



31 Days Before Your CCNA Exam

Second Edition

Allan Johnson



A Day-By-Day Review Guide for the CCNA 640-802 Exam

FREE SAMPLE CHAPTER



SHARE WITH OTHERS

31 Days Before Your CCNA Exam

Second Edition

Allan Johnson



31 Days Before Your CCNA Exam

A Day-by-Day Review Guide for the CCNA 640-802 Exam

Second Edition

Allan Johnson

Copyright© 2009 Cisco Systems, Inc.

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

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

Printed in the United States of America

Sixth Printing: March 2013

Library of Congress Cataloging-in-Publication Data

Johnson, Allan, 1962-

31 days before your CCNA exam : a day-by-day review guide for the
CCNA

640-802 exam / Allan Johnson. -- 2nd ed.

p. cm.

Originally published: Indianapolis, IN : Cisco Press, c2007 under

title: 31 days before your CCNA exam / Scott Bennett.

ISBN 978-1-58713-197-4 (pbk.)

1. Electronic data processing personnel--Certification. 2. Computer networks--Examinations--Study guides. I. Bennett, Scott, CCNA 31 days before your CCNA exam. II. Title. III. Title: Thirty one days before your CCNA exam.

TK5105.5.B443 2008

004.6--dc22

2008044139ISBN-13: 978-1-58713-197-4

ISBN-10: 1-58713-197-8

Associate Publisher

Dave Dusthimer

Cisco Press Program

Manager

Jeff Brady

Executive Editor

Mary Beth Ray

Managing Editor

Patrick Kanouse

Senior Development

Editor

Christopher Cleveland

Project Editor

Mandie Frank

Copy Editor

Barbara Hacha

Technical Editors

Rick Graziani,

Kenneth Stewart

Editorial Assistant

Vanessa Evans

Book & Cover Designer

Louisa Adair

Composition

TnT Design, Inc.

Indexer

Lisa Stumpf

Proofreader

Paula Lowell

This book is part of the Cisco Networking Academy® Program series from Cisco Press. The products in this series support and complement the Cisco Networking Academy Program curriculum. If you are using this book outside the Networking Academy program, then you are not preparing with a Cisco trained and authorized Networking Academy provider.



For information on the Cisco Networking Academy Program or to locate a Networking Academy, please visit www.cisco.com/edu.

Warning and Disclaimer

This book is designed to provide information about exam topics for the Cisco Certified Network Associate (CCNA) Exam 640-802. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Trademark Acknowledgments

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

Corporate and Government Sales

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

U.S. Corporate and Government Sales

1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States please contact:

International Sales international@pearsoned.com

Feedback Information

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

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

We greatly appreciate your assistance.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

CODE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IQ Expertise, the iQ logo, IQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

About the Author

Allan Johnson entered the academic world in 1999 after ten 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 seven 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 the Academy in Learning Systems Development.

About the Technical Reviewers

Rick Graziani teaches computer science and computer networking courses at Cabrillo College in Aptos, California. Rick has worked and taught in the computer networking and information technology field for almost 30 years. Prior to teaching, Rick worked in IT for various companies, including Santa Cruz Operation, Tandem Computers, and Lockheed Missiles and Space Corporation. He holds an M.A. in computer science and systems theory from California State University Monterey Bay. Rick also does consulting work for Cisco Systems and other companies. When Rick is not working, he is most likely surfing. Rick is an avid surfer who enjoys longboarding at his favorite Santa Cruz surf breaks.

Kenneth Stewart teaches computer science and computer networking courses at Flour Bluff High School and Delmar College in Corpus Christi, Texas. Kenneth has worked in the field for more than 18 years and taught for the past 11 years. Prior to teaching, Kenneth was a Nuclear, Biological, and Chemical Warfare Specialist in the 82nd Airborne Division at Ft. Bragg, North Carolina. He holds two degrees in computer science and is earning another in occupational career and technology development from Texas A&M Corpus Christi.

Dedication

For my wife, Becky. Without the sacrifices you made during the project, this work would not have come to fruition. Thank you providing me the comfort and resting place only you can give.

Acknowledgments

As the author of the widely successful first edition of this book, Scott Bennett entrusted me to carry on the mission. Thanks Scott, for allowing me to take over this project.

When I began to think of whom I would like to have as Technical Editors for this work, Rick Graziani and Kenneth Stewart immediately came to mind. Both are outstanding instructors and authors in the Cisco Network Academy community. Thankfully, when Mary Beth Ray contacted them, they were willing and able to do the arduous review work necessary to make sure you get a book that is both technically accurate and unambiguous.

Rick is a long-time technology instructor with a world-renowned reputation among both students and teachers of the CCNA and CCNP curricula. When I began to teach CCNA courses in 2000, it wasn't long before I discovered Rick's outstanding resources online. These are available to anyone who sends him an email requesting the password; just Google his name to find his website. Rick and I coauthored the *Routing Protocols and Concepts: CCNA Exploration Companion Guide*, so I know how he works. I knew he would do an outstanding job editing this material before you see it.

Kenneth Stewart often pulls double duty teaching CCNA courses part time at Del Mar College while maintaining a full load teaching various technology classes at Flour Bluff High School here in my hometown of Corpus Christi. In his spare time, he also likes to write books. His students compete on a national level, including networking, web authoring, and robotics. Ken's excitement in the classroom is contagious, and his commitment to the integrity of the teaching materials he uses is unsurpassed. As the excellent coauthor of *Designing and Supporting Computer Networks: CCNA Discovery Learning Guide*, I knew Ken would serve you, the reader, admirably.

Thank you, Rick and Ken, for not only serving as technical editors to this effort, but for being my friends.

This book is a concise summary of the work of Cisco Press CCNA authors. Wendell Odom's *CCNA Official Exam Certification Library*, Third Edition and Steve McQuerry's *Authorized Self-Study Guide CCNA Preparation Library*, Seventh Edition were two of my main sources. The different approaches these two authors—both CCIEs—take toward the CCNA material gives the reader the breadth and the depth needed to master the CCNA exam topics.

The Cisco Network Academy authors for the Exploration series of Companion Guides take the reader deeper, past the CCNA exam topics, with the ultimate goal of not only preparing the student for CCNA certification, but for more advanced college-level technology courses and degrees, as well. Thank you to Mark Dye, Rick Graziani, Wayne Lewis, Rick McDonald, Antoon W. Rufi, and Bob Vachon for their excellent treatment of the material; it is reflected throughout this book.

Mary Beth Ray, executive editor, amazes me with her ability to juggle multiple projects at once, steering each from beginning to end. I can always count on her to make the tough decisions. Thank you, Mary Beth, for bringing this project to me.

This is my fourth project with Christopher Cleveland as development editor. His dedication to perfection pays dividends in countless, unseen ways. Thank you again, Chris, for providing me with much needed guidance and support. This book could not be a reality without your persistence.

Contents at a Glance

Introduction xxv

Part I: Networking Basics 1

Day 31: Network Devices, Components, and Diagrams 3

Day 30: Network Models and Applications 13

Day 29: Network Data Flow from End-to-End 21

Part II: Switching Concepts and Configuration 31

Day 28: Connecting Switches and Ethernet Technology 33

Day 27: Network Segmentation and Switching Concepts 43

Day 26: Basic Switch Configuration and Port Security 53

Day 25: Verifying and Troubleshooting Basic Switch Configurations 61

Day 24: Switching Technologies and VLAN Concepts 71

Day 23: VLAN and Trunking Configuration and Troubleshooting 87

Day 22: VTP and InterVLAN Routing Configuration and Troubleshooting 97

Part III: Addressing the Network 107

Day 21: IPv4 Address Subnetting 109

Day 20: Host Addressing, DHCP, and DNS 123

Day 19: Basic IPv6 Concepts 137

Part IV: Routing Concepts and Configuration 145

Day 18: Basic Routing Concepts 147

Day 17: Connecting and Booting Routers 161

Day 16: Basic Router Configuration and Verification 167

Day 15: Managing Cisco IOS and Configuration Files 179

Day 14: Static, Default, and RIP Routing 191

Day 13: EIGRP Routing 211

Day 12: OSPF Routing 227

Day 11: Troubleshooting Routing 245

Part V: Wireless Concepts and Configuration	251
Day 10: Wireless Standards, Components, and Security	253
Day 9: Configuring and Troubleshooting Wireless Networks	261
Part VI: Basic Security Concepts and Configuration	265
Day 8: Mitigating Security Threats and Best Practices	267
Part VII: ACL and NAT Concepts and Configuration	277
Day 7: ACL Concepts and Configurations	279
Day 6: Verifying and Troubleshooting ACL Implementations	289
Day 5: NAT Concepts, Configuration, and Troubleshooting	297
Part VIII: WAN Concepts and Configuration	307
Day 4: WAN and VPN Technologies	309
Day 3: PPP Configuration and Troubleshooting	329
Day 2: Frame Relay Configuration and Troubleshooting	337
Day 1: CCNA Skills Review and Practice	353
Part IX: Exam Day and Post-Exam Information	375
Exam Day	377
Post-Exam Information	379
Index	381

Contents

Introduction xxv

Part I: Networking Basics 1

Day 31: Network Devices, Components, and Diagrams 3

CCNA 640-802 Exam Topics 3

Key Points 3

Devices 3

Switches 3

Routers 5

Media 5

LANs and WANs 7

Networking Icons 7

Physical and Logical Topologies 8

The Hierarchical Network Model 9

The Enterprise Architecture 10

Network Documentation 11

Study Resources 12

Day 30: Network Models and Applications 13

CCNA 640-802 Exam Topics 13

Key Points 13

The OSI and TCP/IP Models 13

OSI Layers 14

TCP/IP Layers and Protocols 15

Protocol Data Units and Encapsulation 16

Growth of Network-Based Applications 17

Quality of Service 17

Increased Network Usage 17

The Impact of Voice and Video on the Network 18

Study Resources 19

Day 29: Network Data Flow from End-to-End 21

CCNA 640-802 Exam Topics 21

Key Points 21

The TCP/IP Application Layer	21
The TCP/IP Transport Layer	21
TCP Header	22
Port Numbers	23
Error Recovery	24
Flow Control	25
Connection Establishment and Termination	25
UDP	26
The TCP/IP Internet Layer	26
The TCP/IP Network Access Layer	27
Data Encapsulation Summary	28
Using Layers to Troubleshoot	29
Study Resources	29

Part II: Switching Concepts and Configuration 31

Day 28: Connecting Switches and Ethernet Technology 33

CCNA 640-802 Exam Topics	33
Key Topics	33
Ethernet Overview	33
Legacy Ethernet Technologies	34
CSMA/CD	35
Legacy Ethernet Summary	35
Current Ethernet Technologies	36
UTP Cabling	36
Benefits of Using Switches	37
Ethernet Addressing	38
Ethernet Framing	39
The Role of the Physical Layer	40
Study Resources	41

Day 27: Network Segmentation and Switching Concepts 43

CCNA 640-802 Exam Topics	43
Key Topics	43
Evolution to Switching	43

- Switching Logic 44
- Collision and Broadcast Domains 45
- Frame Forwarding 45
 - Switch Forwarding Methods 45
 - Symmetric and Asymmetric Switching 46
 - Memory Buffering 46
 - Layer 2 and Layer 3 Switching 46
- Accessing and Navigating Cisco IOS 46
 - Connecting to Cisco Devices 46
 - CLI EXEC Sessions 47
 - Using the Help Facility 48
 - CLI Navigation and Editing Shortcuts 48
 - Command History 49
 - IOS Examination Commands 50
 - Subconfiguration Modes 50
- Storing and Erasing Configuration Files 51
- Study Resources 52

Day 26: Basic Switch Configuration and Port Security 53

- CCNA 640-802 Exam Topics 53
- Key Topics 53
- Basic Switch Configuration Commands 53
- Configuring SSH Access 55
- Configuring Port Security 56
- Shutting Down and Securing Unused Interfaces 58
- Study Resources 59

Day 25: Verifying and Troubleshooting Basic Switch Configurations 61

- CCNA 640-802 Exam Topics 61
- Key Points 61
- Troubleshooting Methodology 61
- Verifying Network Connectivity 62
- Interface Status and the Switch Configuration 65
 - Interface Status Codes 65

