CCNA 200-301 Official Cert Guide,
Volume 1

Wendell Odom

Copyright © 2020 Pearson Education, Inc.

Published by:
Cisco Press

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.

ScoutAutomatedPrintCode

Library of Congress Control Number: 2019908180
ISBN-10: 0-13-579273-8

Warning and Disclaimer

This book is designed to provide information about the Cisco CCNA 200-301 exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The 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: Mark Taub

Technical Editor: Elan Beer

Business Operation Manager, Cisco Press: Ronald Fligge

Editorial Assistant: Cindy Teeters

Director ITP Product Management: Brett Bartow

Cover Designer: Chuti Prasertsith

Managing Editor: Sandra Schroeder

Composition: Tricia Bronkella

Development Editor: Christopher Cleveland

Indexer: Ken Johnson

Senior Project Editor: Tonya Simpson

Proofreader: Debbie Williams

Copy Editor: Chuck Hutchinson
About the Author

Wendell Odom, CCIE No. 1624 Emeritus, has been in the networking industry since 1981. He has worked as a network engineer, consultant, systems engineer, instructor, and course developer; he currently works writing and creating certification study tools. This book is his 28th edition of some product for Pearson, and he is the author of all editions of the CCNA Cert Guides about Routing and Switching from Cisco Press. He has written books about topics from networking basics, certification guides throughout the years for CCENT, CCNA R&S, CCNA DC, CCNP ROUTE, CCNP QoS, and CCIE R&S. He maintains study tools, links to his blogs, and other resources at www.certskills.com.
About the Contributing Author

David Hucaby, CCIE No. 4594, CWNE No. 292, is a network engineer for University of Kentucky Healthcare. He has been authoring Cisco Press titles for 20 years, with a focus on wireless and LAN switching topics. David has bachelor of science and master of science degrees in electrical engineering. He lives in Kentucky with his wife, Marci, and two daughters.

About the Technical Reviewer

Elan Beer, CCIE No. 1837, is a senior consultant and Cisco instructor specializing in data center architecture and multiprotocol network design. For the past 27 years, Elan has designed networks and trained thousands of industry experts in data center architecture, routing, and switching. Elan has been instrumental in large-scale professional service efforts designing and troubleshooting internetworks, performing data center and network audits, and assisting clients with their short- and long-term design objectives. Elan has a global perspective of network architectures via his international clientele. Elan has used his expertise to design and troubleshoot data centers and internetworks in Malaysia, North America, Europe, Australia, Africa, China, and the Middle East. Most recently, Elan has been focused on data center design, configuration, and troubleshooting as well as service provider technologies. In 1993, Elan was among the first to obtain the Cisco Certified System Instructor (CCSI) certification, and in 1996, he was among the first to attain the Cisco System highest technical certification, the Cisco Certified Internetworking Expert. Since then, Elan has been involved in numerous large-scale data center and telecommunications networking projects worldwide.
Acknowledgments

Brett Bartow and I have been a team for a few decades. His support and wisdom have been a big help through what is the most significant change to the Cisco CCNA and CCNP certifications since their beginnings back in 1998. He’s always a great partner on working through big picture direction as well as features to make the books the best they can be for our readers. Once again he’s the starting point of the team! (And one of the things he does is gather the rest of the team that you see below…)

I don’t mean this to sound too melodramatic, but I am too psyched: I got Dave Hucaby to join my team as a coauthor for this edition of the book! Dave’s been writing about LAN switching, wireless LANs, and security topics for Cisco Press almost as long as I have, and I’ve always loved the accuracy and style of his books. Cisco added more than a little wireless LAN content to CCNA this time around. One thing led to another, I wondered if Dave might be willing to join in, and now we get Dave on the wireless chapters! I hope you’ll enjoy those chapters as much as I did when preparing the book.

Chris Cleveland did the development editing for the very first Cisco Press exam certification guide way back in 1998, and he still can’t seem to get away from us! Seriously, when Brett and I first discuss any new book, the first question is whether Chris has time to develop the book. It’s always a pleasure working with you, Chris, for what seems like the 20th time or so by now.

The second question for Brett when starting a new book is whether we might be able to get Elan Beer to do the tech editing. Elan has the right wiring, skills, and experience to do a great job for us with all aspects of the tech editing process. Fantastic job as usual; thanks, Elan.

Sometimes, with a short book timeline as with this book, I don’t know who’s working on the project for the production group until I’ve written these notes, but I heard Sandra’s and Tonya’s names early this time. Knowing they would be on the project again really did give me a chance to exhale, and I have to say that knowing they would be on the project gave me a great sense of calm going into the production phase of the book.

Thanks to Sandra Schroeder, Tonya Simpson, and all the production team for making the magic happen. Not to sound too much like a broken record, but getting to work with familiar people who have been a great help in the past really does help reduce the stress when writing, besides getting the highest-quality product out the door in print and e-book forms. From fixing all my grammar and passive-voice sentences to pulling the design and layout together, they do it all; thanks for putting it all together and making it look easy. And Tonya got to juggle two books of mine at the same time (again)—thanks for managing the whole production process again.

Mike Tanamachi, illustrator and mind reader, did a great job on the figures again. I use a different process with the figures than most authors, with Mike drawing new figures as soon as I outline a new section or chapter. It means more edits when I change my mind and lots of mind reading of what Wendell really wanted versus what I drew poorly on my iPad. Mike came through again with some beautiful finished products.
I could not have made the timeline for this book without Chris Burns of Certskills Professional. Chris owns much of the PTP question support and administration process, works on the labs we put on my blog, and then catches anything I need to toss over my shoulder so I can focus on the books. Chris, you are the man!

A special thank you to you readers who write in with suggestions and possible errors, and especially those of you who post online at the Cisco Learning Network and at my blog (blog.certskills.com). Without question, the comments I receive directly and overhear by participating at CLN made this edition a better book.

Thanks to my wonderful wife, Kris, who helps make this sometimes challenging work lifestyle a breeze. I love walking this journey with you, doll. Thanks to my daughter Hannah, launching to college just as this book releases! And thanks to Jesus Christ, Lord of everything in my life.
Contents at a Glance

Introduction xxxv
Your Study Plan 2

Part I Introduction to Networking 11
Chapter 1 Introduction to TCP/IP Networking 12
Chapter 2 Fundamentals of Ethernet LANs 32
Chapter 3 Fundamentals of WANs and IP Routing 58
Part I Review 80

Part II Implementing Ethernet LANs 83
Chapter 4 Using the Command-Line Interface 84
Chapter 5 Analyzing Ethernet LAN Switching 106
Chapter 6 Configuring Basic Switch Management 126
Chapter 7 Configuring and Verifying Switch Interfaces 150
Part II Review 172

Part III Implementing VLANs and STP 175
Chapter 8 Implementing Ethernet Virtual LANs 176
Chapter 9 Spanning Tree Protocol Concepts 210
Chapter 10 RSTP and EtherChannel Configuration 238
Part III Review 260

Part IV IPv4 Addressing 263
Chapter 11 Perspectives on IPv4 Subnetting 264
Chapter 12 Analyzing Classful IPv4 Networks 288
Chapter 13 Analyzing Subnet Masks 302
Chapter 14 Analyzing Existing Subnets 320
Part IV Review 344

Part V IPv4 Routing 347
Chapter 15 Operating Cisco Routers 348
Chapter 16 Configuring IPv4 Addresses and Static Routes 366
Chapter 17  IP Routing in the LAN  392
Chapter 18  Troubleshooting IPv4 Routing  418
Part V Review  436

Part VI  OSPF  439
Chapter 19  Understanding OSPF Concepts  440
Chapter 20  Implementing OSPF  468
Chapter 21  OSPF Network Types and Neighbors  498
Part VI Review  518

Part VII  IP Version 6  521
Chapter 22  Fundamentals of IP Version 6  522
Chapter 23  IPv6 Addressing and Subnetting  540
Chapter 24  Implementing IPv6 Addressing on Routers  554
Chapter 25  Implementing IPv6 Routing  580
Part VII Review  606

Part VIII  Wireless LANs  609
Chapter 26  Fundamentals of Wireless Networks  610
Chapter 27  Analyzing Cisco Wireless Architectures  632
Chapter 28  Securing Wireless Networks  650
Chapter 29  Building a Wireless LAN  666
Part VIII Review  688

Part IX  Appendixes  691
Appendix A  Numeric Reference Tables  693
Appendix B  CCNA 200-301, Volume 1 Exam Updates  699
Appendix C  Answers to the “Do I Know This Already?” Quizzes  701
  Glossary  724
  Index  758
Online Appendixes

Appendix D  Practice for Chapter 12: Analyzing Classful IPv4 Networks
Appendix E  Practice for Chapter 13: Analyzing Subnet Masks
Appendix F  Practice for Chapter 14: Analyzing Existing Subnets
Appendix G  Practice for Chapter 22: Fundamentals of IP Version 6
Appendix H  Practice for Chapter 24: Implementing IPv6 Addressing on Routers
Appendix I  Study Planner
Appendix J  Topics from Previous Editions
Appendix K  Analyzing Ethernet LAN Designs
Appendix L  Subnet Design
Appendix M  Practice for Appendix L: Subnet Design
Appendix N  Variable-Length Subnet Masks
Appendix O  Spanning Tree Protocol Implementation
Appendix P  LAN Troubleshooting
Appendix Q  Troubleshooting IPv4 Routing Protocols
Appendix R  Exam Topics Cross Reference
Contents

Introduction xxxv

Your Study Plan 2

A Brief Perspective on Cisco Certification Exams 2

Five Study Plan Steps 3

Step 1: Think in Terms of Parts and Chapters 3
Step 2: Build Your Study Habits Around the Chapter 4
Step 3: Use Book Parts for Major Milestones 5
Step 4: Use Volume 2’s Final Review Chapter 6
Step 5: Set Goals and Track Your Progress 6

Things to Do Before Starting the First Chapter 7

Bookmark the Companion Website 7
Bookmark/Install Pearson Test Prep 7
Understand This Book’s PTP Databases and Modes 8
Practice Viewing Per-Chapter DIKTA Questions 9
Practice Viewing Per-Part Review Questions 9
Join the Cisco Learning Network CCNA Study Group 9

Getting Started: Now 9

Part I Introduction to Networking 11

Chapter 1 Introduction to TCP/IP Networking 12

“Do I Know This Already?” Quiz 12

Foundation Topics 14
Perspectives on Networking 14
TCP/IP Networking Model 16

History Leading to TCP/IP 16
Overview of the TCP/IP Networking Model 18
TCP/IP Application Layer 19

HTTP Overview 19
HTTP Protocol Mechanisms 19

TCP/IP Transport Layer 20

TCP Error Recovery Basics 21
Same-Layer and Adjacent-Layer Interactions 21
Chapter 2  
Fundamentals of Ethernet LANs  
“Do I Know This Already?” Quiz  
Foundation Topics  
An Overview of LANs  
Typical SOHO LANs  
Typical Enterprise LANs  
The Variety of Ethernet Physical Layer Standards  
Consistent Behavior over All Links Using the Ethernet Data-Link Layer  
Building Physical Ethernet LANs with UTP  
Transmitting Data Using Twisted Pairs  
Breaking Down a UTP Ethernet Link  
UTP Cabling Pinouts for 10BASE-T and 100BASE-T  
Straight-Through Cable Pinout  
Choosing the Right Cable Pinouts  
UTP Cabling Pinouts for 1000BASE-T  
Building Physical Ethernet LANs with Fiber  
Fiber Cabling Transmission Concepts  
Using Fiber with Ethernet  
Sending Data in Ethernet Networks  
Ethernet Data-Link Protocols  
Ethernet Addressing  
Identifying Network Layer Protocols with the Ethernet Type Field  
Error Detection with FCS
Accessing the Cisco Catalyst Switch CLI 86
Cisco Catalyst Switches 86
Accessing the Cisco IOS CLI 87
Cabling the Console Connection 88
Accessing the CLI with Telnet and SSH 90
User and Enable (Privileged) Modes 91
Password Security for CLI Access from the Console 93
CLI Help Features 94
The debug and show Commands 95
Configuring Cisco IOS Software 96
Configuration Submodes and Contexts 97
Storing Switch Configuration Files 99
Copying and Erasing Configuration Files 101
Chapter Review 102

Chapter 5  Analyzing Ethernet LAN Switching 106
“Do I Know This Already?” Quiz 106
Foundation Topics 108
LAN Switching Concepts 108
  Overview of Switching Logic 109
  Forwarding Known Unicast Frames 110
  Learning MAC Addresses 113
  Flooding Unknown Unicast and Broadcast Frames 114
  Avoiding Loops Using Spanning Tree Protocol 114
LAN Switching Summary 115
Verifying and Analyzing Ethernet Switching 116
  Demonstrating MAC Learning 117
  Switch Interfaces 118
  Finding Entries in the MAC Address Table 120
  Managing the MAC Address Table (Aging, Clearing) 121
  MAC Address Tables with Multiple Switches 123
Chapter Review 124

Chapter 6  Configuring Basic Switch Management 126
“Do I Know This Already?” Quiz 126
Foundation Topics 128
Securing the Switch CLI 128
- Securing User Mode and Privileged Mode with Simple Passwords 129
- Securing User Mode Access with Local Usernames and Passwords 133
- Securing User Mode Access with External Authentication Servers 135
- Securing Remote Access with Secure Shell 136

Enabling IPv4 for Remote Access 139
- Host and Switch IP Settings 140
- Configuring IPv4 on a Switch 142
- Configuring a Switch to Learn Its IP Address with DHCP 143
- Verifying IPv4 on a Switch 143

Miscellaneous Settings Useful in the Lab 144
- History Buffer Commands 144
- The logging synchronous, exec-timeout, and no ip domain-lookup Commands 145

Chapter Review 146

Chapter 7 Configuring and Verifying Switch Interfaces 150
“Do I Know This Already?” Quiz 150
Foundation Topics 152
- Configuring Switch Interfaces 152
  - Configuring Speed, Duplex, and Description 152
  - Configuring Multiple Interfaces with the interface range Command 154
  - Administratively Controlling Interface State with shutdown 155
  - Removing Configuration with the no Command 157
  - Autonegotiation 158
    - Autonegotiation Under Working Conditions 158
    - Autonegotiation Results When Only One Node Uses Autonegotiation 160
    - Autonegotiation and LAN Hubs 161
- Analyzing Switch Interface Status and Statistics 162
  - Interface Status Codes and Reasons for Nonworking States 162
  - Interface Speed and Duplex Issues 163
  - Common Layer 1 Problems on Working Interfaces 166

Chapter Review 168
Part II Review 172

Part III Implementing VLANs and STP 175

Chapter 8 Implementing Ethernet Virtual LANs 176

“Do I Know This Already?” Quiz 177
Foundation Topics 179
Virtual LAN Concepts 179
Creating Multiswitch VLANs Using Trunking 180
VLAN Tagging Concepts 181
The 802.1Q and ISL VLAN Trunking Protocols 182
Forwarding Data Between VLANs 183
The Need for Routing Between VLANs 183
Routing Packets Between VLANs with a Router 184
VLAN and VLAN Trunking Configuration and Verification 185
Creating VLANs and Assigning Access VLANs to an Interface 185
VLAN Configuration Example 1: Full VLAN Configuration 186
VLAN Configuration Example 2: Shorter VLAN Configuration 189
VLAN Trunking Protocol 189
VLAN Trunking Configuration 191
Implementing Interfaces Connected to Phones 196
Data and Voice VLAN Concepts 196
Data and Voice VLAN Configuration and Verification 198
Summary: IP Telephony Ports on Switches 200
Troubleshooting VLANs and VLAN Trunks 200
Access VLANs Undefined or Disabled 201
Mismatched Trunking Operational States 202
The Supported VLAN List on Trunks 203
Mismatched Native VLAN on a Trunk 205
Chapter Review 205

Chapter 9 Spanning Tree Protocol Concepts 210

“Do I Know This Already?” Quiz 210
Foundation Topics 212
STP and RSTP Basics 212
The Need for Spanning Tree 213
What Spanning Tree Does 215
How Spanning Tree Works 216
The STP Bridge ID and Hello BPDU 218
E lecting the Root Switch 218
Part III Review  260
Part IV  IPv4 Addressing  263

Chapter 11  Perspectives on IPv4 Subnetting  264
“Do I Know This Already?” Quiz  264
Foundation Topics  266
Introduction to Subnetting  266
   Subnetting Defined Through a Simple Example  267
   Operational View Versus Design View of Subnetting  267
Analyze Subnetting and Addressing Needs  268
   Rules About Which Hosts Are in Which Subnet  268
   Determining the Number of Subnets  270
   Determining the Number of Hosts per Subnet  271
One Size Subnet Fits All—Or Not  272
   Defining the Size of a Subnet  272
   One Size Subnet Fits All  273
   Multiple Subnet Sizes (Variable-Length Subnet Masks)  274
   One Mask for All Subnets, or More Than One  274
Make Design Choices  275
Choose a Classful Network  275
   Public IP Networks  276
   Growth Exhau ts the Public IP Address Space  276
   Private IP Networks  278
   Choosing an IP Network During the Design Phase  278
Choose the Mask  279
   Classful IP Networks Before Subnetting  279
   Borrowing Host Bits to Create Subnet Bits  280
   Choosing Enough Subnet and Host Bits  281
   Example Design: 172.16.0.0, 200 Subnets, 200 Hosts  282
   Masks and Mask Formats  282
Build a List of All Subnets  283
Plan the Implementation  284
   Assigning Subnets to Different Locations  285
   Choose Static and Dynamic Ranges per Subnet  286
Chapter Review  287
Chapter 12 Analyzing Classful IPv4 Networks 288
“Do I Know This Already?” Quiz 288
Foundation Topics 289
Classful Network Concepts 289
IPv4 Network Classes and Related Facts 290
The Number and Size of the Class A, B, and C Networks 291
Address Formats 291
Default Masks 292
Number of Hosts per Network 293
Deriving the Network ID and Related Numbers 293
Unusual Network IDs and Network Broadcast Addresses 295
Practice with Classful Networks 296
Practice Deriving Key Facts Based on an IP Address 296
Practice Remembering the Details of Address Classes 297
Chapter Review 298

Chapter 13 Analyzing Subnet Masks 302
“Do I Know This Already?” Quiz 302
Foundation Topics 304
Subnet Mask Conversion 304
Three Mask Formats 304
Converting Between Binary and Prefix Masks 305
Converting Between Binary and DDN Masks 306
Converting Between Prefix and DDN Masks 308
Practice Converting Subnet Masks 309
Identifying Subnet Design Choices Using Masks 309
Masks Divide the Subnet’s Addresses into Two Parts 311
Masks and Class Divide Addresses into Three Parts 312
Classless and Classful Addressing 312
Calculations Based on the IPv4 Address Format 313
Practice Analyzing Subnet Masks 315
Chapter Review 315

Chapter 14 Analyzing Existing Subnets 320
“Do I Know This Already?” Quiz 320
Foundation Topics 322
Defining a Subnet 322
An Example with Network 172.16.0.0 and Four Subnets 322
Subnet ID Concepts 324
<table>
<thead>
<tr>
<th>Chapter 16</th>
<th>Configuring IPv4 Addresses and Static Routes</th>
<th>366</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Do I Know This Already?” Quiz</td>
<td>367</td>
<td></td>
</tr>
<tr>
<td>Foundation Topics</td>
<td>369</td>
<td></td>
</tr>
<tr>
<td>IP Routing</td>
<td>369</td>
<td></td>
</tr>
<tr>
<td>IPv4 Routing Process Reference</td>
<td>369</td>
<td></td>
</tr>
<tr>
<td>An Example of IP Routing</td>
<td>371</td>
<td></td>
</tr>
<tr>
<td>Host Forwards the IP Packet to the Default Router (Gateway)</td>
<td>372</td>
<td></td>
</tr>
<tr>
<td>Routing Step 1: Decide Whether to Process the Incoming Frame</td>
<td>373</td>
<td></td>
</tr>
<tr>
<td>Routing Step 2: De-encapsulation of the IP Packet</td>
<td>373</td>
<td></td>
</tr>
<tr>
<td>Routing Step 3: Choosing Where to Forward the Packet</td>
<td>374</td>
<td></td>
</tr>
<tr>
<td>Routing Step 4: Encapsulating the Packet in a New Frame</td>
<td>375</td>
<td></td>
</tr>
<tr>
<td>Routing Step 5: Transmitting the Frame</td>
<td>376</td>
<td></td>
</tr>
<tr>
<td>Configuring IP Addresses and Connected Routes</td>
<td>376</td>
<td></td>
</tr>
<tr>
<td>Connected Routes and the ip address Command</td>
<td>376</td>
<td></td>
</tr>
<tr>
<td>The ARP Table on a Cisco Router</td>
<td>378</td>
<td></td>
</tr>
<tr>
<td>Configuring Static Routes</td>
<td>379</td>
<td></td>
</tr>
<tr>
<td>Static Network Routes</td>
<td>379</td>
<td></td>
</tr>
<tr>
<td>Static Host Routes</td>
<td>381</td>
<td></td>
</tr>
<tr>
<td>Floating Static Routes</td>
<td>381</td>
<td></td>
</tr>
<tr>
<td>Static Default Routes</td>
<td>383</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting Static Routes</td>
<td>384</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting Incorrect Static Routes That Appear in the IP Routing Table</td>
<td>385</td>
<td></td>
</tr>
<tr>
<td>The Static Route Does Not Appear in the IP Routing Table</td>
<td>385</td>
<td></td>
</tr>
<tr>
<td>The Correct Static Route Appears but Works Poorly</td>
<td>386</td>
<td></td>
</tr>
<tr>
<td>IP Forwarding with the Longest Prefix Match</td>
<td>386</td>
<td></td>
</tr>
<tr>
<td>Using show ip route to Find the Best Route</td>
<td>386</td>
<td></td>
</tr>
<tr>
<td>Using show ip route address to Find the Best Route</td>
<td>388</td>
<td></td>
</tr>
<tr>
<td>Interpreting the IP Routing Table</td>
<td>388</td>
<td></td>
</tr>
<tr>
<td>Chapter Review</td>
<td>390</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 17  IP Routing in the LAN  392
“Do I Know This Already?” Quiz  393
Foundation Topics  395
VLAN Routing with Router 802.1Q Trunks  395
Configuring ROAS  396
Verifying ROAS  398
Troubleshooting ROAS  400
VLAN Routing with Layer 3 Switch SVIs  401
Configuring Routing Using Switch SVIs  401
Verifying Routing with SVIs  403
Troubleshooting Routing with SVIs  404
VLAN Routing with Layer 3 Switch Routed Ports  406
Implementing Routed Interfaces on Switches  407
Implementing Layer 3 EtherChannels  410
Troubleshooting Layer 3 EtherChannels  413
Chapter Review  414

Chapter 18  Troubleshooting IPv4 Routing  418
“Do I Know This Already?” Quiz  418
Foundation Topics  419
Problem Isolation Using the ping Command  419
Ping Command Basics  419
Strategies and Results When Testing with the ping Command  420
Testing Longer Routes from Near the Source of the Problem  421
Using Extended Ping to Test the Reverse Route  423
Testing LAN Neighbors with Standard Ping  425
Testing LAN Neighbors with Extended Ping  426
Testing WAN Neighbors with Standard Ping  427
Using Ping with Names and with IP Addresses  427
Problem Isolation Using the traceroute Command  428
traceroute Basics  429
How the traceroute Command Works  429
Standard and Extended traceroute  431
Telnet and SSH  432
Common Reasons to Use the IOS Telnet and SSH Client  432
IOS Telnet and SSH Examples  433
Chapter Review  435
Part V Review  436

Part VI   OSPF  439

Chapter 19 Understanding OSPF Concepts  440
“Do I Know This Already?” Quiz  440

Foundation Topics  442
Comparing Dynamic Routing Protocol Features  442
Routing Protocol Functions  443
Interior and Exterior Routing Protocols  444
Comparing IGPs  445
  IGP Routing Protocol Algorithms  445
  Metrics  446
  Other IGP Comparisons  447
Administrative Distance  448

