers**
  - network devices, 1
  - proxy servers, 5
- service level agreement (SLA), 220, 272**
- session control, medianets, 60**
- Session Initiation Protocol (SIP), 15, 102**
  - port numbers, 233
- session layer, OSI model, 202**
- sessions hijacking, 179**
- set-request, 128**
- severity, syslog, 131**
- SFP (small form-factor pluggable), 260**
- SFTP (Secure File Transfer Protocol), 186**
  - port numbers, 232
- shaping QoS, 107**
- shielded twisted-pair (STP), 37**
- shipworm, 85**
- short, copper cable, 259**
- Shortest Path Bridging (SPB), 156**
- show cdp neighbors detail, 264**
- show commands, 264, 271**
- show interface command, 126**
- show interface gigabitethernet 0/0, 126**
- show ip route, 92**
- show mac-address-table, 240, 252**
- SIEM (Security Information and Event Management), 126**
- signal loss, wireless transmissions, 255**
- signal-to-noise ratio, wireless transmissions, 255**
- signature-based IDSs, 4**

Simple Network Management Protocol. *See* SNMP

Simple Network Management Protocol version 3 (SNMPv3), 186

Simple Network Time Protocol (SNTP), port numbers, 233

simultaneous wired/wireless connections, physical layer issues, 264

single-mode fiber (SMF), 43

single point of failure, 183

single sign-on, 189

SIP (Session Initiation Protocol), 15, 102

port numbers, 233

site surveys, WLANs, 172

site-to-site VPNs, 9

Skinny Client Control Protocol (SCCP), 103

SLA (service level agreement), 220, 272

SLAAC (Stateless Address Autoconfiguration), 80-82

small form-factor pluggable (SFP), 260

smart jacks, 26, 272

SMB (Server Message Block), port numbers, 232

SMF (single-mode fiber), 43

SMTP (Simple Mail Transfer Protocol), port numbers, 233

smurf attack, 178

SNAT (Static NAT), 19

snips, 46

SNMP (Simple Network Management Protocol), 127

message types, 127-128

MIB (Management Information), 128-130

port numbers, 233

versions, 128

SNMP Trap, port numbers, 233

SNMPGET, 129

SNMPv1, 128

SNMPv2c, 128

SNMPv3, 128, 186

SNTP (Simple Network Time Protocol), port numbers, 233

SOA (start of authority) record, 18

social engineering, 180

software, patches/updates, 139

Software as a Service (SaaS), 111

software-defined networking (SDN), 110

software firewalls, 195

software procedures, 123

solutions, 237

SONET (Synchronous Optical Network), 30

SOW (statement of work), 220

spanning tree port states, 154

Spanning Tree Protocol (STP), 151, 264

SPB (Shortest Path Bridging), 92, 156

speed mismatch, 264

speed spectrum, 164

speed test sites, 253

speeds, DSL, 27

SPF (Dijkstra Shortest Path First) algorithm, 95-96

SPI (stateful packet inspection) firewalls, 195

split horizon, 94

split horizons, WANs, 271

split pairs, copper cable, 260

spoofing, 179

spread spectrum, 164

SSH (Secure Shell), 14, 186

port numbers, 232

SSID (same service set identifier), 171

SSL (Secure Sockets Layer), 12, 186

S/T reference point, 27

standard business documents, 220

standards, Ethernet, 213

TIA/EIA 568A and 568B standards, 214-215

wired standards, 213-214

wireless standards, 215-216

- star bus topologies, 52
- star topologies, 51