Duplex and Speed Mismatches 66

Common Layer 1 Problems On “Up” Interfaces 67

CDP as a Troubleshooting Tool 68

Study Resources 70

Day 24: Switching Technologies and VLAN Concepts 71

CCNA 640-802 Exam Topics 71

Key Points 71

VLAN Concepts 71

Traffic Types 72

Types of VLANs 72

Voice VLAN Example 73

Trunking VLANs 74

Dynamic Trunking Protocol 75

VTP Concepts 76

VTP Modes 77

VTP Operation 77

VTP Pruning 78

STP Concepts and Operation 78

RSTP Concepts and Operation 80

Configuring and Verifying STP 82

PVST+, PVRST, and MIST 82

Configuring and Verifying the BID 82

PortFast 84

Configuring RSTP 84

Troubleshooting STP 84

Study Resources 85

Day 23: VLAN and Trunking Configuration and Troubleshooting 87

CCNA 640-802 Exam Topics 87

Key Points 87

Sample Topology 87

VLAN Configuration and Verification Commands 88

Configuring and Verifying Trunking 91

Troubleshooting VLAN and Trunking Problems 93

Study Resources 95

Day 22: VTP and InterVLAN Routing Configuration and Troubleshooting 97

CCNA 640-802 Exam Topics 97

Key Points 97

VTP Configuration and Verification 97

VTP Troubleshooting 102

Inter-VLAN Routing Configuration and Verification 103

Troubleshooting Inter-VLAN Routing 105

Study Resources 106

Part III: Addressing the Network 107

Day 21: IPv4 Address Subnetting 109

CCNA 640-802 Exam Topics 109

Key Topics 109

IPv4 Addressing 109

Header Format 109

Classes of Addresses 110

Purpose of the Subnet Mask 111

Subnetting in Four Steps 112

Determine How Many Bits to Borrow 113

Determine the New Subnet Mask 114

Determine the Subnet Multiplier 114

List the Subnets, Host Ranges, and Broadcast Addresses 114

Subnetting Example 1 114

Subnetting Example 2 115

Subnetting Example 3 115

VLSM 116

Summarizing Subnet Addresses 118

Private and Public IP Addressing 119

Study Resources 120

Day 20: Host Addressing, DHCP, and DNS 123

- CCNA 640-802 Exam Topics 123
- Key Topics 123
- Addressing Devices 123
- ARP 124
- DNS 126
- DHCP 127
- Configuring on a Cisco Router as a DHCP Server 128
- Network Layer Testing Tools 132
 - Ping 132
- Study Resources 134

Day 19: Basic IPv6 Concepts 137

- CCNA 640-802 Exam Topics 137
- Key Topics 137
- Overview of IPv6 137
- IPv6 Address Structure 139
 - Conventions for Writing IPv6 Addresses 139
 - Conventions for Writing IPv6 Prefixes 139
 - IPv6 Global Unicast Address 140
 - Reserved, Private, and Loopback Addresses 141
 - The IPv6 Interface ID and EUI-64 Format 141
 - IPv6 Address Management 142
- Transitioning to IPv6 142
- Study Resources 144

Part IV: Routing Concepts and Configuration 145**Day 18: Basic Routing Concepts 147**

- Key Topics 147
- Packet Forwarding 147
 - Path Determination and Switching Function Example 148
- Routing Methods 149

Classifying Dynamic Routing Protocols	150
IGP and EGP	150
Distance Vector Routing Protocols	150
Link-State Routing Protocols	151
Classful Routing Protocols	151
Classless Routing Protocols	152
Dynamic Routing Metrics	152
Administrative Distance	153
IGP Comparison Summary	154
Routing Loop Prevention	155
Link-State Routing Protocol Features	156
Building the LSDB	156
Calculating the Dijkstra Algorithm	157
Convergence with Link-State Protocols	158
Study Resources	158

Day 17: Connecting and Booting Routers 161

CCNA 640-802 Exam Topics	161
Key Topics	161
Router Internal Components	161
IOS	162
Router Bootup Process	162
Router Ports and Interfaces	164
Router Connections	164
Study Resources	166

Day 16: Basic Router Configuration and Verification 167

CCNA 640-802 Exam Topics	167
Key Topic	167
Basic Router Configuration	167
Verifying Network Connectivity	175
Study Resources	177

Day 15: Managing Cisco IOS and Configuration Files 179

CCNA 640-802 Exam Topics	179
Key Topics	179

The Cisco IOS File System	179
IFS Commands	179
URL Prefixes for Specifying File Locations	181
Commands for Managing Configuration Files	182
Cisco IOS File Naming Conventions	182
Manage IOS Images	183
Backing Up an IOS image	184
Restoring an IOS Image	185
Recovering an IOS Image Using a TFTP Server	186
Recovering an IOS Image Using Xmodem	187
Recovering a Lost Password	188
Study Resources	189
Day 14: Static, Default, and RIP Routing	191
CCNA 640-802 Exam Topics	191
Key Topics	191
Static Route Configuration	191
Static Routes Using the “Next Hop” Parameter	193
Static Routes Using the Exit Interface Parameter	193
Default Static Routes	194
RIP Concepts	197
RIPv1 Message Format	197
RIPv1 Operation	198
RIPv1 Configuration	198
RIPv1 Verification and Troubleshooting	199
Passive Interfaces	203
Automatic Summarization	204
Default Routing and RIPv1	206
RIPv2 Configuration	207
Disabling Autosummarization	208
RIPv2 Verification and Troubleshooting	208
Study Resources	209

Day 13: EIGRP Routing 211

- CCNA 640-802 Exam Topics 211
- Key Topics 211
- EIGRP Operation 211
 - EIGRP Message Format 212
 - RTP and EIGRP Packet Types 212
 - DUAL 214
 - Administrative Distance 214
- EIGRP Configuration 214
 - The network Command 215
 - Automatic Summarization 216
 - Manual Summarization 217
 - EIGRP Default Route 219
 - Modifying the EIGRP Metric 219
 - Modifying Hello Intervals and Hold Times 220
- EIGRP Verification and Troubleshooting 221
- Study Resources 226

Day 12: OSPF Routing 227

- CCNA 640-802 Exam Topics 227
- Key Topics 227
- OSPF Operation 227
 - OSPF Message Format 227
 - OSPF Packet Types 228
 - Neighbor Establishment 228
 - Link-State Advertisements 229
 - OSPF Network Types 230
 - DR/BDR Election 230
 - OSPF Algorithm 231
 - Link-State Routing Process 232
- OSPF Configuration 233
 - The router ospf Command 234
 - The network Command 234

Router ID	235
Modifying the OSPF Metric	236
Controlling the DR/BDR Election	237
Redistributing a Default Route	238
Modifying Hello Intervals and Hold Times	238
Verifying and Troubleshooting OSPF	239
Study Resources	243

Day 11: Troubleshooting Routing 245

CCNA 640-802 Exam Topics	245
Key Topics	245
The Basic Commands	245
VLSM Troubleshooting	246
Discontiguous Networks	246
Troubleshooting RIP	247
Troubleshooting EIGRP and OSPF Interface Issues	248
Troubleshooting Neighbor Adjacency Issues	249
Study Resources	250

Part V: Wireless Concepts and Configuration 251

Day 10: Wireless Standards, Components, and Security 253

CCNA 640-802 Exam Topics	253
Key Topics	253
Wireless Standards	253
Wireless Modes of Operation	254
Wireless Frequencies	254
Wireless Encoding and Channels	255
Wireless Coverage Area	256
CSMA/CA	256
Wireless Security Risks	257
Wireless Security Standards	258
Study Resources	259

Day 9: Configuring and Troubleshooting Wireless Networks 261

CCNA 640-802 Exam Topics	261
Key Topics	261

- Implementing a WLAN 261
 - Wireless LAN Implementation Checklist 262
 - Wireless Troubleshooting 264
- Study Resources 264

Part VI: Basic Security Concepts and Configuration 265

Day 8: Mitigating Security Threats and Best Practices 267

- CCNA 640-802 Exam Topics 267
- Key Topics 267
- The Importance of Security 267
 - Attacker Terminology 267
 - Thinking Like an Attacker 268
 - Balancing Security and Availability 269
 - Developing a Security Policy 269
- Common Security Threats 270
 - Vulnerabilities 270
 - Threats to Physical Infrastructure 271
 - Threats to Networks 271
 - Types of Network Attacks 271
- General Mitigation Techniques 273
 - Host and Server Security 273
 - Intrusion Detection and Prevention 273
 - Security Appliances and Applications 273
- Maintaining Security 275
- Study Resources 276

Part VII: ACL and NAT Concepts and Configuration 277

Day 7: ACL Concepts and Configurations 279

- CCNA 640-802 Exam Topics 279
- Key Topics 279
- ACL Concepts 279
 - Defining an ACL 279
 - Processing Interface ACLs 279

Types of ACLs	280
ACL Identification	281
ACL Design Guidelines	281
Configuring Standard Numbered ACLs	282
Standard Numbered ACL: Permit Specific Network	282
Standard Numbered ACL: Deny a Specific Host	283
Standard Numbered ACL: Deny a Specific Subnet	283
Standard Numbered ACL: Deny Telnet Access to the Router	284
Configuring Extended Numbered ACLs	284
Extended Numbered ACL: Deny FTP from Subnets	285
Extended Numbered ACL: Deny Only Telnet from Subnet	285
Configuring Named ACLs	286
Standard Named ACL Steps and Syntax	286
Standard Named ACL: Deny a Single Host from a Given Subnet	286
Extended Named ACL Steps and Syntax	287
Extended Named ACL: Deny a Telnet from a Subnet	287
Adding Comments to Named or Numbered ACLs	287
Complex ACLs	288
Study Resources	288
Day 6: Verifying and Troubleshooting ACL Implementations	289
CCNA 640-802 Exam Topics	289
Key Topics	289
Verifying ACLs	289
Troubleshooting ACLs	291
Problem 1: Host Has No Connectivity	291
Problem 2: Denied Protocols	292
Problem 3: Telnet is Allowed #1	293
Problem 4: Telnet Is Allowed #2	294
Problem 5: Telnet Is Allowed #3	294
Study Resources	295
Day 5: NAT Concepts, Configuration, and Troubleshooting	297
CCNA 640-802 Exam Topics	297
Key Topics	297

- NAT Concepts 297
 - A NAT Example 298
 - Dynamic and Static NAT 299
 - NAT Overload 299
 - NAT Benefits 300
 - NAT Limitations 300
- Configuring Static NAT 301
- Configuring Dynamic NAT 301
- Configuring NAT Overload 303
- Verifying NAT 303
- Troubleshooting NAT 304
- Study Resources 306

Part VIII: WAN Concepts and Configuration 307

Day 4: WAN and VPN Technologies 309

- CCNA 640-802 Exam Topics 309
- Key Topics 309
- WAN Technology Concepts 309
 - WAN Components and Devices 309
 - WAN Physical Layer Standards 311
 - WAN Data Link Protocols 312
 - WAN Switching 312
- WAN Connection Options 313
 - Dedicated Connection Options 314
 - Circuit-Switched Connection Options 314
 - Packet-Switched Connection Options 315
 - Internet Connection Options 317
 - Choosing a WAN Link Option 319
- VPN Technology 320
 - VPN Benefits 320
 - Types of VPN Access 320
 - VPN Components 322
 - Establishing Secure VPN Connections 322
- Study Resources 326

Day 3: PPP Configuration and Troubleshooting 329

- CCNA 640-802 Exam Topics 329
- Key Topics 329
- HDLC 329
 - HDLC Encapsulation 329
 - Configuring HDLC 330
 - Verifying HDLC 331
- PPP Concepts 331
 - The PPP Frame Format 331
 - PPP Link Control Protocol (LCP) 332
- PPP Configuration and Verification 334
 - Basic PPP 334
- Study Resources 336

Day 2: Frame Relay Configuration and Troubleshooting 337

- CCNA 640-802 Exam Topics 337
- Key Topics 337
- Frame Relay Concepts 337
 - Frame Relay Components 338
 - Frame Relay Topologies 339
 - NBMA Limitations and Solutions 340
 - Inverse ARP and LMI Concepts 341
 - Inverse ARP and LMI Operation 342
- Configuring and Verifying Frame Relay 343
 - Full Mesh with One Subnet 344
 - Partial Mesh with One Subnet per PVC 347
 - Frame Relay Verification 348
- Troubleshooting WAN Implementations 349
 - Troubleshooting Layer 1 Problems 350
 - Troubleshooting Layer 2 Problems 350
 - Troubleshooting Layer 3 Problems 351
- Study Resources 352

Day 1: CCNA Skills Review and Practice 353

Key Topics 353

CCNA Skills Practice 353

Introduction 353

Topology Diagram 353

Addressing Table 354

VLAN Configuration and Port Mappings 355

ISP Configuration 355

Task 1: Configure Frame Relay in a Hub-and-Spoke Topology 356

Task 2: Configure PPP with CHAP 356

Task 3: Configure Static and Dynamic NAT on HQ 356

Task 4: Configure Default Routing 357

Task 5: Configure Inter-VLAN Routing 357

Task 6: Configure and Optimize EIGRP Routing 357

Task 7: Configure VTP, Trunking, the VLAN Interface, and VLANs 357

Task 8: Assign VLANs and Configure Port Security 358

Task 9: Configure STP 358

Task 10: Configure DHCP 359

Task 11: Configure a Firewall ACL 359

CCNA Skills Practice (Answers) 360

Task 1: Configure Frame Relay in a Hub-and-Spoke Topology 360

Task 2: Configure PPP with CHAP 362

Task 3: Configure Static and Dynamic NAT on HQ 362

Task 4: Configure Default Routing 364

Task 5: Configure Inter-VLAN Routing 364

Task 6: Configure and Optimize EIGRP Routing 365

Task 7: Configure VTP, Trunking, the VLAN Interface, and VLANs 367

Task 8: Assign VLANs and Configure Port Security 369

Task 9: Configure STP 370

Task 10: Configure DHCP 371

Task 11: Configure a Firewall ACL 372

CCNA Skills Challenge 374

Part IX: Exam Day and Post-Exam Information 375**Exam Day 377**

What You Need for the Exam 377

What You Should Receive After Completion 377

Summary 378

Post-Exam Information 379

Receiving Your Certificate 379

Determining Career Options 379

Examining Certification Options 380

If You Failed the Exam 380

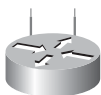
Summary 380

Index 381

Icons Used in This Book



Router



Wireless Router



Wireless Access Point



Hub



Hub (alternate)



Multilayer Switch



Switch



ATM Switch Relay Switch



WAN Switch



PBX Switch



Cisco ASA



Router with Firewall



PIX Firewall



Firewall



VPN Concentrator



DSLAM



CSU/DSU



Access Server



Voice-Enabled Access Server



Modem



IP Phone



Phone



Server



IP/TV Broadcast Server



Network Management Server



Network Management Server



Web Server



Laptop



PC



Network Cloud

 Ethernet Connection

 Serial Line Connection

 Wireless Connection

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.

