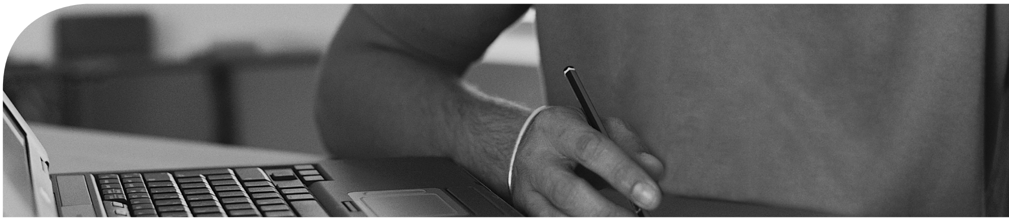


31 Days Before Your
CCNA Routing & Switching Exam

A Day-By-Day Review Guide for the ICND1/CCENT (100-105), ICND2 (200-105), and CCNA (200-125) Certification Exam

Allan Johnson

Cisco Press • 800 East 96th Street • Indianapolis, Indiana 46240 USA

31 Days Before Your CCNA Routing & Switching Exam

Allan Johnson

Copyright © 2017 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

First Printing March 2017

Library of Congress Control Number: 2017932351

ISBN-13: 978-1-58720-590-3

ISBN-10: 1-58720-590-4

Warning and Disclaimer

This book is designed to provide information about exam topics for the Cisco Certified Networking Associate (CCNA) Certification. 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.

Special Sales

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

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

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

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.

Editor-in-Chief	MarkTaub
Alliances Manager, Cisco Press	Ron Fligge
Executive Editor	Mary Beth Ray
Managing Editor	Sandra Schroeder
Development Editor	Ellie Bru
Senior Project Editor	Tonya Simpson
Copy Editor	Krista Hansing Editorial Services, Inc.
Technical Editor(s)	Rick McDonald
Editorial Assistant	Vanessa Evans
Cover Designer	Ockomon Haus
Composition	CodeMantra
Indexer	Erika Millen
Proofreader	Larry Sulky

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.**

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; 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, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, 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. (0812R)

About the Author

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

About the Technical Reviewer

Rick McDonald teaches computer and networking courses via distance from the University of Alaska–Fairbanks campus, where he is a Professor of Information Systems. He holds a BA in English and an M.Ed. in Educational Technology from Gonzaga University in Spokane, Washington. His current academic focus is developing methods for delivering hands-on training in Alaska using web-based teaching tools.

Dedications

For my wife, Becky. Thank you for all your support during this crazy whirlwind of a year. You are the stabilizing force that keeps me grounded.

Acknowledgments

As a technical author, I rely heavily on my technical editor; Rick McDonald had my back for this work. Thankfully, when Mary Beth Ray contacted him, he was willing and able to do the arduous review work necessary to make sure that you get a book that is both technically accurate and unambiguous.

Wendell Odom's *Cisco CCNA Routing and Switching 200-125 Official Cert Guide and Network Simulator Library* was one of my main sources. These two books and the accompanying simulator activities have the breadth and depth needed to master the CCNA exam topics.

The Cisco Network Academy authors for the online curriculum and series of Companion Guides take the reader deeper, past the CCNA exam topics, with the ultimate goal of preparing the student not only for CCNA certification, but for more advanced college-level technology courses and degrees as well. Thank you especially to Rick Graziani, Bob Vachon, Dan Alberghetti, Cheryl Schmidt, Rodrigo Floriano, Suk-Yi Pennock, Dave Holzinger, Jane Gibbons, Allan Reid, Jane Brooke, Martin Benson, and the rest of the ACE team. Their excellent treatment of the material is reflected throughout this book.

Mary Beth Ray, executive editor, amazes me with her ability to juggle multiple projects simultaneously, 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.

Thank you to the professional and thorough review of this work by development editor Ellie Bru, project editor Tonya Simpson, and copy editor Krista Hansing. Their combined efforts ensure that what I authored is ready for publication.

And to the rest of the Pearson family who contributes in countless ways to bring a book to the reader, thank you for all your hard work.

Contents at a Glance

Introduction xxviii

Digital Study Guide xxxiii

Day 31: Networking Models, Devices, and Components 1

Day 30: Ethernet Switching 27

Day 29: Switch Configuration Basics 41

Day 28: VLAN and Trunking Concepts and Configurations 57

Day 27: IPv4 Addressing 77

Day 26: IPv6 Addressing 89

Day 25: Basic Routing Concepts 107

Day 24: Basic Router Configuration 121

Day 23: Static and Default Route Configuration 139

Day 22: RIPv2 Implementation 155

Day 21: VTP and Inter-VLAN Routing Configuration 169

Day 20: OSPF Operation 185

Day 19: Single-Area OSPF Implementation 197

Day 18: Multiarea OSPF Implementation 215

Day 17: Fine-Tuning and Troubleshooting OSPF 225

Day 16: EIGRP Operation 239

Day 15: EIGRP Implementation 249

Day 14: Fine-Tuning and Troubleshooting EIGRP 263

Day 13: CDP and LLDP 273

Day 12: LAN Security and Device Hardening 285

Day 11: STP 297

Day 10: EtherChannel and HSRP 313

Day 9: ACL Concepts 329

Day 8: ACL Implementation 335

Day 7: DHCP and DNS 351

Day 6: NAT 369

Day 5: WAN Overview 381

Day 4: WAN Implementation 393

Day 3: QoS, Cloud, and SDN 409

Day 2: Device Monitoring, Management, and Maintenance 427

Day 1: Troubleshooting Methodologies and Tools 451

Exam Day 465

Post-Exam Information 467

Index 469

Contents

Introduction xxviii

Digital Study Guide xxxiii

Day 31: Networking Models, Devices, and Components 1

CCNA 200-125 Exam Topics 1

Key Points 1

The OSI and TCP/IP Models 1
OSI Layers 2
TCP/IP Layers and Protocols 3
Protocol Data Units and Encapsulation 4

The TCP/IP Application Layer 5

The TCP/IP Transport Layer 5
TCP Header 6
Port Numbers 7
Error Recovery 7
Flow Control 8
Connection Establishment and Termination 9
UDP 10

The TCP/IP Internet Layer 10

The TCP/IP Network Access Layer 11

Data Encapsulation Summary 12

Devices 13
Switches 13
Access Layer Switches 14
Distribution Layer Switches 14
Core Layer Switches 14
Routers 15
Specialty Devices 15
Firewalls 16
IDS and IPS 16
Access Points and Wireless LAN Controllers 17

Physical Layer 19
Network Media Forms and Standards 19

LAN Device Connection Guidelines 21

LANs and WANs 22

Networking Icons 23

Physical and Logical Topologies 23

Hierarchical Campus Designs 24

Study Resources 26

Day 30: Ethernet Switching 27

CCNA 200-125 Exam Topics 27

Key Topics 27

Evolution to Switching 27

Switching Logic 28

Collision and Broadcast Domains 29

Frame Forwarding 29

Switch Forwarding Methods 29

Symmetric and Asymmetric Switching 30

Memory Buffering 30

Layer 2 and Layer 3 Switching 30

Ethernet Overview 30

Legacy Ethernet Technologies 31

CSMA/CD 32

Legacy Ethernet Summary 33

Current Ethernet Technologies 33

UTP Cabling 34

Benefits of Using Switches 35

Ethernet Addressing 36

Ethernet Framing 37

The Role of the Physical Layer 38

Study Resources 39

Day 29: Switch Configuration Basics 41

CCENT 100-101 ICND1 Exam Topics 41

Key Topics 41

Accessing and Navigating the Cisco IOS 41

Connecting to Cisco Devices 41

CLI EXEC Sessions 42

Using the Help Facility 42

CLI Navigation and Editing Shortcuts 43

Command History 44

IOS Examination Commands 44

Subconfiguration Modes 45

Basic Switch Configuration Commands 46

Half-Duplex, Full-Duplex, and Port Speed 47

Automatic Medium-Dependent Interface Crossover (auto-MDIX) 48

Verifying Network Connectivity 48

Troubleshoot Interface and Cable Issues 51

Media Issues 51

Interface Status and the Switch Configuration 52

Interface Status Codes 52

Duplex and Speed Mismatches 52

Common Layer 1 Problems On "Up" Interfaces 54

Study Resources 54

Day 28: VLAN and Trunking Concepts and Configurations 57

CCENT 100-101 ICND1 Exam Topics 57

Key Points 57

VLAN Concepts 57

Traffic Types 58

Types of VLANs 59

Voice VLAN Example 59

Trunking VLANs 60

Dynamic Trunking Protocol 61

VLAN Configuration and Verification 62

Extended VLANs 66

Trunking Configuration and Verification 68

VLAN Troubleshooting 71

Disabled VLANs 72

Trunking Troubleshooting 73

Check Both Ends of a Trunk 73

Check Trunking Operational States 74

Study Resources 75

Day 27: IPv4 Addressing 77

CCENT 100-101 ICND1 Exam Topics 77

Key Topics 77

IPv4 Addressing 77

Header Format 78

Classes of Addresses 78

Purpose of the Subnet Mask 80

Private and Public IP Addressing 81

Subnetting in Four Steps 81
- Determine How Many Bits to Borrow 81
- Determine the New Subnet Mask 82
- Determine the Subnet Multiplier 83
- List the Subnets, Host Ranges, and Broadcast Addresses 83
- Subnetting Example 1 83
- Subnetting Example 2 84
- Subnetting Example 3 84

VLSM 85

Study Resources 87

Day 26: IPv6 Addressing 89

CCNA 200-125 Exam Topics 89

Key Topics 89

Overview and Benefits of IPv6 89

The IPv6 Protocol 90

IPv6 Address Types 91
- Unicast 92
  - Global Unicast Address 92
  - Link-Local Address 95
  - Loopback Address 96
  - Unspecified Address 96
  - Unique Local Address 96
  - IPv4 Embedded Address 97
- Multicast 98
  - Assigned Multicast 98
  - Solicited-Node Multicast 98
- Anycast 100

Representing the IPv6 Address 100
- Conventions for Writing IPv6 Addresses 100
- Conventions for Writing IPv6 Prefixes 101

IPv6 Subnetting 102
- Subnetting the Subnet ID 103
- Subnetting into the Interface ID 103

EUI-64 Concept 103

Stateless Address Autoconfiguration 104

Migration to IPv6 105

Study Resources 106

Day 25: Basic Routing Concepts 107

CCNA 200-125 Exam Topics 107

Key Topics 107

Packet Forwarding 107

Path Determination and Switching Function Example 108

Routing Methods 109

Classifying Dynamic Routing Protocols 110

IGP and EGP 110

Distance Vector Routing Protocols 111

Link-State Routing Protocols 111

Classful Routing Protocols 112

Classless Routing Protocols 112

Dynamic Routing Metrics 112

Administrative Distance 113

IGP Comparison Summary 115

Routing Loop Prevention 115

Link-State Routing Protocol Features 116

Building the LSDB 116

Calculating the Dijkstra Algorithm 117

Convergence with Link-State Protocols 118

Study Resources 119

Day 24: Basic Router Configuration 121

CCNA 200-125 Exam Topics 121

Key Topic 121

Basic Router Configuration with IPv4 121

Command Syntax 122

Configuration Example 122

Verification Example 124

Basic Router Configuration with IPv6 130

Command Syntax 130

Configuration Example 130

Verifying IPv4 and IPv6 Network Connectivity 133

Basic IP Addressing Troubleshooting 136

Default Gateway 136

Duplicate IP Addresses 136

Study Resources 137

Day 23: Static and Default Route Configuration 139

CCNA 200-125 Exam Topics 139

Key Topics 139

Static and Default Routing Overview 139

IPv4 Static Route Configuration 140
- IPv4 Static Routes Using the Next-Hop Parameter 142
- IPv4 Static Routes Using the Exit Interface Parameter 143
- IPv4 Default Route Configuration 144
- IPv4 Summary Static Route Configuration 147
- IPv6 Static Routing 148
- IPv6 Static Route Configuration 149
- IPv6 Default Route Configuration 150
- IPv6 Summary Static Route Configuration 151

Study Resources 152

Day 22: RIPv2 Implementation 155

CCNA 200-125 Exam Topics 155

Key Topic 155

RIP Concepts 155
- RIPv1 Message Format 155
- RIPv1 Operation 156

RIPv1 Configuration 156
- RIPv1 Verification and Troubleshooting 158
- Passive Interfaces 161
- Automatic Summarization 162
- Default Routing and RIPv1 164

RIPv2 Configuration 165
- Disabling Autosummarization 167
- RIPv2 Verification and Troubleshooting 167

Study Resources 168

Day 21: VTP and Inter-VLAN Routing Configuration 169

CCNA 200-125 Exam Topics 169

Key Topics 169

VTP Concepts 169

VTP Configuration and Verification 171

Inter-VLAN Routing Concepts 175
- Legacy Inter-VLAN Routing 175

Router on a Stick 176
Multilayer Switch 177

Router on a Stick Configuration and Verification 177

Multilayer Switch Inter-VLAN Routing Configuration and Verification 180
Creating Additional SVIs 180
Configuring a Layer 3 Routed Port 182

Study Resources 182

Day 20: OSPF Operation 185

CCNA 200-125 Exam Topics 185

Key Topics 185

Single-Area OSPF Operation 185
OSPF Message Format 185
OSPF Packet Types 186
Neighbor Establishment 186
Link-State Advertisements 188
OSPF DR and BDR 189
OSPF Algorithm 189
Link-State Routing Process 190

OSPFv2 Versus OSPFv3 191
Similarities Between OSPFv2 and OSPFv3 191
Differences Between OSPFv2 and OSPFv3 192

Multiarea OSPF Operation 192
Multiarea OSPF Design 192
Multiarea OSPF Improves Performance 194

Study Resources 194

Day 19: Single-Area OSPF Implementation 197

CCNA 200-125 Exam Topics 197

Key Topics 197

Single-Area OSPFv2 Configuration 197
The router ospf Command 198
Router ID 198
The network Command 199
Passive Interfaces 200
Modifying the OSPF Metric 200

Verifying OSPFv2 203

Single-Area OSPFv3 Configuration 206

The Router ID in OSPFv3 208

Verifying OSPFv3 209

Study Resources 212

Day 18: Multiarea OSPF Implementation 215

CCNA 200-125 Exam Topics 215

Key Topics 215

Multiarea OSPFv2 Implementation 215

Multiarea OSPFv3 Implementation 218

Study Resources 223

Day 17: Fine-Tuning and Troubleshooting OSPF 225

CCNA 200-125 Exam Topics 225

Key Topics 225

OSPFv2 Configuration Example 225

Modifying OSPFv2 227

Redistributing a Default Route 227

Modifying Hello and Dead Intervals 228

OSPF Network Types 228

DR/BDR Election 229

Controlling the DR/BDR Election 229

OSPFv3 Configuration Example 231

Modifying OSPFv3 233

Propagating a Default Route 233

Modifying the Timers 234

Troubleshooting OSPF 235

OSPF States 235

OSPF Adjacency 236

OSPF Troubleshooting Commands 236

Study Resources 238

Day 16: EIGRP Operation 239

CCNA 200-125 Exam Topics 239

Key Topics 239

EIGRP Overview 239

EIGRP Characteristics 240

PDMs 240

RTP 240

EIGRP Packet Types 241
EIGRP Message Format 241

EIGRP Processes 243
EIGRP Convergence 243
EIGRP Composite Metric 244
Administrative Distance 244
DUAL 245
DUAL Concepts 245
DUAL FSM 246

Study Resources 247

Day 15: EIGRP Implementation 249

CCNA 200-125 Exam Topics 249

Key Topics 249

EIGRP for IPv4 Configuration 249
EIGRP Topology and Addressing Scheme 249
The network Command 250
The Router ID 250

EIGRP for IPv4 Verification 251
Examining the Protocol Details 251
Examining Neighbor Tables 252
Examining the Topology Tables 253
Examining the Routing Table 255

EIGRP for IPv6 Concepts 255

EIGRP for IPv6 Configuration 256

EIGRP for IPv6 Verification 258
Examining the Protocol Details 258
Examining the Neighbor Table 259
Examining the Routing Table 260

Study Resources 261

Day 14: Fine-Tuning and Troubleshooting EIGRP 263

CCNA 200-125 Exam Topics 263

Key Topics 263

Modifying the EIGRP for IPv4 Configuration 263
Automatic Summarization 263
EIGRP for IPv4 Topology 264
Propagating an IPv4 Default Route 265
Modifying the EIGRP Metric 266
Modifying Hello Intervals and Hold Times 266

Modifying EIGRP for IPv6 267

EIGRP for IPv6 Topology 267

Propagating an IPv6 Default Route 267

Modifying Bandwidth Utilization 268

Modifying Hello Intervals and Hold Times 269

EIGRP Troubleshooting Commands 269

Discontiguous Networks 270

Study Resources 271

Day 13: CDP and LLDP 273

CCNA 200-125 Exam Topics 273

Key Topics 273

CDP Overview 273

CDP Configuration 274

CDP Verification 277

LLDP Overview 279

LLDP Configuration 280

LLDP Verification 281

Study Resources 283

Day 12: LAN Security and Device Hardening 285

CCNA 200-125 Exam Topics 285

Key Topics 285

Port Security Configuration 285

Port Restoration After a Violation 288

LAN Threat Mitigation 289

DHCP Snooping 289

Native and Management VLAN Modification 290

Switch Port Hardening 291

AAA 292

802.1X 293

SSH Configuration 294

Study Resources 296

Day 11: STP 297

CCNA 200-125 Exam Topics 297

Key Topics 297

STP Concepts and Operation 297

STP Algorithm 298

STP Convergence 299

STP Varieties 300

PVST Operation 301
- Port States 302
- Extended System ID 303

Rapid PVST+ Operation 303
- RSTP Interface Behavior 304
- RSTP Port Roles 305
- Edge Ports 305

Configuring and Verifying Varieties of STP 306
- STP Configuration Overview 306
- Configuring and Verifying the BID 307
- Configuring PortFast and BPDU Guard 309
- Configuring Rapid PVST+ 309
- Verifying STP 310

Switch Stacking 310

Study Resources 312

Day 10: EtherChannel and HSRP 313

CCNA 200-125 Exam Topics 313

Key Topics 313

EtherChannel Operation 313
- Benefits of EtherChannel 314
- Implementation Restrictions 314

EtherChannel Protocols 315
- Port Aggregation Protocol 315
- Link Aggregation Control Protocol 315