OSPF Concepts and Operation  449
OSPF Overview  449
  Topology Information and LSAs  450
  Applying Dijkstra SPF Math to Find the Best Routes  451
Becoming OSPF Neighbors  451
  The Basics of OSPF Neighbors  451
  Meeting Neighbors and Learning Their Router ID  452
Exchanging the LSDB Between Neighbors  454
  Fully Exchanging LSAs with Neighbors  454
  Maintaining Neighbors and the LSDB  455
  Using Designated Routers on Ethernet Links  456
Calculating the Best Routes with SPF  457

OSPF Areas and LSAs  459
OSPF Areas  460
  How Areas Reduce SPF Calculation Time  461
(OSPFv2) Link-State Advertisements  462
  Router LSAs Build Most of the Intra-Area Topology  463
  Network LSAs Complete the Intra-Area Topology  464

Chapter Review  465
Chapter 20 Implementing OSPF

Do I Know This Already? Quiz
Foundation Topics
Implementing Single-Area OSPFv2
OSPF Single-Area Configuration
Wildcard Matching with the network Command
Verifying OSPF Operation
Verifying OSPF Configuration
Configuring the OSPF Router ID
Implementing Multiarea OSPF
Using OSPFv2 Interface Subcommands
OSPF Interface Configuration Example
Verifying OSPF Interface Configuration
Additional OSPFv2 Features
OSPF Passive Interfaces
OSPF Default Routes
OSPF Metrics (Cost)
Setting the Cost Directly
Setting the Cost Based on Interface and Reference Bandwidth
OSPF Load Balancing
Chapter Review

Chapter 21 OSPF Network Types and Neighbors

Do I Know This Already? Quiz
Foundation Topics
OSPF Network Types
The OSPF Broadcast Network Type
Verifying Operations with Network Type Broadcast
Configuring to Influence the DR/BDR Election
The OSPF Point-to-Point Network Type
OSPF Neighbor Relationships
OSPF Neighbor Requirements
Issues That Prevent Neighbor Adjacencies
Finding Area Mismatches
Finding Duplicate OSPF Router IDs
Finding OSPF Hello and Dead Timer Mismatches
Shutting Down the OSPF Process
Issues That Allow Adjacencies but Prevent IP Routes 515
   Mismatched MTU Settings 515
   Mismatched OSPF Network Types 515
Chapter Review 516

Part VI Review 518

Part VII  IP Version 6 521

Chapter 22 Fundamentals of IP Version 6 522
   “Do I Know This Already?” Quiz 522
   Foundation Topics 524
   Introduction to IPv6 524
      The Historical Reasons for IPv6 524
      The IPv6 Protocols 526
      IPv6 Routing 527
      IPv6 Routing Protocols 529
   IPv6 Addressing Formats and Conventions 530
      Representing Full (Unabbreviated) IPv6 Addresses 530
      Abbreviating and Expanding IPv6 Addresses 531
         Abbreviating IPv6 Addresses 531
            Expanding Abbreviated IPv6 Addresses 532
      Representing the Prefix Length of an Address 533
      Calculating the IPv6 Prefix (Subnet ID) 533
      Finding the IPv6 Prefix 533
      Working with More-Difficult IPv6 Prefix Lengths 535
   Chapter Review 536

Chapter 23 IPv6 Addressing and Subnetting 540
   “Do I Know This Already?” Quiz 540
   Foundation Topics 542
   Global Unicast Addressing Concepts 542
      Public and Private IPv6 Addresses 542
      The IPv6 Global Routing Prefix 543
   Address Ranges for Global Unicast Addresses 544
   IPv6 Subnetting Using Global Unicast Addresses 545
      Deciding Where IPv6 Subnets Are Needed 546
         The Mechanics of Subnetting IPv6 Global Unicast Addresses 546
            Listing the IPv6 Subnet Identifier 548
Static IPv6 Routes  586
  Static Routes Using the Outgoing Interface  587
  Static Routes Using Next-Hop IPv6 Address  588
    Example Static Route with a Global Unicast Next-Hop Address  589
    Example Static Route with a Link-Local Next-Hop Address  589
  Static Routes over Ethernet Links  591
  Static Default Routes  592
  Static IPv6 Host Routes  593
  Floating Static IPv6 Routes  593
  Troubleshooting Static IPv6 Routes  595
    Troubleshooting Incorrect Static Routes That Appear in the IPv6 Routing Table  595
    The Static Route Does Not Appear in the IPv6 Routing Table  598
The Neighbor Discovery Protocol  598
  Discovering Neighbor Link Addresses with NDP NS and NA  598
  Discovering Routers with NDP RS and RA  600
  Using SLAAC with NDP RS and RA  601
  Discovering Duplicate Addresses Using NDP NS and NA  602
  NDP Summary  603
Chapter Review  603

Part VII Review  606

Part VIII Wireless LANs  609

Chapter 26 Fundamentals of Wireless Networks  610
  “Do I Know This Already?” Quiz  610
  Foundation Topics  612
  Comparing Wired and Wireless Networks  612
  Wireless LAN Topologies  613
    Basic Service Set  614
    Distribution System  616
    Extended Service Set  618
    Independent Basic Service Set  619
  Other Wireless Topologies  620
    Repeater  620
    Workgroup Bridge  621
    Outdoor Bridge  621
    Mesh Network  622
RF Overview 623
  Wireless Bands and Channels 626
  APs and Wireless Standards 628
Chapter Review 629

Chapter 27  Analyzing Cisco Wireless Architectures 632
“Do I Know This Already?” Quiz 632
Foundation Topics 634
  Autonomous AP Architecture 634
  Cloud-based AP Architecture 636
  Split-MAC Architectures 638
Comparing Wireless LAN Controller Deployments 642
  Cisco AP Modes 647
Chapter Review 647

Chapter 28  Securing Wireless Networks 650
“Do I Know This Already?” Quiz 650
Foundation Topics 652
  Anatomy of a Secure Connection 652
  Authentication 653
  Message Privacy 655
  Message Integrity 656
Wireless Client Authentication Methods 656
  Open Authentication 656
  WEP 657
  802.1x/EAP 657
    LEAP 659
    EAP-FAST 659
    PEAP 659
    EAP-TLS 660
Wireless Privacy and Integrity Methods 660
  TKIP 660
  CCMP 661
  GCMP 661
  WPA, WPA2, and WPA3 661
Chapter Review 664
<table>
<thead>
<tr>
<th>Appendix J</th>
<th>Topics from Previous Editions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix K</td>
<td>Analyzing Ethernet LAN Designs</td>
</tr>
<tr>
<td>Appendix L</td>
<td>Subnet Design</td>
</tr>
<tr>
<td>Appendix M</td>
<td>Practice for Appendix L: Subnet Design</td>
</tr>
<tr>
<td>Appendix N</td>
<td>Variable-Length Subnet Masks</td>
</tr>
<tr>
<td>Appendix O</td>
<td>Spanning Tree Protocol Implementation</td>
</tr>
<tr>
<td>Appendix P</td>
<td>LAN Troubleshooting</td>
</tr>
<tr>
<td>Appendix Q</td>
<td>Troubleshooting IPv4 Routing Protocols</td>
</tr>
<tr>
<td>Appendix R</td>
<td>Exam Topics Cross Reference</td>
</tr>
</tbody>
</table>
Reader Services

To access additional content for this book, simply register your product. To start the registration process, go to www.ciscopress.com/register and log in or create an account*. Enter the product ISBN 9780135792735 and click Submit. After 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.

Icons Used in This Book

- Printer
- PC
- Laptop
- Server
- IP Phone
- Router
- Switch
- Layer 3 Switch
- Hub
- Bridge
- Access Point
- ASA
- Network Cloud
- Cable Modem
- CSU/DSU
- Cable (Various)
- Serial Line
- Virtual Circuit
- Ethernet WAN
- Wireless

Command Syntax Conventions

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

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a `show` command).

- **Italic** indicates arguments for which you supply actual values.
Vertical bars (|) separate alternative, mutually exclusive elements.
Square brackets ([ ]) indicate an optional element.
Braces ({ }) indicate a required choice.
Braces within brackets ([{ }]) indicate a required choice within an optional element.
Introduction

About Cisco Certifications and CCNA

Congratulations! If you’re reading far enough to look at this book’s Introduction, you’ve probably already decided to go for your Cisco certification, and the CCNA certification is the one place to begin that journey. If you want to succeed as a technical person in the networking industry at all, you need to know Cisco. Cisco has a ridiculously high market share in the router and switch marketplace, with more than 80 percent market share in some markets. In many geographies and markets around the world, networking equals Cisco. If you want to be taken seriously as a network engineer, Cisco certification makes perfect sense.

The first few pages of this Introduction explain the core features of Cisco’s Career Certification program, of which the Cisco Certified Network Associate (CCNA) serves as the foundation for all the other certifications in the program. This section begins with a comparison of the old to the new certifications due to some huge program changes in 2019. It then gives the key features of CCNA, how to get it, and what’s on the exam.

The Big Changes to Cisco Certifications in 2019

Cisco announced sweeping changes to its career certification program around mid-year 2019. Because so many of you will have read and heard about the old versions of the CCNA certification, this intro begins with a few comparisons between the old and new CCNA as well as some of the other Cisco career certifications.

First, consider Cisco’s career certifications before 2019 as shown in Figure I-1. At that time, Cisco offered 10 separate CCNA certifications in different technology tracks. Cisco also had eight Professional-level (CCNP, or Cisco Certified Network Professional) certifications.

![Figure I-1](image-url)  
*Old Cisco Certification Silo Concepts*
Why so many? Cisco began with one track—Routing and Switching—back in 1998. Over time, Cisco identified more and more technology areas that had grown to have enough content to justify another set of CCNA and CCNP certifications on those topics, so Cisco added more tracks. Many of those also grew to support expert level topics with CCIE (Cisco Certified Internetwork Expert).

In 2019, Cisco consolidated the tracks and moved the topics around quite a bit, as shown in Figure I-2.

![Figure I-2](image_url)

**Figure I-2  New Cisco Certification Tracks and Structure**

All the tracks now begin with the content in the one remaining CCNA certification. For CCNP, you now have a choice of five technology areas for your next steps, as shown in Figure I-2. (Note that Cisco replaced “Routing and Switching” with the term “Enterprise.”)

Cisco made the following changes with the 2019 announcements:

- **CCENT**: Retired the only Entry-level certification (CCENT, or Cisco Certified Entry Network Technician), with no replacement.
- **CCNA**: Retired all the CCNA certifications except what was then known as “CCNA Routing and Switching,” which became simply “CCNA.”
- **CCNP**: Consolidated the Professional level (CCNP) certifications to five tracks, including merging CCNP Routing and Switching and CCNP Wireless into CCNP Enterprise.
- **CCIE**: Achieved better alignment with CCNP tracks through the consolidations.

Cisco needed to move many of the individual exam topics from one exam to another because of the number of changes. For instance, Cisco retired nine CCNA certifications plus the CCDA (Design Associate) certification—but those technologies didn’t disappear! Cisco just moved the topics around to different exams in different certifications.

Consider wireless LANs as an example. The 2019 announcements retired both CCNA Wireless and CCNP Wireless as certifications. Some of the old CCNA Wireless topics landed in the new CCNA, while others landed in the two CCNP Enterprise exams about wireless LANs.
For those of you who want to learn more about the transition, check out my blog (blog.certskills.com) and look for posts in the News category from around June 2019. Now on to the details about CCNA as it exists starting in 2019!

How to Get Your CCNA Certification

As you saw in Figure I-2, all career certification paths now begin with CCNA. So how do you get it? Today, you have one and only one option to achieve CCNA certification:

Take and pass one exam: The Cisco 200-301 CCNA exam.

To take the 200-301 exam, or any Cisco exam, you will use the services of Pearson VUE (vue.com). The process works something like this:

1. Establish a login at https://home.pearsonvue.com/ (or use your existing login).
2. Register for, schedule a time and place, and pay for the Cisco 200-301 exam, all from the VUE website.
3. Take the exam at the VUE testing center.
4. You will receive a notice of your score, and whether you passed, before you leave the testing center.

Types of Questions on CCNA 200-301 Exam

The Cisco CCNA and CCNP exams all follow the same general format, with these types of questions:

- Multiple-choice, single-answer
- Multiple-choice, multiple-answer
- Testlet (one scenario with multiple multiple-choice questions)
- Drag-and-drop
- Simulated lab (sim)
- Simlet

Although the first four types of questions in the list should be somewhat familiar to you from other tests in school, the last two are more common to IT tests and Cisco exams in particular. Both use a network simulator to ask questions so that you control and use simulated Cisco devices. In particular:

**Sim questions:** You see a network topology and lab scenario, and can access the devices. Your job is to fix a problem with the configuration.

**Simlet questions:** This style combines sim and testlet question formats. As with a sim question, you see a network topology and lab scenario, and can access the devices. However, as with a testlet, you also see multiple multiple-choice questions. Instead of changing/fixing the configuration, you answer questions about the current state of the network.
These two question styles with the simulator give Cisco the ability to test your configuration skills with sim questions, and your verification and troubleshooting skills with simlet questions.

Before taking the test, learn the exam user interface by watching some videos Cisco provides about the exam user interface. To find the videos, just go to cisco.com and search for “Cisco Certification Exam Tutorial Videos.”

CCNA 200-301 Exam Content, Per Cisco

Ever since I was in grade school, whenever the teacher announced that we were having a test soon, someone would always ask, “What’s on the test?” We all want to know, and we all want to study what matters and avoid studying what doesn’t matter.

Cisco tells the world the topics on each of its exams. Cisco wants the public to know the variety of topics and get an idea about the kinds of knowledge and skills required for each topic for every Cisco certification exam. To find the details, go to www.cisco.com/go/certifications, look for the CCNA page, and navigate until you see the exam topics.

This book also lists those same exam topics in several places. From one perspective, every chapter sets about to explain a small set of exam topics, so each chapter begins with the list of exam topics covered in that chapter. However, you might want to also see the exam topics in one place, so Appendix R, “Exam Topics Cross Reference,” lists all the exam topics. You may want to download Appendix R in PDF form and keep it handy. The appendix lists the exam topics with two different cross references:

- A list of exam topics and the chapter(s) that covers each topic
- A list of chapters and the exam topics covered in each chapter

Exam Topic Verbs and Depth

Reading and understanding the exam topics, especially deciding the depth of skills required for each exam topic, require some thought. Each exam topic mentions the name of some technology, but it also lists a verb that implies the depth to which you must master the topic. The primary exam topics each list one or more verbs that describe the skill level required. For example, consider the following exam topic:

Configure and verify IPv4 addressing and subnetting

Note that this one exam topic has two verbs (configure and verify). Per this exam topic, you should be able to not only configure IPv4 addresses and subnets, but you should understand them well enough to verify that the configuration works. In contrast, the following exam topic asks you to describe a technology but does not ask you to configure it:

Describe the purpose of first hop redundancy protocol

The describe verb tells you to be ready to describe whatever a “first hop redundancy protocol” is. That exam topic also implies that you do not then need to be ready to configure or verify any first hop redundancy protocols (HSRP, VRRP, and GLBP).

Finally, note that the configure and verify exam topics imply that you should be able to describe and explain and otherwise master the concepts so that you understand what you have configured. The earlier “Configure and verify IPv4 addressing and subnetting”
does not mean that you should know how to type commands but have no clue as to what you configured. You must first master the conceptual exam topic verbs. The progression runs something like this:

Describe, Identify, Explain, Compare/Contrast, Configure, Verify, Troubleshoot

For instance, an exam topic that lists “compare and contrast” means that you should be able to describe, identify, and explain the technology. Also, an exam topic with “configure and verify” tells you to also be ready to describe, explain, and compare/contrast.

The Context Surrounding the Exam Topics

Take a moment to navigate to www.cisco.com/go/certifications and find the list of exam topics for the CCNA 200-301 exam. Did your eyes go straight to the list of exam topics? Or did you take the time to read the paragraphs above the exam topics first?

That list of exam topics for the CCNA 200-301 exam includes a little over 50 primary exam topics and about 50 more secondary exam topics. The primary topics have those verbs as just discussed, which tell you something about the depth of skill required. The secondary topics list only the names of more technologies to know.

However, the top of the web page that lists the exam topics also lists some important information that tells us some important facts about the exam topics. In particular, that leading text, found at the beginning of Cisco exam topic pages of most every exam, tells us

- The guidelines may change over time.
- The exam topics are general guidelines about what may be on the exam.
- The actual exam may include “other related topics.”

Interpreting these three facts in order, I would not expect to see a change to the published list of exam topics for the exam. I’ve been writing the Cisco Press CCNA Cert Guides since Cisco announced CCNA back in 1998, and I’ve never seen Cisco change the official exam topics in the middle of an exam—not even to fix typos. But the introductory words say that they might change the exam topics, so it’s worth checking.

As for the second item in the preceding list, even before you know what the acronyms mean, you can see that the exam topics give you a general but not detailed idea about each topic. The exam topics do not attempt to clarify every nook and cranny or to list every command and parameter; however, this book serves as a great tool in that it acts as a much more detailed interpretation of the exam topics. We examine every exam topic, and if we think a concept or command is possibly within an exam topic, we put it into the book. So, the exam topics give us general guidance, and these books give us much more detailed guidance.

The third item in the list uses literal wording that runs something like this: “However, other related topics may also appear on any specific delivery of the exam.” That one statement can be a bit jarring to test takers, but what does it really mean? Unpacking the statement, it says that such questions may appear on any one exam but may not; in other words, they don’t set about to ask every test taker some questions that include concepts
not mentioned in the exam topics. Second, the phrase “...other related topics...” emphasizes that any such questions would be related to some exam topic, rather than being far afield—a fact that helps us in how we respond to this particular program policy.

For instance, the CCNA 200-301 exam includes configuring and verifying the OSPF routing protocol, but it does not mention the EIGRP routing protocol. I personally would be unsurprised to see an OSPF question that required a term or fact not specifically mentioned in the exam topics. I would be surprised to see one that (in my opinion) ventures far away from the OSPF features in the exam topics. Also, I would not expect to see a question about how to configure and verify EIGRP.

And just as one final side point, note that Cisco does on occasion ask a test taker some unscored questions, and those may appear to be in this vein of questions from outside topics. When you sit down to take the exam, the small print mentions that you may see unscored questions and you won’t know which ones are unscored. (These questions give Cisco a way to test possible new questions.) But some of these might be ones that fall into the “other related topics” category, but then not affect your score.

You should prepare a little differently for any Cisco exam, in comparison to say an exam back in school, in light of Cisco’s “other related questions” policy:

■ Do not approach an exam topic with an “I'll learn the core concepts and ignore the edges” approach.

■ Instead, approach each exam topic with a “pick up all the points I can” approach by mastering each exam topic, both in breadth and in depth.

■ Go beyond each exam topic when practicing configuration and verification by taking a little extra time to look for additional show commands and configuration options, and make sure you understand as much of the show command output that you can.

By mastering the known topics, and looking for places to go a little deeper, you will hopefully pick up the most points you can from questions about the exam topics. Then the extra practice you do with commands may happen to help you learn beyond the exam topics in a way that can help you pick up other points as well.

CCNA 200-301 Exam Content, Per This Book

When we created the Official Cert Guide content for the CCNA 200-301 exam, we considered a few options for how to package the content, and we landed on releasing a two-book set. Figure I-3 shows the setup of the content, with roughly 60 percent of the content in Volume 1 and the rest in Volume 2.

<table>
<thead>
<tr>
<th>Fundamentals</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet LANs</td>
<td>IP Services</td>
</tr>
<tr>
<td>IPv4 Routing</td>
<td>Automation</td>
</tr>
<tr>
<td>IPv6 Routing</td>
<td>Architecture</td>
</tr>
<tr>
<td>Wireless LANs</td>
<td></td>
</tr>
</tbody>
</table>

Vol. 1 - 60% Vol. 2 - 40%

Figure I-3 Two Books for CCNA 200-301
The two books together cover all the exam topics in the CCNA 200-301 exam. Each chapter in each book develops the concepts and commands related to an exam topic, with clear and detailed explanations, frequent figures, and many examples that build your understanding of how Cisco networks work.

As for choosing what content to put into the books, note that we begin and finish with Cisco's exam topics, but with an eye toward predicting as many of the “other related topics” as we can. We start with the list of exam topics and apply a fair amount of experience, discussion, and other secret sauce to come up with an interpretation of what specific concepts and commands are worthy of being in the books or not. At the end of the writing process, the books should cover all the published exam topics, with additional depth and breadth that I choose based on the analysis of the exam. As we have done from the very first edition of the CCNA Official Cert Guide, we intend to cover each and every topic in depth. But as you would expect, we cannot predict every single fact on the exam given the nature of the exam policies, but we do our best to cover all known topics.

**Book Features**

This book includes many study features beyond the core explanations and examples in each chapter. This section acts as a reference to the various features in the book.

**Chapter Features and How to Use Each Chapter**

Each chapter of this book is a self-contained short course about one small topic area, organized for reading and study, as follows:

- **“Do I Know This Already?” quizzes**: Each chapter begins with a pre-chapter quiz.
- **Foundation Topics**: This is the heading for the core content section of the chapter.
- **Chapter Review**: This section includes a list of study tasks useful to help you remember concepts, connect ideas, and practice skills-based content in the chapter.

Figure I-4 shows how each chapter uses these three key elements. You start with the DIKTA quiz. You can use the score to determine whether you already know a lot, or not so much, and determine how to approach reading the Foundation Topics (that is, the technology content in the chapter). When finished, use the Chapter Review tasks to start working on mastering your memory of the facts and skills with configuration, verification, and troubleshooting.

**Figure I-4  Three Primary Tasks for a First Pass Through Each Chapter**

<table>
<thead>
<tr>
<th>DIKTA Quiz</th>
<th>Foundation Topics</th>
<th>Chapter Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Take Quiz</td>
<td>(Skim) Foundation Topics</td>
<td>1) In-Chapter, or...</td>
</tr>
<tr>
<td>High Score</td>
<td>(Read) Foundation Topics</td>
<td>2) Companion Website</td>
</tr>
<tr>
<td>Low Score</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
In addition to these three main chapter features, each “Chapter Review” section uses a variety of other book features, including the following:

- **Review Key Topics:** Inside the “Foundation Topics” section, the Key Topic icon appears next to the most important items, for the purpose of later review and mastery. While all content matters, some is, of course, more important to learn, or needs more review to master, so these items are noted as key topics. The Chapter Review lists the key topics in a table; scan the chapter for these items to review them. Or review the key topics interactively using the companion website.

- **Complete Tables from Memory:** Instead of just rereading an important table of information, you will find some tables have been turned into memory tables, an interactive exercise found on the companion website. Memory tables repeat the table, but with parts of the table removed. You can then fill in the table to exercise your memory, and click to check your work.

- **Key Terms You Should Know:** You do not need to be able to write a formal definition of all terms from scratch; however, you do need to understand each term well enough to understand exam questions and answers. The Chapter Review lists the key terminology from the chapter. Make sure you have a good understanding of each term and use the Glossary to cross-check your own mental definitions. You can also review key terms with the “Key Terms Flashcards” app on the companion website.

- **Labs:** Many exam topics use verbs such as *configure* and *verify*; all these refer to skills you should practice at the user interface (CLI) of a router or switch. The Chapter and Part Reviews refer you to these other tools. The upcoming section titled “About Building Hands-On Skills” discusses your options.

- **Command References:** Some book chapters cover a large number of router and switch commands. The Chapter Review includes reference tables for the commands used in that chapter, along with an explanation. Use these tables for reference, but also use them for study. Just cover one column of the table, and see how much you can remember and complete mentally.

- **Review DIKTA Questions:** Although you have already seen the DIKTA questions from the chapters, re-answering those questions can prove a useful way to review facts. The Part Review suggests that you repeat the DIKTA questions but using the Pearson Test Prep (PTP) exam.