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 CCNA certification. Regardless of how you got to this point in your travels through your CCNA studies, *31 Days Before Your CCNA Exam* most likely represents the last leg of your journey on your way to the destination: to become a Cisco Certified Network Associate. However if you are like me, you might be reading this book at the *beginning* of your studies. If such is the case, this book provides you with an excellent overview of the material you must now spend a great deal of time studying and practicing. I must warn you, though; unless you are extremely well versed in networking technologies and have considerable experience configuring and troubleshooting Cisco routers and switches, this book will *not* serve you well as the sole resource for CCNA exam preparation. Therefore, let me spend some time discussing my recommendations for study resources.

Study Resources

Cisco Press offers an abundance of CCNA-related books to serve as your primary source for learning how to install, configure, operate, and troubleshoot medium-size routed and switched networks. See the inside cover of this book for a quick list of my recommendations.

Foundational Resources

First on the list must be Wendell Odom's *CCNA Official Exam Certification Library*, Third Edition (ISBN: 1587201836). If you do not buy any other books, buy this set of two. Wendell's method of teaching, combined with his technical expertise and down-to-earth style, is unsurpassed in our industry. As you read through his books, you sense that he is sitting right there next to you walking you through the material. The practice exams and study materials on the CD in the back of the book are worth the price of the book. There is no better resource on the market for a CCNA candidate.

Next on the list must be Steve McQuerry's *Authorized Self-Study Guide CCNA Preparation Library*, Seventh Edition (ISBN: 1587054647). These two books are indispensable to those students who take the two Cisco recommended training classes for CCNA preparation: Interconnecting Cisco Network Devices 1 (ICND1) and Interconnecting Cisco Network Devices 2 (ICND2). These courses, available through Cisco Training Partners in a variety of formats, are usually of a very short duration (1 to 6 weeks) and are geared toward the industry professional already working in the field of networking. Steve's books serve the reader well as a concise, but thorough, treatment of the CCNA exam topics. His method and approach often differ from and complement Wendell's approach. I recommend that you also refer to these books.

If you are a Cisco Networking Academy student, you are blessed with access to the online version of the CCNA curriculum and the wildly popular Packet Tracer network simulator. Although there are two versions of the CCNA curriculum—Discovery and Exploration—I chose to use the four CCNA Exploration courses in my daily review of the exam topics. The Exploration curriculum provides a comprehensive overview of networking, from fundamentals to advanced applications and services. The Exploration courses emphasize theoretical concepts and practical application, while providing opportunities for students to gain the skills and hands-on experience needed to design, install, operate, and maintain networks in small-to-medium businesses, as well as enterprise and service provider environments. In an Academy class, not only do you have access to Packet Tracer, but you have access to extensive, guided labs and real equipment on which to practice your CCNA skills. To learn more about CCNA Exploration and to find an Academy near you, visit http://www.cisco.com/web/learning/netacad/course_catalog/CCNAexploration.html.

However, if you are not an Academy student but would like to benefit from the extensive authoring done for these courses, you can buy any or all of the CCNA Exploration Companion Guides (CG) and Lab Study Guides (LSG) of the Academy's popular online curriculum. Although you will not have access to the Packet Tracer network simulator software, you will have access to the tireless work of an outstanding team of Cisco Academy Instructors dedicated to providing students with comprehensive and engaging CCNA preparation course material. The titles and ISBNs for the CCNA Exploration CGs and LSGs are as follows:

- Network Fundamentals (CG ISBN: 1587132087; LSG ISBN: 1587132036)
- Routing Protocols and Concepts (CG ISBN: 1587132060; LSG ISBN: 1587132044)
- LAN Switching and Wireless (CG ISBN: 1587132079; LSG ISBN: 1587132028)
- Accessing the WAN (CG ISBN: 1587132052; LSG ISBN: 158713201X)

You can find these books at www.ciscopress.com by clicking the **CISCO NETWORKING ACADEMY** link.

Supplemental Resources

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

First, Eric Rivard and Jim Doherty are coauthors of *CCNA Flash Cards and Exam Practice Pack*, Third Edition (ISBN: 1587201909). The text portion of the book includes more than 700 flash cards that quickly review exam topics in bite-sized pieces. Also included are nearly 200 pages of quick-reference sheets designed for late-stage exam preparation. And the included CD features a test engine with more than 500 CCNA practice exam questions.

Second, Wendell Odom has put together an excellent collection of more than four hours of personal, visual instruction in one package, titled *CCNA Video Mentor*, Second Edition (ISBN: 1587201917). It contains a DVD with 20 videos and a lab manual. Wendell walks you through common Cisco router and switch configuration topics designed to develop and enhance your hands-on skills.

The Cisco Learning Network

Finally, if you have not done so already, you should now register with the Cisco Learning Network at <http://cisco.hosted.jivesoftware.com/>. Sponsored by Cisco, the Cisco Learning Network is a free social-learning network where IT professionals can engage in the common pursuit of enhancing

and advancing their IT careers. Here you will find many resources to help you prepare for your CCNA exam, as well as a community of like-minded people ready to answer your questions, help you with your struggles, and share in your triumphs.

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 must have it all! I admit it. My bookcase is a testament to my Cisco "geekness." But if you are on a budget, choose one of the foundational study resources and one of the supplemental resources, such as Wendell Odom's certification library and Rivard/Doherty's flash cards. Whatever you choose, you will be in good hands. Any or all of these authors will serve you well.

Goals and Methods

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

- A title for the day that concisely states the overall topic
- A list of one or more CCNA 640-802 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 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 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 CCNA exam. The calendar provides a visual for the time that you can dedicate to each CCNA 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 Book?

The audience for this book is anyone finishing preparation for taking the CCNA 640-802 exam. A secondary audience is anyone needing a refresher review of CCNA exam topics—possibly before attempting to recertify or sit for another certification to which the CCNA is a prerequisite.

Getting to Know the CCNA 640-802 Exam

For the current certifications, announced in June 2007, Cisco created the ICND1 (640-822) and ICND2 (640-816) exams, along with the CCNA (640-802) exam. To become CCNA certified, you can pass both the ICND1 and ICND2 exams, or just the CCNA exam. The CCNA exam covers all the topics on the ICND1 and ICND2 exams, giving you two options for gaining your CCNA certification. The two-exam path gives people with less experience a chance to study for a smaller set

of topics at one time. The one-exam option provides a more cost-effective certification path for those who want to prepare for all the topics at once. This book focuses exclusively on the one-exam path using the entire list of exam topics for the CCNA 640-802 exam.

Currently for the CCNA exam, you are allowed 90 minutes to answer 50–60 questions. Use the following steps to access a tutorial at home that demonstrates the exam environment before you go to take the exam:

Step 1 Visit <http://www.vue.com/cisco>.

Step 2 Look for a link to the certification tutorial. Currently, it can be found on the right side of the web page under the heading Related Links.

Step 3 Click the Certification tutorial link.

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.

When you start the exam, you are asked a series of questions. Each question is presented one at a time and must be answered before moving on to the next question. The exam engine does not let you go back and change your answer. The exam questions can be in one of the following formats:

- Multiple choice
- Fill-in-the-blank
- Drag-and-drop
- Testlet
- Simlet
- Simulation

The multiple-choice format requires that you point and click a circle or check box next to the correct answer or answers. Cisco traditionally tells you how many answers you need to choose, and the testing software prevents you from choosing too many or too few.

Fill-in-the-blank questions typically require you only to type numbers. However if words are requested, the case does not matter unless the answer is a command that is case sensitive (such as passwords and device names when configuring authentication).

Drag-and-drop questions require you to click and hold, move a button or icon to another area, and release the mouse button to place the object somewhere else—typically in a list. For some questions, to get the question correct, you might need to put a list of five things in the proper order.

Testlets contain one general scenario and several multiple-choice questions about the scenario. These are ideal if you are confident in your knowledge of the scenario's content because you can leverage your strength over multiple questions.

A simlet is similar to a testlet in that you are given a scenario with several multiple-choice questions. However, a simlet uses a network simulator to allow you access to a simulation of the command line of Cisco IOS Software. You can then use **show** commands to examine a network's current behavior and answer the question.

A simulation also uses a network simulator, but you are given a task to accomplish, such as implementing a network solution or troubleshooting an existing network implementation. You do this by configuring one or more routers and switches. The exam then grades the question based on the configuration you changed or added. A newer form of the simulation question is the GUI-based simulation, where a graphical interface like that found on a Linksys router or the Cisco Security Device Manager is simulated.

What Topics Are Covered on the CCNA Exam

The topics of the CCNA 640-802 exam focus on the following eight key categories:

- Describe how a network works.
- Configure, verify and troubleshoot a switch with VLANs and interswitch communications.
- Implement an IP addressing scheme and IP Services to meet network requirements in a medium-size enterprise branch office network.
- Configure, verify, and troubleshoot basic router operation and routing on Cisco devices.
- Explain and select the appropriate administrative tasks required for a WLAN.
- Identify security threats to a network and describe general methods to mitigate those threats.
- Implement, verify, and troubleshoot NAT and ACLs in a medium-size enterprise branch office network.
- Implement and verify WAN links.

Although Cisco outlines general exam topics, it is possible that not all topics will appear on the CCNA exam and that topics that are not specifically listed might appear on the exam. The exam topics provided by Cisco and included in this book are a general framework for exam preparation. Be sure to check the Cisco website for the latest exam topics.

Cisco Networking Academy Student Discount Voucher

If you are a Cisco Networking Academy student, you have the opportunity to earn a discount voucher to use when registering and paying for your exam with Pearson VUE. To receive the discount voucher, you must complete all four courses of the CCNA Exploration curriculum and receive a score of 75 percent or higher on your first attempt of the final exam for the final CCNA Exploration course, *Accessing the WAN*. The amount of the discount varies by region and testing center, but typically it has been as much as 50% off the full exam price. Log in to the Academy Connection and click Help at the top of the page to research more information on receiving a discount voucher.

Registering for the CCNA 640-802 Exam

If you are starting your *31 Days to Your CCNA* 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, you should gather the following information in Table I-1 and register right now!

Table I-1 Personal Information for CCNA 640-802 Exam Registration

Item	Notes
Legal Name	
Social Security or Passport Number	
Cisco Certification ID or Test ID ¹	
Cisco Academy Username ²	
Cisco Academy ID Number ²	
Company Name	
Valid Email Address	
Voucher Number ²	
Method of Payment	

¹Applies to exam candidates if you have previously taken a Cisco certification exam (such as the ICND1 exam)

²Applies to Cisco Networking Academy students only

To register for an exam, contact Pearson VUE via one of the following methods:

- **Online:** <http://www.vue.com/cisco>.
- **By phone:** In the United States and Canada call 1-800-829-6387, option 1, then option 4. Check the website for information regarding other countries.

The process and available test times will vary based on the local testing center you choose.

Remember, there is no better motivation for study than an actual test date. *Sign up today.*

Ethernet separates the functions of the data link layer into two distinct sublayers:

- **Logical Link Control (LLC) sublayer:** Defined in the 802.2 standard.
- **Media Access Control (MAC) sublayer:** Defined in the 802.3 standard.

The LLC sublayer handles communication between the network layer and the MAC sublayer. In general, LLC provides a way to identify the protocol that is passed from the data link layer to the network layer. In this way, the fields of the MAC sublayer are not populated with protocol type information, as was the case in earlier Ethernet implementations.

The MAC sublayer has two primary responsibilities:

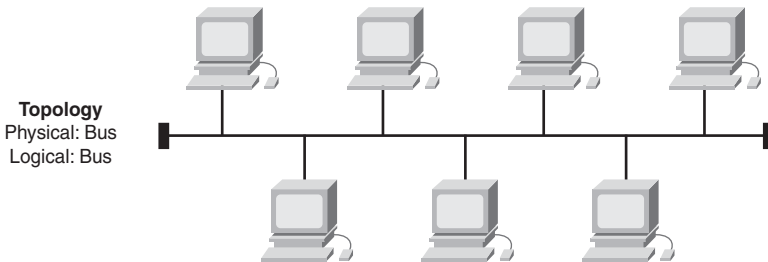
- **Data Encapsulation:** Includes frame assembly before transmission, frame parsing upon reception of a frame, data link layer MAC addressing, and error detection.
- **Media Access Control:** Because Ethernet is a shared media and all devices can transmit at any time, media access is controlled by a method called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

At the physical layer, Ethernet specifies and implements encoding and decoding schemes that enable frame bits to be carried as signals across both unshielded twisted-pair (UTP) copper cables and optical fiber cables. In early implementations, Ethernet used coaxial cabling.