- stateful inspection firewalls, 195
- stateful packet inspection (SPI) firewalls, 195
- Stateless Address Autoconfiguration (SLAAC), 80
  - IPv6, 82
- stateless firewalls, 195
- statement of work (SOW), 220
- static MAC addresses, 188
- Static NAT (SNAT), 19
- static routes, 88
- static routing versus dynamic routing, 87-88
- storage area networks (SANs), 112
  - DAS (directly attached storage), 112
  - fibre channel, 113
  - fibre channel over Ethernet (FCoE), 113-114
  - iSCSI (Internet Small Computer System Interface), 114-115
  - NAS (network attached storage), 112-113
- storage space, 125
- STP (shielded twisted-pair), 37, 152
  - algorithms, 152-153
  - port costs, 154
  - port roles, 155
  - port states, 155
- STP (Spanning Tree Protocol), 151, 264
- STP convergence, 153
- structure, IPv4 addressing, 64-65
- stub networks, 88
- study resources, WLANs, 175-176
- subnet masks, 65, 69
- subnet multipliers, 69
- subnets, 69-70
- subnetting, 68
  - determining how many bits to borrow, 68-69
  - determining subnet masks, 69
    - determining subnet multiplier, 69
    - examples, 70-71
    - listing subnets, host ranges and broadcast addresses, 69-70
- subset advertisement message, 161
- summary advertisement message, 161
- Supervisory Control And Data Acquisition (SCADA), 59
- surveys, wireless site surveys (WLANs), 172
- switch configuration, 143-145
- switch forwarding, MAC addresses, 143
- switch port security, configuring, 186-188
- switch types, 142
- switches
  - e, 249
  - Ethernet switches, 142
  - evolving from bridges, 141-142
  - LAN switches, 143
  - multilayer switches, 1
  - network devices, 1
  - powered, 142
  - r, 249
  - unpowered ports, 142
  - virtual switches, 109
- switching,
  - evolution to, 141
    - from bridges to switches, 141-142*
    - switch types, 142*
  - logic, 142-143
- switching loops, 264
- switchport port-security, 188
- switchport port-security mac-address sticky, 188
- symmetric DSL (SDSL), 27
- Synchronous Optical Network (SONET), 30
- syslog, 130
  - message format, 131-132
  - operations, 130
  - security levels, 130-131

**T**

T1 circuits, 31

T3 circuits, 31

TA (terminal adapter), 27

TACACS (Terminal Access Controller Access-Control System), 268

TACACS+ (Terminal Access Controller Access-Control System Plus), 13

TCP (Transmission Control Protocol), 227

connection establishment, 230

connection termination, 230

error recovery, 228-229

flow control, 229

headers, 228

TCP SYN flood, 178

TCP/IP

application layer, 207

Internet layer, 208

network access layer, 208

*collisions, 209*

*end-to-end communication, 210-211*

*transmission techniques, 209-210*

numbering systems, 211

transport layer, 207-208

TCP/IP models, 201

data flow through layers, 203

TCP/IP Transport Layer, 227

TDM (time-division multiplexing), 209

TE1 (terminal endpoint 1), 27

TE2 (terminal endpoint 2), 27

telco, 25

Telecommunications Electronics

Material Protected from Emanating Spurious, 181

Telecommunications Industry Association (TIA), 215

Telnet, 14

port numbers, 232

TEMPEST (Telecommunications Electronics Material Protected from Emanating Spurious), 181