- **Subnetting Exercises:** Chapters 12, 13, 14, 22, and 24 ask you to perform some math processes related to either IPv4 or IPv6 addressing. The Chapter Review asks you to do additional practice problems. The problems can be found in Appendices D through H, in PDF form, on the companion website. The website also includes interactive versions of most of the exercises from those appendices.

**Part Features and How to Use the Part Review**

The book organizes the chapters into parts for the purpose of helping you study for the exam. Each part groups a small number of related chapters together. Then the study process (described just before Chapter 1) suggests that you pause after each part to do a
review of all chapters in the part. Figure I-5 lists the titles of the eight parts and the chapters in those parts (by chapter number) for this book.

Figure I-5  The Book Parts (by Title), and Chapter Numbers in Each Part

The Part Review that ends each part acts as a tool to help you with spaced review sessions. Spaced reviews—that is, reviewing content several times over the course of your study—help improve retention. The Part Review activities include many of the same kinds of activities seen in the Chapter Review. Avoid skipping the Part Review, and take the time to do the review; it will help you in the long run.

The Companion Website for Online Content Review

We created an electronic version of every Chapter and Part Review task that could be improved though an interactive version of the tool. For instance, you can take a “Do I Know This Already?” quiz by reading the pages of the book, but you can also use our testing software. As another example, when you want to review the key topics from a chapter, you can find all those in electronic form as well.

All the electronic review elements, as well as other electronic components of the book, exist on this book’s companion website. The companion website gives you a big advantage: you can do most of your Chapter and Part Review work from anywhere using the interactive tools on the site. The advantages include

- **Easier to use:** Instead of having to print out copies of the appendixes and do the work on paper, you can use these new apps, which provide you with an easy-to-use, interactive experience that you can easily run over and over.

- **Convenient:** When you have a spare 5–10 minutes, go to the book’s website and review content from one of your recently finished chapters.

- **Untethered from the book:** You can access your review activities from anywhere—no need to have the book with you.

- **Good for tactile learners:** Sometimes looking at a static page after reading a chapter lets your mind wander. Tactile learners might do better by at least typing answers into an app, or clicking inside an app to navigate, to help keep you focused on the activity.
The interactive Chapter Review elements should improve your chances of passing as well. Our in-depth reader surveys over the years show that those who do the Chapter and Part Reviews learn more. Those who use the interactive versions of the review elements also tend to do more of the Chapter and Part Review work. So take advantage of the tools and maybe you will be more successful as well. Table I-1 summarizes these interactive applications and the traditional book features that cover the same content.

**Table I-1 Book Features with Both Traditional and App Options**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Traditional</th>
<th>App</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Topic</td>
<td>Table with list; flip pages to find</td>
<td>Key Topics Table app</td>
</tr>
<tr>
<td>Config Checklist</td>
<td>Just one of many types of key topics</td>
<td>Config Checklist app</td>
</tr>
<tr>
<td>Key Terms</td>
<td>Listed in each “Chapter Review” section, with the Glossary in the back of the book</td>
<td>Glossary Flash Cards app</td>
</tr>
<tr>
<td>Subnetting Practice</td>
<td>Appendices D–H, with practice problems and answers</td>
<td>A variety of apps, one per problem type</td>
</tr>
</tbody>
</table>

The companion website also includes links to download, navigate, or stream for these types of content:

- Pearson Sim Lite Desktop App
- Pearson Test Prep (PT) Desktop App
- Pearson Test Prep (PT) Web App
- Videos as mentioned in book chapters

**How to Access the Companion Website**

To access the companion website, which gives you access to the electronic content with this book, start by establishing a login at www.ciscopress.com and register your book. To do so, simply go to www.ciscopress.com/register and enter the ISBN of the print book: 9780135792735. After you have registered your book, go to your account page and click the Registered Products tab. From there, click the Access Bonus Content link to get access to the book’s companion website.

Note that if you buy the Premium Edition eBook and Practice Test version of this book from Cisco Press, your book will automatically be registered on your account page. Simply go to your account page, click the Registered Products tab, and select Access Bonus Content to access the book’s companion website.

**How to Access the Pearson Test Prep (PTP) App**

You have two options for installing and using the Pearson Test Prep application: a web app and a desktop app.
To use the Pearson Test Prep application, start by finding the registration code that comes with the book. You can find the code in these ways:

- **Print book**: Look in the cardboard sleeve in the back of the book for a piece of paper with your book’s unique PTP code.

- **Premium Edition**: If you purchase the Premium Edition eBook and Practice Test directly from the Cisco Press website, the code will be populated on your account page after purchase. Just log in at www.ciscopress.com, click account to see details of your account, and click the digital purchases tab.

- **Amazon Kindle**: For those who purchase a Kindle edition from Amazon, the access code will be supplied directly from Amazon.

- **Other Bookseller E-books**: Note that if you purchase an e-book version from any other source, the practice test is not included because other vendors to date have not chosen to vend the required unique access code.

**NOTE** Do not lose the activation code because it is the only means with which you can access the QA content with the book.

Once you have the access code, to find instructions about both the PTP web app and the desktop app, follow these steps:

**Step 1.** Open this book’s companion website, as was shown earlier in this Introduction under the heading “How to Access the Companion Website.”

**Step 2.** Click the Practice Exams button.

**Step 3.** Follow the instructions listed there both for installing the desktop app and for using the web app.

Note that if you want to use the web app only at this point, just navigate to www.pearsontestprep.com, establish a free login if you do not already have one, and register this book’s practice tests using the registration code you just found. The process should take only a couple of minutes.

**NOTE** Amazon eBook (Kindle) customers: It is easy to miss Amazon’s email that lists your PTP access code. Soon after you purchase the Kindle eBook, Amazon should send an email. However, the email uses very generic text, and makes no specific mention of PTP or practice exams. To find your code, read every email from Amazon after you purchase the book. Also do the usual checks for ensuring your email arrives like checking your spam folder.

**NOTE** Other eBook customers: As of the time of publication, only the publisher and Amazon supply PTP access codes when you purchase their eBook editions of this book.
Feature Reference

The following list provides an easy reference to get the basic idea behind each book feature:

- **Practice exam:** The book gives you the rights to the Pearson Test Prep (PTP) testing software, available as a web app and desktop app. Use the access code on a piece of cardboard in the sleeve in the back of the book, and use the companion website to download the desktop app or navigate to the web app (or just go to www.pearsontestprep.com).

- **E-book:** Pearson offers an e-book version of this book that includes extra practice tests. If interested, look for the special offer on a coupon card inserted in the sleeve in the back of the book. This offer enables you to purchase the *CCNA 200-301 Official Cert Guide, Volume 1, Premium Edition eBook and Practice Test* at a 70 percent discount off the list price. The product includes three versions of the e-book, PDF (for reading on your computer), EPUB (for reading on your tablet, mobile device, or Nook or other e-reader), and Mobi (the native Kindle version). It also includes additional practice test questions and enhanced practice test features.

- **Subnetting videos:** The companion website contains a series of videos that show you how to calculate various facts about IP addressing and subnetting (in particular, using the shortcuts described in this book).

- **Mentoring videos:** The companion website also includes a number of videos about other topics as mentioned in individual chapters.

- **Subnetting practice apps:** The companion website contains appendixes with a set of subnetting practice problems and answers. This is a great resource to practice building subnetting skills. You can also do these same practice problems with applications from the “Chapter and Part Review” section of the companion website.

- **CCNA 200-301 Network Simulator Lite:** This lite version of the best-selling CCNA Network Simulator from Pearson provides you with a means, right now, to experience the Cisco command-line interface (CLI). No need to go buy real gear or buy a full simulator to start learning the CLI. Just install it from the companion website.

- **CCNA Simulator:** If you are looking for more hands-on practice, you might want to consider purchasing the CCNA Network Simulator. You can purchase a copy of this software from Pearson at http://pearsonitcertification.com/networksimulator or other retail outlets. To help you with your studies, Pearson has created a mapping guide that maps each of the labs in the simulator to the specific sections in each volume of the CCNA Cert Guide. You can get this mapping guide free on the Extras tab on the book product page: www.ciscopress.com/title/9780135792735.

- **PearsonITCertification.com:** The website www.pearsonitcertification.com is a great resource for all things IT-certification related. Check out the great CCNA articles, videos, blogs, and other certification preparation tools from the industry’s best authors and trainers.
Author’s website and blogs: The author maintains a website that hosts tools and links useful when studying for CCNA. In particular, the site has a large number of free lab exercises about CCNA content, additional sample questions, and other exercises. Additionally, the site indexes all content so you can study based on the book chapters and parts. To find it, navigate to blog.certskills.com.

Book Organization, Chapters, and Appendixes

This book contains 29 core chapters, with each chapter covering a subset of the topics on the CCNA exam. The book organizes the chapters into parts of three to five chapters. The core chapters cover the following topics:

- **Part I: Introduction to Networking**
  - Chapter 1, “Introduction to TCP/IP Networking,” introduces the central ideas and terms used by TCP/IP, and contrasts the TCP/IP networking model with the OSI model.
  - Chapter 2, “Fundamentals of Ethernet LANs,” introduces the concepts and terms used when building Ethernet LANs.
  - Chapter 3, “Fundamentals of WANs and IP Routing,” covers the basics of the data-link layer for WANs in the context of IP routing but emphasizes the main network layer protocol for TCP/IP. This chapter introduces the basics of IPv4, including IPv4 addressing and routing.

- **Part II: Implementing Ethernet LANs**
  - Chapter 4, “Using the Command-Line Interface,” explains how to access the text-based user interface of Cisco Catalyst LAN switches.
  - Chapter 5, “Analyzing Ethernet LAN Switching,” shows how to use the Cisco CLI to verify the current status of an Ethernet LAN and how it switches Ethernet frames.
  - Chapter 6, “Configuring Basic Switch Management,” explains how to configure Cisco switches for basic management features, such as remote access using Telnet and SSH.
  - Chapter 7, “Configuring and Verifying Switch Interfaces,” shows how to configure a variety of switch features that apply to interfaces, including duplex/speed.

- **Part III: Implementing VLANs and STP**
  - Chapter 8, “Implementing Ethernet Virtual LANs,” explains the concepts and configuration surrounding virtual LANs, including VLAN trunking.
  - Chapter 9, “Spanning Tree Protocol Concepts,” discusses the concepts behind IEEE Spanning Tree Protocol (STP), including Rapid STP (RSTP) and how they make some switch interfaces block frames to prevent frames from looping continuously around a redundant switched LAN.
  - Chapter 10, “RSTP and EtherChannel Configuration,” shows how to configure and verify RSTP and Layer 2 EtherChannels on Cisco switches.
Part IV: IPv4 Addressing

■ Chapter 11, “Perspectives on IPv4 Subnetting,” walks you through the entire concept of subnetting, from starting with a Class A, B, or C network to a completed subnetting design as implemented in an enterprise IPv4 network.

■ Chapter 12, “Analyzing Classful IPv4 Networks,” explains how IPv4 addresses originally fell into several classes, with unicast IP addresses being in Class A, B, and C. This chapter explores all things related to address classes and the IP network concept created by those classes.

■ Chapter 13, “Analyzing Subnet Masks,” shows how an engineer can analyze the key facts about a subnetting design based on the subnet mask. This chapter shows how to look at the mask and IP network to determine the size of each subnet and the number of subnets.

■ Chapter 14, “Analyzing Existing Subnets,” describes how most troubleshooting of IP connectivity problems starts with an IP address and mask. This chapter shows how to take those two facts and find key facts about the IP subnet in which that host resides.

Part V: IPv4 Routing

■ Chapter 15, “Operating Cisco Routers,” is like Chapter 8, focusing on basic device management, but it focuses on routers instead of switches.

■ Chapter 16, “Configuring IPv4 Addressing and Static Routes,” discusses how to add IPv4 address configuration to router interfaces and how to configure static IPv4 routes.

■ Chapter 17, “IP Routing in the LAN,” shows how to configure and troubleshoot different methods of routing between VLANs, including Router-on-a-Stick (ROAS), Layer 3 switching with SVIs, Layer 3 switching with routed ports, and using Layer 3 EtherChannels.

■ Chapter 18, “Troubleshooting IPv4 Routing,” focuses on how to use two key troubleshooting tools to find routing problems: the ping and traceroute commands.

Part VI: OSPF

■ Chapter 19, “Understanding OSPF Concepts,” introduces the fundamental operation of the Open Shortest Path First (OSPF) protocol, focusing on link state fundamentals, neighbor relationships, flooding link state data, and calculating routes based on the lowest cost metric.

■ Chapter 20, “Implementing OSPF,” takes the concepts discussed in the previous chapter and shows how to configure and verify those same features.

■ Chapter 21, “OSPF Network Types and Neighbors,” takes the next steps in OSPF configuration and verification by looking in more depth at the concepts of how routers enable OSPF on interfaces, and the conditions that must be true before two routers will succeed in becoming OSPF neighbors.

Part VII: IP Version 6

■ Chapter 22, “Fundamentals of IP Version 6,” discusses the most basic concepts of IP version 6, focusing on the rules for writing and interpreting IPv6 addresses.
Chapter 23, “IPv6 Addressing and Subnetting,” works through the two branches of unicast IPv6 addresses—global unicast addresses and unique local addresses—that act somewhat like IPv4 public and private addresses, respectively.

Chapter 24, “Implementing IPv6 Addressing on Routers,” shows how to configure IPv6 routing and addresses on routers, while discussing a variety of special IPv6 addresses.

Chapter 25, “Implementing IPv6 Routing,” shows how to add static routes to an IPv6 router’s routing table.

Part VIII: Wireless LANs

Chapter 26, “Fundamentals of Wireless Networks,” introduces the foundational concepts of wireless 802.11 LANs, including wireless topologies and basic wireless radio communications protocols.

Chapter 27, “Analyzing Cisco Wireless Architectures,” turns your attention to the questions related to systematic and architectural issues surrounding how to build wireless LANs and explains the primary options available for use.

Chapter 28, “Securing Wireless Networks,” explains the unique security challenges that exist in a wireless LAN and the protocols and standards used to prevent different kinds of attacks.

Chapter 29, “Building a Wireless LAN,” shows how to configure and secure a wireless LAN using a Wireless LAN Controller (WLC).

Part IX: Print Appendixes

Appendix A, “Numeric Reference Tables,” lists several tables of numeric information, including a binary-to-decimal conversion table and a list of powers of 2.

Appendix B, “CCNA 200-301, Volume 1 Exam Updates,” is a place for the author to add book content mid-edition. Always check online for the latest PDF version of this appendix; the appendix lists download instructions.

Appendix C, “Answers to the ‘Do I Know This Already?’ Quizzes,” includes the explanations to all the “Do I Know This Already?” quizzes.

The Glossary contains definitions for all the terms listed in the “Key Terms You Should Know” sections at the conclusion of the chapters.

Part X: Online Appendixes

Practice Appendixes

The following appendixes are available in digital format from the companion website. These appendixes provide additional practice for several networking processes that use some math.

Appendix D, “Practice for Chapter 12: Analyzing Classful IPv4 Networks”

Appendix E, “Practice for Chapter 13: Analyzing Subnet Masks”

Appendix F, “Practice for Chapter 14: Analyzing Existing Subnets”

Although the publisher restarts numbering at edition “1” each time, the name of the related exam changes in a significant way. In function, this book is in effect part of the 9th edition of the CCNA Cert Guide materials from Cisco Press. From edition to edition, some readers over the years have asked that we keep some select chapters with the book. Keeping content that Cisco removed from the exam, but that may still be useful, can help the average reader as well as instructors who use the materials to teach courses with this book. The following appendices hold this edition’s content from previous editions:

- **Appendix J, “Topics from Previous Editions,”** is a collection of small topics from prior editions. None of the topics justify a complete appendix by themselves, so we collect the small topics into this single appendix.

- **Appendix K, “Analyzing Ethernet LAN Designs,”** examines various ways to design Ethernet LANs, discussing the pros and cons, and explains common design terminology.

- **Appendix L, “Subnet Design,”** takes a design approach to subnetting. This appendix begins with a classful IPv4 network and asks why a particular mask might be chosen, and if chosen, what subnet IDs exist.

- **Appendix M, “Practice for Appendix L: Subnet Design”**

- **Appendix N, “Variable-Length Subnet Masks,”** moves away from the assumption of one subnet mask per network to multiple subnet masks per network, which makes subnetting math and processes much more challenging. This appendix explains those challenges.

- **Appendix O, “Spanning Tree Protocol Implementation,”** shows how to configure and verify STP on Cisco switches.

- **Appendix P, “LAN Troubleshooting,”** examines the most common LAN switching issues and how to discover those issues when troubleshooting a network. The appendix includes troubleshooting topics for STP/RSTP, Layer 2 EtherChannel, LAN switching, VLANs, and LAN trunking.

- **Appendix Q, “Troubleshooting IPv4 Routing Protocols,”** walks through the most common problems with IPv4 routing protocols, while alternating between OSPF examples and EIGRP examples.

**Miscellaneous Appendices**

- **Appendix I, “Study Planner,”** is a spreadsheet with major study milestones, where you can track your progress through your study.

- **Appendix R, “Exam Topics Cross Reference,”** provides some tables to help you find where each exam objective is covered in the book.
About Building Hands-On Skills

You need skills in using Cisco routers and switches, specifically the Cisco command-line interface (CLI). The Cisco CLI is a text-based command-and-response user interface; you type a command, and the device (a router or switch) displays messages in response. To answer sim and simlet questions on the exams, you need to know a lot of commands, and you need to be able to navigate to the right place in the CLI to use those commands.

This next section walks through the options of what is included in the book, with a brief description of lab options outside the book.

Config Lab Exercises

Some router and switch features require multiple configuration commands. Part of the skill you need to learn is to remember which configuration commands work together, which ones are required, and which ones are optional. So, the challenge level goes beyond just picking the right parameters on one command. You have to choose which commands to use, in which combination, typically on multiple devices. And getting good at that kind of task requires practice.

Each Config Lab lists details about a straightforward lab exercise for which you should create a small set of configuration commands for a few devices. Each lab presents a sample lab topology, with some requirements, and you have to decide what to configure on each device. The answer then shows a sample configuration. Your job is to create the configuration and then check your answer versus the supplied answer.

Config Lab content resides outside the book at the author's blog site (blog.certskills.com). You can navigate to the Config Lab in a couple of ways from the site, or just go directly to https://blog.certskills.com/category/hands-on/config-lab/ to reach a list of all Config Labs. Figure I-6 shows the logo that you will see with each Config Lab.

Figure I-6 Config Lab Logo in the Author's Blogs

These Config Labs have several benefits, including the following:

Untethered and responsive: Do them from anywhere, from any web browser, from your phone or tablet, untethered from the book or DVD.

Designed for idle moments: Each lab is designed as a 5- to 10-minute exercise if all you are doing is typing in a text editor or writing your answer on paper.

Two outcomes, both good: Practice getting better and faster with basic configuration, or if you get lost, you have discovered a topic that you can now go back and reread to complete your knowledge. Either way, you are a step closer to being ready for the exam!
Blog format: The format allows easy adds and changes by me and easy comments by you.

Self-assessment: As part of final review, you should be able to do all the Config Labs, without help, and with confidence.

Note that the blog organizes these Config Lab posts by book chapter, so you can easily use these at both Chapter Review and Part Review. See the “Your Study Plan” element that follows the Introduction for more details about those review sections.

A Quick Start with Pearson Network Simulator Lite

The decision of how to get hands-on skills can be a little scary at first. The good news: You have a free and simple first step to experience the CLI: install and use the Pearson Network Simulator Lite (or NetSim Lite) that comes with this book.

This book comes with a lite version of the best-selling CCNA Network Simulator from Pearson, which provides you with a means, right now, to experience the Cisco CLI. No need to go buy real gear or buy a full simulator to start learning the CLI. Just install it from the companion website.

This latest version of NetSim Lite includes labs associated with Part II of this book, plus a few more from Part III. Part I includes concepts only, with Part II being the first part with commands. So, make sure to use the NetSim Lite to learn the basics of the CLI to get a good start.

Of course, one reason that you get access to the NetSim Lite is that the publisher hopes you will buy the full product. However, even if you do not use the full product, you can still learn from the labs that come with NetSim Lite while deciding about what options to pursue.

The Pearson Network Simulator

The Config Labs and the Pearson Network Simulator Lite both fill specific needs, and they both come with the book. However, you need more than those two tools.

The single best option for lab work to do along with this book is the paid version of the Pearson Network Simulator. This simulator product simulates Cisco routers and switches so that you can learn for CCNA certification. But more importantly, it focuses on learning for the exam by providing a large number of useful lab exercises. Reader surveys tell us that those people who use the Simulator along with the book love the learning process and rave about how the book and Simulator work well together.

Of course, you need to make a decision for yourself and consider all the options. Thankfully, you can get a great idea of how the full Simulator product works by using the Pearson Network Simulator Lite product included with the book. Both have the same base code, same user interface, and same types of labs. Try the Lite version to decide if you want to buy the full product.

Note that the Simulator and the books work on a different release schedule. For a time in 2019 (and probably into 2020), the Simulator will be the one created for the previous versions of the exams (ICND1 100-101, ICND2 200-101, and CCNA 200-120).
Interestingly, Cisco did not add a large number of new topics that require CLI skills to the CCNA 200-301 exam as compared with its predecessor, so the old Simulator covers most of the CLI topics. So, during the interim before the products based on the 200-301 exam come out, the old Simulator products should be quite useful.

On a practical note, when you want to do labs when reading a chapter or doing Part Review, the Simulator organizes the labs to match the book. Just look for the Sort by Chapter tab in the Simulator’s user interface. However, during the months in 2019 for which the Simulator is the older edition listing the older exams in the title, you will need to refer to a PDF that lists those labs versus this book’s organization. You can find that PDF on the book product page under the Downloads tab here: www.ciscopress.com/title/9780135792735.

More Lab Options

If you decide against using the full Pearson Network Simulator, you still need hands-on experience. You should plan to use some lab environment to practice as much CLI as possible.

First, you can use real Cisco routers and switches. You can buy them, new or used, or borrow them at work. You can rent them for a fee. If you have the right mix of gear, you could even do the Config Lab exercises from my blog on that gear or try to re-create examples from the book.

Cisco also makes a simulator that works very well as a learning tool: Cisco Packet Tracer. Cisco now makes Packet Tracer available for free. However, unlike the Pearson Network Simulator, it does not include lab exercises that direct you as to how to go about learning each topic. If interested in more information about Packet Tracer, check out my series about using Packet Tracer at my blog (blog.certskills.com); just search for “Packet Tracer.”

Cisco offers a virtualization product that lets you run router and switch operating system (OS) images in a virtual environment. This tool, the Virtual Internet Routing Lab (VIRL), lets you create a lab topology, start the topology, and connect to real router and switch OS images. Check out http://virl.cisco.com for more information.

You can even rent virtual Cisco router and switch lab pods from Cisco, in an offering called Cisco Learning Labs (https://learningnetworkstore.cisco.com/cisco-learning-labs).

This book does not tell you what option to use, but you should plan on getting some hands-on practice somehow. The important thing to know is that most people need to practice using the Cisco CLI to be ready to pass these exams.

For More Information

If you have any comments about the book, submit them via www.ciscopress.com. Just go to the website, select Contact Us, and type your message.
Cisco might make changes that affect the CCNA certification from time to time. You should always check www.cisco.com/go/ccna for the latest details.

The *CCNA 200-301 Official Cert Guide, Volume 1*, helps you attain CCNA certification. This is the CCNA certification book from the only Cisco-authorized publisher. We at Cisco Press believe that this book certainly can help you achieve CCNA certification, but the real work is up to you! I trust that your time will be well spent.
IP Routing in the LAN

This chapter covers the following exam topics:

1.0 Network Fundamentals
   1.6 Configure and verify IPv4 addressing and subnetting

2.0 Network Access
   2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)

The preceding two chapters showed how to configure an IP address and mask on a router interface, making the router ready to route packets to/from the subnet implied by that address/mask combination. While true and useful, all the examples so far ignored the LAN switches and the possibility of VLANs. In fact, the examples so far show the simplest possible cases: the attached switches as Layer 2 switches, using only one VLAN, with the router configured with one ip address command on its physical interface. This chapter takes a detailed look at how to configure routers so that they route packets to/from the subnets that exist on each and every VLAN.