Legacy Ethernet Technologies

Ethernet is best understood by first considering the two early Ethernet specifications—10BASE5 and 10BASE2. With these two specifications, the network engineer installs a series of coaxial cables connecting each device on the Ethernet network, as shown in Figure 28-2.

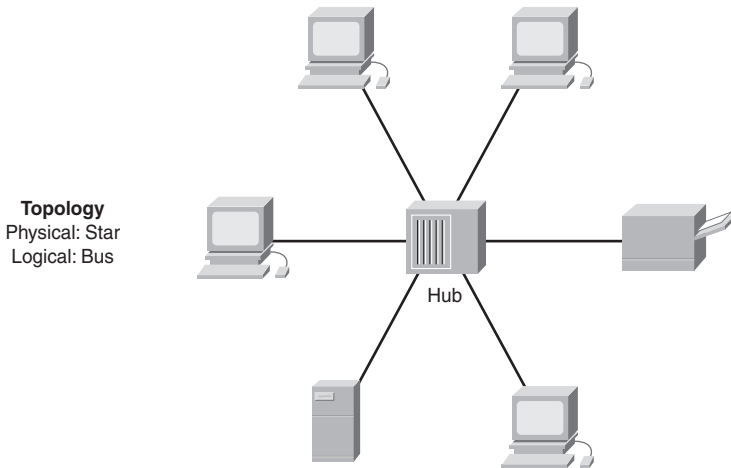
Figure 28-2 Ethernet Physical and Logical Bus Topology



The series of cables creates an electrical circuit, called a bus, which is shared among all devices on the Ethernet. When a computer wants to send some bits to another computer on the bus, it sends an electrical signal, and the electricity propagates to all devices on the Ethernet.

With the change of media to UTP and the introduction of the first hubs, Ethernet physical topologies migrated to a star as shown in Figure 28-3.

Regardless of the change in the physical topology from a bus to a star, hubs logically operate similar to a traditional bus topology and require the use of CSMA/CD.

Figure 28-3 Ethernet Physical Star and Logical Bus Topology

CSMA/CD

Because Ethernet is a shared media where every device has the right to send at any time, it also defines a specification for how to ensure that only one device sends traffic at a time. The CSMA/CD algorithm defines how the Ethernet logical bus is accessed.

CSMA/CD logic helps prevent collisions and also defines how to act when a collision does occur. The CSMA/CD algorithm works like this:

1. A device with a frame to send listens until the Ethernet is not busy.
2. When the Ethernet is not busy, the sender(s) begin(s) sending the frame.
3. The sender(s) listen(s) to make sure that no collision occurred.
4. If a collision occurs, the devices that had been sending a frame each send a jamming signal to ensure that all stations recognize the collision.
5. After the jamming is complete, each sender randomizes a timer and waits that long before trying to resend the collided frame.
6. When each random timer expires, the process starts again from the beginning.

When CSMA/CD is in effect, it also means that a device's network interface card (NIC) is operating in half-duplex mode—either sending or receiving frames. CSMA/CD is disabled when a NIC autodetects that it can operate in—or is manually configured to operate in—full duplex mode. In full duplex mode, a NIC can send and receive simultaneously.

Legacy Ethernet Summary

Today, you might occasionally use LAN hubs, but you will more likely use switches instead of hubs. However, keep in mind the following key points about the history of Ethernet:

- The original Ethernet LANs created an electrical bus to which all devices connected.
- 10BASE2 and 10BASE5 repeaters extended the length of LANs by cleaning up the electrical signal and repeating it—a Layer 1 function—but without interpreting the meaning of the electrical signal.

- Hubs are repeaters that provide a centralized connection point for UTP cabling—but they still create a single electrical bus, shared by the various devices, just like 10BASE5 and 10BASE2.
- Because collisions could occur in any of these cases, Ethernet defines the CSMA/CD algorithm, which tells devices how to both avoid collisions and take action when collisions do occur.

Current Ethernet Technologies

Refer back to Figure 28-1 and notice the different 802.3 standards. Each new physical layer standard from the IEEE requires many differences at the physical layer. However, each of these physical layer standards uses the same 802.3 header, and each uses the upper LLC sublayer as well. Table 28-1 lists today's most commonly used IEEE Ethernet physical layer standards.

Table 28-1 Today's Most Common Types of Ethernet

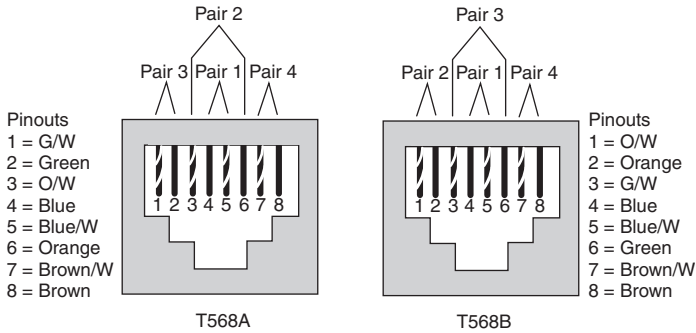
Common Name	Speed	Alternative Name	Name of IEEE Standard	Cable Type, Maximum Length
Ethernet	10 Mbps	10BASE-T	IEEE 802.3	Copper, 100 m
Fast Ethernet	100 Mbps	100BASE-TX	IEEE 802.3u	Copper, 100 m
Gigabit Ethernet	1000 Mbps	1000BASE-LX, 1000BASE-SX	IEEE 802.3z	Fiber, 550 m (SX) 5 km (LX)
Gigabit Ethernet	1000 Mbps	1000BASE-T	IEEE 802.3ab	Copper, 100 m
10GigE (Gigabit Ethernet)	10 Gbps	10GBASE-SR, 10GBASE-LR	IEEE 802.3ae	Fiber, up to 300 m (SR), up to 25 km (LR)
10GigE (Gigabit Ethernet)	10 Gbps	10GBASE-T	IEEE 802.3an	Copper, 100 m

UTP Cabling

The three most common Ethernet standards used today—10BASE-T (Ethernet), 100BASE-TX (Fast Ethernet, or FE), and 1000BASE-T (Gigabit Ethernet, or GE)—use UTP cabling. Some key differences exist, particularly with the number of wire pairs needed in each case and in the type (category) of cabling.

The UTP cabling used by popular Ethernet standards include either two or four pairs of wires. The cable ends typically use an RJ-45 connector. The RJ-45 connector has eight specific physical locations into which the eight wires in the cable can be inserted, called pin positions or, simply, pins.

The Telecommunications Industry Association (TIA) and the Electronics Industry Alliance (EIA) define standards for UTP cabling, color coding for wires, and standard pinouts on the cables. Figure 28-4 shows two TIA/EIA pinout standards, with the color coding and pair numbers listed.

Figure 28-4 TIA/EIA Standard Ethernet Cabling Pinouts

For the exam, you should be well prepared to choose which type of cable (straight-through or crossover) is needed in each part of the network. In short, devices on opposite ends of a cable that use the same pair of pins to transmit need a crossover cable. Devices that use an opposite pair of pins to transmit need a straight-through cable. Table 28-2 lists typical devices and the pin pairs they use, assuming that they use 10BASE-T and 100BASE-TX.

Table 28-2 10BASE-T and 100BASE-TX Pin Pairs Used

Devices That Transmit on 1,2 and Receive on 3,6	Devices That Transmit on 3,6 and Receive on 1,2
PC NICs	Hubs
Routers	Switches
Wireless Access Point (Ethernet interface)	N/A
Networked printers (printers that connect directly to the LAN)	N/A

1000BASE-T requires four wire pairs because Gigabit Ethernet transmits and receives on each of the four wire pairs simultaneously.

However, Gigabit Ethernet does have a concept of straight-through and crossover cables, with a minor difference in the crossover cables. The pinouts for a straight-through cable are the same—pin 1 to pin 1, pin 2 to pin 2, and so on. The crossover cable crosses the same two-wire pair as the crossover cable for the other types of Ethernet—the pair at pins 1,2 and 3,6—as well as crossing the two other pairs (the pair at pins 4,5 with the pair at pins 7,8).

Benefits of Using Switches

A collision domain is a set of devices whose frames could collide. All devices on a 10BASE2, 10BASE5, or any network using a hub risk collisions between the frames that they send, so all devices on one of these types of Ethernet networks are in the same collision domain and use CSMA/CD to detect and resolve collisions.

LAN switches significantly reduce, or even eliminate, the number of collisions on a LAN. Unlike hubs, switches do not create a single shared bus. Instead, switches do the following:

- Switches interpret the bits in the received frame so that they can typically send the frame out the one required port, rather than all other ports.
- If a switch needs to forward multiple frames out the same port, the switch buffers the frames in memory, sending one at a time, thereby avoiding collisions.

In addition, switches with only one device cabled to each port of the switch allow the use of full-duplex operation. Full-duplex means that the NIC can send and receive concurrently, effectively doubling the bandwidth of a 100 Mbps link to 200 Mbps—100 Mbps for sending and 100 Mbps for receiving.

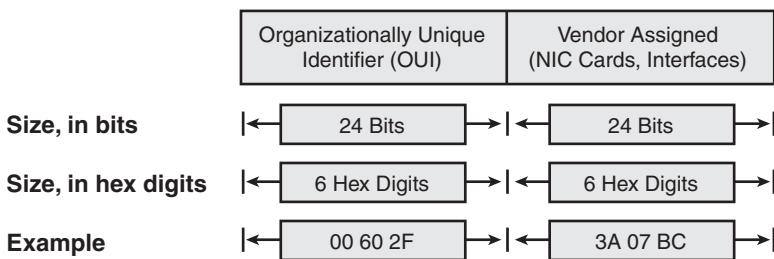
These seemingly simple switch features provide significant performance improvements as compared with using hubs. In particular:

- If only one device is cabled to each port of a switch, no collisions can occur.
- Devices connected to one switch port do not share their bandwidth with devices connected to another switch port. Each has its own separate bandwidth, meaning that a switch with 100 Mbps ports has 100 Mbps of bandwidth per port.

Ethernet Addressing

The IEEE defines the format and assignment of LAN addresses. To ensure a unique MAC address, the first half of the address identifies the manufacturer of the card. This code is called the organizationally unique identifier (OUI). Each manufacturer assigns a MAC address with its own OUI as the first half of the address. The second half of the address is assigned by the manufacturer and is never used on another card or network interface with the same OUI. Figure 28-5 shows the structure of a unicast Ethernet address.

Figure 28-5 Structure of Unicast Ethernet Address



Ethernet also has group addresses, which identify more than one NIC or network interface. The IEEE defines two general categories of group addresses for Ethernet:

- **Broadcast addresses:** The broadcast address implies that all devices on the LAN should process the frame and has a value of FFFF.FFFF.FFFF.
- **Multicast addresses:** Multicast addresses are used to allow a subset of devices on a LAN to communicate. When IP multicasts over an Ethernet, the multicast MAC addresses used by IP follow this format: 0100.5exx.xxxx, where any value can be used in the last half of the address.

Ethernet Framing

The physical layer helps you get a string of bits from one device to another. The framing of the bits allows the receiving device to interpret the bits. The term *framing* refers to the definition of the fields assumed to be in the data that is received. Framing defines the meaning of the bits transmitted and received over a network.

The framing used for Ethernet has changed a couple of times over the years. Each iteration of Ethernet is shown in Figure 28-6, with the current version shown at the bottom.

Figure 28-6 Ethernet Frame Formats

DIX

Preamble 8	Destination 6	Source 6	Type 2	Data and Pad 46 – 1500	FCS 4
----------------------	------------------	-------------	------------------	---------------------------	----------

IEEE 802.3 (Original)

Preamble 7	SFD 1	Destination 6	Source 6	Length 2	Data and Pad 46 – 1500	FCS 4
----------------------	-----------------	------------------	-------------	--------------------	---------------------------	----------

IEEE 802.3 (Revised 1997)

Bytes	Preamble 7	SFD 1	Destination 6	Source 6	Length/ Type 2	Data and Pad 46 – 1500	FCS 4
-------	----------------------	-----------------	------------------	-------------	---------------------------	---------------------------	----------

The fields in the last version shown in Figure 28-6 are explained further in Table 28-3.

Table 28-3 IEEE 802.3 Ethernet Field Descriptions

Field	Field Length in Bytes	Description
Preamble	7	Synchronization
Start Frame Delimiter (SFD)	1	Signifies that the next byte begins the Destination MAC field
Destination MAC address	6	Identifies the intended recipient of this frame
Source MAC address	6	Identifies the sender of this frame
Length	2	Defines the length of the data field of the frame (either length or type is present, but not both)
Type	2	Defines the type of protocol listed inside the frame (either length or type is present, but not both)
Data and Pad	46–1500	Holds data from a higher layer, typically a Layer 3 PDU (generic), and often an IP packet
Frame Check Sequence (FCS)	4	Provides a method for the receiving NIC to determine whether the frame experienced transmission errors

The Role of the Physical Layer

We have already discussed the most popular cabling used in LANs—UTP. But to fully understand the operation of the network, you should know some additional basic concepts of the physical layer.