Configuring EtherChannel 316

Verifying EtherChannel 317

Troubleshooting EtherChannel 319

First-Hop Redundancy Concepts 319

FHRPs 320

HSRP Operation 321
- HSRP Versions 321
- HSRP Priority and Preemption 322

HSRP Configuration and Verification 322

HSRP Load Balancing 323

Troubleshooting HSRP 326

Study Resources 326

Day 9: ACL Concepts 329

CCNA 200-125 Exam Topics 329

Key Topics 329

ACL Operation 329
Defining an ACL 329
Processing Interface ACLs 329
List Logic with IP ACLs 330

Planning to Use ACLs 331
Types of ACLs 332
ACL Identification 333
ACL Design Guidelines 333

Study Resources 334

Day 8: ACL Implementation 335

CCNA 200-125 Exam Topics 335

Key Topics 335

Configuring Standard Numbered IPv4 ACLs 335
Standard Numbered IPv4 ACL: Permit Specific Network 335
Standard Numbered IPv4 ACL: Deny a Specific Host 336
Standard Numbered IPv4 ACL: Deny a Specific Subnet 337
Standard Numbered IPv4 ACL: Deny Telnet or SSH Access to the Router 337

Configuring Extended Numbered IPv4 ACLs 337
Extended Numbered IPv4 ACL: Deny FTP from Subnets 338
Extended Numbered IPv4 ACL: Deny Only Telnet from Subnet 338

Configuring Named IPv4 ACLs 339
Standard Named IPv4 ACL Steps and Syntax 339
Standard Named IPv4 ACL: Deny a Single Host from a Given Subnet 340
Extended Named IPv4 ACL Steps and Syntax 340
Adding Comments to Named or Numbered IPv4 ACLs 340

Verifying IPv4 ACLs 341

Comparing IPv4 and IPv6 ACLs 343

Configuring IPv6 ACLs 343

Step 1: Name the IPv6 ACL 344

Step 2: Create the IPv6 ACL 344

Step 3: Apply the IPv6 ACL 344

Standard IPv6 ACL: Allow SSH Remote Access 344

Extended IPv6 ACL: Allow Only Web Traffic 345

Verifying IPv6 ACLs 346

Troubleshooting ACLs 348

Study Resources 349

Day 7: DHCP and DNS 351

CCNA 200-125 Exam Topics 351

Key Topics 351

DHCPv4 351

DHCPv4 Configuration Options 352

Configuring a Router as a DHCPv4 Server 352

Configuring a Router to Relay DHCPv4 Requests 356

Configuring a Router as a DHCPv4 Client 357

DHCPv6 358

SLAAC 358

Stateless DHCPv6 360

Stateful DHCPv6 360

Stateless and Stateful DHCPv6 Operation 360

DHCPv6 Configuration Options 361

Configuring a Router as a Stateless DHCPv6 Server 361

Configuring a Router as a Stateful DHCPv6 Server 363

DHCP Troubleshooting 363

Resolve IPv4 Address Conflicts 363

Test Connectivity Using a Static IP Address 364

Verify Switch Port Configuration 364

Test DHCPv4 Operation on the Same Subnet or VLAN 364

DNS Operation 364

Troubleshooting DNS 366

Study Resources 367

Day 6: NAT 369

CCNA 200-125 Exam Topics 369

Key Topics 369

NAT Concepts 369
A NAT Example 371
Dynamic and Static NAT 372
NAT Overload 372
NAT Benefits 373
NAT Limitations 373

Configuring Static NAT 374
Configuring Dynamic NAT 375
Configuring NAT Overload 376

Verifying NAT 377

Troubleshooting NAT 378

NAT for IPv6 379
IPv6 Private Address Space 379
Purpose of NAT for IPv6 379

Study Resources 380

Day 5: WAN Overview 381

CCNA 200-125 Exam Topics 381

Key Topics 381

WAN Topologies 381

WAN Connection Options 382
Dedicated Connection Options 383
Circuit-Switched Connection Options 384
Packet-Switched Connection Options 385
Metro Ethernet 385
MPLS 386
Internet Connection Options 386
DSL 386
Cable Modem 387
Wireless 388
Choosing a WAN Link Option 388

VPN Technology 389
VPN Benefits 389
Types of VPN Access 389

Study Resources 391

Day 4: WAN Implementation 393

CCNA 200-125 Exam Topics 393

Key Topics 393

PPP Concepts 393

The PPP Frame Format 393

PPP Link Control Protocol (LCP) 394

Looped-Link Detection 394

Enhanced Error Detection 395

PPP Multilink 395

PPP Authentication 395

PPP Configuration and Verification 396

Basic PPP 396

CHAP 397

PAP 398

PPP Troubleshooting 398

PPPoE Concepts 399

PPPoE Configuration 399

PPPoE Configuration Example 400

PPPoE Troubleshooting 400

GRE Tunneling 401

GRE Characteristics 401

GRE Configuration and Verification 401

GRE Troubleshooting 403

BGP Concepts 403

eBGP Configuration and Verification 404

Study Resources 407

Day 3: QoS, Cloud, and SDN 409

CCNA 200-125 Exam Topics 409

Key Topics 409

QoS 409

Classification and Marking 410

DSCP and IPP 411

EF and AF 412

Congestion Management 413

Policing, Shaping, and TCP Discards 413

QoS and TCP 415

Cloud Computing 416

Server Virtualization 416

Cloud Computing Services 418

Virtual Network Infrastructure 419

Software-Defined Networking 419
Data, Control, and Management Planes 419
Controllers 421
SDN Examples 421
Open SDN and OpenFlow 421
The Cisco Application Centric Infrastructure 422
The Cisco APIC Enterprise Module (APIC-EM) 423
APIC-EM and ACLs 424
Study Resources 426

Day 2: Device Monitoring, Management, and Maintenance 427

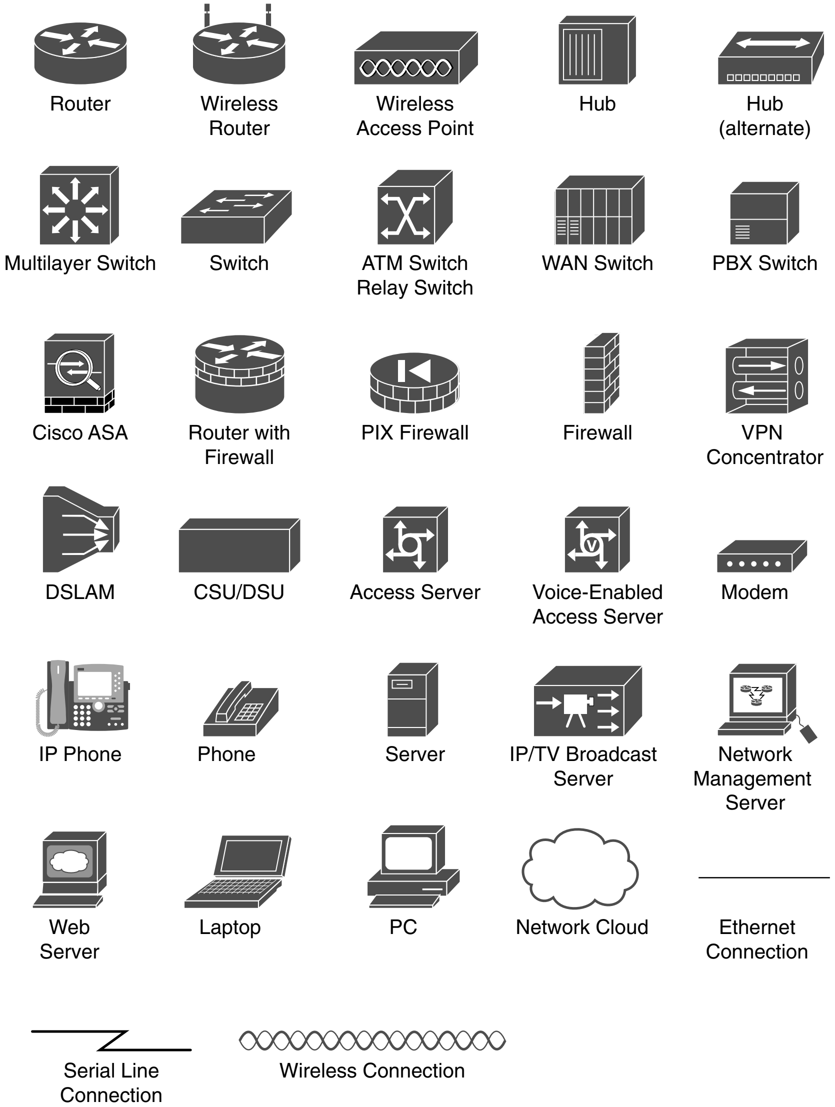
CCNA 200-125 Exam Topics 427
Key Topics 427
SNMP Operation 427
SNMP Components 427
SNMP Messages 427
SNMP Versions 428
The Management Information Base 428
Configuring SNMP 430
Verifying SNMP 430
Syslog 432
Syslog Operation 432
Syslog Configuration and Verification 434
Network Time Protocol 436
Cisco IOS File System and Devices 437
IFS Commands 437
URL Prefixes for Specifying File Locations 440
Commands for Managing Configuration Files 440
Manage Cisco IOS Images 442
Backing Up a Cisco IOS Image 442
Restoring a Cisco IOS Image 443
Managing Cisco IOS Licenses 444
Password Recovery 448
Study Resources 449

Day 1: Troubleshooting Methodologies and Tools 451

CCNA 200-125 Exam Topics 451
Key Topics 451

Troubleshooting Documentation 451
Configuration Files 451
Topology Diagrams 452
Baseline Date 453
Troubleshooting Methods 454
Troubleshooting at Each Layer 455
Physical Layer 455
Data Link Layer 456
Network Layer 456
Transport Layer 457
Application Layer 458
Bottom-Up Method and the Layers 459
Troubleshooting with IP Service Level Agreement 459
Study Resources 462
Exam Day 465
What You Need for the Exam 465
What You Should Receive After Completion 465
Summary 465
Post-Exam Information 467
Receiving Your Certificate 467
Determining Career Options 467
Examining Certification Options 468
If You Failed the Exam 468
Summary 468
Index 469

Icons Used in This Book



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.

Reader Services

Register your copy at www.ciscopress.com/title/9781587205903 for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account*. Enter the product ISBN 9781587205903 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

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

Introduction

If you're reading this introduction, you've probably already spent a considerable amount of time and energy pursuing your CCNA certification. You're taking one of two paths. Either you are planning on taking the two exams, Interconnecting Cisco Network Devices, Part 1 (ICND1 100-105) and ICND2 200-105, or you are planning on taking the full Cisco Certified Network Associate Exam (CCNA 200-125). Regardless of how you got to this point in your travels through your CCNA studies, *31 Days Before Your CCNA Routing & Switching 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 so, this book provides an excellent overview of the material you must now spend a great deal of time studying and practicing. But I must warn you: 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 your exam preparations. Therefore, let me spend some time discussing my recommendations for study resources.

Study Resources

Cisco Press and Pearson IT Certification offer an abundance of CCNA-related books to serve as your primary source for learning how to install, configure, operate, and troubleshoot small to medium-size routed and switched networks.

Safari Books Online

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

Primary Resources

First on the list must be Wendell Odom's *CCNA Routing and Switching 200-125 Official Cert Guide and Network Simulator Library* (ISBN: 9781587206108). If you do not buy any other books, buy this one. 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 DVD in the back of the book, plus the online resources, are worth the price of the book. There is no better resource on the market for a CCNA candidate.

If you are a Cisco Networking Academy student, you are blessed with access to the online version of the CCNA Routing and Switching curriculum and the wildly popular Packet Tracer network simulator. The Cisco Network Academy curriculum has four courses. To learn more about CCNA Routing and Switching courses and to find an Academy near you, visit http://www.netacad.com.

However, if you are not an Academy student but want to benefit from the extensive authoring done for these courses, you can buy any or all of CCNA Routing and Switching Companion Guides (CGs) and Labs & Study Guides (LSGs) of the Academy's popular online curriculum. Although you will not have access to the Packet Tracer files, 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 Routing and Switching CGs and LSGs follow:

- *Introduction to Networks v6 Companion Guide* (ISBN: 9781587133602)
- *Introduction to Networks v6 Labs & Study Guide* (ISBN: 9781587133619)
- *Routing and Switching Essentials v6 Companion Guide* (ISBN: 9781587134289)
- *Routing and Switching Essentials v6 Labs & Study Guide* (ISBN: 9781587134265)
- *Scaling Networks v6 Companion Guide* (ISBN: 9781587134340)
- *Scaling Networks v6 Labs & Study Guide* (ISBN: 9781587134333)
- *Connecting Networks v6 Companion Guide* (ISBN: 9781587134326)
- *Connecting Networks v6 Labs & Study Guide* (ISBN: 9781587134296)

You can find these books at http://www.ciscopress.com by clicking the Cisco Networking Academy link.

Supplemental Resources

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

First is Scott Empson's very popular *CCNA Routing and Switching Portable Command Guide* (ISBN: 9781587205880). This guide is much more than just a listing of commands and what they do. Yes, it summarizes all the CCNA certification-level IOS commands, keywords, command arguments, and associated prompts. But it also provides you with tips and examples of how to apply the commands to real-world scenarios. Configuration examples throughout the book provide you with a better understanding of how these commands are used in simple network designs.

Second, Kevin Wallace's *CCNA Routing and Switching 200-125 Premium Edition Complete Video Course* (ISBN: 9780134580708) is a comprehensive training course that brings Cisco CCNA exam topics to life through the use of real-world demonstrations, animations, live instruction, and configurations, making learning these foundational networking topics easy and fun. Kevin's engaging style and love for the technology is infectious. The course contains more than 25 hours of instruction in more than 300 videos. The course also includes excellent practice tests.

Third, Wendell Odom and Sean Wilkins have created more than 400 structured labs that are available in the *CCNA Routing and Switching 200-125 Network Simulator* (ISBN: 9780789757760). These simulations map precisely to chapters in Wendell's book, but they are also a great practice resource for anyone.

The Cisco Learning Network

Finally, if you have not done so already, you should register with The Cisco Learning Network at https://learningnetwork.cisco.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 can find many resources to help you prepare for your CCNA exam, in addition to 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? The answer to that question depends largely on 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 primary study resources and one of the supplemental resources (such as Wendell Odom's certification library and Scott Empson's command guide). 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 and use the following format:

- A title for the day that concisely states the overall topic
- A list of one or more CCNA 200-125 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 give you a quick reference for locating more in-depth treatment of the day's topics

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

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 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 200-125 exam. A secondary audience is anyone needing a refresher review of CCNA exam topics—possibly before attempting to recertify or sit for another certification for which the CCNA is a prerequisite.

Getting to Know the CCNA 200-125 Exam

For the current certifications (announced in May 2016), Cisco created the ICND1 (100-105) and ICND2 (200-105) exams, along with the CCNA (200-125) exam. To become CCENT certified, you need to pass just the ICND1 exam. To become CCNA Routing and Switching certified, you must pass both the ICND1 and ICND2 exams, or just the CCNA exam. The CCNA exam simply covers all the topics on the ICND1 and ICND2 exams, giving you two options for gaining your CCNA Routing and Switching 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 on the entire list of topics published for the CCNA 200-125 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 appears 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 simply requires that you point and click a circle or check box next to the correct answer(s). 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 usually 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—usually 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, which simulates a graphical interface such as that found on a Linksys router or the Cisco Security Device Manager.

What Topics Are Covered on the CCNA Exam

Table I-1 summarizes the seven domains of the CCNA 200-125 exam:

Table I-1 CCNA 200-125 Exam Domains and Weightings

Domain	% of Examination
1.0 Network Fundamentals	15%
2.0 LAN Switching Technologies	21%
3.0 Routing Technologies	23%
4.0 WAN Technologies	10%
5.0 Infrastructure Services	10%
6.0 Infrastructure Security	11%
7.0 Infrastructure Management	10%

Although Cisco outlines general exam topics, not all topics might appear on the CCNA exam; likewise, topics that are not specifically listed might appear on the exam. The exam topics that Cisco provides and this book covers are a general framework for exam preparation. Be sure to check Cisco's website for the latest exam topics.

Registering for the CCNA 200-125 Exam

If you are starting your *31 Days Before Your CCNA Routing & Switching Exam* today, register for the exam right now. In my testing experience, there is no better motivator than a scheduled test date staring me in the face. I'm willing to bet the same holds true 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, gather the following information in Table I-1 and register right now!

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

You can schedule your exam at any time by visiting www.pearsonvue.com/cisco/. I recommend that you schedule it for 31 days from now. The process and available test times 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*.

Digital Study Guide

Cisco Press offers this book in an online digital format that includes enhancements such as interactive activities and Check Your Understanding questions, plus Packet Tracer activities and a full-length exam.

> *31 Days Before Your CCNA Routing & Switching Exam Digital Study Guide* is available for a discount for anyone who purchases this book. Details about redeeming this offer are found in the back of the book.

- **Read** the complete text of the book on any web browser that supports HTML5, including mobile.
- **Reinforce** key concepts with more than 31 dynamic and interactive hands-on exercises, and see the results with the click of a button. Also included are more than 25 Packet Tracer activities.
- **Test** your understanding of the material at the end of each day with more than 300 fully interactive online quiz questions. You also get a full-length final quiz of 60 questions that mimic the type of questions you will see in the CCNA Routing and Switching Composite certification exam.

To get your copy of Packet Tracer software, go to the companion website for instructions. To access this companion website, follow these steps:

Step 1. Go to http://www.ciscopress.com/register and log in or create a new account.

Step 2. Enter the ISBN 9781587205903.

Step 3. Answer the challenge question as proof of purchase.

Step 4. Click the Access Bonus Content link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

This book contains references to the Digital Study Guide enhancements that look like this:

Activity: Identify the Encapsulation Layer

Refer to the Digital Study Guide to complete this activity.

Packet Tracer Activity: Configure Routing Protocol Authentication

Refer to the Digital Study Guide to access the PKA file for this activity. You must have Packet Tracer software to run this activity.

Check Your Understanding

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

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

Day 24

Basic Router Configuration

CCNA 200-125 Exam Topics

- Configure, verify, and troubleshoot IPv4 addressing and subnetting
- Configure, verify, and troubleshoot IPv6 addressing

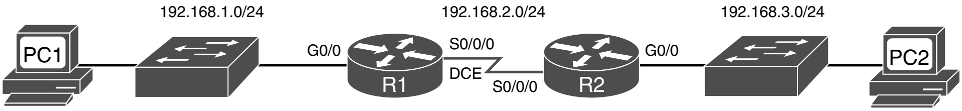
Key Topic

Today we review basic router configuration. First, we focus on configuring and verifying initial settings, including IPv4 addressing. Then we review IPv6 addressing and network connectivity verification. Most of this should be very familiar at this point in your studies because these skills are fundamental to all other router configuration tasks.