Temporal Key Integral Protocol (TKIP), 190

Teredo (RFC 4380), 85

Terminal Access Controller Access-Control System (TACACS), 268

Terminal Access Controller Access-Control System Plus (TACACS+), 13

terminal adapter (TA), 27

terminal endpoint 1 (TE1), 27

terminal endpoint 2 (TE2), 27

terminating dedicated leased lines, 32

testing troubleshooting theories, 236

testing labs, network segmentation, 138

TFTP (Trivial File Transfer Protocol), port numbers, 232

theories, 236

thick Aps, wireless configuration issues, 258

threats, 180. *See also* attacks

insider threats, 180

malicious employees, 180

protocol weaknesses, 179

TIA (Telecommunications Industry Association), 215

TIA/EIA 568A standards, Ethernet, 214-215

TIA/EIA 568B standards, Ethernet, 214-215

time-division multiplexing (TDM), 209

Time to Live (TTL) field, 94

timestamp, syslog, 131

tip and ring, 26

TKIP (Temporal Key Integral Protocol), 190

TLS (Transport Layer Security), 12, 186

Token Ring, 50

toner probe, 253

tools

for cable installation, 45-47

command-line tools, 239-240

*arp, 245-247*

*ifconfig, 240-241*



*ipconfig*, 240-241

*nbtstat*, 250

*netstat*, 247-250

*nslookup*, 250-251

*pathping*, 244-245

*ping*, 242-243

*show mac-address-table*, 252

*tracert*, 241-242

hardware and software tools, 252-253

**top-down approach**, 236

**topologies**

redundant switched topology, 152

VoIP network topology, 15

WLANs, 167

**ToS (type of service)**, 106

**traceroute**, 239, 265, 271

**traceroute -6**, 239

**traceroute6**, 239

**tracert**, 239, 241-242

**tracert -6**, 239

**traffic conditioners**, 107

**training, end-user awareness**, 183

**transition strategies, IPv6 addressing**,  
76

**Transmission Control Protocol (TCP)**,  
227

headers, 228

**transmission methods (WLANs)**,  
164-165

**transmission techniques, TCP/IP**  
network access layer, 209-210

**Transparent Interconnection of Lots of  
Links (TRILL)**, 156

**transparent mode, VTP (VLAN Trunk-  
ing Protocol)**, 160

**transport layer**

OSI model, 202

TCP/IP, 203, 207-208

**Transport Layer Security (TLS)**, 12,  
186

**trap**, 128

**triggered updates**, 94

**TRILL (Transparent Interconnection of  
Lots of Links)**, 156

**Trivial File Transfer Protocol (TFTP)**,  
port numbers, 232

**troubleshooting**, 235

documenting findings, actions, and out-  
comes, 237

establishing plans of action, 236

establishing theories, 236

identifying problems, 235-236

implementing solutions, 237

security, 268-269

security configuration issues, 267-268

testing theories, 236

verifying solutions/implementing preven-  
tative measures, 237

wireless configuration issues, 257-258

wireless transmission issues, 255-256

*interior environmental obstacles*, 256

**trunking VLANs**, 158-159

**TTL (Time to Live) field**, 94

**tunneling, IPv6**, 83-85

**twisted-pair cabling, copper**, 37-39

**two-factor authentication**, 189

**two-post racks**, 224

**two-way satellite system**, 29

**Tx/Rx reverse, copper cable**, 259

**Type 1 Bare Metal Hypervisor  
Approach**, 108

**Type 2 hosted hypervisor**, 108

**Type 2 hypervisors**, 108

**type 11 registered jack (RJ-11)**, 40

**type 45 registered jack (RJ-45)**, 40

**type 48C registered jack (RJ-48C)**, 40

**type of service (ToS)**, 106

**types of switches**, 142

## U

**U reference point**, 27

**UC (unified communications)**, 14-15

**UDP (User Datagram Protocol)**, 227,  
231

headers, 228

- unencrypted channels**, 181
- unicast transmission**, 66
- unidirectional antennas**, 166
- unified communications**, 101-103
  - cloud computing, 111-112
  - CUCM, 104-105
  - PSTN (public switched telephone network), 103
  - QoS. *See* QoS
  - virtualization, 107
    - networking device virtualization*, 109-110
    - server virtualization*, 108-109
    - software-defined networking*, 110
  - VoIP, 102-104
- unified communications (UC)**, 14-15
- Unified Threat Management (UTM) firewalls**, 195
- uninterruptible power supplies (UPS)**, 263
- Unity**, 102-105
- universal serial bus (USB)**, 57
- unmanaged switches**, 142
- unpatched firmware**, 268
- unpowered ports, switches**, 142
- insecure protocols**, 181
- unshielded twisted-pair (UTP)**, 37-38
- untested updates, wireless configuration issues**, 257
- unused network services, disabling**, 186
- updates**, 139, 181
- upgrading**, 139
- UPS (uninterruptible power supplies)**, 263
- USB (universal serial bus)**, 57
- user account policies**, 122
- user authentication**, 188-189
- User Datagram Protocol (UDP)**, 227, 231
  - headers, 228
- UTM (Unified Threat Management) firewalls**, 195
- UTP (unshielded twisted-pair)**, 37-38

## V

- variable-length subnet masking (VLSM)**, 91
- VCs (virtual circuits)**, 32
  - ATM, 33-34
- VDSL (very high bit-rate DSL)**, 27
- verifying solutions**, 237
- versions, SNMP (Simple Network Management Protocol)**, 128
- very high bit-rate DSL (VDSL)**, 27
- video monitoring**, 194
- video conferencing (VTC)**, 60
- virtual circuits (VCs)**, 32
  - ATM, 33-34
- virtual local area networks**. *See* VLANs
- virtual private networks**. *See* VPNs
- Virtual Router Redundancy Protocol (VRRP)**, 99
- virtual switches**, 109
- virtualization**, 107
  - cloud computing. *See* cloud computing
  - networking device virtualization*, 109-110
  - server virtualization*, 108-109
  - software-defined networking*, 110
- VLAN (virtual local area network)**, 156
  - benefits of, 156-157
  - black hole VLAN, 157
  - data VLAN, 157
  - default VLAN, 157
  - management VLANs, 157
  - native VLAN, 157
  - trunking, 158-159
  - voice VLAN, 158
- VLAN assignments**, 187
- VLAN hopping**, 180
- VLAN Trunking Protocol (VTP)**, 159-160
  - modes, 160
  - operations, 160-161
  - pruning, 161-162
- VLSM (variable-length subnet masking)**, 71-73, 91