The OSI physical layer accepts a complete frame from the data link layer and encodes it as a series of signals that are transmitted onto the local media.

The delivery of frames across the local media requires the following physical layer elements:

- The physical media and associated connectors
- A representation of bits on the media
- Encoding of data and control information
- Transmitter and receiver circuitry on the network devices

There are three basic forms of network media on which data is represented:

- Copper cable
- Fiber
- Wireless (IEEE 802.11)

Bits are represented on the medium by changing one or more of the following characteristics of a signal:

- Amplitude
- Frequency
- Phase

The nature of the actual signals representing the bits on the media will depend on the signaling method in use. Some methods may use one attribute of a signal to represent a single 0 and use another attribute of a signal to represent a single 1. The actual signaling method and its detailed operation are not important to your CCNA exam preparation.

Study Resources

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

Resource	Chapter	Topic	Where to Find It
Foundational Resources			
CCNA Exploration Online Curriculum: Network Fundamentals	Chapter 8, "OSI Physical Layer" Chapter 9, "Ethernet" Chapter 10, "Planning and Cabling Networks"	All topics within the chapter Overview of Ethernet Ethernet—Communication through the LAN The Ethernet Frame Ethernet Media Access Control Ethernet Physical Layer Address Resolution Protocol (ARP) Making LAN Connections	Chapter 8 Section 9.1 Section 9.2 Section 9.3 Section 9.4 Section 9.5 Section 9.7 Section 10.2.2
CCNA Exploration Online Curriculum: LAN Switching and Wireless	Chapter 2, "Basic Switch Concepts and Configuration"	Key Elements of Ethernet/802.3 Networks	Section 2.2.1
CCNA Exploration Network Fundamentals Companion Guide	Chapter 8, "OSI Physical Layer" Chapter 9, "Ethernet" Chapter 10, "Planning and Cabling Networks"	All topics within the chapter Overview of Ethernet Ethernet: Communication through the LAN The Ethernet Frame Ethernet MAC Ethernet Physical Layer Address Resolution Protocol (ARP) Making LAN Connections	pp. 279–306 pp. 315–320 pp. 320–324 pp. 324–334 pp. 334–342 pp. 342–347 pp. 355–361 pp. 380–384
CCNA Exploration LAN Switching and Wireless Companion Guide	Chapter 2, "Basic Switch Concepts and Configuration"	Key Elements of Ethernet/802.3 Networks	pp. 46–52
ICND1 Official Exam Certification Guide	Chapter 3, "Fundamentals of LANs"	All topics within the chapter	pp. 45–69
ICND1 Authorized Self-Study Guide	Chapter 1, "Building a Simple Network" Chapter 2, "Ethernet LANs"	Understanding Ethernet Connecting to an Ethernet LAN Understanding the Challenges of Shared LANs	pp. 104–115 pp. 115–124 pp. 139–144
Supplemental Resources			
CCNA Flash Cards and Exam Practice Pack	ICND1, Section 3	Understanding Ethernet	pp. 70–84

Symbols

3DES (Triple DES), 323

10BASE-T, 37

100BASE-TX, 37

802.00i (WPA2), 258

802.11g, 255

802.3. See Ethernet

1000BASE-T, 37

A

access attacks, 272

access control lists. *See* ACLs

access layer switches, 4

acknowledgment (ACK) packets,
EIGRP, 213

ACLs (access control lists), 279

adding comments to named or numbered
ACLs, 287-288

complex ACLs, 288

configuring extended numbered ACLs,
284-285

deny FTP from subnets, 285

deny only Telnet from subnets, 285-286

configuring named ACLs, 286-287

configuring standard numbered ACLs, 282

deny a specific host, 283

deny a specific subnet, 283-284

deny Telnet access to routers, 284

permit specific network, 282-283

defining, 279

design guidelines, 281-282

extended ACLs, 280

identification, 281

interface processing, 279-280

standard ACLs, 280

troubleshooting, 291

denied protocols, 292-293

host has no connectivity, 291-292

Telnet is allowed #1, 293

Telnet is allowed #2, 294

Telnet is allowed #3, 294-295

types of, 280-281

verifying, 289-290

AD (administrative distance), 153-154

ad hoc mode, wireless operations, 254

adding comments to named or numbered
ACLs, 287-288

Address Resolution Protocol (ARP),
16, 148

addresses

broadcast addresses, 38

Ethernet, 38

IPv4, 109

classes of addresses, 110-111

header formats, 109-110

subnet masks, 111-112

IPv6

conventions for writing, 139

loopback addresses, 141

managing, 142

private addresses, 141

reserved addresses, 141

link-local addresses, 141

multicast addresses, 38

private IP addressing, 119-120

public IP addressing, 119-120

site-local addresses, 141

static addresses, 123

subnet addresses, summarizing, 118-119

addressing devices, 123

addressing schemes, 354

EIGRP, 215

OSPF, 233-234

RIPv1, 198

administrative distance (AD), 153-154

EIGRP, 214

Advanced Encryption Standard
(AES), 323

advertisement request message, VTP, 78

AES (Advanced Encryption
Standard), 323

AH (Authentication Header), 325

algorithms, OSPF, 231-232

analog dialup, circuit-switched
connections (WAN), 314-315

ANDing, 112

antivirus software, 273

application layer (TCP/IP), 21

applications, network-based applications, 17

- impact of voice and video, 18
- increased network usage, 17
- QoS (quality of service), 17

ARP (Address Resolution Protocol), 16, 124-126, 148

- Frame Relay, 339

AS (autonomous system), 150**assigning VLANs, 358, 369-370**

- to interfaces, 89

asymmetric switching, 46**ATM, packet-switched connections (WAN), 317****attacker terminology, 267-268****attackers, thinking like, 268-269****authentication**

- PPP, LCP, 333
- VPNs, 325
- wireless security, 257

Authentication Header (AH), 325**auto-cost reference-bandwidth, 236****automatic summarization**

- EIGRP, 216-217
- RIPv1, 204-205

autonomous system (AS), 150**autosummarization, disabling in RIPv2, 208****availability, balancing with security, 269****B****backing up IOS images, 184****backup DR (BDR), 230****backward explicitly congestion notification (BECN), Frame Relay, 339****balancing security and availability, 269****bandwidth command, 220, 236****Basic Rate Interface (BRI), 315****basic router configuration, 167-174****BDR (backup designated router), 230****BECN (backward explicit congestion notification), Frame Relay, 339****BID (bridge ID), configuring, 82-84****binary values, subnet masks, 112****black hats, 268****black hole VLAN, 73****boot system command, 186****bootup process, routers, 162-163****BRI (Basic Rate Interface), 315****broadband wireless, Internet connections (WAN), 319****broadcast addresses, 38**

- subnetting, 114

broadcast domains, 45**broadcast storms, STP, 78****broadcasts, 43****C****cable modems, Internet connections (WAN), 318****cables**

- crossover cables, 6, 164-165
- straight-through cables, 6, 165

calculating Dijkstra algorithm (link-state routing protocols), 157-158**carrier protocols, 323****CDP, troubleshooting tools, 68-69****central office (CO), WAN, 309****channel service unit (CSU), 310****CHAP, configuring PPP, 335, 356, 362****cHDLC (Cisco HDLC), 329****CIR (committed information rate), Frame Relay, 339****circuit-switched connections, WAN, 314**

- analog dialup, 314-315
- ISDN, 315-316

Cisco devices, configuring, 47**Cisco Enterprise Architecture, 10****Cisco HDLC (cHDLC), 329****Cisco Interim Solution, 258****Cisco IOS (Internetwork Operating System), 46. *See also* IOS**

- CLI EXEC sessions, 47
- CLI navigation and shortcuts, 48
- command history, 49-50
- connecting to Cisco devices, 46-47
- examination commands, 50
- file naming conventions, 182-183
- help facility, 48
- storing and erasing configuration files, 51
- subconfiguration modes, 50

Cisco IOS Integrated File System.

See IFS

Cisco IOS OSPF cost values, 236

classes of addresses, IPv4 addressing, 110-111

classful routing protocols, 151-152

classifying dynamic routing protocols, 150

- classful routing protocols, 151-152
- classless routing protocols, 152
- distance vector routing protocols, 150-151
- EGP, 150
- IGP, 150
- link-state routing protocols, 151

classless routing protocols, 152

CLI (command-line interface), 162, 261

navigation and shortcuts, 48-49

CLI EXEC sessions, Cisco IOS, 47

clock rate command, 350

CO (central office), WAN, 309

codes, interface status codes, 65, 171

LAN switches, 65-66

collision domains, 45

command history, Cisco IOS, 49-50

command syntax help, 48

command-line interface (CLI), 162, 261

commands

- auto-cost reference-bandwidth, 236
- bandwidth, 236
 - EIGRP, 220*
- boot system, 186
- clock rate, 350
- command history buffer commands, 49-50
- configure terminal, 50
- copy, 51
 - managing configuration files, 182*
- copy run start, 182
- debug eigrp fsm, 224
- debug frame-relay lmi, 348
- debug ip nat, 305
- debug ip rip, 247
- debug ppp authentication, 351
- default-information originate, 206, 238
- dir, 180
- dynamic auto, 91
- dynamic desirable, 91
- enable password, 55
- enable password password, 169
- enable secret, 55
- encapsulation ppp, 334
- erase startup-config, 51
- examination commands, Cisco IOS, 50
- frame-relay interface-dlci, 348
- interface range command, 55
- ip helper-address, 131
- ip ospf cost, 236
- ip ospf priority interface, 237
- ip route, static routes, 191
- ipconfig/release, 131
- ipconfig/renew, 131
- for managing configuration files, IFS, 182
- network, 215-216, 234-235
- no auto-summary, 208, 216
- no debug ip rip, 248
- no keepalives, 351
- no service dhcp, 129
- no shutdown, 58, 104
- passive-interface, disabling updates, 203
- ping, 11, 62, 132-133
- ppp authentication chap, 335
- ppp authentication pap, 335
- range, 89
- redistribute static, 219
- router ospf, 234
- show access-lists, 289
- show cdp, 68
- show cdp interface, 69
- show cdp neighbors detail, 69
- show controllers, 350
- show file systems, 179-181
- show flash, 185
- show frame-relay map, 348
- show frame-relay pvc, 348
- show interface status, 67
- show interfaces, 66, 172-174, 351
- show interfaces serial, 349
- show interfaces status, 66
- show ip eigrp interfaces, 248
- show ip eigrp neighbors, 245, 249
- show ip interface, 290
- show ip interface brief, 11, 170, 239
- show ip nat statistics, 304
- show ip nat translations, 304
- show ip ospf, 241
- show ip ospf interface, 242-243
- show ip ospf interface brief, 248
- show ip ospf neighbor, 240, 249
- show ip ospf neighbor commands, 245
- show ip protocols, 153, 239-240, 245, 248
 - RIPv1, 200*

- show ip route, 11, 152, 170, 199, 239, 245
 - RIPv1*, 200
- show port-security, 57
- show port-security interface, 57, 94
- show run, 304
- show running-config, 170, 290
- show spanning-tree, 83
- show version, 162-163
- show vlan brief, 88-90
- show vtp status, 98
- spanning-tree mode rapid-pvst, 84
- spanning-tree portfast default, 84
- switch configuration commands, 53-54
- switchport mode access, 103
- switchport mode dynamic desirable, 75
- switchport mode trunk, 75
- switchport mode trunk dynamic auto, 75
- switchport nonegotiate, 75, 103
- switchport port-security violation, 56
- telnet, 11
- ftpdnld, 187
- traceroute, 133-134, 175, 246
- undebg all, 248
- username, 335
- vtp pruning, 98
- vtp version 2, 98
- write erase, 51
- xmodem, 187
- comments, adding to named or numbered ACLs, 287-288**
- committed information rate (CIR), Frame Relay, 339**
- complex ACLs, 288**
- components**
 - of Frame Relay, 338-339
 - of routers, internal components, 161-162
 - for teleworker connectivity, 7
 - of VPNs, 322
 - of WAN, 309
- configuration files**
 - Cisco IOS, 51
 - commands for managing, 182
- configurations, ISP, 355-356**
- configure terminal command, 50**
- configuring**
 - ACLs
 - extended numbered ACLs*, 284-286
 - named ACLs*, 286-287
 - standard numbered ACLs*, 282-284
 - Cisco devices, 47
 - default routing, 357, 364
 - DHCP, 359, 371-372
 - dynamic NAT, 301-302
 - EIGRP, 214-215
 - automatic summarization*, 216-217
 - default routes*, 219
 - manual summarization*, 217-218
 - modifying EIGRP metrics*, 219-220
 - modifying hello intervals and hold times*, 220-221
 - network command*, 215-216
 - EIGRP routing, 357, 365-366
 - firewall ACLs, 359, 372-373
 - Frame Relay, 343-344
 - full mesh with one subnet*, 344-347
 - hub-and-spoke topology*, 356, 360-362
 - partial mesh with one subnet per PVC*, 347-348
 - HDLC, 330
 - inter-VLAN routing, 103-105, 357, 364-365
 - NAT, 356, 362-363
 - NAT overload, 303
 - OSPF, 233
 - controlling DR/BDR election*, 237-238
 - modifying Hello intervals and hold times*, 238-239
 - modifying metrics*, 236-237
 - network command*, 234-235
 - redistributing default routes*, 238
 - router ID*, 235-236
 - router ospf command*, 234
 - port security, 56-58, 358, 369-370
 - PPP, 334
 - CHAP*, 335, 356, 362
 - PAP*, 335-336
 - RIPv1, 198-199
 - RIPv2, 207-208
 - disabling autosummarization*, 208
 - routers, as DHCP servers, 128-132
 - RSTP, 84
 - SSH access, 55-56
 - static NAT, 301
 - static routes, 191-193
 - default static routes*, 194-197
 - with "Next Hop" parameter*, 193
 - with exit interface parameter*, 193-194
 - STP, 82, 358, 370-371
 - BID (bridge ID)*, 82-84
 - PortFast*, 84

trunking, 91-93
 VLANs, 88-91, 357, 367-369
 VTP, 97-100
 Windows PC to use DHCP, 123