Basic Router Configuration with IPv4

Figure 24-1 shows the topology and IPv4 addressing scheme that we use to review basic router configuration and verification tasks.

Figure 24-1 IPv4 Example Topology



Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
PC1	N/A	192.168.1.10	255.255.255.0	192.168.1.1
PC2	N/A	192.168.3.10	255.255.255.0	192.168.3.1

When configuring a router, certain basic tasks are performed:

- Naming the router
- Setting passwords
- Configuring interfaces
- Configuring a banner
- Saving changes on a router
- Verifying basic configuration and router operations

Command Syntax

Table 24-1 shows the basic router configuration command syntax used to configure R1 in the following example.

Table 24-1 Basic Router Configuration Command Syntax

Configuration Task	Commands
Naming the router	`Router(config)# hostname name`
Setting passwords	`Router(config)# enable secret password`
	`Router(config)# line console 0`
	`Router(config-line)# password password`
	`Router(config-line)# login`
	`Router(config)# line vty 0 15`
	`Router(config-line)# transport input ssh`
	`Router(config-line)# login local`
	`Router(config)# username name password password`
Configuring a message-of-the-day banner	`Router(config)# banner motd # message #`
Configuring an interface	`Router(config)# interface type number`
	`Router(config-if)# ip address address mask`
	`Router(config-if)# description description`
	`Router(config-if)# no shutdown`
Saving changes on a router	`Router# copy running-config startup-config`
Examining the output of **show** commands	`Router# show running-config`
	`Router# show ip route`
	`Router# show ip interface brief`
	`Router# show interfaces`

Configuration Example

Let's walk through a basic configuration for R1. First, enter privileged EXEC mode and then global configuration mode:

```
Router> enable
Router# config t
```

Next, name the router and enter the encrypted password for entering privileged EXEC mode. This command overrides the older **enable password** *password* command, so we are not entering that one:

```
Router(config)# hostname R1
R1(config)# enable secret class
```

Next, configure the console password and require that it be entered with the login password:

```
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
```

Configuring SSH and disabling Telnet are security best practices, so configure the vty lines to use only SSH.

NOTE: SSH configuration is not shown here; assume that it is already configured. To review SSH configuration, refer to Day 12, "LAN Security."

```
R1(config)# line vty 0 15
R1(config-line)# transport input ssh
R1(config-line)# login local
R1(config-line)# exit
R1(config)# username admin password cisco
```

Encrypt all the clear-text passwords in the running configuration using the **service-password encryption** command:

```
R1(config)# service-password encryption
```

Configure the message-of-the-day (MOTD) banner. A delimiting character such as a # is used at both the beginning and the end of the message. At a minimum, a banner should warn against unauthorized access. A good security policy prohibits configuring a banner that welcomes an unauthorized user:

```
R1(config)# banner motd #
Enter TEXT message.  End with the character '#'.
******************************************
WARNING!! Unauthorized Access Prohibited!!
******************************************
#
```

Now configure the individual router interfaces with IP addresses and other information. First, enter interface configuration mode by specifying the interface type and number. Next, configure the IP address and subnet mask:

```
R1(config)# interface Serial0/0/0
R1(config-if)# ip address 192.168.2.1 255.255.255.0
```

It is good practice to configure a description on each interface to help document the network information:

```
R1(config-if)# description Ciruit#VBN32696-123 (help desk:1-800-555-1234)
```

Activate the interface:

```
R1(config-if)# no shutdown
```

Assuming that the other side of the link is activated on R2, the serial interface is now up. Finish R1 by configuring the GigabitEthernet 0/0 interface:

```
R1(config-if)# interface GigabitEthernet0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# description R1 LAN
R1(config-if)# no shutdown
```

Assume that R2 is fully configured and can route back to the 192.168.1.0/24 LAN attached to R1. We need to add a static route to R1 to ensure connectivity to R2's LAN. Static routing is reviewed in more detail on Day 25, "Basic Routing Concepts." For now, enter the following command to configure a directly attached static route to R2's LAN:

```
R1(config)# ip route 192.168.3.0 255.255.255.0 Serial 0/0/0
```

To save the configuration, enter the **copy running-config startup-config** command or the **copy run start** command.

Verification Example

You can use the **show running-config** command to verify the full current configuration on the router. However, a few other basic commands can help you not only verify your configuration, but also begin troubleshooting any potential problems.

First, make sure that the networks for your interfaces are now in the routing table by using the **show ip route** command (see Example 24-1).

Example 24-1 The show ip route Command

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Serial0/0/0
L        192.168.2.1/32 is directly connected, Serial0/0/0
S     192.168.3.0/24 is directly connected, Serial0/0/0
R1#
```

If a network is missing, check your interface status with the **show ip interface brief** command (see Example 24-2).

Example 24-2 The show ip interface brief Command

```
R1# show ip interface brief
Interface                   IP-Address      OK? Method   Status                 Protocol
Embedded-Service-Engine0/0  unassigned      YES unset    administratively  down down down
GigabitEthernet0/0          192.168.1.1     YES manual   up                     up
GigabitEthernet0/1          unassigned      YES unset    administratively  down down
Serial0/0/0                 192.168.2.1     YES manual   up                     up
Serial0/0/1                 unassigned      YES unset    administratively  down down
R1#
```

The output from the **show ip interface brief** command provides you with three important pieces of information:

- IP address
- Line status (column 5)
- Protocol status (column 6)

The IP address should be correct, and the status codes should be up and up. Table 24-2 summarizes the two status codes and their meanings.

Table 24-2 Interface Status Codes

Name	Location	General Meaning
Line status	First status code	Refers to the Layer 1 status—for example, is the cable installed, is it the right/wrong cable, is the device on the other end powered on?
Protocol status	Second status code	Refers generally to the Layer 2 status. It is always down if the line status is down. If the line status is up, a protocol status of down is usually caused by mismatched data link layer configuration.

Four combinations of settings are possible for the status codes when troubleshooting a network. Table 24-3 lists the four combinations, along with an explanation of the typical reasons why an interface is in that state.

Table 24-3 Combinations of Interface Status Codes

Line and Protocol Status	Typical Reasons
Administratively down, down	The interface has a **shutdown** command configured on it.
down, down	The interface has a **no shutdown** command configured, but the physical layer has a problem. For example, no cable has been attached to the interface (or with Ethernet), the switch interface on the other end of the cable is shut down, or the switch is powered off.

Line and Protocol Status	Typical Reasons
up, down	This almost always refers to data link layer problems, most often configuration problems. For example, serial links have this combination when one router was configured to use PPP and the other defaults to use HDLC. However, a clocking or hardware issue can also be to blame.
up, up	All is well and the interface is functioning.

If necessary, use the more verbose **show interface** command if you need to track down a problem with an interface, to get the output for every physical and virtual interface. You can also specify one interface. Example 24-3 shows the output for GigabitEthernet 0/0.

Example 24-3 The show interface gigabitethernet 0/0 Command

```
R1# show interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 30f7.0da3.0da0 (bia 30f7.0da3.0da0)
  Description: R1 LAN
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     387 packets input, 59897 bytes, 0 no buffer
     Received 252 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 86 multicast, 0 pause input
     281 packets output, 35537 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     56 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
R1#
```

This command has a lot of output. However, sometimes this is the only way to find a problem.

Table 24-4 parses and explains each important part of the **show interface** output.

Table 24-4 show interface Output Explanation

Output	Description
GigabitEthernet…is {up | down | administratively down}	Whether the interface hardware is currently active or down, or whether an administrator has taken it down.
line protocol is {up | down}	Whether the software processes that handle the line protocol consider the interface usable (that is, whether keepalives are successful). If the interface misses three consecutive keepalives, the line protocol is marked as down.
Hardware	Hardware type (for example, MCI Ethernet, serial communications interface [SCI], cBus Ethernet) and address.
Description	Text string description configured for the interface (max 240 characters).
Internet address	IP address followed by the prefix length (subnet mask).
MTU	Maximum transmission unit (MTU) of the interface.
BW	Bandwidth of the interface, in kilobits per second. The bandwidth parameter is used to compute routing protocol metrics and other calculations.
DLY	Delay of the interface, in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100 percent reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to an interface.
Loopback	Whether loopback is set. Can indicate a problem with the carrier.
Keepalive	Whether keepalives are set.
ARP type	Type of Address Resolution Protocol (ARP) assigned.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface. Useful for knowing when a dead interface failed.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. Useful for knowing when a dead interface failed.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the previous fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics shown in this report (such as number of bytes transmitted and received) were last reset to 0. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. Asterisks indicate elapsed time too large to be displayed. Reset the counters with the **clear interface** command.

Output	**Description**
Output queue, input queue, drops queue	Number of packets in output and input queues. Each number is followed by a slash (/), the maximum size of the queue, and the number of packets dropped because of a full queue.
Five minute input rate, Five minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. If the interface is not in promiscuous mode, it senses network traffic that it sends and receives (instead of all network traffic). The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within 2 percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets the system received.
bytes input	Total number of bytes, including data and MAC encapsulation, in the error-free packets received by the system.
no buffers	Number of received packets discarded because the main system had no buffer space. Compare with ignored count. Broadcast storms on Ethernet are often responsible for no input buffer events.
Received…broadcasts	Total number of broadcast or multicast packets received by the interface. The number of broadcasts should be kept as low as practicable. An approximate threshold is less than 20 percent of the total number of input packets.
runts	Number of Ethernet frames that are discarded because they are smaller than the minimum Ethernet frame size. Any Ethernet frame that is less than 64 bytes is considered a runt. Runts are usually caused by collisions. If more than one runt per million bytes is received, it should be investigated.
giants	Number of Ethernet frames that are discarded because they exceed the maximum Ethernet frame size. Any Ethernet frame that is larger than 1518 bytes is considered a giant.
input error	Runts, giants, no buffer, cyclic redundancy check (CRC), frame, overrun, and ignored counts. Other input-related errors can also increase the input error count, and some datagrams can have more than one error. Therefore, this sum might not balance with the sum of enumerated input error counts.
CRC	CRC generated by the originating LAN station or far-end device not matching the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.

Output	Description
frame	Number of packets received as incorrectly having a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
overrun	Number of times the receiver hardware could not hand-receive data to a hardware buffer because the input rate exceeded the capability of the receiver to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from the system buffers mentioned in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to increase.
input packets with dribble condition detected	Dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented just for informational purposes; the router accepts the frame.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of times that the transmitter has been running faster than the router can handle. This might never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this might not balance with the sum of the enumerated output errors because some datagrams might have more than one error and others might have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted because of an Ethernet collision. This is usually the result of an overextended LAN (too-long Ethernet or transceiver cable, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been completely reset. This can happen if packets queued for transmission were not sent within several seconds. On a serial line, this can be caused by a malfunctioning modem that is not supplying the transmit clock signal, or it can be caused by a cable problem. If the system notices that the carrier detect line of a serial interface is up but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.

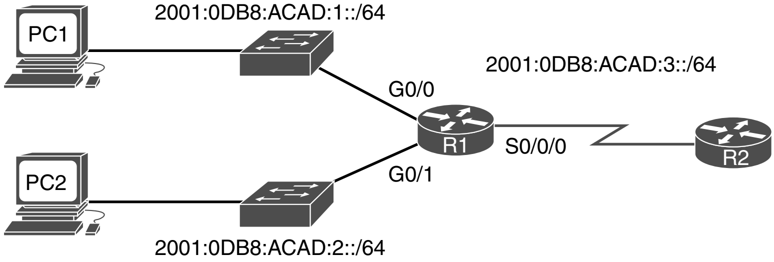
✓ Activity: Order the Steps for IPv4 Router Configuration

Refer to the Digital Study Guide to complete this activity.

Basic Router Configuration with IPv6

In this section, we use the topology in Figure 24-2 to review the basic commands for enabling IPv6 on a router.

Figure 24-2 IPv6 Example Topology



Command Syntax

First, you must enable IPv6 routing using the following command in global configuration mode:

```
R1(config)# ipv6 unicast-routing
```

Among other actions, this command configures the router to begin listening for and responding to Neighbor Discovery (ND) messages on all active IPv6 interfaces.

To configure an IPv6 address on a router's interface, you have one of several options:

- Configure the interface to use the EUI-64 method of addressing:

  ```
  Router(config)# ipv6 address ipv6-prefix/prefix-length eui-64
  ```

- Configure the full global unicast address. To manually configure a full IPv6 address, use the following command syntax:

  ```
  Router(config)# ipv6 address ipv6-address/prefix-length
  ```

- Configure the interface as unnumbered (see Day 26, "IPv6 Addressing").
- Configure the interface as a DHCPv6 client (see Day 7, "DHCP and DNS").

NOTE: To manually configure an interface's link-local address, use the following command syntax:

```
Router(config)# ipv6 address ipv6-address/prefix-length link-local
```

Configuration Example

The preferred method often is to manually configure the full IPv6 address because you can control the number of hexadecimal digits you must type when testing connectivity or troubleshooting a problem. You can see this by comparing the EUI-64 method to a full configuration. In Example 24-4, the interfaces on R1 are all configured using the EUI-64 method.

Example 24-4 Configuring Interfaces Using the EUI-64 Method

```
R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::/64 eui-64
R1(config-if)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::/64 eui-64
R1(config-if)# interface s0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:3::/64 eui-64
R1(config-if)# do show ipv6 interface brief
GigabitEthernet0/0          [up/up]
    FE80::2D0:97FF:FE20:A101
    2001:DB8:ACAD:1:2D0:97FF:FE20:A101
GigabitEthernet0/1          [up/up]
    FE80::2D0:97FF:FE20:A102
    2001:DB8:ACAD:2:2D0:97FF:FE20:A102
Serial0/0/0                  [down/down]
    FE80::20C:CFFF:FE77:A401
    2001:DB8:ACAD:3:20C:CFFF:FE77:A401
<output omitted>
```

Notice the number of hexadecimal digits in the IPv6 addresses highlighted in the output from the **show ipv6 interface brief** command. Imagine having to ping the GigabitEthernet 0/0 address 2001:DB8:ACAD:1:2D0:97FF:FE20:A101.

Furthermore, notice that the link-local addresses are also rather complex. To reduce the complexity of the router's configuration, verification, and troubleshooting, it is a good practice to manually configure the link-local address as well as the IPv6 global unicast address. In Example 24-5, R1 is reconfigured with simpler IPv6 addresses and with FE80::1 as the link-local address on all interfaces. Remember, the link-local address needs to be unique only on that interface's link.

Example 24-5 Full IPv6 Address and Link-Local Address Configuration

```
R1(config-if)# interface g0/0
R1(config-if)# no ipv6 address 2001:db8:acad:1::/64 eui-64
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# interface g0/1
R1(config-if)# no ipv6 address 2001:db8:acad:2::/64 eui-64
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# interface s0/0/0
R1(config-if)# no ipv6 address 2001:db8:acad:3::/64 eui-64
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# do show ipv6 interface brief
```

```
GigabitEthernet0/0          [up/up]
    FE80::1
    2001:DB8:ACAD:1::1
GigabitEthernet0/1          [up/up]
    FE80::1
    2001:DB8:ACAD:2::1
Serial0/0/0                  [down/down]
    FE80::1
    2001:DB8:ACAD:3::1
<output omitted>
```

NOTE: If you do not remove the previous IPv6 address configuration, each interface will have two IPv6 global unicast addresses. This is different than in IPv4, where simply configuring another IPv4 address with the **ip address** command overwrites any previous configuration. However, only one link-local address can exist per interface.

Compare the highlighted output from the **show ipv6 interface brief** command in Example 24-5 with the output in Example 24-4. You can see that simplifying the IPv6 addressing implementation can make your verification and troubleshooting job much easier.

To verify the full configuration of an interface, use the **show ipv6 interface** command. Example 24-6 shows the output for R1's GigabitEthernet 0/0 interface.

Example 24-6 The show ipv6 interface gigabitethernet 0/0 Command

```
R1# show ipv6 interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

Focus on the highlighted output. IPv6 is enabled on this interface with a nice, short link-local address. The global unicast address and its subnet are listed, as is the address of multicast groups that this interface automatically joined. Do you remember what the FF02::1 and FF02::1:FF00:1 addresses are used for? If not, revisit Day 26.

That's all the IPv6 configurations for today. As we continue to review the exam topics in the upcoming days, we will incorporate IPv6 topics.

Activity: Order the Steps for IPv6 Router Configuration

Refer to the Digital Study Guide to complete this activity.

Verifying IPv4 and IPv6 Network Connectivity

As reviewed on Day 29, "Switch Configuration Basics," ping and traceroute are helpful tools for verifying network connectivity. Example 24-7 demonstrates successful ping output on the router.

Example 24-7 Successful ping Output on a Router

```
R1# ping 192.168.3.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
!Pinging an IPv6 destination
R1# ping 2001:db8:acad:1:290:dff:fee5:8095

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1:290:CFF:FEE5:8095, timeout is
2   seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/9/46 ms

R1#
```

Unsuccessful ping output shows periods (.) instead of exclamation points (!), as Example 24-8 demonstrates. The output would be the same in IPv6.

Example 24-8 Unsuccessful ping Output on a Router

```
R1# ping 192.168.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#
```

Example 24-9 shows output from a successful **traceroute** command.

Example 24-9 Successful traceroute Output on a Router

```
R1# traceroute 192.168.3.10
Type escape sequence to abort.
Tracing the route to 192.168.3.10

  1   192.168.2.2      71 msec   70 msec   72 msec
  2   192.168.3.10     111 msec  133 msec  115 msec
R1#
!Tracing to an IPv6 destination.
R2# traceroute 2001:db8:acad:1:290:cff:fee5:8095
Type escape sequence to abort.
Tracing the route to 2001:DB8:ACAD:1:290:CFF:FEE5:8095

  1   2001:DB8:ACAD:3::11 msec    1 msec    1 msec
  2   2001:DB8:ACAD:1:290:CFF:FEE5:80951 msec    1 msec    0 msec
R2#
```

Unsuccessful traces show the last successful hop and the asterisks for each attempt until the user cancels. To cancel the **traceroute** command on a router, use the key combination **Ctrl-Shift-6** and then press the **x** key. Example 24-10 shows unsuccessful **traceroute** output. The output would be the same with IPv6.