**voice over IP.** *See* **VoIP**

**Voice VLANs,** 158

**VoIP (Voice over IP),** 102-104

elements of, 14-15

**VoIP network topology,** 15

**VPN concentrators,** 6

**VPNs (virtual private networks),** 9

client-to-site VPNs, 10

IKE (Internet Key Exchange), 11-12

IPsec (Internet Protocol Security), 11-12

protocols, 12

site-to-site VPNs, 9

**VRRP (Virtual Router Redundancy Protocol),** 99

**VTC (video teleconferencing),** 60

**VTP (VLAN Trunking Protocol),** 159-160

modes, 160

operations, 160-161

pruning, 161-162

**vulnerabilities,** 181

**vulnerability assessments,** 182

**vulnerability patches,** 139

**vulnerability scanning,** 182

## W

**WAN (wide area network),** 59

common issues, 271

*company security policies,* 272

*CPE (customer premises equipment),* 272

*DNS issues,* 271

*interface errors,* 271

*interference,* 272

*loss of Internet connectivity,* 271

*router configurations,* 272

*satellites,* 273

*split horizons,* 271

**WAN link options,** 24

dedicated leased lines, 31

enterprise WANs, 32

*ATM (Asynchronous Transfer Mode),* 33

*Frame Relay,* 32-33

*Metro Ethernet,* 35

*MPLS (Multiprotocol Label Switching),* 34

home and small office networks, 25

*broadband cable,* 28-29

*dialup,* 25-26

*DSL (Digital Subscriber Line),* 27-28

*ISDN,* 26-27

*PPP (Point-to-Point Protocol),* 28

SONET (Synchronous Optical Network), 30

wireless, 29

*cellular technologies,* 30

*satellites,* 29

*WiMAX,* 30

**war chalking,** 180

**war driving,** 180

**wavelength,** 210

**WEP (Wired Equivalent Privacy),** 190

**WEP/WPA attacks,** 180

**Wi-Fi analyzer,** 253

**Wi-Fi Protect Setup (WPS) attacks,** 180

**Wi-Fi Protected Access (WPA),** 190

**wide area networks (WANs),** 59

**WiMAX (Worldwide Interoperability for Microwave Access),** 30

**windowing,** 229

**wire strippers,** 45

**Wired Equivalent Privacy (WEP),** 190

**wired standards, Ethernet,** 213-214

**wireless access points,** 168

**wireless attacks,** 180

**wireless bridges,** 170

**wireless configuration issues,** 257-258

**wireless design considerations for networks,** 119

**wireless installation, WLANs,** 170

channels and frequency bands, 171-172

wireless router configuration, 172-175

wireless site surveys, 172

**wireless LAN.** *See* **WLANs**

**wireless LAN controllers (WLC),** 169

**wireless monitoring,** 125

**wireless networks, 29**

- cellular technologies, 30
- satellites, 29
- WiMAX, 30

**wireless router configuration, WLANs (wireless installation), 172-175****wireless routers, 167-168****wireless security, 190****wireless site surveys, WLANs (wireless installation), 172****wireless standards, 256**

- Ethernet, 215-216

**wireless transmission issues, 255-256****wiring closets, 193, 223****WLANs (wireless LANs), 163**

- antennas, 166
- channels, 165-166
- devices, 167
  - wireless access points, 168*
  - wireless bridges, 170*
  - wireless LAN controllers, 169*
  - wireless routers, 167-168*
- frequencies, 163-164
- study resources, 175-176
- topologies, 167
- transmission methods, 164-165
- wireless installation, 170
  - channels and frequency bands, 171-172*
  - wireless router configuration, 172-175*
  - wireless site surveys, 172*

**WLC (wireless LAN controllers), 169****Worldwide Interoperability for Microwave Access (WiMAX), 30****WPA (Wi-Fi Protected Access), 190****WPA Enterprise, 190****WPA Personal, 190****WPS (Wi-Fi Protected Setup) attacks, 180****writing**

- IPv6 addresses, 76-77
- IPv6 prefixes, 77-78

**wrong antenna type, wireless configuration issues, 257****wrong encryption, wireless configuration issues, 257****wrong SSID, wireless configuration issues, 257****X-Y-Z****zero-day attacks, 180**