Connecting Cisco IOS to Cisco devices, 46-47

connection establishment, TCP/IP, 25

connection-oriented systems, WAN, 313

connectionless protocols, 26

connectionless systems, WAN, 313

connections

- routers, 164-165
- verifying network connectivity, 62-65, 175-176
- WAN
 - circuit-switched connections, 314-316*
 - dedicated connections, 314*
 - Internet connections, 317-319*
 - packet-switched connections, 315-317*
 - WAN link options, 319-320*

conventions

- for writing IPv6 addresses, 139
- for writing IPv6 prefixes, 139-140

converging with link-state protocols, link-state routing protocols, 158

copy command, 51, 182

copy run start command, 182

core layer switches, 4

CPE (Customer Premises Equipment), 309

CPU, 161

crackers, 268

crossover cables, 6, 164-165

CSMA/CA (carrier sense multiple access with collision avoidance), 256-257

CSMA/CD (carrier sense multiple access with collision detection), 34-35

CSU (channel service unit), 310

Customer Premises Equipment (CPE), 309

cut-through switching, 46

D

Data Communications Equipment (DCE), 309, 337

data encapsulation

- MAC sublayer, 34
- TCP/IP, 28

Data Encryption Standard (DES), 323

data service unit (DSU), 310

Data Terminal Equipment (DTE), 309, 337

data VLAN, 72

data-link connection identifier (DLCI), Frame Relay, 338

data-link protocols, WAN, 312

DBD (database description) packets, OSPF, 228

DCE (Data Communications Equipment), 309, 337

DDoS (distributed denial-of-service) attacks, 272

debug eigrp fsm, 224

debug frame-relay lmi, 348

debug ip nat command, 305

debug ip rip commands, 247

debug ppp authentication, 351

dedicated connections, WAN, 314

default file systems, 180

default routes

- EIGRP, 219
- redistributing in OSPF, 238
- RIPv1, 206-207

default routing, configuring, 357, 364

default static routes, configuring, 194-197

default VLAN, 72

default-information originate command, 206, 238

demarcation point, WAN, 309

denial-of-service (DoS) attacks, 272

deny any statements, 279

DES (Data Encryption Standard), 323

design guidelines, ACLs, 281-282

designated router (DR), 230-231

device hardening, 273

devices, 3

- Cisco devices, configuring, 47
- connecting Cisco IOS to Cisco devices, 46-47
- hubs, 3
- switches. *See* switches of WAN, 310

DHCP (Dynamic Host Configuration Protocol), 15, 127

- configuring, 359, 371-372
- configuring Windows PC to use, 123
- verifying operations, 130

DHCP servers, configuring routers as, 128-132**DHCPv6, 142****Dijkstra algorithm, calculating, 157-158****dir command, 180****Direct Sequence Spread Spectrum (DSSS), 255****disabling**

- autosummarization, RIPv2, 208
- updates, passive-interface command, 203

discontiguous networks, 246-247**distance vector routing protocols, 150-151****distance vectors, EIGRP versus, 211****distributed DoS attacks, 272****distribution layer switches, 4****DLCI (data-link connection identifier), Frame Relay, 338****DNS (Domain Name System), 15, 126-127****documentation for networks, 11****domains**

- broadcast domains, 45
- collision domains, 45
- top-level domains, 126

DoS (denial-of-service) attacks, 272**DR (designated router), 230-231****DR/BDR election, OSPF controlling, 237-238****DSL, Internet connections (WAN), 317-318****DSSS (Direct Sequence Spread Spectrum), 255****DSU (data service unit), 310****DTE (Data Terminal Equipment), 309, 337****DTP (Dynamic Trunking Protocol), 75****DUAL, EIGRP, 214****dual stacking, IPv6, 143****duplexes, switches, 66-67****dynamic 6to4 tunnels, 143****dynamic auto, 91****dynamic desirable, 91****Dynamic Host Configuration Protocol (DHCP), 15****dynamic NAT, 299-302****dynamic routing, 191**

- static routing versus, 149

dynamic routing metrics, 152-153**dynamic routing protocols, classifying, 150**

- classful routing protocols, 151-152
- classless routing protocols, 152
- distance vector routing protocols, 150-151
- EIGRP, 150
- IGRP, 150
- link-state routing protocols, 151

Dynamic Trunking Protocol (DTP), 75**E****E1 (External Type 1), 240****E2 (External Type 2), 240****EAP (Extensible Authentication Protocol), 264****EGP (Exterior Gateway Protocols), 150****EIA (Electronics Industry Alliance), 36****EIA/TIA-232, 311****EIA/TIA-449/530, 311****EIA/TIA-612/613, 311****EIGRP (Enhanced Interior Gateway Routing Protocol), 211**

- addressing schemes, 215
- administrative distance, 214
- configuring, 214-215
 - automatic summarization, 216-217*
 - default routes, 219*
 - manual summarization, 217-218*
 - modifying EIGRP metrics, 219-220*
 - modifying hello intervals and hold times, 220-221*
 - network command, 215-216*
- distance vectors versus, 211
- DUAL, 214
- dynamic routing metrics, 153
- message formats, 212
- neighbor requirements, 249
- packet types, 212-213
- troubleshooting, 248
- verifying
 - with show ip eigrp neighbors, 222-224*
 - with show ip protocols, 221*

EIGRP routing, configuring, 357, 365-366

electrical threats, 271

Electronics Industry Alliance (EIA), 36

eliminating routing loops, 155-156

employees, wireless security risks, 257

enable password command, 55

enable password password command, 169

enable secret command, 55

encapsulating protocols, 323

Encapsulating Security Payload (ESP), 325

encapsulation, 322

HDLC, 329-330

OSI models, 16

encapsulation ppp command, 334

encapsulation process, 16

encoding channels, wireless encoding channels, 255

encryption, 257, 322

encryption algorithms, VPNs, 323

Enhanced Interior Gateway Routing Protocol. *See* EIGRP

Enterprise Architecture, 10

Enterprise Branch Architecture, 10

Enterprise Campus Architecture, 10

Enterprise Data Center Architecture, 10

Enterprise Edge Architecture, 10

Enterprise Teleworker Architecture, 10

environmental threats, 271

erase startup-config command, 51

erasing configuration files, Cisco IOS, 51

error detection, LCP, 332

error recovery, TCP/IP, 24

ESP (Encapsulating Security Payload), 325

establishing VPN connections, 322

authentication, 325

encryption algorithms, 323

hashes, 324-325

IPsec Security Protocols, 325

tunneling, 323

Ethernet, 16

addresses, 38

current Ethernet technologies, 36

framing, 39

Gigabit Ethernet, 37

legacy Ethernet technologies, 34-36

CSMA/CD, 35

overview, 33-34

physical layer, role of, 40

switches, 37-38

UTP cabling, 36-37

EtherType field, 74

EUI-64 format, IPv6, 141-142

examinations

exam day information, 377

post-exam information

career options, 379-380

receiving your certificate, 379

retesting, 380

examination commands, Cisco IOS, 50

exit interface parameter, configuring static routes, 193-194

extended ACLs, 280

extended numbered ACLs, configuring, 284

deny FTP from subnets, 285

deny only Telnet from subnets, 285-286

Extensible Authentication Protocol (EAP), 264

Exterior Gateway Protocols (EGP), 150

external threats, 271

External Type 1 (E1), 240

External Type 2 (E2), 240

F

FC (Feasibility Condition), 223

FCC (Federal Communications Commission), 253-254

FD (Feasible Distance), 223

Feasible Successor (FS), 223

FECN (forward explicit congestion notification), Frame Relay, 339

FHSS (Frequency Hopping Spread Spectrum), 255

file naming conventions, IOS, 182-183

file systems, default file systems, 180

File Transfer Protocol (FTP), 15

firewall ACLs, configuring, 359, 372-373

firewalls, 273

flash memory, 162

flow control, TCP/IP, 25

forward explicit congestion notification (FECN), Frame Relay, 339

forwarding, frame forwarding, 45

- asymmetric switching, 46
- Layer 2 switching, 46
- Layer 3 switching, 46
- memory buffering, 46
- switch forwarding methods, 45
- symmetric switching, 46

FRAD (Frame Relay Access Devices), 337

frame format, PPP, 331-332

frame forwarding, 45-46

Frame Relay, 16, 337

- backward explicit congestion notification (BECN), 339
- committed information rate (CIR), 339
- components of, 338-339
- configuring, 344
 - full mesh with one subnet, 344-347*
 - hub-and-spoke topology, 356, 360-362*
 - partial mesh with one subnet per PVC, 347-348*
- configuring and verifying, 343
- data-link connection identifier (DLCI), 338
- DCE, 337
- DTE, 337
- forward explicit congestion notification (FECN), 339
- Inverse Address Resolution Protocol (ARP), 339
- Inverse ARP, 341-343
- LMI, 341-343
- local access rate, 338
- Local Management Interface (LMI), 339
- NBMA (nonbroadcast multi-access), 340
- packet-switched connections, WAN, 317
- permanent virtual circuit (PVC), 338
- switched virtual circuit (SVC), 338
- topologies, 339
- verifying, 348
- virtual circuit (VC), 338

Frame Relay Access Devices (FRAD), 337

frame-relay interface-dlci command, 348

framing, Ethernet, 39

Frequency Hopping Spread Spectrum (FHSS), 255

FS (Feasible Successor), 223

FTP (File Transfer Protocol), 15

full-mesh topology, Frame Relay, 339

G

Gigabit Ethernet, 37

global unicast addresses, IPv6, 140-141

GUI (graphical user interface), 162, 261

H

hackers, 257, 267

hardware threats, 271

hashes, VPNs, 324-325

HDLC

- configuring, 330
- encapsulation, 329-330
- verifying, 331

HDLC (High-Level Data Link Control), 329

header formats, IPv4 addressing, 109-110

hello intervals and hold times

- modifying (EIGRP), 220-221
- modifying (OSPF), 238-239

Hello packets

- EIGRP, 213
- OSPF, 228
 - neighbor adjacency, 228-229*

help facilities, Cisco IOS, 48

hierarchical network models, 9

High-Level Data Link Control (HDLC), 329

HIPS (host-based intrusion prevention), 273

history of commands, Cisco IOS, 49-50

HMAC (hashed message authentication code), 324-325

hold-down timers, preventing routing loops, 155

host and server security, mitigation techniques, 273

host ranges, subnetting, 114

host-based intrusion prevention (HIPS), 273

HTTP (Hypertext Transfer Protocol), 15

HTTP request, 21

HTTP response, 21

hub-and-spoke configuration, Frame Relay, 340

hub-and-spoke topology, Frame Relay (configuring), 356, 360-362

hubs, 3

Hypertext Transfer Protocol (HTTP), 15

I

ICMP (Internet Control Message Protocol), 16, 147

identification, ACLs, 281

IDS (intrusion detection systems), 273

IEEE, 253

IETF (Internet Engineering Task Force), 137, 227

IFS (Integrated File System)