Example 24-10 Unsuccessful traceroute Output on a Router

```
R1# traceroute 192.168.3.2
Type escape sequence to abort.
Tracing the route to 192.168.3.2

  1   192.168.2.2      71 msec   70 msec   72 msec
  2   *      *      *
  3   *      *      *
  4   *      *      *
  5   *
R1#
```

Using Telnet or SSH to remotely access another device also tests connectivity. More important, these remote access methods test whether a device has been correctly configured so that you can access it for management purposes. This can be important when a device is truly remote (for example, across town or in another city). Day 12 reviews SSH configuration and verification in greater detail.

During the basic configuration tasks earlier, we entered the commands to properly configure the vty lines for SSH remote access. If you are accessing a device configured with SSH from a PC, you use the SSH setting in your terminal client. However, you can use the **ssh** command on a router or switch to access another device configured with SSH. Example 24-11 shows how to use SSH to remotely access R2 from R1.

Example 24-11 Remote Access Using SSH

```
R1# ssh?
  -c     Select encryption algorithm
  -l     Log in using this user name
  -m     Select HMAC algorithm
  -o     Specify options
  -p     Connect to this port
  -v     Specify SSH Protocol Version
  -vrf   Specify vrf name
  WORD   IP address or hostname of a remote system

R1# ssh -l?
  WORD   Login name

R1# ssh -l admin?
  -c     Select encryption algorithm
  -m     Select HMAC algorithm
  -o     Specify options
  -p     Connect to this port
  -v     Specify SSH Protocol Version
  -vrf   Specify vrf name
  WORD   IP address or hostname of a remote system

R1# ssh -l admin 192.168.2.2
Password:

******************************************
WARNING!! Unauthorized Access Prohibited!!
******************************************

R2>
```

NOTE: During your CCNA studies and lab practice, you most likely used a Telnet configuration to remotely access your lab equipment. Although Telnet is easier to use than SSH, remember that SSH is considered best practice. Therefore, during the CCNA exam, be ready to use SSH to remotely access devices on simulation questions because Telnet might not be configured or allowed.

Packet Tracer Activity: Dual-Stack Router Address Configuration

Refer to the Digital Study Guide to access the PKA file for this activity. You must have Packet Tracer software to run this activity. See the Introduction for details.

Basic IP Addressing Troubleshooting

If you are sure you manually configured the correct IP address and subnet mask (IPv4) or network prefix (IPv6), then basic IP addressing issues are usually the result of a misconfigured default gateway or duplicate addresses.

Default Gateway

A misconfigured default gateway is one of the most common problems in either a static or dynamically assigned IP addressing scheme. For a device to communicate across multiple networks, it must be configured with an IP address, a subnet mask or network prefix, and a default gateway.

The default gateway is used when the host wants to send a packet to a device on another network. The default gateway address is generally the router interface address attached to the local network to which the host is connected.

To resolve a default gateway that was manually configured incorrectly, consult the topology and addressing documentation to verify what the device's default gateway should be—normally, a router attached to the same LAN.

NOTE: A misconfigured DHCP server can also cause a default gateway issue. Some DHCP server configurations, such as the Easy IP IOS feature, might require the administrator to manually configure the default gateway address. If this is configured incorrectly, no devices will have access beyond the LAN. DHCP is reviewed on Day 7.

Duplicate IP Addresses

Under some circumstances, duplicate IP address conflicts can occur between a statically configured network device and a PC obtaining automatic IP addressing information from the DHCP server. To resolve such an IP addressing conflict, you can do one of the following:

- Convert the network device with the static IP address to a DHCP client
- On the DHCP server, exclude the static IP address of the end device from the DHCP pool of addresses

The first solution is a quick fix that you can do in the field. However, the device more than likely needs a static configuration. The second solution might be the better long-term choice. However, it requires that you have administrative privileges to configure the DHCP server.

You might also encounter IP addressing conflicts when manually configuring IP on an end device in a network that uses only static IP addresses. In this case, you must determine which IP addresses are available on the particular IP subnet and configure accordingly. This case illustrates why it is so important for a network administrator to maintain detailed documentation, including IP address assignments and topologies, for end devices.

Study Resources

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

Resource	Location	Topic
Primary Resources		
Routing and Switching Essentials	1	Router Initial Configuration
ICND1 Official Cert Guide	17	Enabling IPv4 Support on Cisco Router Interfaces
	30	Implementing Unicast IPv6 Addresses on Routers
Supplemental Resources		
CCNA Portable Command Guide	11	All
CCNA Video Series	3	Lesson 2: Basic Router Configuration and Verification
CCNA Network Simulator	ICND1	Chapter 17: New Job I
		Chapter 17: Rebuild a Configuration
		Chapter 17: Router CLI Exec Mode I–II
		Chapter 17: Router CLI Configuration Process
		Chapter 17: Setting Router Passwords
		Chapter 30: IPv6 Configuration I–II
		Chapter 30: IPv6 Address Configuration I–IX
		Chapter 30: IPv6 EUI-64 Calculation Drills I–X
		Chapter 30: IPv6 Addressing Troubleshooting

Check Your Understanding

Refer to the Digital Study Guide to take a short quiz covering the content of this day.

Index

Symbols

- *** (asterisk), 165, 438**
- **? command, 42–43**
- **3-1-4 Rule, 92**
- **3G connections, 388**
- **3-tiered campus design, 24–26**
- **4G connections, 388**
- **10BASE-T, 21, 27, 34**
- **10GBASE-LX4, 21**
- **10GBASE-SX4, 21**
- **10GBASE-T, 21**
- **10GigE, 34**
- **100BASE-FX, 21**
- **100BASE-TX, 21**
- **802.1D. *See* STP (Spanning Tree Protocol)**
- **802.1x, 293–294**
- **1000BASE-LX, 21**
- **1000BASE-SX, 21**
- **1000BASE-T, 21**
- **1000BASE-TX, 21**

A

- **A record (DNS), 365**
- **AAA (Authentication, Authorization, and Accounting) framework, 292**
- **AAAA record (DNS), 365**
- **access control lists. *See* ACLs (access control lists)**
- **access layer, 24**
- **access layer switches, 14**
- **access points, 17–19**
- **access-list command, 336, 337–338, 375**
- **ACI (Application Centric Infrastructures), 422–423**
- **Acknowledgment field (TCP), 7–8**
- **Acknowledgment packets (EIGRP), 241**
- **ACL Analysis tool (APIC-EM), 424–425**
- **ACL Path Trace tool (APIC-EM), 424–425**
- **ACLs (access control lists), 337–339**
  - APIC-EM (Application Policy Infrastructure Controller Enterprise Module) and, 424–425
  - defining, 329
  - design guidelines, 333–334
  - identification numbers, 333
  - interface processing ACLs, 329–330
  - IPv4 ACLs
    - *comments, 340–341*
    - *compared to IPv6 ACLs, 343*
    - *extended named IPv4 ACLs, 340*
    - *extended numbered IPv4 ACLs, 337–339*
    - *standard named IPv4 ACLs, 339–340*
    - *standard numbered IPv4 ACLs, 335–337*
    - *verification, 341–343*
  - IPv6 ACLs
    - *applying, 344*
    - *compared to IPv4 ACLs, 343*
    - *creating, 344*
    - *extended IPv6 ACLs, 345*
    - *naming, 343–344*
    - *standard IPv6 ACLs, 344–345*
    - *troubleshooting, 348–349*
    - *verification, 346–348*
  - list logic with, 330–331
  - operation, 329
  - planning for, 331
  - types of, 332
- **Active mode (LACP), 316**
- **AD (administrative distance), 113–115, 244–245**
- **AD (advertised distance), 245**
- **address conflicts, resolving, 363–364**
- **Address Resolution Protocol (ARP), 4, 364**
- **addresses, MAC, 11, 28**
- **addressing, Ethernet, 36**
- **addressing, IPv4, 77**
  - binary and alphanumeric representations, 90–91
  - classes of addresses, 78–80
  - conventions for writing, 100–102
  - header format, 78
  - IPv4-mapped IPv6 address, 97
  - NAT (network address translation)
    - *benefits of, 373*
    - *concepts, 369–371*
    - *dynamic NAT, 371, 375–376*

example, 371
limitations of, 373
overloading, 372–373, 376
static NAT, 371, 374–375
troubleshooting, 378–379
verification, 377
private addresses, 81
public addresses, 81
subnetting
bits borrowed, determining, 81–82
examples of, 83–85
overview of, 81
subnet addressing scheme, 83
subnet masks, 80, 82
subnet multiplier, 83
variable-length subnet masking (VLSM), 85–87
troubleshooting, 136

addressing, IPv6
anycast addresses, 100
assigned multicast addresses, 98
benefits of, 89–90
binary and alphanumeric representations, 90–91
EUI-64 concept, 103–104
global unicast addresses, 92–95
IPv4 embedded addresses, 97
link-local addresses, 95–96
loopback addresses, 96
migration to, 105–106
NAT (network address translation)
private address space, 379
purpose of, 379–380
prefixes, 101–102
solicited-node multicast addresses, 98–100
stateless address autoconfiguration, 104–105
subnetting, 102–103
troubleshooting, 136
ULAs (unique local addresses), 96–97
unspecified addresses, 96

addressing schemes
EIGRP (Enhanced Interior Gateway Routing Protocol)
for IPv4, 249
for IPv6, 257
IPv4 static routing, 141
IPv6 static routing, 148–149
OSPF (Open Shortest Path First), 197
multiarea OSPFv2 implementation, 216
multiarea OSPFv3 implementation, 219
OSPFv2, 226
OSPFv3, 232

adjacency (OSPF), 228, 236

administrative distance (AD), 113–115, 244–245

advertised distance (AD), 245

advertisements (VTP), 170

AF (Assured Forwarding), 412–413

algorithms
Dijkstra Shortest Path First (SPF) algorithm, 117–118
DUAL (Diffusing Update Algorithm), 245–246
OSPF (Open Shortest Path First), 189–190
Pseudo-Random Global ID Algorithm, 96
STP (Spanning Tree Protocol), 298–299

alphanumeric representation (IP addresses), 90–91

anycast addresses, 100

APIC (Cisco Application Policy Infrastructure Controller), 423

APIC-EM (Application Policy Infrastructure Controller Enterprise Module), 423–425

Application Centric Infrastructures (ACI), 422–423

application layer
OSI model, 2
TCP/IP model, 5
troubleshooting, 458

Application Policy Infrastructure Controller (APIC), 423

Application Policy Infrastructure Controller Enterprise Module (APIC-EM), 423–425

applying ACLs (access control lists), 344

APs (access points), 17–19

ARP (Address Resolution Protocol), 4, 364

assigned multicast addresses, 98

assigning VLANs (virtual local-area networks), 65–66

Assured Forwarding (AF), 412–413

asterisk (*), 165, 438

asymmetric switching, 30

authentication
AAA (Authentication, Authorization, and Accounting) framework, 292
authentication servers, 293
PPP (Point-to-Point Protocol), 395–396

Auto mode (PAgP), 315

auto-cost reference-bandwidth command, 201, 208

automatic medium-dependent interface crossover (auto-MDIX), 48

automatic summarization
EIGRP (Enhanced Interior Gateway Routing Protocol), 263–264
RIPv1 (Routing Information Protocol version 1), 162–164
RIPv2 (Routing Information Protocol version 2), 167

auto-MDIX (automatic medium-dependent interface crossover), 48

autonomous system (AS), 110

Autonomous System Number field (EIGRP), 243

auto-summary command, 264

B

backing up
IOS images, 442–443
licenses, 447

backup designated routers (BDR), 189

balancing load, 323–325

bandwidth
definition of, 409
modifying usage of
EIGRP for IPv4, 266
EIGRP for IPv6, 268–269
reference bandwidth, 200–203

bandwidth command, 202–203, 244, 254, 266

banner login command, 47

baseline data, 453–454

Basic Rate Interface (BRI), 384

BD/BDR election, 229–231

BDR (backup designated routers), 189, 229–231

BGP (Border Gateway Protocol)
concepts, 403–404
eBGP (external BGP)
configuration, 404–407
verification, 406–407

BID (bridge ID), 298–299, 307–309

bidirectional communication, 47

binary representation (IP addresses), 90–91

binary values (subnet masks), 80–82

bits borrowed for subnets, determining, 81–82

black hole VLANs (virtual local-area networks), 59

Border Gateway Protocol. ***See*** **BGP (Border Gateway Protocol)**

bottom-up troubleshooting, 459

BPDU (bridge protocol data unit), 298

BPDU guard, 309

BRI (Basic Rate Interface), 384

bridge ID (BID), 298–299, 307–309

bridge protocol data unit (BPDU), 298

broadcast addresses, 36

broadcast domains, 29

broadcast multiaccess networks, 228

broadcast storms, 297

buffering memory, 30

C

cable modems, 387

cabling
copper cable, 19–20
fiber-optic cable, 19–20
UTP (unshielded twisted pair) cabling, 34–35

Canonical Format Identifier (CFI), 61

CAPWAP (Control and Provisioning of Wireless Access Points), 19

Carrier Sense Multiple Access with Collision Detection (CSMA/CD), 32–33

CBWFQ (Class-Based Weighted Fair Queueing), 413

CCNA Routing and Switching **200–125** ***Premium Edition Complete Video Course*** **(Wallace), 425**

CCNA Routing and Switching ICND2 **200–105** ***Official Cert Guide*** (Odom), **404, 421**

CDP (Cisco Discovery Protocol)
configuration, 274–276
disabling, 275–276
overview of, 273–274
verification, 277–279

cdp holdtime command, 280

cellular Internet connections, 388

CFI (Canonical Format Identifier), 61

Challenge Handshake Authentication Protocol (CHAP), 397–398

channel-group command, 316, 319

CHAP (Challenge Handshake Authentication Protocol), 397–398

CIR (Committed Information Rate), 414

circuit-switched connections, 384–385

Cisco 1941 router, 15

Cisco ACI (Application Centric Infrastructures), 422–423

Cisco APIC-EM (Application Policy Infrastructure Controller Enterprise Module), 423–425

Cisco Application Policy Infrastructure Controller (APIC), 423

Cisco devices, connecting to, 41

Cisco Discovery Protocol. *See* CDP (Cisco Discovery Protocol)

Cisco IOS Integrated File System. *See* IFS (Integrated File System)

Cisco Open SDN Controller (OSC), 422

Class of Service (CoS), 411

Class Selector (CS) values, 411

Class-Based Weighted Fair Queueing (CBWFQ), 413

classes of IPv4 addresses, 78–80

classful routing protocols, 112

classification
AF (Assured Forwarding), 412–413
definition of, 410–411
DSCP (differentiated service code point), 411–412
EF (Expedited Forwarding), 412–413
IPP (IP precedence), 411–412

classless routing protocols, 112

clear command, 378

clear ip nat translation command, 377

clear ip ospf process command, 230, 236

clear spanning-tree detected protocols command, 309

CLI (command-line interface). *See* commands

clients, DHCPv4, 357–358

cloud computing
overview of, 416
server virtualization, 416–418
services, 418–419
virtual network infrastructure, 419

collisions
collision domains, 29
troubleshooting, 54

command history, 44

commands
? 42–43
access-list, 336, 337–338, 375
auto-cost reference-bandwidth, 201, 208
auto-summary, 264
bandwidth, 202–203, 244, 254, 266
banner login, 47
basic switch configuration commands, 46–47
cdp holdtime, 280
channel-group, 316, 319
clear, 378
clear ip nat translation, 377
clear ip ospf process, 230, 236
clear spanning-tree detected protocols, 309
command history, 44
configure terminal, 45
copy, 440–442
copy run start, 124
copy running-config startup-config, 124
copy startup-config running-config, 448
copy tftp flash, 444
crypto key generate rsa, 295
crypto key zeroize rsa, 295
debug, 378
debug ip nat, 378
debug ip rip, 160–161, 164
debug ppp, 398
default-information originate, 165, 227, 233
default-router, 353
dir, 438–440, 443
dns-server, 353

domain-name, 353
duplex, 52
duplex auto, 46
eigrp router-id, 250, 257
enable password, 47, 122
encapsulation ppp, 396
exit, 46
frequency, 460
hostname, 46, 397
icmp-echo, 460
interface port-channel, 316
interface range, 47, 316
interface tunnel, 402
interface vlan, 181
ip access-group, 336
ip access-list extended, 340
ip access-list standard, 339
ip address, 46
ip address dhcp, 357
ip bandwidth-percent eigrp, 268
ip default-gateway, 46
ip dhcp excluded-address, 352
ip dhcp pool, 352
ip domain-name, 277, 295
ip forward-protocol udp, 357
ip hello-interval eigrp, 266–267
ip helper-address, 356–357
ip hold-time eigrp, 266–267
ip http authentication enable, 46
ip http server, 46
ip nat inside, 374, 375
ip nat inside source list, 375
ip nat inside source static, 374
ip nat outside, 374, 375
ip nat pool name, 375
ip ospf cost, 202–203
ip ospf priority, 229
ip route, 140
ip routing, 181
ip sla, 460
ip sla schedule, 460
ipconfig, 49, 355–356
ipv6 access-class, 344
ipv6 access-list, 344
ipv6 address, 130
ipv6 address autoconfig, 362, 363
ipv6 address dhcp, 363
ipv6 eigrp, 257
ipv6 hello-interval eigrp, 269
ipv6 hold-time eigrp, 269
ipv6 nd, 359–360
ipv6 route, 149
ipv6 router eigrp, 257
ipv6 router ospf, 208
ipv6 traffic-filter, 344
ipv6 unicast-routing, 98, 130, 257, 361
lease, 353
license install, 445–447
license save, 447
line console, 46
lldp holdtime, 280
lldp reinit, 280
lldp run, 280
lldp timer, 280
logging buffered, 434
logging console, 434
logging source-interface, 435
logging trap, 435
login, 46
mdix auto, 46
neighbor, 405–406
netbios-name-server, 353
network, 199–200, 250, 353, 406
no cdp enable, 275–276
no cdp run, 273
no debug ip rip, 161
no lldp receive, 280
no lldp transmit, 280
no service dhcp, 354
no shutdown, 257, 275, 291
no switchport, 182
ntp server, 436
passive-interface, 161–162, 208
password, 46
ping, 48–50, 133
ppp authentication chap, 397, 398
ppp authentication pap, 398
pppoe enable, 400
range, 65
redistribute static, 265, 267
remark, 340
reset, 448
router bgp, 405
router ospf, 198
router rip, 163
router-id, 198–199, 208
service password-encryption, 47
service sequence-numbers, 433
service timestamps, 433
service-password encryption, 123
show, 44–45
show access-lists, 341, 346–347