Because Layer 2 switches do not forward Layer 2 frames between VLANs, a network must use routers to route IP packets between subnets to allow those devices in different VLANs/subnets to communicate. To review, Ethernet defines the concept of a VLAN, while IP defines the concept of an IP subnet, so a VLAN is not equivalent to a subnet. However, the set of devices in one VLAN are typically also in one subnet. By the same reasoning, devices in two different VLANs are normally in two different subnets. For two devices in different VLANs to communicate with each other, routers must connect to the subnets that exist on each VLAN, and then the routers forward IP packets between the devices in those subnets.

This chapter discusses the configuration and verification steps related to three methods of routing between VLANs with three major sections:

- **VLAN Routing with Router 802.1Q Trunks:** The first section discusses how to configure a router to use VLAN trunking as connected to a Layer 2 switch. The router does the routing, with the switch creating the VLANs. The link between the router and switch use trunking so that the router has an interface connected to each VLAN/subnet. This feature is known as routing over a VLAN trunk and also known as router-on-a-stick (ROAS).

- **VLAN Routing with Layer 3 Switch SVIs:** The second section discusses using a LAN switch that supports both Layer 2 switching and Layer 3 routing (called a Layer 3 switch or multilayer switch). To route, the Layer 3 switch configuration uses interfaces called switched virtual interfaces (SVI), which are also called VLAN interfaces.

- **VLAN Routing with Layer 3 Switch Routed Ports:** The third major section of the chapter discusses an alternative to SVIs called routed ports, in which the physical switch ports are made to act like interfaces on a router. This third section also introduces the concept of an EtherChannel as used as a routed port in a feature called Layer 3 EtherChannel.
“Do I Know This Already?” Quiz

Take the quiz (either here or use the PTP software) if you want to use the score to help you decide how much time to spend on this chapter. The letter answers are listed at the bottom of the page following the quiz. Appendix C, found both at the end of the book as well as on the companion website, includes both the answers and explanations. You can also find both answers and explanations in the PTP testing software.

Table 17-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

<table>
<thead>
<tr>
<th>Foundation Topics Section</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Routing with Router 802.1Q Trunks</td>
<td>1, 2</td>
</tr>
<tr>
<td>VLAN Routing with Layer 3 Switch SVIs</td>
<td>3, 4</td>
</tr>
<tr>
<td>VLAN Routing with Layer 3 Switch Routed Ports</td>
<td>5, 6</td>
</tr>
</tbody>
</table>

1. Router 1 has a Fast Ethernet interface 0/0 with IP address 10.1.1.1. The interface is connected to a switch. This connection is then migrated to use 802.1Q trunking. Which of the following commands could be part of a valid configuration for Router 1’s Fa0/0 interface? (Choose two answers.)
   - a. interface fastethernet 0/0.4
   - b. dot1q enable
   - c. dot1q enable 4
   - d. trunking enable
   - e. trunking enable 4
   - f. encapsulation dot1q 4

2. Router R1 has a router-on-a-stick (ROAS) configuration with two subinterfaces of interface G0/1: G0/1.1 and G0/1.2. Physical interface G0/1 is currently in a down/down state. The network engineer then configures a shutdown command when in interface configuration mode for G0/1.1 and a no shutdown command when in interface configuration mode for G0/1.2. Which answers are correct about the interface state for the subinterfaces? (Choose two answers.)
   - a. G0/1.1 will be in a down/down state.
   - b. G0/1.2 will be in a down/down state.
   - c. G0/1.1 will be in an administratively down state.
   - d. G0/1.2 will be in an up/up state.
3. A Layer 3 switch has been configured to route IP packets between VLANs 1, 2, and 3 using SVIs, which connect to subnets 172.20.1.0/25, 172.20.2.0/25, and 172.20.3.0/25, respectively. The engineer issues a `show ip route connected` command on the Layer 3 switch, listing the connected routes. Which of the following answers lists a piece of information that should be in at least one of the routes?
   a. Interface Gigabit Ethernet 0/0.3
   b. Next-hop router 172.20.2.1
   c. Interface VLAN 2
   d. Mask 255.255.255.0

4. An engineer has successfully configured a Layer 3 switch with SVIs for VLANs 2 and 3. Hosts in the subnets using VLANs 2 and 3 can ping each other with the Layer 3 switch routing the packets. The next week, the network engineer receives a call that those same users can no longer ping each other. If the problem is with the Layer 3 switching function, which of the following could have caused the problem? (Choose two answers.)
   a. Six (or more) out of 10 working VLAN 2 access ports failing due to physical problems
   b. A `shutdown` command issued from interface VLAN 4 configuration mode
   c. VTP on the switch removing VLAN 3 from the switch's VLAN list
   d. A `shutdown` command issued from VLAN 2 configuration mode

5. A LAN design uses a Layer 3 EtherChannel between two switches SW1 and SW2, with port-channel interface 1 used on both switches. SW1 uses ports G0/1, G0/2, and G0/3 in the channel. Which of the following are true about SW1's configuration to make the channel be able to route IPv4 packets correctly? (Choose two answers.)
   a. The `ip address` command must be on the port-channel 1 interface.
   b. The `ip address` command must be on interface G0/1 (lowest numbered port).
   c. The port-channel 1 interface must be configured with the `no switchport` command.
   d. Interface G0/1 must be configured with the `routedport` command.

6. A LAN design uses a Layer 3 EtherChannel between two switches SW1 and SW2, with port-channel interface 1 used on both switches. SW1 uses ports G0/1 and G0/2 in the channel. However, only interface G0/1 is bundled into the channel and working. Think about the configuration settings on port G0/2 that could have existed before adding G0/2 to the EtherChannel. Which answers identify a setting that could prevent IOS from adding G0/2 to the Layer 3 EtherChannel? (Choose two answers.)
   a. A different STP cost (`spanning-tree cost value`)
   b. A different speed (`speed value`)
   c. A default setting for switchport (`switchport`)
   d. A different access VLAN (`switchport access vlan vlan-id`)
Foundation Topics

VLAN Routing with Router 802.1Q Trunks

Almost all enterprise networks use VLANs. To route IP packets in and out of those VLANs, some devices (either routers or Layer 3 switches) need to have an IP address in each subnet and have a connected route to each of those subnets. Then the IP addresses on those routers or Layer 3 switches can serve as the default gateways in those subnets.

This chapter breaks down the LAN routing options into four categories:

■ Use a router, with one router LAN interface and cable connected to the switch for each and every VLAN (typically not used)
■ Use a router, with a VLAN trunk connecting to a LAN switch (known as router-on-a-stick, or ROAS)
■ Use a Layer 3 switch with switched virtual interfaces (SVI)
■ Use a Layer 3 switch with routed interfaces (which may or may not be Layer 3 EtherChannels)

Of the items in the list, the first option works, but to be practical, it requires far too many interfaces. It is mentioned here only to make the list complete.

As for the other three options, this chapter discusses each in turn as the main focus of one of the three major sections in this chapter. Each feature is used in real networks today, with the choice to use one or the other driven by the design and needs for a particular part of the network. Figure 17-1 shows cases in which these options could be used.

Figure 17-1 shows two switches, labeled A and B, which could act as Layer 3 switches—both with SVIs and routed interfaces. The figure shows a central site campus LAN on the left, with 12 VLANs. Switches A and B act as Layer 3 switches, combining the functions of a router and a switch, routing between all 12 subnets/VLANs, as well as routing to/from the Core router. Those Layer 3 switches could use SVIs, routed interfaces, or both.

Figure 17-1 also shows a classic case for using a router with a VLAN trunk. Sites like the remote sites on the right side of the figure may have a WAN-connected router and a LAN
switch. These sites might use ROAS to take advantage of the router’s ability to route over an 802.1Q trunk.

Note that Figure 17-1 just shows an example. The engineer could use Layer 3 switching at each site or routers with VLAN trunking at each site.

Configuring ROAS

This next topic discusses how routers route packets to subnets associated with VLANs connected to a router 802.1Q trunk. That long description can be a bit of a chore to repeat each time someone wants to discuss this feature, so over time, the networking world has instead settled on a shorter and more interesting name for this feature: router-on-a-stick (ROAS).

ROAS uses router VLAN trunking configuration to give the router a logical router interface connected to each VLAN. Because the router then has an interface connected to each VLAN, the router can also be configured with an IP address in the subnet that exists on each VLAN.

Routers use subinterfaces as the means to have an interface connected to a VLAN. The router needs to have an IP address/mask associated with each VLAN on the trunk. However, the router has only one physical interface for the link connected to the trunk. Cisco solves this problem by creating multiple virtual router interfaces, one associated with each VLAN on that trunk (at least for each VLAN that you want the trunk to support). Cisco calls these virtual interfaces subinterfaces. The configuration can then include an `ip address` command for each subinterface.

Figure 17-2 shows the concept with Router B1, one of the branch routers from Figure 17-1. Because this router needs to route between only two VLANs, the figure also shows two subinterfaces, named G0/0.10 and G0/0.20, which create a new place in the configuration where the per-VLAN configuration settings can be made. The router treats frames tagged with VLAN 10 as if they came in or out of G0/0.10 and frames tagged with VLAN 20 as if they came in or out of G0/0.20.

![Figure 17-2 Subinterfaces on Router B1](image-url)

In addition, note that most Cisco routers do not attempt to negotiate trunking, so both the router and switch need to manually configure trunking. This chapter discusses the router side of that trunking configuration; the matching switch interface would need to be configured with the `switchport mode trunk` command.

Answers to the “Do I Know This Already?” quiz:

1. A, F
2. B, C
3. C
4. C
5. A, C
6. B, C
Example 17-1 shows a full example of the 802.1Q trunking configuration required on Router B1 in Figure 17-2. More generally, these steps detail how to configure 802.1Q trunking on a router:

**Step 1.** Use the `interface type number.subint` command in global configuration mode to create a unique subinterface for each VLAN that needs to be routed.

**Step 2.** Use the `encapsulation dot1q vlan_id` command in subinterface configuration mode to enable 802.1Q and associate one specific VLAN with the subinterface.

**Step 3.** Use the `ip address address mask` command in subinterface configuration mode to configure IP settings (address and mask).

### Example 17-1 Router Configuration for the 802.1Q Encapsulation Shown in Figure 17-2

```
B1# show running-config
! Only pertinent lines shown
interface gigabitethernet 0/0
! No IP address up here! No encapsulation up here!

interface gigabitethernet 0/0.10
encapsulation dot1q 10
ip address 10.1.10.1 255.255.255.0

interface gigabitethernet 0/0.20
encapsulation dot1q 20
ip address 10.1.20.1 255.255.255.0
```

First, look at the subinterface numbers. The subinterface number begins with the period, like .10 and .20 in this case. These numbers can be any number from 1 up through a very large number (over 4 billion). The number just needs to be unique among all subinterfaces associated with this one physical interface. In fact, the subinterface number does not even have to match the associated VLAN ID. (The `encapsulation` command, and not the subinterface number, defines the VLAN ID associated with the subinterface.)

**NOTE** Although not required, most sites do choose to make the subinterface number match the VLAN ID, as shown in Example 17-1, just to avoid confusion.

Each subinterface configuration lists two subcommands. One command (`encapsulation`) enables trunking and defines the VLAN whose frames are considered to be coming in and out of the subinterface. The `ip address` command works the same way it does on any other interface. Note that if the physical Ethernet interface reaches an up/up state, the subinterface should as well, which would then let the router add the connected routes shown at the bottom of the example.

Now that the router has a working interface, with IPv4 addresses configured, the router can route IPv4 packets on these subinterfaces. That is, the router treats these subinterfaces like
any physical interface in terms of adding connected routes, matching those routes, and forwarding packets to/from those connected subnets.

The configuration and use of the native VLAN on the trunk require a little extra thought. The native VLAN can be configured on a subinterface, or on the physical interface, or ignored as in Example 17-1. Each 802.1Q trunk has one native VLAN, and if the router needs to route packets for a subnet that exists in the native VLAN, then the router needs some configuration to support that subnet. The two options to define a router interface for the native VLAN are

- Configure the `ip address` command on the physical interface, but without an `encapsulation` command; the router considers this physical interface to be using the native VLAN.
- Configure the `ip address` command on a subinterface and use the `encapsulation dot1q vlan-id native` subcommand to tell the router both the VLAN ID and the fact that it is the native VLAN.

Example 17-2 shows both native VLAN configuration options with a small change to the same configuration in Example 17-1. In this case, VLAN 10 becomes the native VLAN. The top part of the example shows the option to configure the router physical interface to use native VLAN 10. The second half of the example shows how to configure that same native VLAN on a subinterface. In both cases, the switch configuration also needs to be changed to make VLAN 10 the native VLAN.

**Example 17-2  Router Configuration Using Native VLAN 10 on Router B1**

```plaintext
! First option: put the native VLAN IP address on the physical interface
interface gigabitethernet 0/0
  ip address 10.1.10.1 255.255.255.0

! Second option: like Example 17-1, but add the native keyword
interface gigabitethernet 0/0.10
  encapsulation dot1q 10 native
  ip address 10.1.10.1 255.255.255.0
```

**Verifying ROAS**

Beyond using the `show running-config` command, ROAS configuration on a router can be best verified with two commands: `show ip route [connected]` and `show vlans`. As with any router interface, as long as the interface is in an up/up state and has an IPv4 address configured, IOS will put a connected (and local) route in the IPv4 routing table. So, a first and obvious check would be to see if all the expected connected routes exist. Example 17-3 lists the connected routes per the configuration shown in Example 17-1.
Example 17-3  Connected Routes Based on Example 17-1 Configuration

```
B1# show ip route connected
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
| Legend omitted for brevity |
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C  10.1.10.0/24 is directly connected, GigabitEthernet0/0.10
L  10.1.10.1/32 is directly connected, GigabitEthernet0/0.10
C  10.1.20.0/24 is directly connected, GigabitEthernet0/0.20
L  10.1.20.1/32 is directly connected, GigabitEthernet0/0.20
```

As for interface and subinterface state, note that the ROAS subinterface state does depend to some degree on the physical interface state. In particular, the subinterface state cannot be better than the state of the matching physical interface. For instance, on Router B1 in the examples so far, physical interface G0/0 is in an up/up state, and the subinterfaces are in an up/up state. But if you unplugged the cable from that port, the physical port would fail to a down/down state, and the subinterfaces would also fail to a down/down state. Example 17-4 shows another example, with the physical interface being shut down, with the subinterfaces then automatically changed to an administratively down state as a result.

Example 17-4  Subinterface State Tied to Physical Interface State

```
B1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
B1(config)# interface g0/0
B1(config-if)# shutdown
B1(config-if)# ^Z
B1# show ip interface brief | include 0/0
  GigabitEthernet0/0         unassigned      YES manual administratively down down
  GigabitEthernet0/0.10      10.1.10.1       YES manual administratively down down
  GigabitEthernet0/0.20      10.1.20.1       YES manual administratively down down
```

Additionally, the subinterface state can also be enabled and disabled independently from the physical interface, using the no shutdown and shutdown commands in subinterface configuration mode.

Another useful ROAS verification command, show vlans, spells out which router trunk interfaces use which VLANs, which VLAN is the native VLAN, plus some packet statistics. The fact that the packet counters are increasing can be useful when verifying whether traffic is happening or not. Example 17-5 shows a sample, based on the Router B1 configuration in Example 17-2 (bottom half), in which native VLAN 10 is configured on subinterface G0/0.10. Note that the output identifies VLAN 1 associated with the physical interface, VLAN 10 as the native VLAN associated with G0/0.10, and VLAN 20 associated with G0/0.20. It also lists the IP addresses assigned to each interface/subinterface.
Example 17-5  Sample show vlans Command to Match Sample Router Trunking Configuration

R1# show vlans
Virtual LAN ID: 1 (IEEE 802.1Q Encapsulation)

VLAN Trunk Interface: GigabitEthernet0/0

Protocols Configured: Address: Received: Transmitted:
Other 0 83

69 packets, 20914 bytes input
147 packets, 11841 bytes output

Virtual LAN ID: 10 (IEEE 802.1Q Encapsulation)

VLAN Trunk Interface: GigabitEthernet0/0.10

This is configured as native Vlan for the following interface(s):
GigabitEthernet0/0 Native-vlan Tx-type: Untagged

Protocols Configured: Address: Received: Transmitted:
IP 10.1.10.1 2 3
Other 0 1

3 packets, 722 bytes input
4 packets, 264 bytes output

Virtual LAN ID: 20 (IEEE 802.1Q Encapsulation)

VLAN Trunk Interface: GigabitEthernet0/0.20

Protocols Configured: Address: Received: Transmitted:
IP 10.1.20.1 0 134
Other 0 1

0 packets, 0 bytes input
135 packets, 10498 bytes output

Troubleshooting ROAS

The biggest challenge when troubleshooting ROAS has to do with the fact that if you mis-configure only the router or misconfigure only the switch, the other device on the trunk has no way to know that the other side is misconfigured. That is, if you check the show ip route and show vlans commands on a router, and the output looks like it matches the intended configuration, and the connected routes for the correct subinterfaces show up, routing may still fail because of problems on the attached switch. So, troubleshooting ROAS often begins with checking the configuration on both the router and switch because there is no status output on either device that tells you where the problem might be.
Chapter 17: IP Routing in the LAN

First, to check ROAS on the router, you need to start with the intended configuration and ask questions about the configuration:

1. Is each non-native VLAN configured on the router with an `encapsulation dot1q vlan-id` command on a subinterface?
2. Do those same VLANs exist on the trunk on the neighboring switch (`show interfaces trunk`), and are they in the allowed list, not VTP pruned, and not STP blocked?
3. Does each router ROAS subinterface have an IP address/mask configured per the planned configuration?
4. If using the native VLAN, is it configured correctly on the router either on a subinterface (with an `encapsulation dot1q vlan-id native` command) or implied on the physical interface?
5. Is the same native VLAN configured on the neighboring switch's trunk in comparison to the native VLAN configured on the router?
6. Are the router physical or ROAS subinterfaces configured with a `shutdown` command?

For some of these steps, you need to be ready to investigate possible VLAN trunking issues on the LAN switch. The reason is that on many Cisco routers, router interfaces do not negotiate trunking. As a result, ROAS relies on static trunk configuration on both the router and switch. If the switch has any problems with VLANs or the VLAN trunking configuration on its side of the trunk, the router has no way to realize that the problem exists.

For example, imagine you configured ROAS on a router just like in Example 17-1 or Example 17-2. However, the switch on the other end of the link had no matching configuration. For instance, maybe the switch did not even define VLANs 10 and 20. Maybe the switch did not configure trunking on the port connected to the router. Even with blatant misconfiguration or missing configuration on the switch, the router still shows up/up ROAS interfaces and subinterfaces, IP routes in the output of `show ip route`, and meaningful configuration information in the output of the `show vlans` command.

VLAN Routing with Layer 3 Switch SVIs

Using a router with ROAS to route packets makes sense in some cases, particularly at small remote sites. In sites with a larger LAN, network designers choose to use Layer 3 switches for most inter-VLAN routing.

A Layer 3 switch (also called a multilayer switch) is one device, but it executes logic at two layers: Layer 2 LAN switching and Layer 3 IP routing. The Layer 2 switch function forwards frames inside each VLAN, but it will not forward frames between VLANs. The Layer 3 forwarding (routing) logic forwards IP packets between VLANs.

Layer 3 switches typically support two configuration options to enable IPv4 routing inside the switch, specifically to enable IPv4 on switch interfaces. This section explains one option, an option that uses switched virtual interfaces (SVI). The final major section of the chapter deals with the other option for configuring IPv4 addresses on Layer 3 switches: routed interfaces.

Configuring Routing Using Switch SVIs

The configuration of a Layer 3 switch mostly looks like the Layer 2 switching configuration shown back in Parts II and III of this book, with a small bit of configuration added for
the Layer 3 functions. The Layer 3 switching function needs a virtual interface connected to
each VLAN internal to the switch. These VLAN interfaces act like router interfaces, with
an IP address and mask. The Layer 3 switch has an IP routing table, with connected routes
off each of these VLAN interfaces. (These interfaces are also referred to as switched virtual
interfaces [SVI].)

To show the concept of Layer 3 switching with SVIs, the following example uses the same
branch office with two VLANs shown in the earlier examples, but now the design will use
Layer 3 switching in the LAN switch. Figure 17-3 shows the design changes and configura-
tion concept for the Layer 3 switch function with a router icon inside the switch, to empha-
size that the switch routes the packets.

![Figure 17-3: Routing on VLAN Interfaces in a Layer 3 Switch](image)

Note that the figure represents the internals of the Layer 3 switch within the box in the
middle of the figure. The branch still has two user VLANs (10 and 20), so the Layer 3 switch
needs one VLAN interface for each VLAN. The figure shows a router icon inside the gray
box to represent the Layer 3 switching function, with two VLAN interfaces on the right side
of that icon. In addition, the traffic still needs to get to router B1 (a physical router) to access
the WAN, so the switch uses a third VLAN (VLAN 30 in this case) for the link to Router
B1. The physical link between the Layer 3 switch and router B1 would not be a trunk, but
instead be an access link.

The following steps show how to configure Layer 3 switching using SVIs. Note that on some
switches, like the 2960 and 2960-XR switches used for the examples in this book, the ability
to route IPv4 packets must be enabled first, with a reload of the switch required to enable
the feature. The steps that occur after the reload would apply to all models of Cisco switches
that are capable of doing Layer 3 switching.

**Step 1.** Enable IP routing on the switch, as needed:

A. Use the `sdm prefer lanbase-routing` command (or similar) in global config-
   uration mode to change the switch forwarding ASIC settings to make space
   for IPv4 routes at the next reload of the switch.

B. Use the `reload` EXEC command in enable mode to reload (reboot) the
   switch to pick up the new `sdm prefer` command setting.

C. Once reloaded, use the `ip routing` command in global configuration mode
to enable the IPv4 routing function in IOS software and to enable key com-
   mands like `show ip route`.
Step 2. Configure each SVI interface, one per VLAN for which routing should be done by this Layer 3 switch:

A. Use the interface vlan vlan_id command in global configuration mode to create a VLAN interface and to give the switch's routing logic a Layer 3 interface connected into the VLAN of the same number.

B. Use the ip address address mask command in VLAN interface configuration mode to configure an IP address and mask on the VLAN interface, enabling IPv4 routing on that VLAN interface.

C. (As needed) Use the no shutdown command in interface configuration mode to enable the VLAN interface (if it is currently in a shutdown state).

Example 17-6 shows the configuration to match Figure 17-3. In this case, switch SW1 has already used the sdm prefer global command to change to a setting that supports IPv4 routing, and the switch has been reloaded. The example shows the related configuration on all three VLAN interfaces.

Example 17-6 VLAN Interface Configuration for Layer 3 Switching

```
ip routing

interface vlan 10
  ip address 10.1.10.1 255.255.255.0

interface vlan 20
  ip address 10.1.20.1 255.255.255.0

interface vlan 30
  ip address 10.1.30.1 255.255.255.0
```

Verifying Routing with SVIs

With the VLAN configuration shown in the previous section, the switch is ready to route packets between the VLANs as shown in Figure 17-3. To support the routing of packets, the switch adds connected IP routes as shown in Example 17-7; note that each route is listed as being connected to a different VLAN interface.