commands, 179-181

commands for managing configuration files, 182

URL prefixes for specifying file locations, 181

IGP (Interior Gateway Protocols), 150

comparison summary, 154

images, IOS images, 183

backing up, 184

recovering with TFTP servers, 186-187

recovering with Xmodem, 187-188

restoring, 185-186

IMAP (Internet Message Access Protocol), 15

implementing WLAN, 261

checklist for implementing, 262-264

infrastructure mode, wireless operations, 254

inside global address, NAT, 297

inside local address, NAT, 297

Integrated File System. *See* IFS

Inter-Switch Link (ISL), 103

inter-VLAN routing

configuring, 103-105, 357, 364-365

troubleshooting, 105

verifying, 105

interface ID, IPv6, 141-142

interface processing, ACLs, 279-280

interface range command, 55

interface status codes, 65-66, 171

interfaces

assigning VLANs to, 89

passive interfaces, RIPv1, 203-204

routers, 164

unused interfaces, shutting down and securing, 58

up interfaces, layer 1 problems, 67

Interior Gateway Protocols. *See* IGP

internal threats, 271

Internet connections, WAN

broadband wireless, 319

cable modems, 318

DSL, 317-318

Metro Ethernet, 319

Internet Control Message Protocol (ICMP), 16, 147

Internet Engineering Task Force (IETF), 137

internet information queries, 271

Internet layer, TCP/IP, 26

Internet Message Access Protocol (IMAP), 15

Internet Protocol (IP), 16

Internetwork Operating System. *See* Cisco IOS

Intrastate Automatic Tunnel Addressing Protocol (ISATAP), 143

intrusion detection and prevention, mitigation techniques, 273

intrusion detection systems (IDS), 273

intrusion tools, wireless security, 257

Inverse Address Resolution Protocol (ARP), Frame Relay, 339

Inverse ARP, Frame Relay, 341-343

IOS (Internetwork Operating System), 162

file naming conventions, 182-183

IOS images

managing, 183

backing up, 184

restoring, 185-186

recovering with TFTP servers, 186-187

recovering with Xmodem, 187-188

IP (Internet Protocol), 16

IP addressing, 119-120

ip helper-address command, 131

IP multicast, 72

ip ospf cost command, 236

ip ospf priority interface command, 237

ip route command, static routes, 191

IP telephony, 72

ipconfig/release commands, 131

ipconfig/renew command, 131

IPsec Security Protocols, VPNs, 325

IPv4

addresses

classes of addresses, 110-111

header formats, 109-110

subnet masks, 111-112

versus IPv6, 137

IPv6

addresses

conventions for writing, 139

global unicast addresses, 140-141

loopback addresses, 141

managing, 142

private addresses, 141

reserved addresses, 141

interface ID and EUI-64 format, 141-142

versus IPv4, 137

overview of, 137-138

prefixes, conventions for writing, 139-140

transitioning to, 142-143

ISATAP (Intrasite Automatic Tunnel Addressing Protocol), 143

ISDN, circuit-switched connections (WAN), 315-316

ISL (Inter-Switch Link), 103

ISP (Internet service provider), configurations, 355-356

ITU-R, 253

J-K-L

jitter, 18

LAN cabling, standards for, 6

LAN switches, 45

interface status codes, 65-66

LANs (local-area networks), 7

Layer 1 problems, troubleshooting, 350

Layer 1 problems, up interfaces, 67

Layer 2 problems, troubleshooting, 350-351

Layer 2 switching, 46

Layer 3 problems, troubleshooting, 351-352

Layer 3 switching, 46

layers

OSI models, 14-15

TCP/IP models, 15-16

troubleshooting with, 29

LCP (PPP Link Control Protocol), 332-333

legacy Ethernet technologies, 34-36

CSMA/CD, 35

link-local addresses, 141

link-state advertisements (LSA), 228

link-state database (LSDB), building, 156-157

link-state protocols, converging with link-state routing protocols, 158

link-state routing process, OSPF, 232-233

link-state routing protocols, 151, 156

calculating Dijkstra algorithms, 157-158

convergence with link-state protocols, 158

LSDB, building, 156-157

LLC (Logical Link Control) sublayer, 34

LMI (Local Management Interface)

Frame Relay, 339-343

local access rate, Frame Relay, 338

local loop, 309

Local Management Interface (LMI), Frame Relay, 339

Logical Link Control (LLC) sublayer, 34

logical switching, 44-45

logical topologies, 9

loopback addresses, IPv6, 141

loopback configurations, OSPF, 235

looped link detection, LCP, 332

loss, 18

low delay, 18

LSA (link-state advertisements), 156, 228-229

LSack (link-state acknowledgment) packets, OSPF, 228

LSDB (link-state database), building, 156-157

LSR (link-state request) packets, OSPF, 228

LSU (link-state update) packets, OSPF, 228-229

M

MAC (Media Access Control) sublayer, 34

MAC addresses, switch forwarding, 45

MAC database instability, STP, 79

MAC sublayer, 34

maintaining security, 275-276

maintenance threats, 271

malicious code attacks, 272

man-in-the-middle attacks, 272

management VLAN, 73

managing

addresses, IPv6, 142

IOS images, 183

backing up, 184

restoring, 185-186

manual summarization, EIGRP, 217-218

MCT (manually configured tunnels), 143

media, 5-6

networking, 5

standards for LAN cabling, 6

Media Access Control (MAC) sublayer, 34

memory, 162

memory buffering, 46

message-of-the-day (MOTD), 169

messages

EIGRP, 212

OSPF, 227-228

RIPv1, 197

methodologies, troubleshooting, 61-62

metrics, dynamic routing metrics, 152-153

Metro Ethernet, Internet connections (WAN), 319

MIST (Multiple Instances of Spanning Tree), 82

mitigation techniques, 273

host and server security, 273

intrusion detection and prevention, 273

security appliances and applications, 273-274

models

network models, benefits of, 13

OSI models, 13

layers, 14-15

PDUs and encapsulation, 16

TCP/IP models, 13-16

modes of VTP, 77

modifying

EIGRP metrics, 219-220

Hello intervals and hold times

EIGRP, 220-221

OSPF, 238-239

OSPF metrics, 236-237

MOTD (message-of-the-day), 169

multicast addresses, 38

multilink PPP, LCP, 333

multiple frame transmission, STP, 79

Multiple Instances of Spanning Tree (MIST), 82

municipal Wi-Fi, 319

mutual authentication, wireless security, 257

N

named ACLs, configuring, 286-287

naming conventions, IOS, 182-183

NAT (Network Address Translation), 297

benefits of, 300

configuring, 356, 362-363

dynamic NAT, 299-302

example of PC1 sending traffic to Internet, 298-299

inside global address, 297

inside local address, 297

limitations of, 300

outside global address, 297

outside local address, 297

overloading, 300

static NAT, 299-301

troubleshooting, 304-305

verifying, 303-304

NAT overload, 299-300, 303

native VLAN, 73

navigation, CLI, 48-49

NBMA (nonbroadcast multi-access), Frame Relay, 340

NCPs (Network Control Protocols), 332

neighbor adjacency issues, troubleshooting, 248-250

neighbors, OSPF
 Hello packets, 228-229
 verifying, 240

network access layer, TCP/IP, 27-28

Network Address Translation. See NAT

network admission control, 274

network command, 215-216, 234-235

network connectivity, verifying, 62-65, 175-176

Network Control Protocols (NCPs), 332

network documentation, 11

network interface card (NIC), 261

network layer testing tools
 ping, 132-133
 traceroute, 133-134

network management, 72

network models, benefits of, 13

network statements, 209, 247

network usage, network-based applications, 17

network-based applications, 17-18

networking, media, 5

networking icons, 7

networks
 discontinuous networks, 246-247
 OSPF, 230
 threats to, 271

networks attacks, types of, 271-272

“Next Hop” parameter, configuring static routes, 193

NIC (network interface card), 261

no auto-summary command, 208, 216

no debug ip rip, 248

no keepalives command, 351

no service dhcp command, 129

no shutdown command, 58, 104

nonbroadcast multi-access (NBMA), 340

normal data, 72

NVRAM (nonvolatile random-access memory), 162

O

OFDM (Orthogonal Frequency Division Multiplexing), 255

Open Shortest Path First. See OSPF

operating system patches, 273

organizationally unique identifier (OUI), 38

Orthogonal Frequency Division Multiplexing (OFDM), 255

OSI models, 13
 OSI layers, 14-15
 PDUs (protocol data units), 16

OSPF (Open Shortest Path First), 227
 addressing schemes, 233-234
 algorithms, 231-232
 configuring, 233
controlling DR/BDR election, 237-238
modifying Hello intervals and hold times, 238-239
modifying metrics, 236-237
network command, 234-235
redistributing default routes, 238
router ID, 235-236
router ospf command, 234
 DR/BDR election, 230-231
 Hello packets, neighbor adjacency, 228-229
 link-state routing process, 232-233
 loopback configurations, 235
 LSA packets, 229
 LSU packets, 229
 message format, 227-228
 neighbor requirements, 249-250
 network types, 230
 packet types, 228
 troubleshooting, 239-240, 248
 verifying, 240-243

OUI (organizationally unique identifier), 38

outside global address, NAT, 297

outside local address, 297

overloading NAT, 299-300

P

- packet capturing sniffers, 271**
- packet forwarding, 147**
 - path determination and switching function
 - example, 148-149
- packet-switched connections, WAN, 315**
 - ATM, 317
 - Frame Relay, 317
 - X.25, 315
- packets**
 - EIGRP, 212-213
 - OSPF, 228
 - RTP, 212-213
- PAP, configuring PPP, 335-336**
- parameters**
 - exit interface, configuring static routes, 193-194
 - “Next Hop,” configuring static routes, 193
- partial-mesh topology, Frame Relay, 339**
- passenger protocols, 323**
- passive interfaces, RIPv1, 203-204**
- passive-interface command, disabling updates, 203**
- password attacks, 272**
- passwords, recovering, 188**
- PAT (Port Address Translation), 299**
- path determination, packet forwarding, 148-149**
- PDUs (protocol data units), OSI models, 16**
- Per-VLAN Rapid Spanning Tree (PVRST), 82**
- permanent virtual circuit (PVC), Frame Relay, 338**
- personal firewalls, 273**
- phishers, 268**
- phreakers, 268**
- physical (MAC) addresses, ARP, 125**
- physical infrastructures, threats to, 271**
- physical layer**
 - Ethernet, 40
 - WAN, 311
- physical topologies, 8**
- ping, 11, 62, 132-133**
 - verifying network connectivity, 175
- ping sweeps, 271**
- ping-of-death attacks, 272**
- Point-to-Point Protocol. *See* PPP**
- policies, developing security policies, 269-270**
- POP3 (Post Office Protocol), 15**
- Port Address Translation (PAT), 299**
- port mappings, VLAN, 355**
- port numbers, 23**
- port redirection, 272**
- port roles, RSTP and STP, 81**
- port scans, 271**
- port security, configuring, 56-58, 358, 370**
- port states, RSTP and STP, 81**
- port examination, post-exam information (receiving your certificate), 379**
- port-based memory, 46**
- PortFast, 84**
- ports, routers, 164**
- Post Office Protocol (POP3), 15**
- PPP (Point-to-Point Protocol), 329-330**
 - configuring, 334
 - CHAP, 335
 - PAP, 335-336
 - with CHAP, 356, 362
 - frame format, 331-332
 - LCP (Link Control Protocol), 332-333
- ppp authentication chap command, 335**
- ppp authentication pap command, 335**
- PPP Link Control Protocol. *See* LCP**
- prefixes**
 - IPv6, conventions for writing, 139-140
 - URL prefixes for specifying file locations, 181
- preshared key (PSK), 325**
- preventing routing loops, 155-156**
- PRI (Primary Rate Interface), 315**
- private addresses, IPv6, 141**
- private IP addressing, 119-120**
- privileged EXEC mode, 47**
- pruning, VTP, 78**
- PSK (preshared key), 325**
- PSTN (public switched telephone network), 310**
- public IP addressing, 119-120**

PVC (permanent virtual circuit)

- Frame Relay, 338
- WAN, 313

PVRST (Per-VLAN Rapid Spanning Tree), 82**Q****QoS (Quality of Service), network-based applications, 17**

- quad-zero routes, 194

- quartets, 139

- query packets, EIGRP, 213

R

- RAM, 161

- range command, 89

Rapid Per-VLAN Spanning Tree (RPVST), 82

- Rapid STP. *See* RSTP

- reconnaissance attacks, 271

recovering

- IOS images
 - with TFTP servers, 186-187
 - with Xmodem, 187-188
- passwords, 188

- redistribute static command, 219

- redistributing default routes, OSPF, 238

- reference bandwidth, 236

- Reliable Transport Protocol. *See* RTP

- remote-access VPNs, 321

- reply packets, EIGRP, 213

- reserved addresses, IPv6, 141

- restoring IOS images, 185-186

RIP, 197

- routes, interpreting, 200
- troubleshooting, 247-248

RIPv1, 198

- addressing schemes, 198
- automatic summarization, 204-205
- configuring, 198-199
- default routing, 206-207
- message format, 197
- passive interfaces, 203-204
- verifying, 199-202

RIPv2

- configuring, 207-208
- verifying, 208-209

Rivest, Shamir, and Adleman (RSA), 323

- rogue AP, wireless security risks, 257

ROM, 161

- router ID, configuring OSPF, 235-236

- router ospf command, 234

routers, 5

- AD (administrative distance), 153-154
- basic router configuration, 167-174
- bootup process, 162-163
- configuring as DHCP servers, 128-132
- connections, 164-165
- internal components of, 161-162
- ports and interfaces, 164

- routes, tracing from Windows PC, 65

routing

- EIGRP. *See* EIGRP
- inter-VLAN routing, configuring and verifying, 103-105
- OSPF. *See* OSPF
- troubleshooting, 245