show cdp, 275
show cdp interface, 274
show cdp neighbors, 275
show cdp neighbors detail, 278–279
show cdp traffic, 279
show etherchannel summary, 318
show file systems, 437–438
show flash, 438–439, 443
show history, 44
show interface, 126–129
show interface switchport, 318–319
show interface Tunnel, 403
show interfaces, 52–53, 65–66, 397
show interfaces status, 52–53
show interfaces switchport, 71, 74
show interfaces trunk, 69, 73–74
show ip bgp, 406–407
show ip bgp summary, 406–407
show ip dhcp binding, 354
show ip dhcp conflict, 364
show ip dhcp server statistics, 354
show ip eigrp interface, 269
show ip eigrp interfaces, 270
show ip eigrp neighbors, 252–253, 269
show ip eigrp topology, 253
show ip eigrp topology all-links, 254
show ip interface, 341–342
show ip interface brief, 125, 179–180, 270, 274, 403, 448
show ip interface brief,203–204
show ip nat statistics, 377
show ip nat translations, 377, 378
show ip ospf, 198, 205–206, 236
show ip ospf database, 218
show ip ospf interface, 236
show ip ospf interface brief, 206, 217
show ip ospf interfaces, 198
show ip ospf neighbor, 204–205, 236
show ip protocols, 114, 159–160, 167, 198, 203–204, 217, 236, 251–252, 269, 270
show ip route, 112–113, 124, 141–146, 158–159, 179–180, 182, 203–204, 406–407
show ip route eigrp, 255, 265, 269
show ip route ospf, 217, 236
show ip sla configuration, 461
show ip sla statics, 462
show ip ssh, 294–295
show ipv6 access-list, 347
show ipv6 eigrp interface, 270
show ipv6 eigrp neighbors, 259–260, 270
show ipv6 interface, 132–133, 347–348, 362
show ipv6 interface brief, 131–132
show ipv6 ospf, 209–210
show ipv6 ospf database, 211
show ipv6 ospf interface, 210
show ipv6 ospf interface brief, 211, 221
show ipv6 ospf neighbor, 211
show ipv6 ospf neighbors, 233
show ipv6 protocols, 210, 220, 258, 270
show ipv6 route, 149–150, 268
show ipv6 route eigrp, 260–261, 270
show ipv6 route ospf, 212, 221, 233
show license feature, 444
show license udi, 445
show lldp interface, 281
show lldp neighbors, 282
show lldp neighbors detail, 282–283
show lldp traffic, 283
show logging, 434, 435–436
show mac address-table, 71
show ntp associations, 437
show ntp status, 437
show port-security, 286–287
show port-security interface, 286–287
show run, 68, 317, 346, 377
show running-config, 124, 342–343
show snmp, 430–431
show snmp community, 431
show spanning-tree, 308, 310
show spanning-tree active, 310
show spanning-tree brief, 310
show spanning-tree detail, 310
show spanning-tree interface, 310
show spanning-tree summary, 310
show spanning-tree vlan, 310
show standby, 322–323
show standby brief, 322–325
show version, 442, 448
show vlan, 71–72
show vlan brief, 63, 65
show vlans, 179–180
show vtp password, 173
show vtp status, 172, 173–175
snmpget, 429
snmp-server community, 430
snmp-server contact, 430
snmp-server location, 430
spanning-tree bpduguard default, 309
spanning-tree link-type point-to-point, 309
spanning-tree mode rapid-pvst, 309

spanning-tree portfast default, 309
spanning-tree vlan, 307–308
speed, 52
speed auto, 46
ssh, 134–135
standby preempt, 322
standby priority, 322
switchport access vlan, 46, 71, 291
switchport mode access, 46, 285
switchport mode dynamic auto, 74
switchport mode dynamic desirable, 62
switchport mode trunk, 62
switchport mode trunk dynamic auto, 62
switchport nonegotiate, 62
switchport port-security, 285
switchport port-security mac-address, 286
switchport port-security mac-address sticky, 286
switchport port-security maximum, 285
switchport port-security violation {protect | restrict | shutdown} 285
switchport trunk native vlan, 291
terminal history, 44
terminal no history, 44
traceroute, 134
tracert, 50
tunnel mode gre ip, 402
undebug all, 161
username, 397
vtp domain, 171
vtp mode, 171
vtp password, 171
vtp pruning, 171

comments (IPv4 ACLs), 340–341

Committed Information Rate (CIR), 414

community clouds, 419

composite metric (EIGRP), 244

configuration

CDP (Cisco Discovery Protocol), 274–276
DHCPv4, 352–358
clients, 357–358
request relay, 356–357
servers, 352–356
DHCPv6
SLAAC (stateless address autoconfiguration), 358–360
stateful DHCPv6, 360–361, 363
stateless DHCPv6, 360–362
eBGP (external BGP), 404–406
EIGRP for IPv4
addressing scheme, 249
network command, 250
router IDs, 250–251
topology, 249–250
verification, 251–255
EIGRP for IPv6
addressing scheme, 257
configuration commands, 257–258
topology, 256
verification, 258–261
EtherChannel, 316–317
GRE (generic route encapsulation), 401–402
HSRP (Hot Standby Router Protocol), 322
IPv4 ACLs
comments, 340–341
extended named IPv4 ACLs, 340
extended numbered IPv4 ACLs, 337–339
standard named IPv4 ACLs, 339–340
standard numbered IPv4 ACLs, 335–337
IPv4 default route configuration, 144–146
IPv4 static route configuration
addressing scheme, 141
example of, 141–142
exit interface parameter, 143–144
ip route command, 140
next-hop parameter, 142–143
summary route configuration, 147–148
topology, 140–141
IPv6 ACLs
applying, 344
creating, 344
extended IPv6 ACLs, 345
naming, 343–344
standard IPv6 ACLs, 344–345
IPv6 default route configuration, 150–151
IPv6 static route configuration
addressing scheme, 148–149
ipv6 route command, 149
show ipv6 route command, 149–150
summary route configuration, 151–152
topology, 148
LLDP (Link Layer Discovery Protocol), 280–281
multilayer switch inter-VLAN routing
Layer 3 routed ports, 182
SVIs (switch virtual interfaces), 180–181

NAT (network address translation)
dynamic NAT, 375–376
overloading, 376
static NAT, 374–375
NTP (Network Time Protocol), 436–437
OSPFv2
addressing scheme, 226
BD/BDR election, 229–231
dead intervals, 228
default route redistribution, 227
example of, 225–227
hello intervals, 228
multiarea OSPFv2, 216
network types, 228–229
single-area OSPFv2, 197–203
topology, 225
OSPFv3
addressing scheme, 232
dead intervals, 234
default route propagation, 233–234
example of, 231–233
hello intervals, 234
multiarea OSPFv3, 220
single-area OSPFv3, 209–212
timers, 234–235
topology, 231
port security, 285–287
PPP (Point-to-Point Protocol), 396–397
PPPoE (PPP over Ethernet), 399–400
RIPv1 (Routing Information Protocol version 1), 156–157
RIPv2 (Routing Information Protocol version 2), 165–167
router configuration with IPv4
command syntax, 122
example of, 122–124
IP addressing, troubleshooting, 136
network connectivity, verifying, 133–135
topology, 121
verification, 124–129
router configuration with IPv6
command syntax, 130
example of, 130–133
IP addressing, troubleshooting, 136
network connectivity, verifying, 133–135
topology, 130
router on a stick, 177–179
SNMP (Simple Network Management Protocol), 430
SSH (Secure Shell), 294–295
STP (Spanning Tree Protocol), 306–307
BID (bridge ID), 307–309
BPDU guard, 309
PortFast, 309
Rapid PVST+, 309
switches
auto-MDIX, 48
basic switch configuration commands, 46–47
Cisco devices, connecting to, 41
CLI EXEC sessions, 42
CLI navigation and editing shortcuts, 43–44
command history, 44
full-duplex communication, 47
half-duplex communication, 47
help facility, 42–43
network connectivity, verifying, 48–51
port speed, 47
subconfiguration modes, 45
troubleshooting, 51–54
Syslog, 434–435
VLANs (virtual local-area networks), 62–64
extended VLANs, 67
trunking, 68–69, 170–173
VTP (VLAN Trunking Protocol), 170–173

configuration files, 440–442, 451

configure terminal command, 45

congestion management, 413

connectionless protocols, 10

connections. *See also* configuration
EIGRP (Enhanced Interior Gateway Routing Protocol), 243
TCP (Transmission Control Protocol), 9
WANs (wide area networks)
circuit-switched connections, 384–385
comparison of, 388
dedicated connections, 383–384
Internet connections, 386–388
overview of, 382–383
packet-switched connections, 385–386

console terminal, 41

Control and Provisioning of Wireless Access Points (CAPWAP), 19

control planes, 419–420

controllers, 421

convergence
with link-state protocols, 118–119
STP (Spanning Tree Protocol), 299–300

copper cable, 19–20

copy command, 440–442

copy run start command, 124

copy running-config startup-config command, 124

copy startup-config running-config command, 448

copy tftp flash command, 444

core layer, 24

core layer switches, 14

CoS (Class of Service), 411

creating ACLs (access control lists), 344

crypto key generate rsa command, 295

crypto key zeroize rsa command, 295

CS (Class Selector) values, 411

CSMA/CD (Carrier Sense Multiple Access with Collision Detection), 32–33

cut-through switching, 30

D

DAD (duplicate address detection), 96, 99, 358

data center topology, 417–418

data encapsulation, 12–13

data link layer
- overview of, 2
- troubleshooting, 456

data planes, 419–420

data VLANs (virtual local-area networks), 59

databases, LSDB (link-state database), 116–117

DBD (database description) packets, 186

dead intervals
- OSPFv2, 228
- OSPFv3, 234

debug command, 378

debug ip nat command, 378

debug ip rip command, 160–161, 164

debug ppp command, 398

dedicated WAN connections, 383–384

default gateways, troubleshooting, 136

default routing
- EIGRP (Enhanced Interior Gateway Routing Protocol)
  - *for IPv4, 265–266*
  - *for IPv6, 267–268*
- IPv4 default route configuration, 144–146
- IPv6 default route configuration, 150–151
- OSPFv2, 227
- OSPFv3, 233–234
- overview of, 139–140
- RIPv1 (Routing Information Protocol version 1), 164–165

default VLANs (virtual local-area networks), 59

default-information originate command, 165, 227, 233

default-router command, 353

defining ACLs (access control lists), 329

delay, 409

on-demand self-service, 418

deny statement, 338

denying
- FTP (File Transfer Protocol), 338
- hosts, 336, 340
- subnets, 337
- Telnet, 338–339
- Telnet/SSH access, 337

design guidelines
- ACLs (access control lists), 333–334
- hierarchical campus network designs, 24–26
- multiarea OSPF (Open Shortest Path First) operation, 192–194

designated routers (DR), 189

Desirable mode (PAgP), 315

device discovery. *See* discovery

device management
- Cisco devices, connecting to, 41
- configuration files, 440–442
- IFS (Integrated File System)
  - *commands, 437–440*
  - *definition of, 437*
  - *URL prefixes, 440*
- IOS images
  - *backing up, 442–443*
  - *licenses, 444–447*
  - *restoring, 443–444*
  - *TFTP topology, 442*
- licenses, 444–447
- NTP (Network Time Protocol), 436–437
- password recovery, 448
- routers, 15

SNMP (Simple Network Management Protocol)
components, 427
configuration, 430
messages, 427–428
MIB (Management Information Base), 428–429
operation, 427
verification, 430–431
versions, 428
switches, 13
Syslog
configuration, 434–435
definition of, 432
operation, 432–433
verification, 435–436

DHCP (Dynamic Host Configuration Protocol), 3
DHCP snooping, 289–290
DHCPv4
configuration, 352–358
overview of, 351
testing, 364
verification, 354–355
DHCPv6
SLAAC (stateless address autoconfiguration), 358–360
stateful DHCPv6, 360–361, 363
stateless DHCPv6, 360–362
troubleshooting, 363–364

DHCPACK packet, 351

DHCPDISCOVER packet, 351

DHCPNAK packet, 351

DHCPOFFER packet, 351

DHCPREQUEST packet, 351

diagrams, topology, 19–21

dialer pool, 400

differentiated service code point (DSCP), 411–412

Diffusing Update Algorithm (DUAL), 245–246

digital subscriber line (DSL), 386–387

Dijkstra Shortest Path First (SPF) algorithm, 117–118

dir command, 438–440, 443

directly connected routes, 109

disabling
CDP (Cisco Discovery Protocol), 275–276
RIPv2 automatic summarization, 167
VLANs (virtual local-area networks). *See* configuration

discards (TCP), 415

discontiguous networks (EIGRP), 270–271

discovery
CDP (Cisco Discovery Protocol)
configuration, 274–276
disabling, 275–276
overview of, 273–274
verification, 277–279
LLDP (Link Layer Discovery Protocol)
configuration, 280–281
overview of, 279–280
verification, 281–283

distance vector protocols, 111

distribution layer, 24

distribution layer switches, 14

DNS (Domain Name System), 3
operation, 364–366
troubleshooting, 366

dns-server command, 353

documentation, 451
baseline data, 453–454
configuration files, 451
topology diagrams, 452–453

Domain Name System (DNS), 3

domain-name command, 353

domains
broadcast domains, 29
collision domains, 29
VTP domains, 169

DR (designated routers), 189, 229–231

DSCP (differentiated service code point), 411–412

DSL (digital subscriber line), 386–387

DTP (Dynamic Trunking Protocol), 61–62

DUAL (Diffusing Update Algorithm), 245–246

dual-homed point-to-point WANs (wide area networks), 381

dual-stacking, 105–106

duplex and speed mismatches, 52–53

duplex auto command, 46

duplex command, 52

duplicate address detection (DAD), 96, 99, 358

duplicate IP addresses, 136

Dynamic Host Configuration Protocol (DHCP), 3

dynamic multipoint VPNs (virtual private networks), 390

dynamic NAT (network address translation)
- configuration, 375–376
- definition of, 371

dynamic routing
- AD (administrative distance), 113–115
- classful routing protocols, 112
- classless routing protocols, 112
- compared to static routing, 109
- distance vector protocols, 111
- EGP (exterior gateway protocols), 110–111
- IGP (interior gateway protocols), 110–111, 115
- link-state routing protocols, 115–116
  - *convergence with, 118–119*
  - *Dijkstra Shortest Path First (SPF) algorithm, 117–118*
  - *LSDB (link-state database), building, 116–117*
  - *overview of, 111*
- metrics, 112–113
- timeline of routing protocols, 110

Dynamic Trunking Protocol (DTP), 61–62

E

eBGP (external BGP)
- configuration, 404–406
- verification, 406–407

edge ports, Rapid PVST+ and, 305–306

EF (Expedited Forwarding), 412–413

EGP (exterior gateway protocols), 110–111

eHWIC (enhanced high-speed WAN interface card) slots, 15

EIA (Electronics Industry Alliance), 34

EIGRP (Enhanced Interior Gateway Routing Protocol)
- administrative distance, 244–245
- composite metric, 244
- convergence, 243
- discontiguous networks, 270–271
- DUAL (Diffusing Update Algorithm), 245–246
- IPv4 implementation
  - *addressing scheme, 249*
  - *automatic summarization, 263–264*
  - *bandwidth utilization, modifying, 266*
  - *default route propagation, 265–266*
  - *hello intervals and hold times, 266–267*
  - *network command, 250*
  - *router IDs, 250–251*
  - *topology, 249–250, 264–265*
  - *verification, 251–255*
- IPv6 implementation
  - *addressing scheme, 257*
  - *bandwidth utilization, modifying, 268–269*
  - *concepts, 255–256*
  - *configuration commands, 257–258*
  - *default route propagation, 267–268*
  - *hello intervals and hold times, 269*
  - *topology, 256, 267*
  - *verification, 258–261*
- message format, 241–243
- overview of, 239
- packet types, 241
- PDMs (protocol-dependent modules), 240
- RTP (Reliable Transport Protocol), 240–241
- troubleshooting commands, 269–270

eigrp router-id command, 250, 257

elasticity (cloud), 418

election, BD/BDR, 229–231

Electronics Industry Alliance (EIA), 34

enable password command, 47, 122

enabling. *See* configuration

encapsulation
- data encapsulation, 12–13
- encapsulation process, 4
- PDUs (protocol data units), 4–5

encapsulation ppp command, 396

enhanced high-speed WAN interface card (eHWIC) slots, 15

Enhanced Interior Gateway Routing Protocol. *See* EIGRP (Enhanced Interior Gateway Routing Protocol)

err-disable state, 288

error detection (PPP), 394

error recovery (TCP), 7–8

EtherChannel
- benefits of, 314
- configuration, 316–317
- implementation restrictions, 314
- LACP (Link Aggregation Control Protocol), 315–316
- operation, 313–314
- overview of, 313
- PAgP (Port Aggregation Protocol), 315
- troubleshooting, 319
- verification, 317–319

Ethernet switching
- asymmetric switching, 30
- benefits of, 35–36
- broadcast domains, 29
- collision domains, 29
- CSMA/CD (Carrier Sense Multiple Access with Collision Detection), 32–33
- Ethernet addressing, 36
- Ethernet standards, 21, 30–31, 33–34
- evolution to, 27–28
- frame formats, 37
- frame forwarding, 29–30
- Layer 2/Layer 3 switching, 30
- legacy Ethernet technologies, 31–33
- memory buffering, 30
- overview of, 4
- physical layer, 38
- switching logic, 28–29
- symmetric switching, 30
- UTP (unshielded twisted pair) cabling, 34–35

EUI-64 concept, 103–104

EXEC sessions, 42

exit command, 46

exit interface parameter (IPv4), 143–144

EXP field (DSCP), 412

Expedited Forwarding (EF), 412–413

extended IPv4 ACLs (access control lists), 332

extended IPv6 ACLs (access control lists), 332, 345

extended named IPv4 ACLs (access control lists), 340

extended system ID, 303

extended VLANs (virtual local-area networks), 66–68

exterior gateway protocols (EGP), 110–111

external BGP. *See* eBGP (external BGP)

F

Fast Ethernet, 34

FC (feasible conditions), 245

FCS (frame check sequence), 61

FD (feasible distance), 245

FDDI (Fiber Distributed Data Interface), 24

feasible conditions (FC), 245

feasible distance (FD), 245

feasible successors (FS), 245

FHRPs (First Hop Redundancy Protocols), 313
- concepts, 319–320
- GLBP (Gateway Load Balancing Protocol), 320
- HSRP (Hot Standby Router Protocol)
  - *configuration, 322*
  - *definition of, 320*
  - *load balancing, 323–325*
  - *operation, 321*
  - *priority and preemption, 322*
  - *troubleshooting, 326*
  - *verification, 322–323*
  - *versions, 321*
- VRRP (Virtual Router Redundancy Protocol), 320