Example 17-7 Connected Routes on a Layer 3 Switch

```
SW1# show ip route
  legend omitted for brevity

   10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C   10.1.0.0/24 is directly connected, Vlan10
L   10.1.10.0/24 is directly connected, Vlan10
C   10.1.20.0/24 is directly connected, Vlan20
L   10.1.20.0/24 is directly connected, Vlan20
C   10.1.30.0/24 is directly connected, Vlan30
L   10.1.30.0/24 is directly connected, Vlan30
```
The switch would also need additional routes to the rest of the network (not shown in the figures in this chapter). The Layer 3 switch could use static routes or a routing protocol, depending on the capabilities of the switch. For instance, if you then enabled OSPF on the Layer 3 switch, the configuration and verification would work the same as it does on a router, as discussed in Chapter 20, “Implementing OSPF.” The routes that IOS adds to the Layer 3 switch’s IP routing table would list the VLAN interfaces as outgoing interfaces.

NOTE Some models of Cisco enterprise switches, based on model, IOS version, and IOS feature set, support different capabilities for IP routing and routing protocols, so for real networks, check the capabilities of the switch model by browsing at Cisco.com. In particular, check the Cisco Feature Navigator (CFN) tool at http://www.cisco.com/go/cfn.

Troubleshooting Routing with SVIs
There are two big topics to investigate when troubleshooting routing over LANs with SVIs. First, you have to make sure the switch has been enabled to support IP routing. Second, the VLAN associated with each VLAN interface must be known and active on the local switch; otherwise, the VLAN interfaces do not come up.

First, about enabling IP routing, note that some models of Cisco switches default to enable Layer 3 switching, and some do not. So, to make sure your switch supports Layer 3 routing, look to those first few configuration commands listed in the configuration checklist found in the earlier section “Configuring Routing Using Switch SVIs.” Those commands are `sdm prefer` (followed by a `reload`) and then `ip routing` (after the `reload`).

The `sdm prefer` command changes how the switch forwarding chips allocate memory for different forwarding tables, and changes to those tables require a reload of the switch. By default, many access switches that support Layer 3 switching still have an SDM default that does not allocate space for an IP routing table. Once changed and reloaded, the `ip routing` command then enables IPv4 routing in IOS software. Both are necessary before some Cisco switches will act as a Layer 3 switch.

Example 17-8 shows some symptoms on a router for which Layer 3 switching had not yet been enabled by the `sdm prefer` command. As you can see, both the `show ip route` EXEC command and the `ip routing config` command are rejected because they do not exist to IOS until the `sdm prefer` command has been used (followed by a `reload` of the switch).

Example 17-8 Evidence That a Switch Has Not Yet Enabled IPv4 Routing

```
SW1# show ip route
^% Invalid input detected at '^' marker.

SW3# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)# ip routing
^% Invalid input detected at '^' marker.
```
The second big area to investigate when troubleshooting SVIs relates to the SVI state, a state that ties to the state of the associated VLANs. Each VLAN interface has a matching VLAN of the same number, and the VLAN interface's state is tied to the state of the VLAN in certain ways. In particular, for a VLAN interface to be in an up/up state:

**Step 1.** The VLAN must be defined on the local switch (either explicitly or learned with VTP).

**Step 2.** The switch must have at least one up/up interface using the VLAN, either/both:

A. An up/up access interface assigned to that VLAN

B. A trunk interface for which the VLAN is in the allowed list, is STP forwarding, and is not VTP pruned

**Step 3.** The VLAN (not the VLAN interface) must be administratively enabled (that is, not shutdown).

**Step 4.** The VLAN interface (not the VLAN) must be administratively enabled (that is, not shutdown).

When working through the steps in the list, keep in mind that the VLAN and the VLAN interface are related but separate ideas, and the configuration items are separate in the CLI. The VLAN interface is a switch's Layer 3 interface connected to the VLAN. If you want to route packets for the subnets on VLANs 11, 12, and 13, the matching VLAN interfaces must be numbered 11, 12, and 13. And both the VLANs and the VLAN interfaces can be disabled and enabled with the `shutdown` and `no shutdown` commands (as mentioned in Steps 3 and 4 in the previous list), so you have to check for both.

Example 17-9 shows three scenarios, each of which leads to one of the VLAN interfaces in the previous configuration example (Figure 17-3, Example 17-6) to fail. At the beginning of the example, all three VLAN interfaces are up/up. VLANs 10, 20, and 30 each have at least one access interface up and working. The example works through three scenarios:

- **Scenario 1:** The last access interface in VLAN 10 is shut down (F0/1), so IOS shuts down the VLAN 10 interface.
- **Scenario 2:** VLAN 20 (not VLAN interface 20, but VLAN 20) is deleted, which results in IOS then bringing down (not shutting down) the VLAN 20 interface.
- **Scenario 3:** VLAN 30 (not VLAN interface 30, but VLAN 30) is shut down, which results in IOS then bringing down (not shutting down) the VLAN 30 interface.

### Example 17-9  Three Examples That Cause VLAN Interfaces to Fail

<table>
<thead>
<tr>
<th>SW1# show interfaces status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only ports related to the example are shown</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>Fa0/1</td>
</tr>
<tr>
<td>Fa0/2</td>
</tr>
<tr>
<td>Fa0/3</td>
</tr>
<tr>
<td>Fa0/4</td>
</tr>
<tr>
<td>Gi0/1</td>
</tr>
</tbody>
</table>
SW# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

<table>
<thead>
<tr>
<th>Case 1: Interface F0/1, the last up/up access interface in VLAN 10, is shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW1(config)# interface fastEthernet 0/1</td>
</tr>
<tr>
<td>SW1(config-if)# shutdown</td>
</tr>
<tr>
<td>SW1(config-if)#</td>
</tr>
<tr>
<td>*Apr 2 19:54:08.784: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to down</td>
</tr>
<tr>
<td>SW1(config-if)#</td>
</tr>
<tr>
<td>*Apr 2 19:54:10.772: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down</td>
</tr>
<tr>
<td>*Apr 2 19:54:11.779: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case 2: VLAN 20 is deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW1(config)# no vlan 20</td>
</tr>
<tr>
<td>SW1(config)#</td>
</tr>
<tr>
<td>*Apr 2 19:54:39.688: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to down</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case 3: VLAN 30, the VLAN from the switch to the router, is shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW1(config)# vlan 30</td>
</tr>
<tr>
<td>SW1(config-vlan)# shutdown</td>
</tr>
<tr>
<td>SW1(config-vlan)# exit</td>
</tr>
<tr>
<td>SW1(config)#</td>
</tr>
<tr>
<td>*Apr 2 19:55:25.204: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to down</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Final status of all three VLAN interfaces are below</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW1# show ip interface brief</td>
</tr>
<tr>
<td>Vlan1</td>
</tr>
<tr>
<td>Vlan10</td>
</tr>
<tr>
<td>Vlan20</td>
</tr>
<tr>
<td>Vlan30</td>
</tr>
</tbody>
</table>

Note that the example ends with the three VLAN interfaces in an up/down state per the show ip interface brief command.

VLAN Routing with Layer 3 Switch Routed Ports

When Layer 3 switches use SVIs, the physical interfaces on the switches act like they always have: as Layer 2 interfaces. That is, the physical interfaces receive Ethernet frames. The switch learns the source MAC address of the frame, and the switch forwards the frame based on the destination MAC address. To perform routing, any Ethernet frames destined for any of the SVI interface MAC addresses trigger the processing of the Layer 2 switching logic, resulting in normal routing actions like stripping data-link headers, making a routing decision, and so on.
Chapter 17: IP Routing in the LAN

Alternately, the Layer 3 switch configuration can make a physical port act like a router interface instead of a switch interface. To do so, the switch configuration makes that port a routed port. On a routed port, the switch does not perform Layer 2 switching logic on that frame. Instead, frames arriving in a routed port trigger the Layer 3 routing logic, including:

1. Stripping off the incoming frame’s Ethernet data-link header/trailer
2. Making a Layer 3 forwarding decision by comparing the destination IP address to the IP routing table
3. Adding a new Ethernet data-link header/trailer to the packet
4. Forwarding the packet, encapsulated in a new frame

This third major section of the chapter examines routed interfaces as configured on Cisco Layer 3 switches, but with a particular goal in mind: to also discuss Layer 3 EtherChannels. The exam topics do not mention routed interfaces specifically, but the exam topics do mention L3 EtherChannels, meaning Layer 3 EtherChannels.

You might recall that Chapter 10, “RSTP and EtherChannel Configuration,” discussed Layer 2 EtherChannels. Like Layer 2 EtherChannels, Layer 3 EtherChannels also treat multiple links as one link. Unlike Layer 2 EtherChannels, however, Layer 3 EtherChannels treat the channel as a routed port instead of switched port. So this section first looks at routed ports on Cisco Layer 3 switches and then discusses Layer 3 EtherChannels.

Implementing Routed Interfaces on Switches

When a Layer 3 switch needs a Layer 3 interface connected to a subnet, and only one physical interface connects to that subnet, the network engineer can choose to use a routed port instead of an SVI. Conversely, when the Layer 3 switch needs a Layer 3 interface connected to a subnet, and many physical interfaces on the switch connect to that subnet, an SVI needs to be used. (SVIs forward traffic internally into the VLAN, so that then the Layer 2 logic can forward the frame out any of the ports in the VLAN. Routed ports cannot.)

To see why, consider the design in Figure 17-4, which repeats the same design from Figure 17-3 (used in the SVI examples). In that design, the gray rectangle on the right represents the switch and its internals. On the right of the switch, at least two access ports sit in both VLAN 10 and VLAN 20. However, that figure shows a single link from the switch to Router B1. The switch could configure the port as an access port in a separate VLAN, as shown with VLAN 30 in Examples 17-6 and 17-7. However, with only one switch port needed, the switch could configure that link as a routed port, as shown in the figure.

![Figure 17-4 Routing on a Routed Interface on a Switch](image-url)
Enabling a switch interface to be a routed interface instead of a switched interface is simple: just use the `no switchport` subcommand on the physical interface. Cisco switches capable of being a Layer 3 switch use a default of the `switchport` command to each switch physical interface. Think about the word `switchport` for a moment. With that term, Cisco tells the switch to treat the port like it is a port on a switch—that is, a Layer 2 port on a switch. To make the port stop acting like a switch port and instead act like a router port, use the `no switchport` command on the interface.

Once the port is acting as a routed port, think of it like a router interface. That is, configure the IP address on the physical port, as implied in Figure 17-4. Example 17-10 shows a completed configuration for the interfaces configured on the switch in Figure 17-4. Note that the design uses the exact same IP subnets as the example that showed SVI configuration in Example 17-6, but now, the port connected to subnet 10.1.30.0 has been converted to a routed port. All you have to do is add the `no switchport` command to the physical interface and configure the IP address on the physical interface.

**Example 17-10 Configuring Interface G0/1 on Switch SW1 as a Routed Port**

```plaintext
ip routing

interface vlan 10
  ip address 10.1.10.1 255.255.255.0

interface vlan 20
  ip address 10.1.20.1 255.255.255.0

interface gigabitethernet 0/1
  no switchport
  ip address 10.1.30.1 255.255.255.0
```

Once configured, the routed interface will show up differently in command output in the switch. In particular, for an interface configured as a routed port with an IP address, like interface GigabitEthernet0/1 in the previous example:

- **show interfaces**: Similar to the same command on a router, the output will display the IP address of the interface. (Conversely, for switch ports, this command does not list an IP address.)
- **show interfaces status**: Under the “VLAN” heading, instead of listing the access VLAN or the word `trunk`, the output lists the word `routed`, meaning that it is a routed port.
- **show ip route**: Lists the routed port as an outgoing interface in routes.
- **show interfaces type number switchport**: If a routed port, the output is short and confirms that the port is not a switch port. (If the port is a Layer 2 port, this command lists many configuration and status details.)

Example 17-11 shows samples of all four of these commands as taken from the switch as configured in Example 17-10.
Example 17-11  Verification Commands for Routed Ports on Switches

```
SW1# show interfaces g0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
   Hardware is Gigabit Ethernet, address is bcc4.938b.e541 (bia bcc4.938b.e541)
   Internet address is 10.1.30.1/24

SW1# show interfaces status

          Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1  Fa0/1                        connected    10         a-full  a-100 10/100BaseTX
Fa0/2  Fa0/2                        notconnect   10           auto   auto 10/100BaseTX
Fa0/3  Fa0/3                        connected    20         a-full  a-100 10/100BaseTX
Fa0/4  Fa0/4                        connected    20         a-full  a-100 10/100BaseTX
Gi0/1  Gi0/1                        connected    routed     a-full a-1000 10/100/1000BaseTX

SW1# show interfaces g0/1 switchport
Name: Gi0/1
Switchport: Disabled
```

So, with two options—SVI and routed ports—where should you use each?

For any topologies with a point-to-point link between two devices that do routing, a routed interface works well.

Figure 17-5 shows an example of where to use SVIs and where to use routed ports in a typical core/distribution/access design. In this design, the core (Core1, Core2) and distribution (D11 through D14) switches perform Layer 3 switching. All the ports that are links directly between the Layer 3 switches can be routed interfaces. For VLANs for which many interfaces (access and trunk) connect to the VLAN, SVIs make sense because the SVIs can send and receive traffic out multiple ports on the same switch. In this design, all the ports on Core1 and Core2 will be routed ports, while the four distribution switches will use some routed ports and some SVIs.
Implementing Layer 3 EtherChannels

So far, this section has stated that routed interfaces can be used with a single point-to-point link between pairs of Layer 3 switches, or between a Layer 3 switch and a router. However, in most designs, the network engineers use at least two links between each pair of distribution and core switches, as shown in Figure 17-6.

While each individual port in the distribution and core could be treated as a separate routed port, it is better to combine each pair of parallel links into a Layer 3 EtherChannel. Without using EtherChannel, you can still make each port on each switch in the center of the figure be a routed port. It works. However, once you enable a routing protocol but don’t use EtherChannels, each Layer 3 switch will now learn two IP routes with the same neighboring switch as the next hop—one route over one link, another route over the other link.

Using a Layer 3 EtherChannel makes more sense with multiple parallel links between two switches. By doing so, each pair of links acts as one Layer 3 link. So, each pair of switches has one routing protocol neighbor relationship with the neighbor, and not two. Each switch learns one route per destination per pair of links, and not two. IOS then balances the traffic, often with better balancing than the balancing that occurs with the use of multiple IP routes to the same subnet. Overall, the Layer 3 EtherChannel approach works much better than leaving each link as a separate routed port and using Layer 3 balancing.
Compared to what you have already learned, configuring a Layer 3 EtherChannel takes only a little more work. Chapter 10 already showed you how to configure an EtherChannel. This chapter has already shown how to make a port a Layer 3 routed port. Next, you have to combine the two ideas by combining both the EtherChannel and routed port configuration. The following checklist shows the steps, assuming a static definition.

**Step 1.** Configure the physical interfaces as follows, in interface configuration mode:

A. Add the `channel-group number mode` command to add it to the channel. Use the same number for all physical interfaces on the same switch, but the number used (the channel-group number) can differ on the two neighboring switches.

B. Add the `no switchport` command to make each physical port a routed port.

**Step 2.** Configure the PortChannel interface:

A. Use the `interface port-channel number` command to move to port-channel configuration mode for the same channel number configured on the physical interfaces.

B. Add the `no switchport` command to make sure that the port-channel interface acts as a routed port. (IOS may have already added this command.)

C. Use the `ip address address mask` command to configure the address and mask.

**NOTE** Cisco uses the term *EtherChannel* in concepts discussed in this section and then uses the term *PortChannel*, with command keyword *port-channel*, when verifying and configuring EtherChannels. For the purposes of understanding the technology, you may treat these terms as synonyms. However, it helps to pay close attention to the use of the terms *PortChannel* and *EtherChannel* as you work through the examples in this section because IOS uses both.

Example 17-12 shows an example of the configuration for a Layer 3 EtherChannel for switch SW1 in Figure 17-7. The EtherChannel defines port-channel interface 12 and uses subnet 10.1.12.0/24.

![Diagram](image_url)
Example 17-12  Layer 3 EtherChannel Configuration on Switch SW1

```plaintext
interface GigabitEthernet1/0/13
   no switchport
   no ip address
   channel-group 12 mode on

interface GigabitEthernet1/0/14
   no switchport
   no ip address
   channel-group 12 mode on

interface Port-channel12
   no switchport
   ip address 10.1.12.1 255.255.255.0
```

Of particular importance, note that although the physical interfaces and PortChannel interface are all routed ports, the IP address should be placed on the PortChannel interface only. In fact, when the `no switchport` command is configured on an interface, IOS adds the `no ip address` command to the interface. Then configure the IP address on the PortChannel interface only.

Once configured, the PortChannel interface appears in several commands, as shown in Example 17-13. The commands that list IP addresses and routes refer to the PortChannel interface. Also, note that the `show interfaces status` command lists the fact that the physical ports and the port-channel 12 interface are all routed ports.

Example 17-13  Verification Commands Listing Interface Port-Channel 12 from Switch SW1

```plaintext
SW1# show interfaces port-channel 12
Port-channel12 is up, line protocol is up (connected)
   Hardware is EtherChannel, address is bcc4.938b.e543 (bia bcc4.938b.e543)
   Internet address is 10.1.12.1/24
   ! lines omitted for brevity

SW1# show interfaces status
! Only ports related to the example are shown.
<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Status</th>
<th>Vlan</th>
<th>Duplex</th>
<th>Speed</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/13</td>
<td>connected</td>
<td>routed</td>
<td></td>
<td>a-full</td>
<td>a-1000</td>
<td>10/100/1000BaseTX</td>
</tr>
<tr>
<td>Gi1/0/14</td>
<td>connected</td>
<td>routed</td>
<td></td>
<td>a-full</td>
<td>a-1000</td>
<td>10/100/1000BaseTX</td>
</tr>
<tr>
<td>Po12</td>
<td>connected</td>
<td>routed</td>
<td></td>
<td>a-full</td>
<td>a-1000</td>
<td></td>
</tr>
</tbody>
</table>

SW1# show ip route
! legend omitted for brevity
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C      10.1.2.0/24 is directly connected, Vlan2
L      10.1.2.1/32 is directly connected, Vlan2
C     10.1.12.0/24 is directly connected, Port-channel12
C     10.1.12.1/32 is directly connected, Port-channel12
```
For a final bit of verification, you can examine the EtherChannel directly with the `show etherchannel summary` command as listed in Example 17-14. Note in particular that it lists a flag legend for characters that identify key operational states, such as whether a port is bundled (included) in the PortChannel (P) and whether it is acting as a routed (R) or switched (S) port.

**Example 17-14  Verifying the EtherChannel**

```
SW1# show etherchannel 12 summary
Flags: D - down        P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
--------------------------
12 Po12(RU) - Gi1/0/13(P) Gi1/0/14(P)
```

**Troubleshooting Layer 3 EtherChannels**

When you are troubleshooting a Layer 3 EtherChannel, there are two main areas to consider. First, you need to look at the configuration of the `channel-group` command, which enables an interface for an EtherChannel. Second, you should check a list of settings that must match on the interfaces for a Layer 3 EtherChannel to work correctly.

As for the `channel-group` interface subcommand, this command can enable EtherChannel statically or dynamically. If dynamic, this command's keywords imply either Port Aggregation Protocol (PaGP) or Link Aggregation Control Protocol (LACP) as the protocol to negotiate between the neighboring switches whether they put the link into the EtherChannel.

If all this sounds vaguely familiar, it is the exact same configuration covered way back in the Chapter 10 section “Configuring Dynamic EtherChannels.” The configuration of the `channel-group` subcommand is exactly the same, with the same requirements, whether configuring Layer 2 or Layer 3 EtherChannels. So, it might be a good time to review those EtherChannel configuration details from Chapter 10. However, regardless of when you review and master those commands, note that the configuration of the EtherChannel (with the `channel-group` subcommand) is the same, whether Layer 2 or Layer 3.
Additionally, you must do more than just configure the `channel-group` command correctly for all the physical ports to be bundled into the EtherChannel. Layer 2 EtherChannels have a longer list of requirements, but Layer 3 EtherChannels also require a few consistency checks between the ports before they can be added to the EtherChannel. The following is the list of requirements for Layer 3 EtherChannels:

**no switchport**: The PortChannel interface must be configured with the `no switchport` command, and so must the physical interfaces. If a physical interface is not also configured with the `no switchport` command, it will not become operational in the EtherChannel.

**Speed**: The physical ports in the channel must use the same speed.

**duplex**: The physical ports in the channel must use the same duplex.

**Chapter Review**

One key to doing well on the exams is to perform repetitive spaced review sessions. Review this chapter's material using either the tools in the book or interactive tools for the same material found on the book’s companion website. Refer to the “Your Study Plan” element for more details. Table 17-2 outlines the key review elements and where you can find them. To better track your study progress, record when you completed these activities in the second column.

**Table 17-2  Chapter Review Tracking**

<table>
<thead>
<tr>
<th>Review Element</th>
<th>Review Date(s)</th>
<th>Resource Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review key topics</td>
<td></td>
<td>Book, website</td>
</tr>
<tr>
<td>Review key terms</td>
<td></td>
<td>Book, website</td>
</tr>
<tr>
<td>Repeat DIKTA questions</td>
<td></td>
<td>Book, PTP</td>
</tr>
<tr>
<td>Review config checklists</td>
<td></td>
<td>Book, website</td>
</tr>
<tr>
<td>Review command checklists</td>
<td></td>
<td>Book</td>
</tr>
<tr>
<td>Do labs</td>
<td></td>
<td>Blog</td>
</tr>
<tr>
<td>Watch video</td>
<td></td>
<td>Website</td>
</tr>
</tbody>
</table>

**Review All the Key Topics**

**Table 17-3  Key Topics for Chapter 17**

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 17-2</td>
<td>Concept of VLAN subinterfaces on a router</td>
<td>396</td>
</tr>
<tr>
<td>List</td>
<td>Two alternative methods to configure the native VLAN in a ROAS configuration</td>
<td>398</td>
</tr>
<tr>
<td>List</td>
<td>Troubleshooting suggestions for ROAS configuration</td>
<td>401</td>
</tr>
<tr>
<td>Figure 17-3</td>
<td>Layer 3 switching with SVIs concept and configuration</td>
<td>402</td>
</tr>
</tbody>
</table>
**Key Topic Element** | **Description** | **Page Number**
--- | --- | ---
List | Troubleshooting suggestions for correct operation of a Layer 3 switch that uses SVIs | 405
Figure 17-4 | Layer 3 switching with routed ports concept and configuration | 407
List | show commands that list Layer 3 routed ports in their output | 408
Figure 17-7 | Layer 3 EtherChannel concept and configuration | 411
List | List of configuration settings that must be consistent before IOS will bundle a link with an existing Layer 3 EtherChannel | 414

**Key Terms You Should Know**
- router-on-a-stick (ROAS), switched virtual interface (SVI), VLAN interface, Layer 3 EtherChannel (L3 EtherChannel), routed port, Layer 3 switch, multilayer switch, subinterfaces

**Command References**
Tables 17-4 and 17-5 list configuration and verification commands used in this chapter. As an easy review exercise, cover the left column in a table, read the right column, and try to recall the command without looking. Then repeat the exercise, covering the right column, and try to recall what the command does.