- routing loop prevention, 155-156

routing methods, 149

- dynamic routing protocols, classifying, 150-152
- dynamic versus static routing, 149

RPVST (Rapid Per-VLAN Spanning Tree), 82

- RSA (Rivest, Shamir, and Adleman), 323

RSTP (Rapid STP), 80-81

- configuring, 84
- port roles, 81
- port states, 81

- RTP (Reliable Transport Protocol), 212

- packets, 212-213

S

- satellite Internet, 319

- scavenger class, 72

- securing unused interfaces, 58

security, 267

- attacker terminology, 267-268
- balancing security and availability, 269
- common threats
 - to networks, 271
 - to physical infrastructures, 271
 - vulnerabilities, 270

- configuring, 369
- developing security policies, 269-270
- importance of, 267
- maintaining, 275-276
- mitigation techniques, 273-274
- network attacks, 271-272
- port security, configuring, 56-58
- thinking like attackers, 268-269
- wireless security risks, 257
- wireless security standards, 258
- security appliances and applications, mitigation techniques, 273-274**
- security communications, 274**
- security violations, 57**
- service set identifier (SSID), 261**
- shared memory, 46**
- shortcuts, CLI, 48-49**
- show access-lists command, 289**
- show cdp commands, 68**
- show cdp interface command, 69**
- show cdp neighbor detail, 11, 69**
- show controllers command, 350**
- show file systems command, 179-181**
- show flash command, 185**
- show frame-relay map command, 348**
- show frame-relay pvc command, 348**
- show interface status, 67**
- show interfaces, 66, 171-174**
- show interfaces command, 351**
- show interfaces serial command, 349**
- show interfaces status, 66**
- show ip eigrp interfaces, 248**
- show ip eigrp neighbors, 222-224, 245, 249**
- show ip interface brief, 11, 170, 239**
- show ip interface command, 290**
- show ip interface e0 command, 290**
- show ip nat statistics command, 304**
- show ip nat translations command, 304**
- show ip ospf command, 241**
- show ip ospf interface brief, 242-243, 248**
- show ip ospf neighbor, 240, 245, 249**
- show ip protocols, 153, 239-240, 245, 248**
 - EIGRP, 221
 - RIPv1, 200
- show ip route, 11, 152, 170, 199, 239, 245**
 - RIPv1, 200
- show port-security command, 57**
- show port-security interface command, 57**
- show portsecurity interface, 94**
- show run command, 304**
- show running-config command, 170, 290**
- show spanning-tree command, 83**
- show version command, 162-163**
- show vlan brief, 88-90**
- show vtp status command, 98**
- shutting down unused interfaces, 58**
- site-local addresses, 141**
- site-to-site VPNs, 320**
- SMTP (Simple Mail Transfer Protocol), 15**
- SNMP (Simple Network Management Protocol), 15**
- spammers, 268**
- Spanning Tree Protocol. *See* STP**
- spanning-tree mode rapid-pvst, 84**
- spanning-tree portfast default, 84**
- speed mismatches, switches, 66-67**
- split horizons, preventing routing loops, 155**
- SSH, configuring access, 55-56**
- SSID (service set identifier), 261**
- standard ACLs, 280**
- standard numbered ACLs, configuring, 282**
 - deny a specific host, 283
 - deny a specific subnet, 283-284
 - deny Telnet access to routers, 284
 - permit specific network, 282-283
- star topology, Frame Relay, 340**
- stateless autoconfiguration, IPv6, 142**
- statements**
 - deny any, 279
 - network, 247
- static addresses, 123**
- static NAT, 299-301**
- static routes**
 - configuring, 191-192
 - default static routes, 194-197*
 - with exit interface parameter, 193-194*
 - with "Next Hop" parameter, 193*

static routing, dynamic routing
versus, 149

store-and-forward switching, 46

storing configuration files, Cisco IOS, 51

STP (Spanning Tree Protocol), 79-80

broadcast storms, 78

configuring, 82, 358, 370-371

BID (bridge ID), 82-84

PortFast, 84

MAC database instability, 79

multiple frame transmission, 79

port roles, 81

troubleshooting, 84

straight-through cables, 6, 165

structured threats, 271

Structured Wireless-Aware Network (SWAN), 257

subconfiguration modes, Cisco IOS, 50

subnet addresses, summarizing, 118-119

subnet masks, IPv4 addresses, 111-112

subnet multipliers, 114

subnets, subnetting, 114

subnetting, 112-113

determining how many bits to borrow, 113

determining net subnet masks, 114

determining subnet multipliers, 114

examples, 114-116

listing subnets, host ranges and broadcast addresses, 114

VLSM. *See* VLSM

subset advertisement, VTP, 78

successor, EIGRP, 223

summarization

automatic summarization

EIGRP, 217

RIPv1, 204-205

manual summarization, EIGRP, 217-218

summary advertisement, VTP, 78

SVC (switched virtual circuit)

Frame Relay, 338

WAN, 313

SWAN (Structured Wireless-Aware Network), 257

switch configuration commands, 53-54

switch forwarding methods

based on MAC addresses, 45

frame forwarding, 45

switched virtual circuit (SVC), Frame Relay, 338

switches, 3, 37-38

access layer switches, 4

broadcast domains, 45

collision domains, 45

core layer switches, 4

distribution layer switches, 4

duplex and speed mismatches, 66-67

frame forwarding, 45-46

LAN switches, 45, 65-66

layer 1 problems on up interfaces, 67

VTP, 102

WAN switches, 310

switching

evolution to, 43-44

logical switching, 44-45

WAN, 312-313

switching function, packet forwarding, 148-149

switchport mode access, 103

switchport mode dynamic desirable command, 75

switchport mode trunk, 75

switchport mode trunk dynamic auto command, 75

switchport nonegotiate, 75, 103

switchport port-security violation command, 56

symmetric switching, 46

SYN flood attacks, 272

T

TCP (Transmission Control Protocol), 15

TCP header, 22

TCP/IP

application layer, 21

data encapsulation, 28

Internet layer, 26

layers, troubleshooting with, 29

network access layer, 27-28

transport layer, 21

connection establishment and termination, 25

error recovery, 24

flow control, 25

port numbers, 23

TCP header, 22

UDP, 26

TCP/IP models, 13-16

TCP/IP protocols, 15-16

TCP/IP stacks, testing on Windows PC, 63

Telecommunications Industry Association (TIA), 36

Telnet, 15, 176

telnet command, 11

Temporal Key Integrity Protocol (TKIP), 264

Teredo tunneling, IPv6, 143

termination, TCP/IP, 25

testing

- connectivity
 - to default gateways on Windows PC, 63*
 - to destinations on Windows PC, 64*
- TCP/IP stacks on Windows PC, 63

TFTP servers, recovering IOS images, 186-187

ftpdnld command, 187

threat control, 274

threats

- to networks, 271-272
- to physical infrastructures, 271
- vulnerabilities, 270

TIA (Telecommunications Industry Association), 36

TKIP (Temporal Key Integrity Protocol), 264

tools for troubleshooting, CDP, 68-69

top-level domains, 126

topologies, 8, 339

traceroute, 133-134, 175, 246

tracert, 132-134

tracing routes from Windows PC, 65

traffic types, VLANs, 72

transitioning to IPv6, 142-143

Transmission Control Protocol (TCP), 15

transport layer (TCP/IP), 21-22

- connection establishment and termination, 25
- error recovery, 24
- flow control, 25
- port numbers, 23
- TCP header, 22
- UDP, 26

Triple DES (3DES), 323

Trojan horses, 272

troubleshooting

- ACLs, 291
 - denied protocols, 292-293*
 - host has no connectivity, 291-292*
 - Telnet is allowed #1, 293*
 - Telnet is allowed #2, 294*
 - Telnet is allowed #3, 294-295*
- EIGRP, 248
- inter-VLAN routing, 105
- with layers, 29
- methodology, 61-62
- NAT, 304-305
- neighbor adjacency issues, 248-250
- OSPF, 239-240, 248
- RIP, 247-248
- RIPv2, 208-209
- routing, 245
- STP, 84
- tools, CDP, 68-69
- trunking, 93-94
- VLAN, 93-94
- VLSM, 246
- VTP, 102-103
- WAN implementations, 349
 - Layer 1 problems, 350*
 - Layer 2 problems, 350-351*
 - Layer 3 problems, 351-352*
- WLAN, 264

trunking

- configuring, 91-93
- troubleshooting, 93-94
- verifying, 91-93

trunking VLANs, 74-75

trust exploitation, 272

tunneling, 322. *See also* encapsulation

- IPv6, 143
- Teredo tunneling, IPv6, 143
- VPNs, 323

U

UDP (User Datagram Protocol), 15

- TCP/IP, 26

undebug all, 248

unshielded twisted-pair (UTP), 164

unstructured threats, 271

up interfaces, layer 1 problems, 67

update packets, EIGRP, 213

URL prefixes for specifying file locations, IFS, 181

usage of networks, network-based applications, 17

User Datagram Protocol (UDP), 15

user EXEC mode, 47

username command, 335

UTP (unshielded twisted-pair), 164

UTP cabling, 36-37

V

V.35, 311

variable-length subnet masking. *See* VLSM

VC (virtual circuit), Frame Relay, 338

verifying

ACLs, 289-290

BID, 82-84

DHCP operations, 130

EIGRP

show ip eigrp neighbors, 222-224

show ip protocols, 221

Frame Relay, 343, 348

HDLC, 331

inter-VLAN routing configurations, 105

NAT, 303-304

network connectivity, 62-65

OSPF, 240-243

RIPv1, 199-202

RIPv2, 208-209

speed and duplex settings, 66-67

trunking, 91-93

VLAN, 88-91

VTP, 99-100

synchronized databases, 101-102

VLAN configurations on VTP servers, 100-101

verifying network connectivity, 175-176

video, impact on network-based applications, 18

virtual circuit (VC), Frame Relay, 338

virtual private networks. *See* VPNs

viruses, 272

VLAN configurations and port mappings, 355

VLAN tag fields, 74

VLAN Trunking Protocol. *See* VTP

VLANs (virtual local-area networks)

assigning, 358, 369-370

to interfaces, 89

benefits of, 71-72

black hole VLAN, 73

configuring, 88-91, 357, 367-369

creating, 88

data VLAN, 72

default VLAN, 72

DTP (Dynamic Trunking Protocol), 75

management VLAN, 73

native VLAN, 73

overview, 71

traffic types, 72

troubleshooting, 93-94

trunking VLANs, 74-75

verification commands, 88-91

voice VLAN, 73-74

VLSM (variable-length subnet masking), 116-118, 246

troubleshooting, 246

voice, impact on network-based applications, 18

voice VLAN, 73-74

VoIP (voice over IP), 18

VPNs (virtual private networks), 320

benefits of, 320

components of, 322

establishing connections, 322

authentication, 325

encryption algorithms, 323

hashes, 324-325

IPsec Security Protocols, 325

tunneling, 323

types of access, 320

remote-access VPNs, 321

site-to-site VPNs, 320

VTP (VLAN Trunking Protocol), 76-77, 97

advertisement request message, 78

configuring, 97-100

modes, 77

pruning, 78

subset advertisement, 78

summary advertisement, 78

switches, 102

troubleshooting, 102-103

verifying, 99

synchronized databases, 101-102

VLAN on VTP servers, 100-101

VTP operation, 77-78

vtp pruning, 98

vtp version 2, 98

vulnerabilities, 270

W

WAN

components of, 309

connections, 165

circuit-switched connections, 314-316

dedicated connections, 314

Internet connections, 317-319

packet-switched connections, 315-317

WAN link options, 319-320

data-link protocols, 312

devices, 310

physical layer standards, 311

PVC, 313

SVC, 313

switching, 312-313

WAN implementations,

troubleshooting, 349

Layer 1 problems, 350

Layer 2 problems, 350-351

Layer 3 problems, 351-352

WAN link options, 319-320

WAN switches, 310

WANs (wide-area networks), 7

war drivers, wireless security risks, 257

WEP (Wired Equivalent Privacy), 258, 261

white hats, 267

Wi-Fi Alliance, 253

Wi-Fi Protected Access (WPA), 258, 261

WiMAX (Worldwide Interoperability for Microwave Access), 319

windowing, 25

Windows PC

configuring to use DHCP, 123

testing

connectivity to default gateways, 63

connectivity to destinations, 64

TCP/IP stacks, 63

tracing routes, 65

Wired Equivalent Privacy (WEP), 258, 261

wireless access points, 261

wireless coverage areas, 256

wireless encoding channels, 255

wireless frequencies, 254

wireless LAN. See WLAN

wireless modes of operation, 254

wireless security risks, 257

wireless security standards, 258

wireless standards, 253

WLAN

implementing, 261

checklist for, 262-264

modes of operation, 254

speed and frequency reference, 256

standards for, 254

troubleshooting, 264

word help, 48

Worldwide Interoperability for Microwave Access (WiMAX), 319

worms, 272

WPA (Wi-Fi Protected Access), 258, 261

write erase command, 51

X-Y-Z

X.21, 311

X.25, packet-switched connections (WAN), 315

Xmodem, recovering IOS images, 187-188

xmodem command, 187