Fiber Distributed Data Interface (FDDI), 24

fiber-optic cable, 19–20

FIFO (first-in, first-out), 409

File Transfer Protocol (FTP), 3

files
- configuration files, 440–442, 451
- IOS images
  - *backing up, 442–443*
  - *licenses, 444–447*
  - *restoring, 443–444*
  - *TFTP topology, 442*

FIN bits, 9

fine-tuning. *See* configuration

finite state machine (FSM), 246

firewalls, 16

First Hop Redundancy Protocols. *See* FHRPs (First Hop Redundancy Protocols)

first-in, first-out (FIFO), 409

flash: alias, 438

flooding LSAs (link-state advertisements), 116–117, 229

flow control (TCP), 8–9

forwarding
- AF (Assured Forwarding), 412–413
- EF (Expedited Forwarding), 412–413
- frame forwarding, 29–30
- packet forwarding, 107–109

fragment-free switching, 30

frame check sequence (FCS), 61

Frame Relay links, 11

frames, 37
- FCS (frame check sequence), 61
- frame forwarding, 29–30
- Frame Relay links, 11
- multiple frame transmission, 297
- PPP (Point-to-Point Protocol), 393–394

frequency command, 460

FS (feasible successors), 245

FSM (finite state machine), 246

FTP (File Transfer Protocol)
- denying, 338
- overview of, 3

full mesh WANs (wide area networks), 381

a-full setting, 53

full-duplex communication, 47

G

Gateway Load Balancing Protocol (GLBP), 320

gateways, default, 136

generic route encapsulation. *See* GRE (generic route encapsulation)

get-bulk-request, 428

get-next-request, 428

get-request, 428

get-response, 428

Gigabit Ethernet, 34

GLBP (Gateway Load Balancing Protocol), 320

global unicast addresses, 92–95

Graziani, Rick, 89, 380

GRE (generic route encapsulation)
- characteristics of, 401
- configuration, 401–402
- troubleshooting, 403
- verification, 403

GRE (generic route encapsulation) tunneling, 401

H

half-duplex communication, 47

hardening, switch port, 291

HDLC frame, 393

headers
- EIGRP (Enhanced Interior Gateway Routing Protocol), 243
- TCP (Transmission Control Protocol), 6

headers (IPv4), 78

hello intervals
- EIGRP (Enhanced Interior Gateway Routing Protocol)
  - *IPv4 implementation, 266–267*
  - *IPv6 implementation, 269*
- OSPFv2, 228
- OSPFv3, 234

Hello packets
- EIGRP (Enhanced Interior Gateway Routing Protocol), 241
- OSPF (Open Shortest Path First), 186

help, 42–43

hierarchical campus network designs, 24–26

hold times (EIGRP)
- IPv4 implementation, 266–267
- IPv6 implementation, 269

hold-down timers, 116

hostname command, 46, 397

hosts, denying, 336, 340

hot keys, 43–44

Hot Standby Router Protocol. *See* HSRP (Hot Standby Router Protocol)

HSRP (Hot Standby Router Protocol)
- configuration, 322
- definition of, 320
- load balancing, 323–325
- operation, 321

overview of, 313
priority and preemption, 322
troubleshooting, 326
verification, 322–323
versions, 321

HTTP (Hypertext Transfer Protocol), 3

hub-and-spoke WANs (wide area networks), 381

hybrid clouds, 419

Hypertext Transfer Protocol (HTTP), 3

I

IaaS (Infrastructure as a Service), 419

IANA (Internet Assigned Numbers Authority), 93

ICMP (Internet Control Message Protocol), 4

icmp-echo command, 460

icons, networking, 23

identification numbers (ACLs), 333

IDS (Intrusion Detection Systems), 16–17

IDs, router, 198–199, 250–251

IEEE 802.1D. ***See*** **STP (Spanning Tree Protocol)**

IEEE 802.1x, 293–294

IETF (Internet Engineering Task Force), 89, 185

IFS (Integrated File System)
commands, 437–440
definition of, 437
URL prefixes, 440

IGP (interior gateway protocols), 110–111, 115, 403

IGRP (Interior Gateway Routing Protocol), 112

images. ***See*** **IOS images**

IMAP (Internet Message Access Protocol), 3

Infrastructure as a Service (IaaS), 419

inside global addresses, 370

inside local addresses, 370

installing licenses, 445–447

Integrated File System. ***See*** **IFS (Integrated File System)**

interface port-channel command, 316

interface range command, 47, 316

interface status codes, 52, 125–126

interface tunnel command, 402

interface vlan command, 181

interfaces
ACLs (access control lists), 329–330
Rapid PVST+, 304

interior gateway protocols (IGP), 110–111, 115, 403

Interior Gateway Routing Protocol (IGRP), 112

Intermediate System-to-Intermediate System (IS-IS), 185

Internet Assigned Numbers Authority (IANA), 93

Internet connections, 386–388

Internet Control Message Protocol (ICMP), 4

Internet Engineering Task Force (IETF), 89, 185

Internet layer (TCP/IP model), 10–11

Internet Message Access Protocol (IMAP), 3

Internet Protocol. ***See*** **IPv4; IPv6**

internetworks, 22

inter-VLAN routing
legacy inter-VLAN routing, 175–176
multilayer switch
configuration, 180–182
overview of, 177
overview of, 175
router on a stick
configuration, 177–179
overview of, 176
verification, 179–180

Intrusion Detection Systems (IDS), 16–17

Intrusion Prevention Systems (IPS), 16–17

IOS images
backing up, 442–443
licenses, 444–447
restoring, 443–444
TFTP topology, 442

ip access-group command, 336

ip access-list extended command, 340

ip access-list standard command, 339

ip address command, 46

ip address dhcp command, 357

ip bandwidth-percent eigrp command, 268

ip default-gateway command, 46

ip dhcp excluded-address command, 352

ip dhcp pool command, 352

ip domain-name command, 277, 295

ip forward-protocol udp command, 357

ip hello-interval eigrp command, 266–267

ip helper-address command, 356–357

ip hold-time eigrp command, 266–267

ip http authentication enable command, 46

ip http server command, 46

ip nat inside command, 374, 375

ip nat inside source list command, 375

ip nat inside source static command, 374

ip nat outside command, 374, 375

ip nat pool name command, 375

ip ospf cost command, 202–203

ip ospf priority command, 229

IP precedence (IPP), 411–412

ip route command, 140

ip routing command, 181

ip sla command, 460

ip sla schedule command, 460

ipconfig command, 49, 355–356

IPP (IP precedence), 411–412

IPS (Intrusion Prevention Systems), 16–17

IPv4. ***See also*** **IPv6; OSPF (Open Shortest Path First)**
- ACLs (access control lists)
  - *comments, 340–341*
  - *compared to IPv6 ACLs, 343*
  - *extended IPv4 ACLs, 332*
  - *extended named IPv4 ACLs, 340*
  - *extended numbered IPv4 ACLs, 337–339*
  - *identification numbers, 333*
  - *list logic with, 330–331*
  - *named IPv4 ACLs, 332*
  - *numbered IPv4 ACLs, 332*
  - *standard IPv4 ACLs, 332*
  - *standard named IPv4 ACLs, 339–340*
  - *standard numbered IPv4 ACLs, 335–337*
  - *verification, 341–343*
- addressing, 77
  - *binary and alphanumeric representations, 90–91*
  - *classes of addresses, 78–80*
  - *embedded addresses, 97*
  - *header format, 78*
  - *IPv4-mapped IPv6 addresses, 97*
  - *private addresses, 81*
  - *public addresses, 81*
  - *subnet masks, 80*
  - *troubleshooting, 136*
- EIGRP (Enhanced Interior Gateway Routing Protocol)
  - *addressing scheme, 249*
  - *automatic summarization, 263–264*
  - *bandwidth utilization, modifying, 266*
  - *default route propagation, 265–266*
  - *hello intervals and hold times, 266–267*
  - *network command, 250*
  - *router IDs, 250–251*
  - *topology, 249–250, 264–265*
  - *verification, 251–255*
- NAT (network address translation), 369–370
  - *benefits of, 373*
  - *concepts, 369–371*
  - *dynamic NAT, 371, 375–376*
  - *example, 371*
  - *limitations of, 373*
  - *overloading, 372–373, 376*
  - *static NAT, 371, 374–375*
  - *troubleshooting, 378–379*
  - *verification, 377*
- router configuration
  - *command syntax, 122*
  - *example of, 122–124*
  - *IP addressing, troubleshooting, 136*
  - *network connectivity, verifying, 133–135*
  - *topology, 121*
  - *verification, 124–129*
- SLA (service level agreement), 459–462
- subnetting
  - *bits borrowed, determining, 81–82*
  - *examples of, 83–85*
  - *overview of, 81*
  - *subnet addressing scheme, 83*
  - *subnet masks, 80, 82*
  - *subnet multiplier, 83*
  - *variable-length subnet masking (VLSM), 85–87*

IPv6. ***See also*** **IPv4; OSPF (Open Shortest Path First)**
ACLs (access control lists), 330–331, 343
extended IPv6 ACLs, 332
named IPv6 ACLs, 332
addressing
anycast addresses, 100
assigned multicast addresses, 98
benefits of, 89–90
binary and alphanumeric representations, 90–91
conventions for writing, 100–102
EUI-64 concept, 103–104
global unicast addresses, 92–95
IPv4 embedded addresses, 97
link-local addresses, 95–96
loopback addresses, 96
prefixes, 101–102
solicited-node multicast addresses, 98–100
stateless address autoconfiguration, 104–105
subnetting, 102–103
troubleshooting, 136
ULAs (unique local addresses), 96–97
unspecified addresses, 96
EIGRP (Enhanced Interior Gateway Routing Protocol)
addressing scheme, 257
bandwidth utilization, modifying, 268–269
concepts, 255–256
configuration commands, 257–258
default route propagation, 267–268
hello intervals and hold times, 269
topology, 256, 267
verification, 258–261
migration to, 105–106
NAT (network address translation)
private address space, 379
purpose of, 379–380
router configuration
command syntax, 130
example of, 130–133
IP addressing, troubleshooting, 136
network connectivity, verifying, 133–135
topology, 130

ipv6 access-class command, 344

ipv6 access-list command, 344

ipv6 address autoconfig command, 362, 363

ipv6 address command, 130

ipv6 address dhcp command, 363

ipv6 eigrp command, 257

IPv6 Fundamentals **(Graziani), 89, 380**

ipv6 hello-interval eigrp command, 269

ipv6 hold-time eigrp command, 269

ipv6 nd command, 359–360

ipv6 route command, 149

ipv6 router eigrp command, 257

ipv6 router ospf command, 208

ipv6 traffic-filter command, 344

ipv6 unicast-routing command, 98, 130, 257, 361

IS-IS (Intermediate System-to-Intermediate System), 185

J-K

jitter, 409

keywords. ***See also*** **commands**
deny, 338
overload, 376
permit, 338, 345
primary, 308
secondary, 308

L

LACP (Link Aggregation Control Protocol), 315–316

LANs (local-area networks), 22
device connection guidelines, 21
ports
security configuration, 285–287
switch port hardening, 291
violation verification and restoration, 287–289
SSH (Secure Shell) configuration, 294–295
threat mitigation
802.1x, 293–294
Authentication, Authorization, and Accounting (AAA) framework, 292
DHCP snooping, 289–290
native and management VLAN modification, 290–291
switch port hardening, 291
WLANs (wireless LANs), 17

large link-state database (LSDB), 192

latency, 409

Layer 1 problems on "up" interfaces, troubleshooting, 54

Layer 2 protocols
CDP (Cisco Discovery Protocol)
configuration, 274–276
disabling, 275–276
overview of, 273–274
verification, 277–279
LLDP (Link Layer Discovery Protocol)
configuration, 280–281
overview of, 279–280
verification, 281–283

Layer 2 switching, 30

Layer 3 routed ports, 182

Layer 3 switching, 30

LCP (Link Control Protocol), 394–396

lease command, 353

leased lines, 383–384

legacy Ethernet technologies, 31–33

legacy inter-VLAN routing, 175–176

license install command, 445–447

license save command, 447

licenses, 444–447
backing up, 447
installing, 445–447
licensing process, 444–445
uninstalling, 447
verification, 445–447

Lightweight Access Point Protocol (LWAPP), 19

line console command, 46

Link Aggregation Control Protocol (LACP), 315–316

Link Control Protocol (LCP), 394–396

Link Layer Discovery Protocol. *See* LLDP (Link Layer Discovery Protocol)

Link Quality Monitoring (LQM), 395

link-local addresses, 95–96

link-state acknowledgment (LSAck) packets, 186

link-state advertisements (LSA), 116, 188, 229

link-state database (LSDB), building, 116–117

link-state request (LSR) packets, 186

link-state routing protocols, 115–116, 190–191
convergence with, 118–119
Dijkstra Shortest Path First (SPF) algorithm, 117–118
LSDB (link-state database), building, 116–117
overview of, 111

link-state update (LSU) packets, 186

list logic (IP ACLs), 330–331

LLC (Logical Link Control) sublayer, 31

LLDP (Link Layer Discovery Protocol)
configuration, 280–281
overview of, 279–280
verification, 281–283

lldp holdtime command, 280

lldp reinit command, 280

lldp run command, 280

lldp timer command, 280

LLQ (Low Latency Queueing), 413

load balancing, 323–325

local area network security. *See* LANs (local-area networks)

logging buffered command, 434

logging console command, 434

logging source-interface command, 435

logging trap command, 435

logic
list logic (IP ACLs), 330–331
switching logic, 28–29

Logical Link Control (LLC) sublayer, 31

logical network topologies, 23–24

login command, 46

Long-Term Evolution (LTE), 388

loopback addresses, 96

looped-link detection, 394

loops, routing loop prevention, 115–116

loss, 409

Low Latency Queueing (LLQ), 413

LQM (Link Quality Monitoring), 395

LSA (link-state advertisements), 116, 188, 229

LSAck (link-state acknowledgment) packets, 186

LSDB (link-state database), 116–117, 192

LSR (link-state request) packets, 186

LSU (link-state update) packets, 186

LTE (Long-Term Evolution), 388

LWAPP (Lightweight Access Point Protocol), 19

M

MAC (Media Access Control), 11, 28, 31

Management Information Base (MIB), 428–429

management planes, 420

management VLANs (virtual local-area networks), 59, 290–291

marking
- AF (Assured Forwarding), 412–413
- definition of, 410–411
- DSCP (differentiated service code point), 411–412
- EF (Expedited Forwarding), 412–413
- IPP (IP precedence), 411–412

masks, subnet, 80, 82, 85–87

maximum transmission unit (MTU), 400

mdix auto command, 46

media (network), 19–21

Media Access Control (MAC), 11, 28, 31

media issues, troubleshooting, 51

memory buffering, 30

message format
- EIGRP (Enhanced Interior Gateway Routing Protocol)
  - *message format, 241–243*
  - *packet types, 241–243*
- OSPF (Open Shortest Path First), 185
- SNMP (Simple Network Management Protocol), 427–428
- Syslog, 433

message-of-the-day (MOTD) banner, 123

methods, troubleshooting, 454–455

metrics
- dynamic routing, 112–113
- OSPF (Open Shortest Path First), 200–203

MetroE (Metro Ethernet), 385

MIB (Management Information Base), 428–429

migration to IPv6, 105–106

models. ***See*** **networking models**

modes (VTP), 170–171

modifying
- CLI (command-line interface) shortcuts, 43–44
- EIGRP (Enhanced Interior Gateway Routing Protocol) bandwidth usage
  - *for IPv4, 266*
  - *for IPv6, 268–269*
- hello intervals (EIGRP)
  - *IPv4 implementation, 266–267*
  - *IPv6 implementation, 269*
- hold times (EIGRP)
  - *IPv4 implementation, 266–267*
  - *IPv6 implementation, 269*
- OSPFv2
  - *BD/BDR election, 228–229*
  - *dead intervals, 228*
  - *default route redistribution, 227*
  - *hello intervals, 228*
  - *network types, 228–229*
- OSPFv3
  - *dead intervals, 234*
  - *default route propagation, 233–234*
  - *hello intervals, 234*
  - *timers, 234–235*

MOTD (message-of-the-day) banner, 123

MPLS (Multiprotocol Label Switching), 11, 36, 386

MSTP (Multiple Spanning Tree Protocol), 301

MTU (maximum transmission unit), 400

multiarea OSPF (Open Shortest Path First)
- multiarea OSPFv2 implementation
  - *addressing scheme, 216*
  - *configuration, 216*
  - *topology, 215*
  - *verification, 216–218*
- multiarea OSPFv3 implementation
  - *addressing scheme, 219*
  - *configuration, 220*
  - *topology, 218–219*
  - *verification, 220–223*
- operation
  - *multiarea design, 192–194*
  - *overview of, 192*
  - *performance of, 194*

multicast addresses (IPv6), 36
- anycast addresses, 100
- assigned multicast addresses, 98
- definition of, 98
- solicited-node multicast addresses, 98–100

multilayer switch inter-VLAN routing
- configuration
  - *Layer 3 routed ports, 182*
  - *SVIs (switch virtual interfaces), 180–181*
- overview of, 177

multilink PPP (Point-to-Point Protocol), 394

multiple frame transmission, 297

Multiple Spanning Tree Protocol (MSTP), 301

Multiprotocol Label Switching (MPLS), 11, 36, 386

municipal Wi-Fi, 388

MX record (DNS), 365

N

named ACLs (access control lists), 343–344
- IPv4, 332
  - *extended named IPv4 ACLs, 340*
  - *standard named IPv4 ACLs, 339–340*
- IPv6, 332

NAT (network address translation)
- benefits of, 373
- concepts, 369–371
- dynamic NAT
  - *configuration, 375–376*
  - *definition of, 371*
- example, 371
- limitations of, 373
- NAT for IPv6
  - *private address space, 379*
  - *purpose of, 379–380*
- NAT64, 97
- NAT-PT, 97
- overloading
  - *configuration, 376*
  - *definition of, 372–373*
- static NAT
  - *configuration, 374–375*
  - *definition of, 371*
- topology, 369–370
- troubleshooting, 378–379
- verification, 377