**Table 17-4** Chapter 17 Configuration Command Reference

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface type number.subint</code></td>
<td>Router global command to create a subinterface and to enter configuration mode for that subinterface</td>
</tr>
<tr>
<td><code>encapsulation dot1q vlan-id [native]</code></td>
<td>Router subinterface subcommand that tells the router to use 802.1Q trunking, for a particular VLAN, and with the <code>native</code> keyword, to not encapsulate in a trunking header</td>
</tr>
<tr>
<td><code>[no] ip routing</code></td>
<td>Global command that enables (ip routing) or disables (no ip routing) the routing of IPv4 packets on a router or Layer 3 switch</td>
</tr>
<tr>
<td><code>interface vlan vlan-id</code></td>
<td>A switch global command on a Layer 3 switch to create a VLAN interface and to enter configuration mode for that VLAN interface</td>
</tr>
<tr>
<td><code>sdm prefer lanbase-routing</code></td>
<td>Command on some Cisco switches that reallocates forwarding chip memory to allow for an IPv4 routing table</td>
</tr>
<tr>
<td><code>[no] switchport</code></td>
<td>Layer 3 switch subcommand that makes the port act as a Layer 2 port (switchport) or Layer 3 routed port (no switchport)</td>
</tr>
</tbody>
</table>
### Command Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface port-channel channel-number</code></td>
<td>A switch command to enter PortChannel configuration mode and also to create the PortChannel if not already created.</td>
</tr>
<tr>
<td>`channel-group channel-number mode {auto</td>
<td>desirable</td>
</tr>
</tbody>
</table>

### Table 17-5  Chapter 17 EXEC Command Reference

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip route</code></td>
<td>Lists the router's entire routing table.</td>
</tr>
<tr>
<td><code>show ip route [connected]</code></td>
<td>Lists a subset of the IP routing table.</td>
</tr>
<tr>
<td><code>show vlans</code></td>
<td>Lists VLAN configuration and statistics for VLAN trunks configured on routers.</td>
</tr>
<tr>
<td><code>show interfaces [interface type number]</code></td>
<td>Lists detailed status and statistical information, including IP address and mask, about all interfaces (or the listed interface only).</td>
</tr>
<tr>
<td><code>show interfaces [interface type number] status</code></td>
<td>Among other facts, for switch ports, lists the access VLAN or the fact that the interface is a trunk; or, for routed ports, lists “routed”.</td>
</tr>
<tr>
<td><code>show interfaces interface-id switchport</code></td>
<td>For switch ports, lists information about any interface regarding administrative settings and operational state; for routed ports, the output simply confirms the port is a routed (not switched) port.</td>
</tr>
<tr>
<td><code>show interfaces vlan number</code></td>
<td>Lists the interface status, the switch’s IPv4 address and mask, and much more.</td>
</tr>
<tr>
<td><code>show etherchannel [channel-group-number] summary</code></td>
<td>Lists information about the state of EtherChannels on this switch, including whether the channel is a Layer 2 or Layer 3 EtherChannel.</td>
</tr>
</tbody>
</table>
Symbols

? command, 94-95
:: (double colon), 531

Numbers

2-way state (OSPF), 453-454, 457
2.4-GHz band, 626
5-GHz band, 626
10BASE-T, 37, 42-45
100BASE-T, 37
100BASE-T, 37, 42-45
802.11, 628-629
  BSS, 614-616
  DS, 616-618
  ESS, 618
  IBSS, 619
  WLAN, 614
802.1D STP, 228, 232
802.1Q, 182
802.1w RSTP, 228-232
802.1x, EAP integration, 658
1000BASE-LX, 37
1000BASE-T, UTP cabling pinouts, 45-46

A

AAA (Authentication, Authorization, and Accounting) servers, 136
abbreviating IPv6 addresses, 531-532

ABR (Area Border Routers), 460-461
access
  CLI, 87-94, 128-139, 355-356
  protected credentials, 659
  WPA, 662-663
  WPA2, 662-663
  WPA3, 662-663

access interfaces, 185

access points. See AP

access switches, 241

ad hoc wireless networks. See IBSS

addresses
  BIA, 52
  broadcast addresses, 50-52
  calculating hosts and subnets in networks, 313-315
  classless versus classful addressing, 312-313
  Ethernet addresses, 50-52
  exhaustion, 525
  experimental, 290
  first usable, 293-294
  group addresses, 51
  host addresses, 293
  IPv4 addresses. See individual entry
  IPv6 addresses. See individual entry
  LAN addresses, 52
  last usable, 293-294
  loopback address, 295
  MAC addresses, 50-52, 111-114, 117-124, 218
  multicast addresses, 50-52, 290
  NAT, 277
  network broadcast addresses, 293-295
network numbers, 293-295
NIC addresses, 52
prefix part, 309-311
private addresses, 542
public addresses, 542
range of subnet addresses, finding, 331
sender MAC, 661
subnet addresses, 272, 283, 324-327, 334-338
unicast addresses, 50-52, 290, 322
universal addresses, 51
adjacencies (OSPF neighbors), troubleshooting, 510-516
adjacent-layer interaction, 21-22
adjacent neighbors, 457
administrative distance, 382-383, 448-449, 594-595
administrative mode, trunking, 191
administratively shutdown interfaces, 217
AES (Advanced Encryption Standard), 661
aging MAC address tables, 121-122
algorithms
AES, 661
CSMA/CD, 55
Dijkstra SPF, 451
IGP routing protocol algorithm, 445
key mixing, 661
RC4 cipher, 657
SPF, 457-459
STA, 216
alternate ports, 229-232
anycast addresses (IPv6), 574-576
AP (Access Points), 35, 614, 629
authentication, 654
autonomous, 634-635, 638
Bridge mode, 647
BSSID, 615
cloud-based AP architectures, 636-637
ESS, 618
fake, 654
Flex+Bridge mode, 647
FlexConnect mode, 647
IBSS, 619
LAP, 638-640
Local mode, 647
management interface, 674
Monitor mode, 647
multiple SSID, supporting, 617
noninfrastructure modes, 620-622
passing through, 615
roaming, 618
Rogue Detector mode, 647
SE Connect mode, 647
Sniffer mode, 647
SSID, 615
VLAN, 668
WLAN, 668-669
application layer (TCP/IP), 19-20
architectures
autonomous, 634-635, 638
centralized, 642-643
cloud-based
AP, 636-637
WLC deployments, 643
networking, 16
split-MAC, 638-642
area design (OSPF), 459-462
ARIN (American Registry for Internet Numbers), 445
ARP (Address Resolution Protocol), 72, 77, 378-379
AS (Authentication Servers), 658
AS (Autonomous Systems), 444-445
ASN (AS Numbers), 445
assigning
IPv6 addresses to hosts, 550
IPv6 subnets to internetwork topology, 549
subnets to different locations, 285
authentication. See also security
AP, 654
AS, 658
clients, 653
EAP, 657-658
EAP-FAST, 659
EAP-TLS, 660
external authentication servers, 135-136
LEAP, 659
open authentication, 656
PEAP, 659
web (WebAuth), 657
WEP, 657
WLAN, 682
WLC, 642
WPA, 662-663
WPA2, 662-663
WPA3, 662-663
authenticators, 658
auto-cost reference-bandwidth command, 492, 496
auto-mdix, 45
autonegotiation, 158-162
autonomous AP (Access Points), 634-635, 638
autonomous architectures, 634-635, 638
autonomous systems. See AS
auxiliary ports (routers), 362

backbone areas, 460-461
backbone routers, 461
backup ports, 230, 233
bandwidth
frequencies, 626-627
reference, 492
router serial interfaces, 361
bandwidth command, 492, 496
Basic Service Areas. See BSA
Basic Service Sets. See BSS
BDR (Backup DR), 456-457, 504-506
Bellman-Ford protocols. See distance vector protocols
Berners-Lee, Tim, 20
BGP (Border Gateway Protocol), 445
BIA (Burned-In Addresses), 52
BID (Bridge ID)
STP, 218-219
system ID extensions, 243-244
bidirectional communication, 613
binary/hexadecimal conversion chart (IPv6), 531
binary masks, 304-308
binary subnet analysis, 326
binary practice problems, 328-329
Boolean math, 331
finding
range of addresses, 331
subnet ID, 327
shortcut for binary process, 330
blocking state, interfaces, 215-217
blueprint (networking), 16
Boolean AND, 331
Boolean OR, 331
borrowing host bits to create subnet bits, 280-281
BPDU (Bridge Protocol Data Units), 218, 225
BPDU Guard, 236
BPDU tunneling, 247
bridge ID. See BID
Bridge mode (AP), 647
bridges. See switches
bridging tables. See MAC address tables
broadcast addresses, 50-52, 325-327
broadcast network type (OSPF), 500-506
broadcast storms, 213-215
BSA (Basic Service Areas), 614
BSS (Basic Service Sets), 614-618, 629
AP, 614
associations, 615
BSSID, 615
DS, 616-618
IBSS, 619
stations, 615
traffic flows, 615
burned-in MAC addresses, 218
cells. See BSA
centralized architectures, 642-643
centralized controllers
dynamic interfaces, creating, 678
RADIUS servers, configuration, 676
WLAN security, 682
certificate authorities. See CA
CFN (Cisco Feature Navigator), 404
channel-group command, 248-249, 259
EtherChannels, 416
Layer 3 EtherChannels, troubleshooting, 413
channel-group number mode on command, 411
channels, 627
dynamic assignment, 642
nonoverlapping, 628
CIDR (Classless Interdomain Routing), subnet masks, 305
circuits. See leased-line WAN
Cisco Binary Game, 306
Cisco Catalyst switches, 86
Cisco integrated services routers, 352
cladding (fiber-optic cable), 47
Class A networks, 290-295, 312
Class B networks, 290-293, 312
Class C networks, 290-295, 312
Class D networks, 290
Class E networks, 290
classful IP addresses, 312-313
classful IP networks, 289, 296-297
address formats, 291-292
before subnetting, 279-280
calculating hosts per network, 293
classes in, 290-291
default masks, 292
network ID, 293-295
number of, 291
octet values, 290
size of, 291
classful IP networks

- subnet masks, 302
- unusual addresses, 295
- classful networks, 276-279
- classful routing protocols, 447-448
- classless addressing, 312-313
- classless routing protocols, 447-448
- clear ip arp [ip-address] command, 378, 391
- clear ip ospf process command, 481, 497
- clear mac address-table dynamic command, 122, 125

CLI (Command-Line Interface)
- accessing, 87-94
- cabling console connections, 88-90
- Cisco Catalyst switches, 86
- command edit and recall, 95
- common command prompts, 98
- configuration files, 99-102
- configuration mode, 96-97
- configuration submodes and contexts, 97-99
- help, 94-95
- overview, 84-86
- privileged EXEC mode, 91-93
- router CLI, 355-356
- security, 128-139
- user EXEC mode, 91-93

clients
- authentication, 653, 656-660
- load balancing, 642
- roaming, 642
- Telnet clients, 91
- WLAN, 684

CLN (Cisco Learning Network), 306

clock rates, router serial interfaces, 361

cloud-based architectures, 636-637, 643

collisions, 167

commands
- ?, 94-95
- auto-cost reference-bandwidth, 496
- bandwidth, 496
- channel-group, 248-249, 259, 413, 416
- channel-group number mode on, 411
- clear ip arp [ip-address], 378, 391
- clear ip ospf process, 481, 497
- clear mac address-table dynamic, 122, 125
- com?, 94
- command, 495
- command ?, 94
- command parm?, 94
- command parm<Tab>, 94
- command parm1 ?, 94
- configure terminal, 97, 101, 104, 132, 189, 355
- copy, 356
- copy running-config startup-config, 102-104
- copy startup-config running-config, 104
- crypto key, 137
- crypto key generate rsa, 137-139, 148
- debug, 96
- default-information originate, 489, 496
- default-information originate always, 490
- delete vlan.dat, 117
- description, 153, 170, 363
- disable, 104
- duplex, 152-154, 165, 170, 355, 363
- enable, 91, 104, 130
- enable password, 131
- enable secret, 131, 148
- enable secret love, 94
- encapsulation, 397-398
- encapsulation dot1q, 415
- encapsulation dot1q vlan_id, 397
encapsulation dot1q vlan-id, 401
end, 104, 355
erase nvram, 104
erase startup-config, 104, 117
exec-timeout, 145, 148
exit, 98, 101-103, 355
history size, 145, 148
hostname, 99-103, 117, 138, 148
hostname Fred, 97
how interfaces status, 156
interface, 97, 103, 169, 185, 198, 356, 363, 391, 415
interface ethernet, 357
interface fastetherent, 357
interface gigabitetherent, 357
interface loopback, 470, 481, 496
interface port-channel, 416
interface port-channel number, 411
interface range, 154, 169, 187
interface type number.subint, 397
interface vlan, 148, 415
interface vlan 1, 142
interface vlan vlan_id, 403
ip -6 neighbor show, 600
ip address, 142, 148, 360, 363, 381, 391-392, 397-398, 470
ip address address mask, 397, 403, 411
ip address dhcp, 148
ip default-gateway, 142, 148
ip domain-name, 139
ip mtu, 515
ip name-server, 142, 148
ip ospf, 495
ip ospf cost, 492, 496
ip ospf dead-interval, 517
ip ospf hello-interval, 517
ip ospf process-id, 511
ip ospf process-id area area-id, 483-485
ip route, 367, 376, 380-385, 391
ip routing, 391, 402-404, 415
ip ssh version 2, 139
ipv6 address, 557, 560, 564-568, 576-578, 583
ipv6 address dhcp, 578
ipv6 address eui-64, 563
ipv6 address link-local, 568
ipv6 enable, 568-569, 576-578
ipv6 route, 586-597, 604
ipv6 unicast-routing, 558, 578
line aux 0, 362
line con 0, 130-131
line console 0, 97-98, 103, 147, 356
line vty, 132, 147
logging console, 145, 148
logging synchronous, 145, 148
login, 94, 103, 130-132, 147
login local, 147
mac-address, 564
maximum-paths, 494-496
name, 185, 207
ndp -an, 600
netsh interface ipv6 show neighbors, 600
network, 473-475, 480-486, 511
no debug all, 104
no description, 157, 170
no duplex, 157, 170
no ip address, 412
no ip domain-lookup, 146
no logging console, 145, 148
no passive-interface, 487, 496
no password, 134
no shutdown, 142, 155-157, 170, 207, 253, 356, 363, 399, 403-405
[no] shutdown vlan number, 201
no speed, 157, 170
no switchport, 408, 411-415
passive-interface, 487, 496, 517
passive-interface default, 488
password, 97, 103, 130-132, 147
password faith, 94
ping, 78, 419-429, 587
port-channel load-balance method, 254
quit, 104
reload, 91-92, 102-104, 117, 402-404
router-id, 470, 496
router ospf, 470, 495
router ospf 1, 472, 480
router ospf process-id, 480, 510
sdm prefer, 402-404
sdm prefer lanbase-routing, 402, 415
show, 95, 166, 361, 480, 508
show crypto key mypubkey rsa, 149
show dhcp lease, 143-144, 149
show etherchannel, 248, 259, 416
show etherchannel 1 summary, 250
show etherchannel summary, 413
show history, 145, 149
show interfaces, 119-120, 156, 162-164, 167-170, 357-358, 361, 364, 376, 408, 416, 515-517, 583
show interfaces description, 162, 170
show interfaces interface-id trunk, 203-205
show interfaces status, 118, 125, 153, 162-165, 408, 412
show interfaces switchport, 192-199, 202-203, 208
show interfaces trunk, 193-194, 199-205, 208, 401
show interfaces type number switchport, 199
show interfaces type number trunk, 200
show interfaces vlan, 143-144, 149, 416
show ip arp, 391
show ip default-gateway, 144, 149
show ip interface brief, 357-361, 364, 406
show ip ospf, 481, 496, 510-511, 517
show ip ospf database, 450, 462, 475, 497
show ip ospf interface, 486-488, 496, 503-505, 510-513, 517
show ip ospf interface [brief], 479-480, 511
show ip ospf interface brief, 488, 491, 496, 503, 5.5, 508-510, 514, 517
show ip ospf interface G0/0, 505
show ip ospf neighbor, 452-453, 457, 475, 480, 497, 502, 505, 508-517
show ip ospf neighbor interface brief, 513
show ip protocols, 479, 485, 496, 517
show ip route, 324, 356, 367, 376-391, 400-402, 408, 416, 449, 475-478, 497, 585
show ip route address, 388
show ip route [connected], 398
show ip route EXEC, 404
show ip route ospf, 387, 497
show ip route static, 380, 490
show ip ssh, 139, 149
show ipv6 interface, 558-559, 567, 570-573, 579
show ipv6 interface brief, 558-560, 567, 575, 579
show ipv6 route, 566, 579, 585-590, 605
show ipv6 route connected, 560, 586
show ipv6 route local, 585-586
show ipv6 route static, 587-590, 593, 595
show mac address-table, 120, 125, 356
show mac address-table aging-time, 122, 125
show mac address-table count, 122, 125
show mac address-table dynamic, 96, 117, 123-125, 170
show mac address-table dynamic address, 125
show mac address-table dynamic interface, 120-121, 125
show mac address-table dynamic vlan, 125
show mac address-table static, 170
show mac address-table vlan, 121
show protocols, 361, 364
show running-config, 93, 101, 104, 132-133, 143, 149, 155, 158, 170, 398, 479, 488, 511, 584
show running-config | interface, 170
show spanning-tree, 249, 259
show spanning-tree vlan, 259
show spanning-tree vlan vlan-id, 204
show ssh, 139, 149
show startup-config, 101, 104, 158
show vlan, 201, 208
show vlan brief, 186-189, 202
show vlan id, 187
show vlans, 398-401, 416
show vtp status, 190, 208
shutdown, 143, 155, 170, 207, 253, 356, 359, 363, 399-401, 405
shutdown command, 163
spanning-tree, 259
spanning-tree mode, 242-243, 259
spanning-tree x root primary,
244-245
spanning-tree x root secondary,
244-245
speed, 98-99, 152-154, 165, 170, 355, 363
switchport, 408, 415
switchport access vlan, 185-189, 198-199, 207
switchport mode, 191, 207
switchport mode access, 185, 188, 198-199
switchport mode dynamic auto, 202
switchport mode dynamic desirable,
193
switchport mode trunk, 191, 203, 396
switchport nonegotiate, 195, 203, 207
switchport trunk allowed vlan, 204, 207
switchport trunk encapsulation, 191, 207
switchport trunk native vlan, 207
switchport trunk native vlan vlan-id,
205
switchport voice vlan, 198-199, 207
switchport voice vlan vlan-id, 200
terminal history size, 145, 149
test etherchannel load-balance EXEC,
255
traceroute, 428-432, 587
transport input, 138, 148, 356
transport input all, 139
transport input none, 139
transport input ssh, 139
transport input telnet ssh, 139
undebug all, 104
username, 134
username secret, 134, 147
vlan, 185, 198, 207
vlan number, 201
tf mode, 207
vtp mode, 190
vtp mode transparent, 190
write erase, 104
communication
bidirectional, 613
passing through, 615
unidirectional, 613
configuration BPDU. See Hello BPDU
configuration changes (STP topology, influencing), 223
configuration files, 99-102
configuration mode (CLI), 96-97
configure terminal command, 97, 101, 104, 132, 189, 355
connected routes, 366, 376-378, 583-585
connectors
  - pins, 40
  - RJ-45, 41
console connections, cabling, 88-90
cable connections, cabling, 88-90
collection passwords, 129
collection ports, 672
collection-setting commands, 97
controller plane (cloud-based AP architectures), 637
controllers
  - centralized, 676-678, 682
  - dynamic interfaces, 674-675
  - interfaces, 673, 681
  - management interfaces, 674
  - ports, 672-673
  - redundancy management, 674
  - service port interfaces, 674
  - virtual interfaces, 674
  - VLANs, mapping, 673
  - WLAN controller configuration, 685
  - WLC, 639-642
convergence, 216, 443
converting subnet mask formats, 305-309
copy command, 356
copy running-config startup-config command, 102-104
copy startup-config running-config command, 104
cores (fiber-optic cable), 47
costs (metrics)
  - EIGRP, 446
  - IGP, 446-447
  - OSPF, 491-493
  - ports, 247
    - IEEE default, 223
    - STP, 221
  - RIPv2, 446-447
  - CRC (Cyclic Redundancy Checks), 167-168
crossover cable pinouts, 44-45
crosstalk, 40
crypto key command, 137
crypto key generate rsa command, 137-139, 148
CSMA/CD (Carrier Sense Multiple Access with Collision Detection), 55, 167
CUCM (Cisco Unified Communication Manager), 196
cycles, waves, 625

D

DAD (Duplicate Address Detection), 598, 602
data
  - decryption, 655
  - encapsulation
    - OSI terminology, 30
    - TCP/IP terminology, 27-28
  - integrity, 656
  - privacy, 655
  - privacy/integrity methods, 660-661
data centers, 108
data link layer
  - Ethernet, 38-39, 49-50
  - TCP/IP, 25-26
data-link protocols, leased-line WAN, 63-64
data paths, autonomous wireless networks, 635
data plane (cloud-based AP architectures), 637
Data VLAN (Virtual Local Area Networks), 197-199
DDN (Dotted-Decimal Notation), 24, 305-309
de-encapsulating IP packets, 373-374
Dead Interval timers, 455
dead timers, troubleshooting, 512-513
debg command, 96
decimal masks. See DDN
decimal subnet analysis, 331
difficult masks, 334-338
easy masks, 332
finding
   subnet broadcast addresses, 336-338
   subnet IDs, 334-336
predictability in interesting octets, 333-334
reference table: DDN mask values and binary equivalent, 338-339
decrypting data, 655
default gateways, 70, 370-372
default-information originate always command, 490
default-information originate command, 489, 496
default OSPF routes, 489-491
default routers, 70, 370-372
default routes, 379, 383-384
default VLAN (Virtual Local Area Networks), 186
delete vlan.dat command, 117
description command, 153, 170, 363
designated ports. See DP
DHCP (Dynamic Host Configuration Protocol), 143, 286
diagrams (networking), 15, 26
difficult subnet masks, 334-338
digital certificates, split-MAC architectures, 640
Dijkstra SPF algorithm, 451
directed broadcast addresses, 283
disable command, 104
disabling
   autonegotiation, 160
   DTP, 203
   ports, 230
   switch interfaces, 155-156
   VLAN, troubleshooting, 201-202
   WLAN, 680
discarding state (RSTP), 229-230
discovering
duplicate addresses, 602
neighbor link addresses, 598-600
routers, 600-601
distance vector protocols, 446
distributed architectures, 634-638
distribution switches, 241
distribution system ports, 672-673
distribution systems. See DS
DNS (Domain Name Systems), 76-77
documentation, subnet plans, 267
double colon (::), 531
DP (Designated Ports), 217, 222-223, 230
DR (Designated Routers)
   BDR, 456-457
elections, configuration with broadcast network type (OSPF), 504-506
DRAM (Dynamic Random-Access Memory), 99
DROthers routers, 457
DS (Distribution Systems), 616-618
DTP (Dynamic Trunking Protocol), 203
dual stacks, 529, 556
duplex command, 152-154, 165, 170, 355, 363
duplexes
   configuration on switch interfaces, 152-154
   mismatches, 161
   troubleshooting, 161-166
Duplicate Address Detection. See DAD
dynamic auto trunking, 191
dynamic desirable trunking, 191
dynamic EtherChannels, configuration, 250-251
Dynamic Host Configuration Protocol (DHCP), 143, 286
dynamic interfaces, 674-675, 678
dynamic IP address configuration, DHCP, 143
dynamic ranges per subnet, choosing, 286-287
dynamic unicast address configuration (IPv6), 564