National Institute of Standards and Technology (NIST), 418

native VLANs (virtual local-area networks), 59, 290–291

navigating CLI (command-line interface), 43–44

NBI (northbound interface), 421

NBMA (nonbroadcast multiaccess) networks, 228

NDP (Neighbor Discovery Protocol), 98, 359

neighbor command, 405–406

Neighbor Discovery Protocol (NDP), 98, 359

neighbor establishment, 186–188. *See also* discovery

Neighbor Solicitation (NS) message, 358

neighbor tables (EIGRP)
- IPv4, 252–253
- IPv6, 259–260

netbios-name-server command, 353

NetConf, 422

network access layer (TCP/IP model), 11–12

network address translation. *See* NAT (network address translation)

network command, 199–200, 250, 353, 406

network connectivity, verifying, 48–51, 133–135

network interface cards (NIC), 47

network layer
- overview of, 2
- troubleshooting, 456

network management system (NMS), 427

Network Time Protocol (NTP), 436–437

networking models
- OSI (Open Systems Interconnection), 1–3
- overview of, 1
- TCP/IP (Transmission Control Protocol/Internet Protocol)
  - *application layer, 5*
  - *overview of, 1–3*
  - *PDUs (protocol data units), 4–5*
  - *transport layer, 5–10*

networks. ***See also*** **LANs (local-area networks); networking models; WANs (wide area networks)**
- APs (access points), 17–19
- data encapsulation, 12–13
- discontiguous networks (EIGRP), 270–271
- firewalls, 16
- hierarchical campus designs, 24–26
- IDS (Intrusion Detection Systems), 16–17
- internetworks, 22
- IPS (Intrusion Prevention Systems), 16–17
- media, 19–21
- network connectivity, verifying, 48–51
- networking icons, 23
- permitting specific, 335–336
- physical layer, 19
- routers, 15
- SDN (software-defined networking)
  - *control planes, 419–420*
  - *controllers, 421*
  - *data planes, 419–420*
  - *examples, 421–424*
  - *management planes, 420*
  - *overview of, 419*
- SOHO (small offices or home offices), 22
- switches, 13–14
- topologies, 23–24
- types of, 228–229
- virtual network infrastructure, 419
- VLANs (virtual local-area networks)
  - *concepts, 57–58*
  - *configuration, 62–64*
  - *enabling/disabling, 72–73*
  - *extended VLANs, 66–68*
  - *native and management VLAN modification, 290–291*
  - *traffic types, 58*
  - *troubleshooting, 71–72*
  - *trunking, 60–62, 68–70, 73–75*
  - *types of, 59*
  - *verification, 64–66*
  - *voice VLAN example, 59–60*
- WLANs (wireless LANs), 17

next-hop parameter (IPv4), 142–143

NICs (network interface cards), 47

NIST (National Institute of Standards and Technology), 418

NMS (network management system), 427

no cdp enable command, 275–276

no cdp run command, 273

no debug ip rip command, 161

no lldp receive command, 280

no lldp transmit command, 280

no service dhcp command, 354

no shutdown command, 257, 275, 291

no switchport command, 182

noise, troubleshooting, 54

nonbroadcast multiaccess (NBMA) networks, 228

northbound interface (NBI), 421

NS (Neighbor Solicitation) message, 358

NS record (DNS), 365

NTP (Network Time Protocol), 436–437

ntp server command, 436

numbered IPv4 ACLs, 332

O

object IDs (OIDs), 428

Odom, Wendell, 404, 421

OIDs (object IDs), 428

On mode
- LACP (Link Aggregation Control Protocol), 316
- PAgP (Port Aggregation Protocol), 315

ONF (Open Networking Foundation), 421–422

Opcode field (EIGRP), 243

Open Networking Foundation (ONF), 421–422

Open SDN Controller (OSC), 422

Open Systems Interconnection (OSI) model, 1–3

OpenDaylight, 421

OpenFlow, 421–422

OpFlex, 423

OSC (Open SDN Controller), 422

OSI (Open Systems Interconnection) model, 1–3

OSPF (Open Shortest Path First), 182
- algorithm, 189–190
- BDR (backup designated routers), 189

DR (designated routers), 189
link-state advertisements, 188
link-state routing process, 190–191
message format, 185
multiarea operation
multiarea design, 192–194
overview of, 192
performance of, 194
multiarea OSPFv2
addressing scheme, 216
configuration, 216
topology, 215
verification, 216–218
multiarea OSPFv3
addressing scheme, 219
configuration, 220
topology, 218–219
verification, 220–223
neighbor establishment, 186–188
OSPFv2 configuration
addressing scheme, 226
BD/BDR election, 229–231
compared to OSPFv3, 191–192
dead intervals, 228
default route redistribution, 227
example of, 225–227
hello intervals, 228
network types, 228–229
topology, 225
OSPFv3 configuration
addressing scheme, 232
compared to OSPFv2, 191–192
dead intervals, 234
default route propagation, 233–234
example of, 231–233
hello intervals, 234
timers, 234–235
topology, 231
packet types, 186
single-area operation, 185
single-area OSPFv2
addressing scheme, 197
configuration, 197–203
OSPF metric, 200–203
passive interfaces, 200
router IDs, 198–199
topology, 197–198
verification, 203–206
single-area OSPFv3
configuration, 206–209
verification, 209–212
troubleshooting, 235
adjacency, 236
states, 235
troubleshooting commands, 236–237

outside global addresses, 370

outside local addresses, 370

overload keyword, 376

overloading NAT (network address translation)
configuration, 376
definition of, 372–373

P

PaaS (Platform as a Service), 418

packets
CDP (Cisco Discovery Protocol), verifying, 279
DHCPACK, 351
DHCPDISCOVER, 351
DHCPNAK, 351
DHCPOFFER, 351
DHCPREQUEST, 351
EIGRP (Enhanced Interior Gateway Routing Protocol), 241
forwarding, 107–109
path determination, 108–109
switching functions, 108–109
topology, 108
OSPF (Open Shortest Path First), 186

packet-switched connections, 385–386

PAgP (Port Aggregation Protocol), 315

PAP (Password Authentication Protocol), 398

PAR (positive acknowledgment with retransmission), 8

passive interfaces
RIPv1 (Routing Information Protocol version 1), 161–162
single-area OSPFv2, 200

Passive mode (LACP), 316

passive-interface command, 161–162, 208

Password Authentication Protocol (PAP), 398

password command, 46

passwords
recovery, 448
VTP (VLAN Trunking Protocol), 170

PAT (Port Address Translation), 372–373

path determination, 108–109

PDMs (protocol-dependent modules), 240

PDUs (protocol data units), 4–5

performance, multiarea OSPF (Open Shortest Path First) operation, 194

permit statement, 338, 345

physical layer, 19
- overview of, 2
- role of, 38
- troubleshooting, 455–456

physical network topologies, 23–24

pi rule, 92

ping command, 48–50, 133

planes (network), 419–420

planning for ACLs (access control lists), 331

Platform as a Service (PaaS), 418

point-to-multipoint networks, 228

Point-to-Point Protocol. *See* PPP (Point-to-Point Protocol)

point-to-point WANs (wide area networks), 228, 381

poison reverse, 116

policing, 413–415

POP3 (Post Office Protocol), 3

Port Address Translation (PAT), 372–373

Port Aggregation Protocol (PAgP), 315

PortFast, 309

ports
- Layer 3 routed ports, 182
- PAgP (Port Aggregation Protocol), 315
- port numbers, 7
- port speed, 47
- PVST+ port states, 302
- Rapid PVST+
  - *edge ports, 305–306*
  - *port roles, 305*
  - *port states, 304*
- security
  - *configuration, 285–287*
  - *switch port hardening, 291*
  - *violation verification and restoration, 287–289*
- speed, 47
- verification, 364

positive acknowledgment, 7

positive acknowledgment with retransmission (PAR), 8

Post Office Protocol (POP3), 3

PPP (Point-to-Point Protocol), 11. *See also* PPPoE (PPP over Ethernet)
- CHAP (Challenge Handshake Authentication Protocol), 397–398
- concepts, 393
- configuration, 396–397
- frame format, 393–394
- LCP (Link Control Protocol), 394–396
- PAP (Password Authentication Protocol), 398
- topology, 396
- troubleshooting, 398

ppp authentication chap command, 397, 398

ppp authentication pap command, 398

PPPoE (PPP over Ethernet)
- concepts, 399
- configuration, 399–400
- troubleshooting, 400–401

pppoe enable command, 400

preemption (HSRP), 322

prefixes (IPv6), 101–102

presentation layer (OSI model), 2

preventing routing loops, 115–116

PRI (Primary Rate Interface), 384

primary keyword, 308

Primary Rate Interface (PRI), 384

priority (HSRP), 322

private address space (IPv6), 379

private clouds, 419

private IPv4 addresses, 81

processes (EIGRP)
- administrative distance, 244–245
- composite metric, 244
- convergence, 243
- DUAL (Diffusing Update Algorithm), 245–246

processing interface ACLs (access control lists), 329–330

protocol data units (PDUs), 4–5

protocol-dependent modules (PDMs), 240

Pseudo-Random Global ID Algorithm, 96

public clouds, 419

public IPv4 addresses, 81

PVST+
- definition of, 301
- extended system ID, 303
- features of, 301
- operation, 301–302
- port states, 302
- Rapid PVST+
  - *configuration, 309*
  - *definition of, 301*
  - *features of, 301*

Q

QoS (Quality of Service), 409–410
- classification and marking
  - *AF (Assured Forwarding), 412–413*
  - *definition of, 410–411*
  - *DSCP (differentiated service code point), 411–412*
  - *EF (Expedited Forwarding), 412–413*
  - *IPP (IP precedence), 411–412*
- congestion management, 413
- overview of, 409–410
- policing, 413–415
- shaping, 413–415
- TCP discards, 415

Query packets (EIGRP), 241

R

RA (Router Advertisement) message, 358

RADIUS (Remote Authentication Dial-In User Service), 292

range command, 65

Rapid PVST+
- configuration, 309
- definition of, 301
- edge ports, 305–306
- features of, 301
- interface behavior, 304
- operation, 303–304
- port roles, 305
- port states, 304

Rapid STP (RSTP)
- definition of, 301
- features of, 301

rate limiting, 290

RD (reported distance), 245

records (DNS), 365

recovery, password, 448

redistribute static command, 265, 267

redistribution, OSPFv2 default routes, 227

reference bandwidth, 200–203

Regional Internet Registries (RIR), 93

reliability, 7

Reliable Transport Protocol (RTP), 240–241

remark keyword, 340

remote access with SSH (Secure Shell), 134–135

Remote Authentication Dial-In User Service (RADIUS), 292

remote terminal, 41

remote-access VPNs (virtual private networks), 389

Reply packets (EIGRP), 241

reported distance (RD), 245

Request messages
- DHCP (Dynamic Host Configuration Protocol), 356–357
- RIPv1 (Routing Information Protocol version 1), 156

reset command, 448

resolving address conflicts, 363–364

resource pooling, 418

restoring
- IOS images, 443–444
- ports, 287–289

retransmission timeout (RTO), 253

RFC 2328, 185

RIPv1 (Routing Information Protocol version 1)
- automatic summarization, 162–164
- configuration, 156–157
- default routing, 164–165
- operation, 156
- passive interfaces, 161–162
- troubleshooting, 158–161
- verification, 158–161

RIPv2 (Routing Information Protocol version 2)
- automatic summarization, 167
- configuration, 165–167
- troubleshooting, 167–168
- verification, 167–168

RIR (Regional Internet Registries), 93

roles, Rapid PVST+ ports and, 305

route poisoning, 116

Router Advertisement (RA) message, 358

router bgp command, 405

router configuration, 15. *See also* routing

DHCPv4 clients, 357–358

DHCPv4 servers, 352–356

IP addressing, troubleshooting, 136

IP SLA (service level agreement), 459–462

with IPv4

command syntax, 122

example of, 122–124

network connectivity, verifying, 133–135

topology, 121

verification, 124–129

with IPv6

command syntax, 130

example of, 130–133

network connectivity, verifying, 133–135

topology, 130

to relay DHCPv4 requests, 356–357

router IDs, 198–199, 250–251

router on a stick

configuration, 177–179

overview of, 176

verification, 179–180

router on a stick

configuration, 177–179

overview of, 176

verification, 179–180

router ospf command, 198

router rip command, 163

Router Solicitation (RS) message, 358

router-id command, 198–199, 208

routing. *See also* EIGRP (Enhanced Interior Gateway Routing Protocol); OSPF (Open Shortest Path First); router configuration

directly connected routes, 109

dynamic routing

AD (administrative distance), 113–115

classful routing protocols, 112

classless routing protocols, 112

compared to static routing, 109

distance vector protocols, 111

EGP (exterior gateway protocols), 110–111

IGP (interior gateway protocols), 110–111, 115

link-state routing protocols, 111, 115–119

metrics, 112–113

timeline of routing protocols, 110

inter-VLAN routing

legacy inter-VLAN routing, 175–176

multilayer switch, 177, 180–182

overview of, 175

router on a stick, 176, 177–180

IPv4 default route configuration, 144–146

IPv4 static route configuration

addressing scheme, 141

example of, 141–142

exit interface parameter, 143–144

ip route command, 140

next-hop parameter, 142–143

summary route configuration, 147–148

topology, 140–141

IPv6 default route configuration, 150–151

IPv6 static route configuration

addressing scheme, 148–149

ipv6 route command, 149

show ipv6 route command, 149–150

summary route configuration, 151–152

topology, 148

packet forwarding, 107–109

path determination, 108–109

RIPv1 (Routing Information Protocol version 1)

automatic summarization, 162–164

configuration, 156–157

default routing, 164–165

operation, 156

passive interfaces, 161–162

troubleshooting, 158–161

verification, 158–161

RIPv2 (Routing Information Protocol version 2)

automatic summarization, 167

configuration, 165–167

troubleshooting, 167–168

verification, 167–168

routing loop prevention, 115–116

routing tables

EIGRP for IPv4, 255

EIGRP for IPv6, 260–261

static routing, 109

switching functions, 108–109

VTP (VLAN Trunking Protocol)
concepts, 169–171
configuration, 170–173
verification, 173–175

RS (Router Solicitation) message, 358

RSTP (Rapid STP)
definition of, 301
features of, 301

RTO (retransmission timeout), 253

RTP (Reliable Transport Protocol), 240–241

S

SaaS (Software as a Service), 418

satellite Internet, 388

SBI (southbound interface), 421

SDN (software-defined networking)
control planes, 419–420
controllers, 421
data planes, 419–420
examples, 421–424
Cisco ACI (Application Centric Infrastructures), 422–423
Cisco APIC-EM (Application Policy Infrastructure Controller Enterprise Module), 423–425
Open SDN and OpenFlow, 421–422
management planes, 420
overview of, 419

secondary keyword, 308

Secure Shell (SSH)
configuration, 294–295
remote access with, 134–135

security
ACLs (access control lists)
defining, 329
design guidelines, 333–334
identification numbers, 333
interface processing ACLs, 329–330
IP ACLs, list logic with, 330–331
operation, 329
planning for, 331
types of, 332
firewalls, 16
IDS (Intrusion Detection Systems), 16–17
IPS (Intrusion Prevention Systems), 16–17
password recovery, 448
ports
configuration, 285–287
switch port hardening, 291
violation verification and restoration, 287–289
SSH (Secure Shell) configuration, 294–295
threat mitigation
802.1x, 293–294
Authentication, Authorization, and Accounting (AAA) framework, 292
DHCP snooping, 289–290
native and management VLAN modification, 290–291
switch port hardening, 291

Sequence field (TCP), 7

servers
authentication servers, 293
DHCPv4 servers, 352–356
virtualization, 416–418

service password-encryption command, 47

service sequence-numbers command, 433

service timestamps command, 433

service-password encryption command, 123

services, cloud computing, 418–419

session layer (OSI model), 2

set-request, 428

severity levels (Syslog), 432

shaping, 413–415

shortcut keys, 43–44

Shortest Path First (SPF) algorithm, 117–118

show access-lists command, 341, 346–347

show cdp command, 275

show cdp interface command, 274

show cdp neighbors command, 275

show cdp neighbors detail command, 278–279

show cdp traffic command, 279

show command, 44–45

show etherchannel summary command, 318

show file systems command, 437–438
show flash command, 438–439, 443
show history command, 44
show interface command, 126–129
show interface switchport command, 318–319
show interface Tunnel command, 403
show interfaces command, 52–53, 65–66, 397
show interfaces status command, 52–53
show interfaces switchport command, 71, 74
show interfaces trunk command, 69, 73–74
show ip bgp command, 406–407
show ip bgp summary command, 406–407
show ip dhcp binding command, 354
show ip dhcp conflict command, 364
show ip dhcp server statistics command, 354
show ip eigrp interface command, 269
show ip eigrp interfaces commands, 270
show ip eigrp neighbors command, 252–253
show ip eigrp neighbors commands, 269
show ip eigrp topology all-links command, 254
show ip eigrp topology command, 253
show ip interface brief command, 125, 179–180, 203–204, 270, 274, 403, 448
show ip interface command, 341–342
show ip nat statistics command, 377
show ip nat translations command, 377, 378
show ip ospf command, 198, 205–206, 236
show ip ospf database command, 218
show ip ospf interface brief command, 206, 217
show ip ospf interface command, 236
show ip ospf interfaces command, 198
show ip ospf neighbor command, 204–205, 236
show ip protocols command, 114, 159–160, 167, 198, 203–204, 217, 236, 251–252, 269, 270
show ip route command, 112–113, 124, 141–146, 158–159, 179–180, 182, 203–204, 406–407
show ip route eigrp command, 255, 265, 269
show ip route ospf command, 217, 236
show ip sla configuration command, 461
show ip sla statics command, 462
show ip ssh command, 294–295
show ipv6 access-list command, 347
show ipv6 eigrp interface command, 270
show ipv6 eigrp neighbors command, 259–260, 270
show ipv6 interface, 362
show ipv6 interface brief command, 131–132
show ipv6 interface command, 132–133, 347–348
show ipv6 ospf command, 209–210
show ipv6 ospf database command, 211, 221–223
show ipv6 ospf interface brief command, 211, 221
show ipv6 ospf interface command, 210
show ipv6 ospf neighbor command, 211
show ipv6 ospf neighbors command, 233
show ipv6 protocols command, 210, 220, 258, 270
show ipv6 route command, 149–150, 268
show ipv6 route eigrp command, 260–261, 270
show ipv6 route ospf command, 212, 221, 233
show license feature command, 444
show license udi command, 445
show lldp interface command, 281
show lldp neighbors command, 282

show lldp neighbors detail command, 282–283

show lldp traffic command, 283

show logging command, 434, 435–436

show mac address-table command, 71

show ntp associations command, 437

show ntp status command, 437

show port-security command, 286–287

show port-security interface command, 286–287

show run command, 68, 317, 346, 377

show running-config command, 124, 342–343

show snmp command, 430–431

show snmp community command, 431

show spanning-tree active command, 310

show spanning-tree brief command, 310

show spanning-tree command, 308, 310

show spanning-tree detail command, 310

show spanning-tree interface command, 310

show spanning-tree summary command, 310

show spanning-tree vlan command, 310

show standby brief command, 322–325

show standby command, 322–323

show version command, 442, 448

show vlan brief command, 63, 65

show vlan command, 71–72

show vlans command, 179–180

show vtp password command, 173

show vtp status command, 172, 173–175

Simple Mail Transfer Protocol (SMTP), 3

Simple Network Management Protocol (SNMP), 3

single-area OSPF (Open Shortest Path First)
- neighbor establishment, 186–188
- operation, 185
- single-area OSPFv2
  - *addressing scheme, 197*
  - *configuration, 197–203*
  - *OSPF metric, 200–203*
  - *passive interfaces, 200*
  - *router IDs, 198–199*
  - *topology, 197–198*
  - *verification, 203–206*
- single-area OSPFv3
  - *configuration, 206–209*
  - *verification, 209–212*

site-to-site VPNs (virtual private networks), 389

SLAAC (stateless address autoconfiguration), 104–105, 358–360

small offices or home offices (SOHO), 22

smooth round trip timer (SRTT), 253

SMTP (Simple Mail Transfer Protocol), 3

SNMP (Simple Network Management Protocol), 3
- components, 427
- configuration, 430
- messages, 427–428
- MIB (Management Information Base), 428–429
- operation, 427
- verification, 430–431
- versions, 428

snmpget command, 429

snmp-server community command, 430

snmp-server contact command, 430

snmp-server location command, 430

snooping (DHCP), 289–290

Software as a Service (SaaS), 418

software-defined networking. *See* SDN (software-defined networking)

SOHO (small offices or home offices), 22

solicited-node multicast addresses, 98–100

southbound interface (SBI), 421

Spanning Tree Protocol. *See* STP (Spanning Tree Protocol)

spanning-tree bpduguard default command, 309

spanning-tree link-type point-to-point command, 309

spanning-tree mode rapid-pvst command, 309

spanning-tree portfast default command, 309

spanning-tree vlan command, 307–308

speed
- duplex and speed mismatches, 52–53
- port speed, 47

speed auto command, 46

speed command, 52

SPF (Shortest Path First) algorithm, 117–118

split horizon, 116

SRTT (smooth round trip timer), 253

SSH (Secure Shell)
- allowing, 344–345
- configuration, 294–295
- denying, 337
- remote access with, 134–135

ssh command, 134–135

stacking switches, 310–312

standard IPv4 ACLs (access control lists), 332

standard IPv6 ACLs (access control lists), 344–345

standard named IPv4 ACLs (access control lists), 339–340

standard numbered IPv4 ACLs (access control lists), 335–337

standards
- Ethernet, 21, 30–31, 33–34
- network media, 19–21

standby preempt command, 322

standby priority command, 322

stateful DHCPv6, 360–361, 363

stateless address autoconfiguration (SLAAC), 104–105, 358–360

stateless DHCPv6, 360–362

states
- OSPF (Open Shortest Path First), 235
- port states
  - *PVST+, 302*
  - *RSTP (Rapid STP), 304*

static NAT (network address translation)
- configuration, 374–375
- definition of, 371

static routing, 109
- IPv4 static route configuration
  - *addressing scheme, 141*
  - *example of, 141–142*
  - *exit interface parameter, 143–144*
  - *ip route command, 140*
  - *next-hop parameter, 142–143*
  - *summary route configuration, 147–148*
  - *topology, 140–141*
- IPv6 static route configuration
  - *addressing scheme, 148–149*
  - *ipv6 route command, 149*
  - *show ipv6 route command, 149–150*
  - *summary route configuration, 151–152*
  - *topology, 148*
- overview of, 139–140

status codes (interface), 52, 125–126

store-and-forward switching, 29

STP (Spanning Tree Protocol)
- algorithm, 298–299
- configuration, 306–307
  - *BID (bridge ID), 307–309*
  - *BPDU guard, 309*
  - *PortFast, 309*
  - *Rapid PVST+, 309*
- convergence, 299–300
- MSTP (Multiple Spanning Tree Protocol), 301
- overview of, 297
- PVST+
  - *definition of, 301*
  - *extended system ID, 303*
  - *features of, 301*
  - *operation, 301–302*
  - *port states, 302*
- Rapid PVST+
  - *configuration, 309*
  - *definition of, 301*
  - *edge ports, 305–306*
  - *features of, 301*
  - *interface behavior, 304*
  - *operation, 303–304*
  - *port roles, 305*
  - *port states, 304*
- RSTP (Rapid STP)
  - *definition of, 301*
  - *features of, 301*
- switch stacking, 310–312
- verification, 310

subconfiguration modes, 45

subnet addressing scheme, 83

subnet masks, 80, 82, 85–87

subnet multiplier, determining, 83

subnets, denying, 337

subnetting

IPv4

bits borrowed, determining, 81–82

examples of, 83–85

overview of, 81

subnet addressing scheme, 83

subnet masks, 80, 82

subnet multiplier, 83

variable-length subnet masking (VLSM), 85–87

IPv6, 102–103

successors, 245

summarization, automatic. *See* automatic summarization

summary route configuration

IPv4, 147–148

IPv6, 151–152

SVIs (switch virtual interfaces), 180–181

switches, 13, 221–223

access layer switches, 14

configuration

auto-MDIX, 48

basic switch configuration commands, 46–47

Cisco devices, connecting to, 41

CLI EXEC sessions, 42

CLI navigation and editing shortcuts, 43–44

command history, 44

full-duplex communication, 47

half-duplex communication, 47

help facility, 42–43

IOS examination commands, 44

network connectivity, verifying, 48–51

port speed, 47

subconfiguration modes, 45

troubleshooting, 51–54

core layer switches, 14

distribution layer switches, 14

Ethernet switching

asymmetric switching, 30

benefits of, 35–36

broadcast domains, 29

collision domains, 29

CSMA/CD (Carrier Sense Multiple Access with Collision Detection), 32–33

Ethernet addressing, 36

Ethernet standards, 21, 30–31, 33–34

evolution to, 27–28

frame formats, 37

frame forwarding, 29–30

Layer 2/Layer 3 switching, 30

legacy Ethernet technologies, 31–33

memory buffering, 30

overview of, 4

physical layer, 38

switching logic, 28–29

symmetric switching, 30

UTP (unshielded twisted pair) cabling, 34–35

multilayer switch

configuration, 180–182

overview of, 177

switch forwarding, 29–30

switch port hardening, 291

switch stacking, 310–312

switching, Ethernet. *See* Ethernet switching

switchport access vlan command, 46, 71, 291

switchport mode access command, 46, 285

switchport mode dynamic auto command, 74

switchport mode dynamic desirable command, 62

switchport mode trunk command, 62

switchport mode trunk dynamic auto command, 62

switchport nonegotiate command, 62

switchport port-security command, 285

switchport port-security mac-address command, 286

switchport port-security mac-address sticky command, 286

switchport port-security maximum command, 285

switchport port-security violation command, 285

switchport trunk native vlan command, 291

symmetric switching, 30

Syslog

configuration, 434–435

definition of, 432

operation, 432–433

verification, 435–436

T

tables (EIGRP)
- neighbor tables, 252–253, 259–260
- routing tables, 255, 260–261
- topology tables, 253–255

TACACS+ (Terminal Access Controller Access-Control System Plus), 292

tag protocol ID (TPID), 61

TCP (Transmission Control Protocol)
- connection establishment and termination, 9
- definition of, 3
- error recovery, 7–8
- flow control, 8–9
- headers, 6
- port numbers, 7
- QoS (Quality of Service), 415
- windowing, 8–9

TCP/IP (Transmission Control Protocol/Internet Protocol) model
- application layer, 5
- Internet layer, 10–11
- network access layer, 11–12
- overview of, 1–3
- PDUs (protocol data units), 4–5
- transport layer
  - *overview of, 5–6*
  - *TCP (Transmission Control Protocol), 6–9*
  - *UDP (User Datagram Protocol), 10*

Telecommunications Industry Association (TIA), 34

Telnet
- denying, 337, 338–339
- overview of, 3

Terminal Access Controller Access-Control System Plus (TACACS+), 292

terminal history command, 44

terminal no history command, 44

terminating TCP connections, 9

testing DHCPv4 operation, 364

TFTP (Trivial File Transfer Protocol)
- location, specifying, 440
- topology, 442

threat mitigation
- 802.1x, 293–294
- Authentication, Authorization, and Accounting (AAA) framework, 292
- DHCP snooping, 289–290
- native and management VLAN modification, 290–291
- switch port hardening, 291

three-tiered campus design, 24–26

TIA (Telecommunications Industry Association), 34

TID (Traffic Identifier) field, 412

Time to Live (TTL) field, 116

timeline of routing protocols, 110

timers (OSPFv3), 234–235

TLV field (EIGRP), 242

Token Ring, 24

top of rack (ToR) switches, 417

topology
- data centers, 417–418
- EIGRP (Enhanced Interior Gateway Routing Protocol), 253–255
  - *for IPv4, 249–250, 264–265*
  - *for IPv6, 256, 267*
- IPv4 static routing, 140–141
- IPv6 static routing, 148
- multiarea OSPFv2 implementation, 215
- multiarea OSPFv3 implementation, 218–219
- NAT (network address translation), 369–370
- network topologies, 23–24
- OSPF (Open Shortest Path First), 197–198
  - *OSPFv2, 225*
  - *OSPFv3, 231*
- packet forwarding, 108
- PPP (Point-to-Point Protocol), 396
- router configuration
  - *with IPv4, 121*
  - *with IPv6, 130*
- TFTP, 442
- topology diagrams, 452–453
- VTP (VLAN Trunking Protocol), 171
- WANs (wide area networks), 381–382

ToR (top of rack) switches, 417

TPID (tag protocol ID), 61

traceroute command, 134

tracert command, 50

Traffic Identifier (TID) field, 412

traffic types, 58, 409–410

Transmission Control Protocol/Internet

Protocol. *See* TCP/IP (Transmission Control Protocol/Internet Protocol) model

transport layer
- TCP/IP model
  - *overview of, 5–6*
  - *TCP (Transmission Control Protocol), 6–9*
  - *UDP (User Datagram Protocol), 10*
- troubleshooting, 457–458

transport layer (OSI model), 2

triggered updates, 116

Trivial File Transfer Protocol. *See* TFTP (Trivial File Transfer Protocol)

troubleshooting
- application layer, 458
- bottom-up, 459
- data link layer, 456
- DHCP (Dynamic Host Configuration Protocol), 363–364
- DNS (Domain Name System), 366
- documentation, 451
  - *baseline data, 453–454*
  - *configuration files, 451*
  - *topology diagrams, 452–453*
- EIGRP (Enhanced Interior Gateway Routing Protocol), 269–270
- EtherChannel, 319
- GRE (generic route encapsulation), 403
- HSRP (Hot Standby Router Protocol), 326
- IP addressing, 136
- with IP SLA (service level agreement), 459–462
- IPv6 ACLs, 348–349
- methods, 454–455
- NAT (network address translation), 378–379
- network layer, 456
- OSPF (Open Shortest Path First), 235
  - *adjacency, 236*
  - *states, 235*
  - *troubleshooting commands, 236–237*
- physical layer, 455–456
- PPP (Point-to-Point Protocol), 398
- PPPoE (PPP over Ethernet), 400–401
- RIPv1 (Routing Information Protocol version 1), 158–161
- RIPv2 (Routing Information Protocol version 2), 167–168
- switch configuration
  - *duplex and speed mismatches, 52–53*
  - *interface status codes, 52*
  - *Layer 1 problems on "up" interfaces, 54*
  - *media issues, 51*
- tools
  - *ping, 133*
  - *SSH (Secure Shell), 134–135*
  - *traceroute, 134*
- transport layer, 457–458
- VLANs (virtual local-area networks), 71–72, 73–75

trunking VLANs (virtual local-area networks)
- configuration, 68–69
- DTP (Dynamic Trunking Protocol), 61–62
- example of, 60–61
- troubleshooting, 73–75
- verification, 69–70
- VTP (VLAN Trunking Protocol)
  - *concepts, 169–171*
  - *configuration, 170–173*
  - *verification, 173–175*

trusted ports, 290

TTL (Time to Live) field, 116

tunnel mode gre ip command, 402

tunneling
- GRE (generic route encapsulation)
  - *characteristics of, 401*
  - *configuration, 401–402*
  - *overview of, 401*
  - *troubleshooting, 403*
  - *verification, 403*
- overview of, 105–106

Type/Length/Value field (EIGRP), 242

U

UDP (User Datagram Protocol), 4, 10

ULAs (unique local addresses), 96–97

undebug all command, 161

unicast addresses
- definition of, 92
- IPv6
  - *global unicast addresses, 92–95*
  - *IPv4 embedded addresses, 97*
  - *link-local addresses, 95–96*
  - *loopback addresses, 96*
  - *ULAs (unique local addresses), 96–97*
  - *unspecified addresses, 96*

Uniform Resource Identifier (URI), 364

uninstalling licenses, 447

unique local addresses (ULAs), 96–97

Universal Resource Locator (URL), 365, 440

unshielded twisted pair (UTP) cabling, 34–35

unspecified addresses, 96

untrusted ports, 290

"up" interfaces, troubleshooting Layer 1 problems on, 54

Update packets (EIGRP), 241

URI (Uniform Resource Identifier), 364

URL (Universal Resource Locator), 365, 440

User Datagram Protocol (UDP), 4, 10

username command, 397

UTP (unshielded twisted pair) cabling, 34–35

V

variable-length subnet masking (VLSM), 85–87

vectors, distance, 111

verification
- BID (bridge ID), 307–309
- CDP (Cisco Discovery Protocol), 277–279
- DHCPv4, 354–355
- eBGP (external BGP), 406–407
- EIGRP for IPv4, 251–255
  - *neighbor tables, 252–253*
  - *protocol details, 251–252*
  - *routing tables, 255*
  - *topology tables, 253–255*
- EIGRP for IPv6
  - *neighbor tables, 259–260*
  - *overview of, 258*
  - *protocol details, 258–259*
  - *routing tables, 260–261*
- EtherChannel, 317–319
- GRE (generic route encapsulation), 403
- HSRP (Hot Standby Router Protocol), 322–323
- IPv4 ACLs, 341–343
- IPv6 ACLs, 346–348
- licenses, 445–447
- LLDP (Link Layer Discovery Protocol), 281–283
- NAT (network address translation), 377
- network connectivity, 48–51, 133–135
- NTP (Network Time Protocol), 436–437
- OSPF (Open Shortest Path First)
  - *multiarea OSPFv2, 216–218*
  - *multiarea OSPFv3, 220–223*
  - *single-area OSPFv2, 203–206*
  - *single-area OSPFv3, 209–212*
- port security, 287–289
- RIPv1 (Routing Information Protocol version 1), 158–161
- RIPv2 (Routing Information Protocol version 2), 167–168
- routers
  - *with IPv4, 124–129*
  - *router on a stick, 179–180*
- SNMP (Simple Network Management Protocol), 430–431
- STP (Spanning Tree Protocol), 310
- Syslog, 435–436
- VLANs (virtual local-area networks), 64–66
  - *trunking, 69–70*
  - *VTP (VLAN Trunking Protocol), 173–175*

versions (SNMP), 428

VID (VLAN ID), 61

viewing EIGRP (Enhanced Interior Gateway Routing Protocol) tables
- neighbor tables, 252–253
- routing tables, 255
- topology tables, 253–255

virtual links, 228

virtual local-area networks. *See* VLANs (virtual local-area networks)

virtual machines (VMs), 416

virtual network functions (VNF), 419

virtual network infrastructure, 419

Virtual Router Redundancy Protocol (VRRP), 320

virtualization, 416–418

VLAN Trunking Protocol. *See* VTP (VLAN Trunking Protocol)

VLANs (virtual local-area networks)
concepts, 57–58
configuration, 62–64
enabling/disabling, 72–73
extended VLANs, 66–68
inter-VLAN routing
legacy inter-VLAN routing, 175–176
multilayer switch, 177, 180–182
overview of, 175
router on a stick, 176, 177–180
native and management VLAN modification, 290–291
traffic types, 58
troubleshooting, 71–72
trunking
configuration, 68–69
DTP (Dynamic Trunking Protocol), 61–62
example of, 60–61
troubleshooting, 73–75
verification, 69–70
VTP (VLAN Trunking Protocol), 169–175
types of, 59
verification, 64–66
VID (VLAN ID), 61
voice VLAN example, 59–60
VTP (VLAN Trunking Protocol)
concepts, 169–171
configuration, 170–173
modes, 170–171
topology, 171
verification, 173–175

VLSM (variable-length subnet masking), 85–87

VMs (virtual machines), 416

VNF (virtual network functions), 419

voice VLANs (virtual local-area networks), 59–60

VPNs (virtual private networks)
benefits of, 389
types of, 389–391

VRRP (Virtual Router Redundancy Protocol), 320

VTP (VLAN Trunking Protocol)
concepts, 169–171
configuration, 170–173
modes, 170–171
topology, 171
verification, 173–175

vtp domain command, 171

vtp mode command, 171

vtp password command, 171

vtp pruning command, 171

W-X-Y-Z

Wallace, Kevin, 425

WANs (wide area networks), 22
BGP (Border Gateway Protocol)
concepts, 403–404
eBGP, 404–407
connection options
circuit-switched connections, 384–385
comparison of, 388
dedicated connections, 383–384
Internet connections, 386–388
overview of, 382–383
packet-switched connections, 385–386
GRE (generic route encapsulation)
characteristics of, 401
configuration, 401–402
overview of, 401
troubleshooting, 403
verification, 403
PPP (Point-to-Point Protocol)
CHAP (Challenge Handshake Authentication Protocol), 397–398
concepts, 393
configuration, 396–397
frame format, 393–394
LCP (Link Control Protocol), 394–396
PAP (Password Authentication Protocol), 398
topology, 396
troubleshooting, 398
PPPoE (PPP over Ethernet)
concepts, 399
configuration, 399–400
troubleshooting, 400–401
topologies, 381–382
VPNs (virtual private networks)
benefits of, 389
types of, 389–391

web traffic, allowing, 345

wide area networks. ***See*** **WANs (wide area networks)**

Wi-Fi, 388
WiMAX (Worldwide Interoperability for Microwave Access), 388
windowing, 8–9
wireless connections, 19–20, 388
WLANs (wireless LANs), 17
WLCs (wireless LAN controllers), 17–19
Worldwide Interoperability for Microwave Access (WiMAX), 388
writing IPv6 addresses, 100–102