E

E-Line, 66
EAP (Extensible Authentication Protocol), 657-660
EAP-FAST (EAP Flexible Authentication by Secure Tunneling), 659
EAP-TLS (EAP Transport Layer Security), 660
easy subnet masks, 332
echo requests/replies (ICMP), 78, 419
edge ports, 233
EGP (Exterior Gateway Protocol), 444
EIGRP (Enhanced Interior Gateway Routing Protocol), 446
EIGRPv6 (EIGRP for IPv6), 529
electric waves, traveling, 624
embedded WLC deployments, 644
enable command, 91, 104, 130
enable mode, 91-93
enable passwords, 130-131
enable secret command, 131, 148
enable secret love command, 94
encapsulation
IPv4, 70
OSI terminology, 30
TCP/IP terminology, 27-28
capsulation command, 397-398
capsulation dot1q command, 415
capsulation dot1q vlan_id command, 397, 401
encoding schemes, 39
encryption (data), 655
end command, 104, 355
end-user perspectives on networking, 14-15
enterprise LAN (Local Area Networks), 36-37
enterprise mode (WPA), 663
enterprise networks, 15, 268, 350-352
terprise routers, 350-353
EoMPLS (Ethernet over MPLS), 66
erase nvram command, 104
erase startup-config command, 104, 117
erasing switch configuration files, 102
errors
detection, FCS field, 53
TCP error recovery rates, 21
ESS (Extended Service Sets), 618
EtherChannel, 234, 407
configuration, 247-257
dynamic EtherChannels, 250-251
Layer 3 EtherChannels, 392, 410-414
load distribution, 253-257
manual Layer 2 EtherChannels, 248-250
troubleshooting, 251-253
Ethernet, 26
addresses, 52
cables, 35
E-Line, 66
emulation, 66-68
EoMPLS, 66
GBIC, 42
IPv6 static routes over Ethernet links, 591
LAN. See also subnets
enterprise LAN, 36-37
enterprise networks, 350
Ethernet addressing, 50-52
Ethernet data link protocols, 38-50
Ethernet frames, 38
Ethernet physical layer standards, 37
Ethernet ports, 40
Ethernet Type field, 52
FCS field, 53
full-duplex logic, 53-56
half-duplex logic, 54-56
overview, 32-34
SOHO LAN, 35
switches, 35, 106-124, 152-162
troubleshooting, 162-168
UTP cables, 37-46, 49
VLAN, 179-205
links, 40
OSPF
  Ethernet links, 456-457
  Ethernet WAN, 506-508
point-to-point, 56
shared media, 56
switches, fiber-optic cables, 48
WAN
  enterprise networks, 350
  EoMPLS, 66
  Ethernet emulation, 66-68
  overview, 65-66
  point-to-point network type (OSPF), 506-508
Ethernet Alliance web page, 38
EtherType, 52
EUI-64 (extended unique identifier), 560-564
EXEC modes
  privileged EXEC mode, 91-93
  simple password configuration, 130-133
  user EXEC mode, 91-93
exec-timeout command, 145, 148
exit command, 98, 101-103, 355
expanding IPv6 addresses, 532
experimental addresses, 290
extended ping command, 423-426
extended traceroute command, 431-432
external authentication servers, 135-136

default interfaces, 217
fake AP, 654
Fast Ethernet, 37
FCS (Frame Check Sequence) field, 53
fiber-optic cables, 37-38, 46-49
finding
  IPv6 prefixes, 533-536
  MAC address table entries, 120-121
  mismatched Hello/dead timers, 512
  range of subnet addresses, 331
  routers best routes, 451
  subnet broadcast addresses, 327, 336-338
  subnet ID, 327, 334-336
first octet values, classes by, 290
first usable IP addresses, deriving, 293-294
flash memory, 100
Flex+Bridge mode (APs), 647
FlexConnect mode (APs), 647
floating static routes, 381-383, 593-595
flooding, 114, 450
Forward delay timers (STP), 225
forward secrecy, 663
forward-versus-filter decisions, 113
forwarding, 115
data. See routes/routing
  IP packets, 68-75, 374-375
  known unicast frames, 110-113
forwarding state, interfaces, 215-217
frames, 26-28, 38
  broadcast storms, 213-215
  CRC, 167
  flooding, 114
  giants, 167
  IP routing, 373-376
  looping frames, 213-215
  multiple frame transmissions, 214-215
frames

packet output errors, 167
runts, 167
unknown unicast frames, 114
frequencies, 613, 625-627
full addresses (IPv6), 530
full duplex logic, 53-56
full VLAN configuration example, 186-188
fully adjacent neighbors, 457, 502

G

G0/0 status code, 359
G0/1 status code, 359
gateways (default), 370-372
GBIC (Gigabit Ethernet Interface Converter), 42
GCMP (Galois/Counter Mode Protocol), 661
Get IEEE 802 program, 228
GET requests (HTTP), 20
GHz (Gigahertz), 625
giants, 167
Gigabit Ethernet, 37
global routing prefix (IPv6), 543-544
global unicast addresses, 542-550
global unicast next-hop addresses, 589
group addresses, 51
groupings (IP address), 70
GTC (Generic Token Cards), 660

H

half-duplex logic, 54-56
HDLC (High-Level Data Link Control), 63-64
headers
  Ethernet header fields, 50
  HDLC, 63

HTTP, 20
  IP headers, 73
Hello BPDU, 218, 225
Hello Interval timers, 455
Hello messages, 219, 452
Hello timers, 225, 512-513
hexadecimal/binary conversion chart (IPv6), 531
history buffer commands, 144-145
history size command, 145, 148
hopping (VLAN), 205
host addresses, calculating number per network, 293
host bits, 272
host forwarding logic (IPv4), 69
host part (of IP addresses), 292, 302, 311
host routes, 378-379
  IPv4 routing process, 370
  static host routes, 381
hostname command, 97-103, 117, 138, 148
hostnames, 76, 427-428
hosts, 68
  analyzing subnet needs, 269-271
  assigning addresses to, 550
  calculating, 313-315
  host bits, 272
  IP settings, 24, 140-142
  NDP, 598-603
  subnets, 268-271
HTTP (Hypertext Transfer Protocol), 19-20
hubs
  autonegotiation, 161-162
  LAN hubs, 54-56
Hypertext Transfer Protocol (HTTP), 19-20
Hz (Hertz), 625
IANA (Internet Assigned Numbers Authority), 445, 540
IBSS (Independent Basic Service Sets), 619. See also BSS
ICANN (Internet Corporation for Assigned Names and Numbers), 540
ICMP (Internet Control Message Protocol), 78, 419
ICMPv6 (Internet Control Message Protocol version 6), 526
ID (identification)
ID numbers, WLAN, 680
interface ID, 547
subnet ID, 272, 283, 324, 327, 330, 334-336, 548
system ID extensions, 245-246
VLAN ID, 180
IEEE (Institute of Electrical and Electronic Engineers), 18
802.1D Spanning-Tree states, 227
802.1D standard, 228
802.1w amendment, 228
802.1x, EAP integration, 658
default port costs, 223
Get IEEE 802 program, 228
IGP (Interior Gateway Protocol), 444-448
IGRP (Interior Gateway Routing Protocol), 446
inferior Hello messages, 219
infrastructure mode, 614
input errors, 166-167
integrated services routers (Cisco), 352
interarea routes, 461
interesting octets, predictability in, 333-334
interface command, 97, 103, 169, 185, 198, 356, 363, 391, 415
interface ethernet command, 357
interface gigabitethernet command, 357
interface ID, 547
interface loopback command, 470, 481, 496
interface port-channel command, 416
interface port-channel number command, 411
interface range command, 154, 169, 187
interface type number, subint command, 397
interface vlan command, 148, 415
interface vlan 1 command, 142
interface vlan vlan_id command, 403
interfaces, 87
administratively shutdown, 217
blocking state, 215
controllers, 673, 681
dynamic interfaces, 674-675, 678
EtherChannels, adding, 251-253
failed interfaces, 217
forwarding state, 215
Layer 1 problems, 166-168
learning state, 227
listening state, 227
management interfaces, 674
OSPF
metrics, 493
passive interfaces, 487-488
OSPFv2 configuration, 483-486
physical interface configuration, 251-253
ports, compared, 671
routed interfaces, Layer 3 (multilayer) switches, 407-409
routers, 356-357
bandwidth, 361
clock rates, 361
IP addresses, 360-361
status codes, 358-359
service port interfaces, 674
speed and duplex issues, 163-166
states, 216-217, 227
status codes, 162-163, 358-359
subcommands, 97
subinterfaces, 396-397
SVI, 392, 401-406
switch interface configuration, 152-162
troubleshooting, 162-168
virtual interfaces, 674
VLAN interfaces, 402
WLC interfaces, 673-675
working interfaces, 217
interference, simultaneous transmissions, 613
internal routers, 461
Internet Protocol. See IP
internetworks, 72, 268
intra-area routes, 461
intrusion protection, WLC, 642
IOS configuration, 96-102
IP (Internet Protocol), 22. See also IPv4; IPv6
addresses
management, 635
ping command, 427-428
subnets, 283-284
forwarding
IP packets, 374-375
longest prefix matches, 386-389
IGP metrics, 446-447
routing, 366
ARP tables, 378-379
de-encapsulating IP packets, 373-374
encapsulating IP packets in new frames, 375
example of, 371-376
frames, 373-376
host forwarding of IP packets to default routers (gateways), 372
IP forwarding, 374-375, 386-389
IPv4 routing process, 369-371
troubleshooting, 419-434
routing tables, 70-72, 388-389
telephony, 196-200
ip -6 neighbor show command, 600
ip address address mask command, 397, 403, 411
ip address command, 142, 148, 360, 363, 381, 391-392, 398
IP addresses on loopback interfaces, 470
subinterfaces, 397
ip address dhcp command, 148
ip address subcommand, 376
ip_address parameter, network command, 473
ip default-gateway command, 142, 148
ip domain-name command, 139
ip mtu command, 515
ip name-server command, 142, 148
ip ospf command, 495
ip ospf cost command, 492, 496
ip ospf dead-interval command, 517
ip ospf hello-interval command, 517
ip ospf process-id area area-id command, 483-485
ip ospf process-id command, 511
ip route command, 367, 376, 379-385, 391, 402-404, 415
ip ssh version 2 command, 139
IPv4 (Internet Protocol Version 4). See also IP
address exhaustion, 525
ARP, 72, 77
calculating hosts and subnets in network, 313-315
classes in, 290-291
classful IP networks, 289-297
classless versus classful addressing, 312-313
configuration on switch, 142-143
DNS, 76-77
dynamic IP address configuration with DHCP, 143
headers, 73
hosts, 24, 140-142
networks, 70-73, 293-295
overview, 22-23, 68
private addresses, 542
public addresses, 542
router support
  auxiliary ports, 362
  CLI access, 355-356
  interfaces, 356-361
routing, 24-25, 369-371
  logic, 68-72
  protocols, 74-75
subnets, 70, 73, 264-267, 322-339
  hosts, 268-271
  multiple subnet sizes, 274
  number of hosts, 271
  number of subnets, 270
  one-size subnets, 273
  single-size subnets, 273
  size of, 272-274
  subnet addresses, 272
  subnet ID, 272
  subnet masks, 272, 275, 279-283, 302-312, 315
  subnet numbers, 272
switch settings, 140-142
testing connectivity, 78
troubleshooting tools
  ping command, 419-429
  SSH, 432-434
  Telnet, 432-434
  tracert command, 428-432
unusual addresses within classes, 295
verifying on switch, 143-144
VLSM, 275

IPv6 (Internet Protocol Version 6). See also IP
abbreviating addresses, 531-532
address configuration summary, 576
assigning subnets to internetwork topology, 549
dual-stack strategies, 556
dynamic unicast address configuration, 564
expanding addresses, 532
global routing prefix, 543-544
global unicast addresses, 542-550
hexadecimal/binary conversion chart, 531
history of, 524-525
interface ID, 547
link-local addresses, 566-569
loopback addresses, 574
multicast addresses, 569-576
NDP, 573-574, 598-603
overview, 524
prefix length, 533-536
protocols, 526-527
representing full IPv6 addresses, 530
routing, 527-530, 583-598
static unicast address configuration, 557-564
subnets, 543
  global unicast addresses, 545-549
  router anycast addresses, 549
  unique local addresses, 551-552
unicast addresses, 556
unique local addresses, 542, 551-553
unknown addresses, 574
ipv6 address command, 557, 560, 564-568, 576-578, 583
ipv6 address dhcp command, 578
ipv6 address eui-64 command, 563
ipv6 address link-local command, 563
ipv6 enable command, 568-569, 576-578
ipv6 route command, 586-597, 604
ipv6 unicast-routing command, 558, 578
IS-IS (Integrated Intermediate System to Intermediate System), 446
ISL (Inter-Switch Link), 182
ISO (International Organization for Standardization), 17
IV (Initialization Vectors), 661

J - K

keys
forward secrecy, 663
mixing algorithm, 661
PKIs, 660
shared-key security, 657
TKIP, 660-661
WEP, 657
kHz (kilohertz), 625
kilohertz (kHz), 625
known unicast frames, forwarding, 110-113

LAN switching, 106-124
neighbors, testing, 425-426
redundancy, 210, 214
STP security exposures, 236
switching, 35
analyzing, 116
flooding, 114
interface configuration, 152-162
MAC address table, 113-114, 117-124
overview, 106-109
STP, 114-115
summary, 115-116
switch forwarding and filtering decisions, 110-113
switch interfaces, 118-120, 152-162
switching logic, 109-110
verifying, 116
VLAN
AP, 668
collection, 185-195, 198-199
Data VLAN, 197-199
default VLAN, 186
disabled VLAN, 201-202
IP telephony, 196-200
native VLAN, 183, 205
overview, 179-180
routing, 183-184
supported VLAN list on trunks, 203-205
tagging, 181-182
troubleshooting, 201-205
trunking, 180-182, 189-195
undefined VLAN, 201-202
VLAN ID, 180
Voice VLAN, 197-199
VTP, 189-190
WLAN, 32
802.11 WLAN, 614
advanced settings, 684-685
LSDB (Link-State Database)  775

AP, 668-669
BSS, 614-616
client session timeouts, 684
configuration, 675-678, 681-685
controller configuration, 685
creating, 679-681
creating too many, 676
defined, 675
displaying list of, 679
DS, 616-618
ESS, 618
IBSS, 619
limiting, 676
management access, 685
mesh networks, 622
outdoor bridges, 621-622
QoS, 683-684
repeaters, 620-621
security, 681-684
topologies, 614-622
WGBs, 621
WLCs, 669-675

LAP (Lightweight Access Points), 639-642
last usable IP addresses, deriving, 293-294
late collisions, 167
Layer 1 problems, troubleshooting, 166-168
Layer 2 switches, 141, 183
Layer 3 EtherChannel, 392
Layer 3 (multilayer) switches, 141, 184
routed ports, 406-414
SVI, 401-406
LEAP (Lightweight EAP), 659
learning state, interfaces, 227
leased-line WAN (Wide Area Networks), 61-65
lightweight AP (Access Points), 638
line aux 0 command, 362
line con 0 command, 130-131
line console 0 command, 97-98, 103, 147, 356
line vty command, 132, 147
link-local addresses (IPv6), 566-569
link-local next-hop address, 589-590
link-state protocols, 446
list of subnets
building, 283-284
IPv6 subnets, 548-549
listening state, interfaces, 227
load balancing
clients, 642
OSPF, 494
load distribution, EtherChannel, 253-257
Local mode (AP), 647
local routes, 378, 583-586
local scope multicast addresses, 569-573
logging console command, 145, 148
logging synchronous command, 145, 148
logical networks, user segregation, 676
login command, 94, 103, 130-132, 147
login local command, 147
loopback address, 295, 574
looping frames, 213-215
loops, avoiding with STP, 114-115
LSA (Link-State Advertisements), 449, 454
flooding, 450
LSDB relationship, 450
network LSA, 464
OSPF, 454-456, 459-464
router LSAs, 463
LSDB (Link-State Database)
area design, 461-462
best routes, finding, 451
LSA relationship, 450
OSPF/LSDB neighbor exchanges, 454-456
LSU (Link-State Update) packets, 454
LWAPP (Lightweight Access Point Protocol), 639

M

MAC address tables, 111
  aging, 121-122
clearing, 122
finding entries in, 120-121
instability, 214-215
multiple switches, 123-124
overview, 113-114
showing, 117-118
mac-address command, 564
MAC addresses, 50-52
  burned-in, 218
  sender MAC addresses, 661
  source MAC addresses, 113
  split-MAC architectures, 638-642
macrobending, 163
magic number, 334
magnetic waves, traveling, 624
man-in-the-middle attacks, 654
management access (WLAN), allowing, 685
management interfaces (controllers), 674
management IP addresses, autonomous AP, 635
manual Layer 2 EtherChannels, 248-250
mapping VLAN, 673
MaxAge timer (STP), 225
maximum-paths command, 494-496
memory, 99-100
Meraki, 636-637
mesh networks, 622
messages
  Hello, 219
  Hello BPDU, 218, 225
inferior Hello, 219
integrity, 656, 660-661
OSPF Hello, 452
privacy, 655, 660-661
RSTP, 232
sending, 623-624
superior Hello, 219
metrics (costs)
  EIGRP, 446
  IGP, 446-447
  OSPF, 491-493
  ports, 247
    IEEE default, 223
    STP, 221
  RIPv2, 446-447
MHZ (Megahertz), 625
MIC (Message Integrity Checks), 656, 660-661
Mobility Express WLC deployments, 645
models, networking
  OSI, 17, 28-30
  TCP/IP, 16-29
modified EUI-64 (Extended Unique Identifier-64), 560-564
Monitor mode (AP), 647
MP BGP-4 (Multiprotocol BGP version 4), 529
MSCHAPv2 (Microsoft Challenge Authentication Protocol version 2), 660
MSTP (Multiple Spanning Tree Protocol), 242-243
MTU (Maximum Transmission Units), 50, 515
multiarea OSPF (Open Shortest Path First), 482
multicast addresses, 50-52, 290, 569-576
multilayer switches, 141, 184, 401-414
multimode fiber-optic cables, 47-49
NA (Neighbor Advertisement), 599
name command, 185, 207
NAT (Network Address Translation), 277, 542
native VLAN (Virtual Local-Area Networks), 183, 205, 398
NDP (Neighbor Discovery Protocol), 526, 573-574, 598-603
 NDP -an command, 600
neighbors
adjacent neighbors, 457
fully adjacent neighbors, 457, 502
link addresses, discovering, 598-600
NA, 599
NS, 599
OSPF, 451
broadcast network type, 502-506
LSA exchanges, 454-456
LSDB exchanges, 454-456
requirements, 508-510
RID, 452
states, 453, 457
troubleshooting adjacencies, 510-516
testing, 425-426
netsh interface ipv6 show neighbors
command, 600
network command, 473-475, 480-486, 495, 511
network ID. See network numbers
network layer, 22-25
ARP, 77
DNS, 76-77
protocols, identifying with Ethernet
Type field, 52
routing
LAN/WAN, 70-72
logic, 68-70
testing connectivity, 78
network numbers, 293-295
network types (OSPF)
broadcast, 500-506
point-to-point, 500-501, 506-508
troubleshooting mismatched network
types, 515-516
networks
architectures, 16
blueprint, 16
broadcast addresses, 293-295
classful IP networks, 289-297
classful networks, 276-278
definition of, 268
diagrams, 15, 26
diagnostic process, 14-15
diagnosis, 14-15
enterprise networks, 15, 268, 350-352
internet networks, 268
IP networks, 70-73, 292, 302, 312
logical networks, user segregation, 676
LSA, 464
masks, 376
mesh, 622
NAT, 277
networking model overview, 16
OSI, 17, 28-30
overview, 12-14
private IP networks, 277-278
public IP networks, 276-278
routes, 379
SOHO networks, 15
subnets versus, 324
TCP/IP, 16-29
VLAN switches, 140
WAN, 60
Ethernet WAN, 65-68
leased-line WAN, 61-65
wireless networks, 628-629, 662-663
next-hop IPv6 addresses, 589-590
NIC addresses, 52
NIM (Network Interface Modules), 352
no debug all command, 104
no description command, 157, 170
no duplex command, 157, 170
no ip address command, Layer 3 Ether-
Channels, 412
no ip domain-lookup command, 146
no logging console command, 145, 148
no network network-id area area-id
subcommands, 483
no passive-interface command, 487, 496
no password command, 134
no shutdown command, 142, 155-157, 170, 207, 253, 356, 363, 399, 403-405
[no] shutdown vlan number command, 201
no speed command, 157, 170
no switchport command, 408, 411-415
nonoverlapping channels, 628
nonworking states, troubleshooting, 162-163
NS (Neighbor Solicitation), 599
numbers
DDN, 24
magic number, 334
SEQ, 21
subnet numbers, 272, 283, 324, 327, 334-336
NVRAM (nonvolatile RAM), 100

one-size subnets, 273-274
open authentication, 656
operational view of subnetting, 267-268
optical transmitters (fiber-optic cable), 47
OSI (Open Systems Interconnection), 17, 28-30

OSPF (Open Shortest Path First), 450
2-way state, 453-454, 457
area design, 459-462
backbone areas, 460
broadcast network type, 500-506
calculating best routes with SPF, 457-459
configuration, 472, 479-481
default routes, 489-491
Dijkstra SPF algorithm, 451
DR, 456-457
Ethernet links, 456-457
Hello/dead timers, 512-513
Hello messages, 452
interfaces, 493
load balancing, 494
LSAs, 450, 459-456
metrics, 446-447, 491-493
mismatched network types, 515-516
MTU mismatched settings, 515
multiarea OSPF, 482
neighbors, 451
broadcast network type, 502-506
LSA exchanges, 454-456
LSDB exchanges, 454-456
requirements, 508-510
RIDs, 452
states, 453, 457
troubleshooting adjacencies, 510-516
passive interfaces, 487-488
point-to-point network type, 500-501, 506-508
process-id, 472
processes, shutting down, 513-514
RID, 480-481, 511
verifying
configuration, 479-480
operation, 475-478
OSPFv2 (OSPF version 2), 440, 463
- interface configuration, 483-486
- load balancing, 494
- metrics, 493
- single-area configuration, 470-475
OSPFv3 (OSPF version 3), 526, 529
- outdoor bridges, 621-622
- outgoing interfaces, IPv6 static routes with, 587-588

PAC (Protected Access Credentials), 659
- packets, 28
  - data packets, routing VLAN, 184
- IP packets
  - de-encapsulating, 373-374
  - encapsulating in new frames, 375
  - forwarding, 68-75, 374-375
  - hot forwarding to default routers (gateways), 372
- output errors, 167

PAgP (Port Aggregation Protocol), 250
- passing through (communications), 615
- passive-interface command, 487, 496, 517
- passive-interface default command, 488
- password command, 97, 103, 130-132, 147
- password faith command, 94
- passwords
  - CLI, 93-94, 130-135
  - console passwords, 129
  - enable passwords, 130
  - shared passwords, 130
  - Telnet passwords, 129
- path selection, 69, 442

PBX (Private Branch Exchange), 196

PDU (Protocol Data Units), 30

PEAP (Protected EAP), 659
- permanent keywords, 385
- personal mode (WPA), 663
- physical console connections, 88-90
- physical interfaces, configuration, 251-253
- physical layer (TCP/IP), 25-26
- ping command, 78, 419-429, 587
- pinouts (cables)
  - 10BASE-T, 42-45
  - 100BASE-T, 42-45
  - 1000BASE-T, 45-46
  - rollover pinouts, 89
- pins (connectors), 40

PKIs (Public Key Infrastructures), 660
- point-to-multipoint outdoor bridges, 622
- point-to-point (Ethernet), 56
- point-to-point edge ports, 233
- point-to-point lines. See leased-line WAN
- point-to-point network type (OSPF), 500-501, 506-508
- point-to-point outdoor bridges, 622
- point-to-point ports, 233
- policies, WLAN client exclusion, 684
- Port Aggregation Protocol. See PAgP
- port-channel load-balance method command, 254
- PortChannels. See EtherChannel

PortFast, 235
- ports, 87
  - 802.1w RSTP roles, 230
  - alternate, 229-232
  - backup, 230
  - blocking, choosing, 212
  - console ports, 672
  - controllers, 672-673
  - costs, 247
    - IEEE default, 223
    - STP, 221
ports

disabled ports, 230
distribution system ports, 672-673
DP, 217, 222-223, 230
Ethernet ports, 40
interfaces, compared, 671
redundancy ports, 672
RJ-45, 40
routed ports, VLAN routing, 406-414
router auxiliary ports, 362
RP, 217, 220, 230
RSTP
  backup, 233
  roles, 230
service ports, 672-674
states, 232
switch ports, 110
switch roots, choosing, 220-221
USB ports, 89
WLC ports, 672-673
postal service forwarding, 22
predictability in interesting octet, 333-334
prefixes
  IP addresses, 292, 302
    defined, 309-310
    dividing into network and subnet parts, 312
    host part and, 311
    length of, 533-536
  masks, 305-309
  routing, 378
primary root switches, 247
priority, switches, 245-246
privacy
  CCMP, 661
data, 655
  GCMP, 661
  TKIP, 660-661
private addresses (IPv4), 542
private branch exchange. See PBX
private IP networks, 277-278
private lines. See leased-line WAN
privileged EXEC mode, 91-93
problem isolation, traceroute command, 429-431
process-ids (OSPF), 472
proprietary routing protocols, 446
protected access credentials. See PAC
protocols
  BGP, 445
  BPDU, 218, 225
  CAPWAP, 639
  CCMP, 661
definition of, 16
distance vector, 446
  DTP, 203
  EAP, 657-658
  EAP-FAST, 659
  EAP-TLS, 660
  GCMP, 661
  IGRP, 446
  LACP, 250
  LEAP, 659
  link-state, 446
  LWAPP, 639
  MSTP, 242-243
  NDP, 573-574
  OSPF, 450
    2-way state, 453-454, 457
    area design, 459-462
    backbone areas, 460
    broadcast network type, 500-506
    calculating best routes with SPF, 457-459
    configuration, 472, 479-481
    default routes, 489-491
    Dijkstra SPF algorithm, 451
    DR, 456-457
    Ethernet links, 456-457
    Hello/dead timers, 512-513
    Hello messages, 452
    interfaces, 493
load balancing, 494
LSAs, 450, 459-464
metrics, 446-447, 491-493
mismatched network types, 515-516
MTU mismatched settings, 515
multiarea OSPF, 482
neighbors, 451-457, 502-516
passive interfaces, 487-488
point-to-point network type, 500-501, 506-508
process-id, 472
processes, shutting down, 513-514
RID, 480-481, 511
verifying operation, 475-478
OSPFv2, 440, 463
interface configuration, 483-486
load balancing, 494
metrics, 493
single-area configuration, 470-475
OSPFv3, 526, 529
PAgP, 250
PEAP, 659
PVST+, 242-243
RIP, 446
routable protocols, 442
routed protocols, 442
routing protocols, 376-378, 442-449
RPVST+, 242-243, 246
RSTP, 228, 242-243
alternate ports, 230-232
backup port role, 233
BID, 218
BPDUs, 218, 225
configurable priority values, 244
collection, 240, 243-244
convergence, 216
EtherChannels, 234, 247-251
Forward delay timer, 225
forwarding or blocking criteria, 216-217
Hello timer, 225
interface states, changing, 227
LAN redundancy, 210, 214
LAN segment DP, 222-223
link types, 233
looping frames, preventing, 213
multiple spanning tree support, 246
need for, 213-215
ports, 212, 230-233
processes, 232
purpose of, 215-217
root switches, 218, 247
STA, 216
standards, 228
steady-state operation, 225
STP, compared, 229-230
switches, 219-221, 247
topology influences, 223-225
STA, 216
STP, 114-115
802.1D standard, 228
BID, 218-219, 243-244
BPDUs, 218, 225
configurable priority values, 244
collection, 240, 243-244
convergence, 216
EtherChannels, 234, 247-251
Forward delay timer, 225
forwarding or blocking criteria, 216-217
Hello timer, 225
interface states, changing, 227
LAN redundancy, 210, 214
LAN segment DP, 222-223
looping frames, 213
MaxAge timer, 225
modes, 242
multiple STP, 241
need for, 213-215
PortFast, 235
ports, 212, 221, 232
purpose of, 215-217
roles, 227
root switches, 218-219
RSTP, 229-230
security, 236
STA, 216
standards, 242
states, 227
steady-state operation, 225
switch reactions to changes, 226-227
switch RP, 220-221
system ID extensions, 243-244
timers, 226-227
topology influences, 223-225
TCP, 20-21
TCP/IP
application layer, 19-20
compared to OSI, 29
data encapsulation terminology, 27-28
data-link layer, 25-26
history of, 16-17
HTTP, 19-20
IPv4, 22-25, 68-78, 140-144
network layer, 22-25, 68-72, 76-78
overview, 18
physical layer, 25-26
RFC, 18
transport layer, 20-22
TKIP, 660-661
public addresses (IPv4), 542
public IP networks, 276-278
Public Key Infrastructures. See PKIs
PVST+ (Per VLAN Spanning Tree), 242-243

Q - R

QoS (Quality of Service), WLAN, 683-684
quit command, 104
RA (Router Advertisement), 600
radio frequencies. See RF
radios, selecting WLAN, 680
RADIUS servers
configuration, 676
WLAN authentication, 682
RAM (Random Access Memory), 99
ranges for global unicast addresses, 544-545
RC4 cipher algorithm, 657
receivers, communication, 613
redundancy
LAN, 210, 214
management, 674
ports, 672
reference bandwidth, defined, 492
registered private IP networks, 277-278
registered public IP networks, 276-278
reload command, 91-92, 102-104, 117, 402-404
remote subnets, 375
repeaters, 620-621
replies
ARP replies, 77
HTTP, 20
ICMP echo replies, 78
requests
ARP requests, 77
ICMP echo requests, 78
reserved multicast addresses, 569-571
resident subnets, 322
reverse routes, testing, 423-425
RF (Radio Frequencies), 613, 626, 642
RID (Router ID)
defined, 470
OSPF, 511
neighbors, 452
RID configuration, 480-481
troubleshooting, 511

Public Key Infrastructures. See PKIs

private subnets, 322
public IP networks, 276-278
Public Key Infrastructures. See PKIs
PVST+ (Per VLAN Spanning Tree), 242-243

QoS (Quality of Service), WLAN, 683-684
quit command, 104
RA (Router Advertisement), 600
radio frequencies. See RF
radios, selecting WLAN, 680
RADIUS servers
configuration, 676
WLAN authentication, 682
RAM (Random Access Memory), 99
ranges for global unicast addresses, 544-545
RC4 cipher algorithm, 657
receivers, communication, 613
redundancy
LAN, 210, 214
management, 674
ports, 672
reference bandwidth, defined, 492
registered private IP networks, 277-278
registered public IP networks, 276-278
reload command, 91-92, 102-104, 117, 402-404
remote subnets, 375
repeaters, 620-621
replies
ARP replies, 77
HTTP, 20
ICMP echo replies, 78
requests
ARP requests, 77
ICMP echo requests, 78
reserved multicast addresses, 569-571
resident subnets, 322
reverse routes, testing, 423-425
RF (Radio Frequencies), 613, 626, 642
RID (Router ID)
defined, 470
OSPF, 511
neighbors, 452
RID configuration, 480-481
troubleshooting, 511
RIP (Routing Information Protocol), 446
RIPng (RIP next generation), 529
RIPv2 (Routing Information Protocol version 2), 446-447
RIR (Regional Internet Registries), 524
RJ-45 connectors, 41
RJ-45 ports, 40
roaming
    AP, 618
    clients, 642
ROAS (Router-On-A-Stick), 392, 396-401
Rogue Detector mode (AP), 647
roles
    alternate ports, 230-232
    ports, 230, 233
    RSTP port, 230
    STP, 227
rollover pinouts (cables), 89
ROM (Read-Only Memory), 100
root bridge ID, 218
root costs, switches, 216
root ports. See RP
root switches, 217
    electing, 218-219
    RSTP root switches, 247
    timer values, 218
routable protocols, 442
route redistribution, 448
routed ports, VLAN routing, 406
    EtherChannels, 410-414
    routed interfaces, 407-409
routed protocols, 442
router-id command, 470, 496
router ospf command, 470, 495
router ospf 1 command, 472, 480
router ospf process-id command, 480, 510
routers/routing, 35
    ABR, 460-461
    ARP tables, 378-379
    auxiliary ports, 362
    backbone, 461
    best routes, finding, 451
    candidate default routes, 384
    Cisco integrated services routers, 352
    classful versus classless, 313
    CLI, 355-356
    connected routes, 366, 376-378
    default routers, 70, 370-372
    default routes, 379, 383-384
    discovering with NDP, 600-601
    DR, 456-457
    DROthers, 457
    dynamic unicast address configuration, 564
    enterprise routers, 350-353
    floating static routes, 381-383
    flooding, 450
    host routes, 378-379
        logic, 370
        static host routes, 381
    installation, 350-354
    interfaces, 356-361
    internal routers, 461
    IP routing, 366, 369
        ARP tables, 378-379
        de-encapsulating IP packets, 373-374
        encapsulating IP packets in new frames, 375
        example of, 371-376
        forwarding, 374-375, 386-389
        host forwarding of IP packets to default routers (gateways), 372
        IPv4 routing, 24-25, 68-75, 355-362, 369-371, 527
        IPv6 routing, 527-530, 558, 583-598
        processing incoming frames, 373
        tables, 388-389
transmitting frames, 376
troubleshooting, 419-434
link-local address configuration, 566-569
local routes, 378
logic
host routing, 370
IPv4 routing, 371
LSA, 463
network masks, 378
network routes, 379
OSPF interface costs, 493
overview, 348
path selection, 69
prefixes, 378
protocol codes, 378
protocols, 376
administrative distance, 448-449
algorithms, 445
AS, 444
classful versus classless, 313
classless/classful, 447-448
convergence, 443
defined, 442
distance vector, 446
EGP, 444
EIGRP, 446
functions, 443
IGP, 444-448
link-state, 446
OSPF, 446-447, 450-464, 475-482, 487-491
path selections, 442
proprietary, 446
RIPv2, 446-447
route redistribution, 448
remote subnets, 375
reverse routes, testing, 423-425
ROAS
configuration, 396-398
subinterfaces, 399-401
troubleshooting, 400-401
verifying, 398-400
SOHO routers, 354
static unicast address configuration, 557-564
static routes, 367, 376
configuration, 379-384
default routes, 379
floating static routes, 381-383
host routes, 379-381
static default routes, 383-384
static network routes, 379
troubleshooting, 385-386
subnet router anycast addresses, 576
VLAN routing, 183-184, 395
Layer 3 (multilayer) switch
routed ports, 406-414
Layer 3 (multilayer) switch SVI, 401-406
ROAS, 396-401
WAN, 64-65
RP (Root Ports), 217, 220-221, 230
RPVST+ (Rapid Per VLAN Spanning Tree+), 242-243, 246
RS (Router Solicitation), 600
RSTP (Rapid Spanning Tree Protocol), 228, 242-243
alternate ports, 230-232
backup port role, 233
BID, 218
blocking criteria, 216-217
BPDUs, 218, 225
configurable priority values, 244
configuration, 240
discarding state, 229
forwarding criteria, 216-217
LAN segment DP, 222-223
link types, 233
looping frames, preventing, 213
multiple spanning tree support, 246
need for, 213-215
ports, 233
  blocking, 212
  roles, 230
  states, 232
processes, 232
purpose of, 215-217
root switches, 218, 247
STA, 216
standards, 228
steady-state operation, 225
STP, compared, 229-230
switches
  electing, 219
  priority, 247
  RP, choosing, 220-221
topology influences, 223-225
running-config file, 100
runt, 167

S

SO/0/0 status code, 359
same-layer interaction, 21-22
scopes of multicast addresses, 571-572
sdm prefer command, 402-404
sdm prefer lanbase-routing command, 402, 415
SE Connect mode (APs), 647
secondary root switches, 247
Secure Shell. See SSH
security. See also authentication
attacks, 654
CLI, 93-94, 128-139
data integrity, 656
data privacy, 655
decryption, 655
encryption, 655
fake AP, 654
forward secrecy, 663
intrusion protection, 642
MIC, 656
privacy/integrity methods, 660-661
shared-key, 657
STP, 236
transmissions reaching unintended recipients, 652
WLAN, 681-684
WLC authentication, 642
WPA, 662-663
WPA2, 662-663
WPA3, 662-663
self-healing coverage, 642
sender MAC addresses, 661
SEQ (Sequence Numbers), 21
sequence counters (TKIP), 661
sequence numbers (SEQ), 21
serial lines. See leased-line WAN
Serial WAN (Wide Area Networks), 350
servers
  AAA servers, 136
  AS, 658
  external authentication servers, 135-136
  RADIUS, 676, 682
  Telnet servers, 91
service ports, 672-674
service set identifiers. See SSID
session timeouts (WLAN), 684
SFP (Small Form Pluggable), 42, 48
SFP+ (Small Form Pluggable Plus), 42, 48
shared-key security, 657
shared media (Ethernet), 56
shared passwords, 130
shared ports, 234
shorter VLAN configuration example, 189
Shortest Path First algorithm. See SPF algorithm
show arp command, 391
show command, 95, 166, 361, 480, 508
show crypto key mypubkey rsa command, 149
show dhcp lease command, 143-144, 149
show etherchannel 1 summary command, 250
show etherchannel command, 248, 259, 416
show etherchannel summary command, 413
show history command, 145, 149
show interfaces command, 119-120, 156, 162-164, 167-170, 357-358, 361, 364, 376, 408, 416, 515-517, 583
show interfaces description command, 162, 170
show interfaces interface-id trunk command, 203-205
show interfaces status command, 118, 125, 153, 156, 162-165
Layer 3 EtherChannels, 412
routed ports, 408
show interfaces switchport command, 192-195, 199, 202-203, 208
show interfaces trunk command, 193-194, 199-200, 203-205, 208, 401
show interfaces type number switchport command, 199
show interfaces type number trunk command, 200
show interfaces vlan command, 143-144, 149, 416
show ip arp command, 391
show ip default-gateway command, 144, 149
show ip interface brief command, 357-361, 364, 406
show ip ospf command, 481
defined, 496, 517
duplicate OSPF RID, 511
OSPF neighbors, troubleshooting, 510
show ip ospf database command, 450, 462, 475, 497
show ip ospf interface brief command, 479-480, 488, 491, 503-505, 508, 511, 514
defined, 496, 517
OSPF neighbors, troubleshooting, 510
show ip ospf interface command, 488, 503-505, 513
defined, 496, 517
Hello/dead timer mismatches, 512
OSPF neighbors, troubleshooting, 510
OSPFv2 interface configuration, 486
show ip ospf interface G0/0 command, 505
show ip ospf neighbor command, 452-453, 457, 475, 480, 497, 502, 505, 508-511, 513-517
show ip ospf neighbor interface brief command, 513
show ip protocols command
defined, 496, 517
OSPFv2 interface configuration, 485
show ip route address command, 388
show ip route command, 324, 356, 367, 376, 378-391, 400-402, 408, 475-478, 585
administrative distance, 449
defined, 497
routing tables, displaying, 416
show ip route [connected] command, 398
show ip route EXEC command, 404
show ip route ospf command, 387, 497
show ip route static command, 380, 490
show ip ssh command, 139, 149
show ipv6 interface brief command, 558-560, 567, 575, 579
show ipv6 interface command, 558-559, 567, 570-573, 579
show ipv6 route command, 566, 579, 585-590, 605
show ipv6 route connected command, 560, 586
show ipv6 route local command, 585-586
show ipv6 route static command, 587-590, 593-595
show mac address-table aging-time command, 122, 125
show mac address-table command, 120, 125, 356
show mac address-table count command, 122, 125
show mac address-table dynamic address command, 125
show mac address-table dynamic command, 96, 117, 123-125, 170
show mac address-table dynamic interface command, 120-121, 125
show mac address-table dynamic vlan command, 125
show mac address-table static command, 170
show mac address-table vlan command, 121
show protocols command, 361, 364
show running-config | interface command, 170
show running-config command, 93, 101, 104, 132-133, 143, 149, 155, 158, 170, 398, 479, 488, 511, 584
show spanning-tree command, 249, 259
show spanning-tree vlan command, 259
show spanning-tree vlan vlan-id command, 204
show ssh command, 139, 149
show startup-config command, 101, 104, 158
show vlan brief command, 186-189, 202
show vlan command, 201, 208, 398-401, 416
show vlan id command, 187
show vtp status command, 190, 208
shutdown command, 143, 155, 163, 170, 207, 253, 356, 359, 363, 399-401, 405
signals
  sending messages, 623
  waves, 623-627
single-area OSPF, 459
single-area OSPFv2, 470-475
single-mode fiber-optic cables, 47-49
single-size subnets, 273-274
SLAAC (Stateless Address Auto Configuration), 560, 598, 601
slash masks, 305
small office/home office (SOHO) LANs, 35
small office/home office (SOHO) networks, 15
SNA (Systems Network Architecture), 16
Sniffer mode (APs), 647
software configuration
  common command prompts, 98
  configuration files, 99-102
  configuration mode, 96-97
  configuration submodes and contexts, 97-99
SOHO (Small Offices/Home Offices)
  LAN, 35
  networks, 15
  routers, 354
solicited-node multicast addresses, 573-574
source MAC addresses, 113
spanning-tree algorithm. See STA
spanning-tree commands, 259
spanning-tree mode command, 242-243, 259
Spanning Tree Protocol. See STP
spanning-tree vlan command, 244
spanning-tree vlan x root primary command, 244-245
spanning-tree vlan x root secondary command, 244-245
speed, switch interface configurations, 152-154
speed command, 98-99, 152-154, 165, 170, 355, 363
SPF (Shortest Path First) algorithm
Dijkstra SPF, 451
OSPF best routes, calculating, 457-459
split-MAC architectures, 638-643
SSH (Secure Shell), 91, 136-139, 432-434
SSID (Service Set Identifiers), 615
broadcasting, 681
multiple on one AP, supporting, 617
STA (spanning-tree algorithm), 216
startup-config file, 100
state change reactions (STP topology), 224-225
Stateless Address Auto Configuration. See SLAAC
states
discarding, 230
interfaces, 215-217, 227
ports, 232
STP, 227
static default routes (IPv6), 592-593
static host routes (IPv6), 593
static ranges per subnet, choosing, 286-287
static routes, 367, 376
configuration, 379-384
default routes, 379
floating static routes, 381-383, 593-595
global unicast next-hop address, 589
host routes, 379-381
link-local next-hop address, 589-590
outgoing interface, 587-588
over Ethernet links, 591
overview, 586
static default routes, 383-384, 592-593
static host routes, 593
static network routes, 379
troubleshooting, 385-386, 595-598
static unicast address configuration (IPv6)
configuration full 128-bit address, 557-558
enabling IPv6 routing, 558
generating unique interface ID with modified EUI-64, 560-564
verifying, 558-560
status codes
routers, 358-359
troubleshooting, 162-163
STP (Spanning Tree Protocol), 114-115, 210, 243
802.1D standard, 228
BID, 218-219, 243-244
blocking criteria, 212, 216-217
BPDUs, 218, 225
configurable priority values, 244
configuration, 240, 243-244
corvergence, 216
EtherChannels, 234, 247-251
Forward delay timer, 225
forwarding criteria, 216-217
Hello timer, 225
interface states, changing, 227
LAN
redundancy, 210, 214
segment DPs, choosing, 222-223
subnets 789

looping frames, preventing, 213
MaxAge timer, 225
modes, 242
multiple STP, 241
need for, 213-215
PortFast, 235
ports
  blocking criteria, 212, 216-217
cost, 221
states, 232
purpose of, 215-217
roles, 227
root switches, electing, 218-219
RSTP, compared, 229-230
security, 236
STA, 216
standards, 242
states, 227
steady-state operation, 225
switch reactions to changes, 226-227
switch RP, choosing, 220-221
system ID extensions, 243-244
timers, 226-227
topology influences, 223-225
straight-through cable pinouts, 42-45
subcommands, 97
  auto-cost reference-bandwidth, 493
  bandwidth, 492
  ip address, 376
  no network network-id area area-id, 483
  switchport trunk allowed vlan, 204
subdivided networks. See subnets
subinterfaces, 396-401
subnet masks, 272, 302. See also subnets
classful IP networks before subnetting, 279-280
converting between formats, 305-309
difficult masks, 334-338
easy masks, 332
formats for, 304-305
hosts
  borrowing bits to create subnet bits, 280-281
calculating in network, 313-315
  choosing bits, 281
mask formats, 282-283
prefix part, 309-312
sample design, 282
VLSM, 275
subnet numbers, 272, 283, 334-336
subnets, 543. See also subnet masks
classful IP networks before subnetting, 279-280
addresses, 272, 283, 324, 327, 334-336
analyzing
  subnet needs, 269, 271
  with decimal math, 332, 339
assigning to different locations, 285
binary math, 326
Boolean math, 331
  finding range of addresses, 331
  finding subnet IDs, 327
  practice problems, 328-329
  shortcut for binary process, 330
Boolean math, 331
broadcasts, 272, 283, 325-327, 336-338
building list of, 283-284
calculating, 313-315
decimal math, 331
difficult masks, 334-338
easy masks, 332
finding subnet broadcast addresses, 336-338
predictability in interesting octet, 333-334
reference table: DDN mask values and binary equivalent, 339
definition of, 267, 322
design choices, 276-284
design views, 267-268
dynamic ranges, choosing, 286-287
examples of
  networks with four subnets, 322-323
  simple example, 267
hosts, 268-271
ID, 272, 283, 324, 330
  finding with binary math, 327
  finding with decimal math, 334-336
IPv4, 548
IPv6, 548
IP addresses, 283-284, 302, 312
IPv4, 70, 73, 545
IPv6
  assigning to internetwork topology, 549
  interface ID, 547
  listing, 548-549
  with global unicast addresses, 545-549
  with unique local addresses, 551-552
multiple subnet sizes, 274
networks versus, 324
number of hosts, 271
number of subnets, 270
one-size subnets, 273
operational view, 267-268
overview, 266
plan documents, 267
planning implementations, 284-287
range of usable addresses, 325
remote subnets, 375
resident subnets, 322
router anycast addresses, 549, 576
simple example, 267
single-size subnets, 273
size of, 272-274
static ranges, choosing, 286-287
subnet numbers, 272, 283, 324, 327, 334-336
VLSM, 275
superior Hello messages, 219
supplicants, 658
SVI (Switched Virtual Interfaces), 392, 401-406
switch ports, 110
switches
  access switches, 241
  alternate ports, 229
  auto-mdix, 45
  backup ports, 230
  BID, 218, 243-244
  BPDU, 218, 225
  Cisco Catalyst switches, 86
  configuration files, 99-102
  DHCP, 143
  distribution switches, 241
  EtherChannels, 234
  Ethernet switches, 48
  filtering decisions, 110-113
  forwarding decisions, 110-113
  history buffer commands, 144-145
interfaces, 87, 110, 118-120
  autonegotiation, 158-162
  description, 152-154
  duplex, 152-154, 163-166
  enabling/disabling interfaces, 155-156
  Layer 1 problems, 166-168
  multiple interfaces, 154-155
  overview, 152
  removing configuration, 157-158
  speed, 152-154, 163-166
  status codes, 162-163
  troubleshooting, 162-168
IPv4, 140-144
LAN segment DP, choosing, 222-223
LAN switches, 35
- analyzing, 116
- flooding, 114
- interface configuration, 152-162
- MAC address table, 113-114, 117-124
- overview, 106-109
- STP, 114-115
- summary, 115-116
- switch forwarding and filtering decisions, 110-113
- switch interfaces, 118-120, 152-162
- switching logic, 109-110
- verifying, 116
 Layer 2 switches, 141, 183
 Layer 3 (multilayer) switches, 141, 184, 401-414
 links, 233
 MAC address tables, 111, 214-215
management
- DHCP, 143
- history buffer commands, 144-145
- IPv4, 140-144
- overview, 126
- security, 128-139
 multi layer switches, 184
 PortFast, 235
 ports, 87, 230-233
 priority, 245-246
 root costs, 216
 root switches, 217-219, 247
 RP, choosing, 220-221
 RSTP switch priority, 247
 security, 128-139
 STP
- reacting to changes, 226-227
- topology influences, 223-225
 system ID extensions, 245-246
 unknown unicast frames, 114
 VLAN configuration, 140
 voice switches, 196
 switching tables. See MAC address tables
 switchport access vlan command, 185-189, 198-199, 207
 switchport command
 Layer 3 switches, 415
 routed ports, 408
 switchport mode access command, 185, 188, 198-199
 switchport mode command, 191, 207
 switchport mode dynamic auto command, 202
 switchport mode dynamic desirable command, 193
 switchport mode trunk command, 191, 203, 396
 switchport nonegotiate command, 195, 203, 207
 switchport trunk allowed vlan command, 204, 207
 switchport trunk encapsulation command, 191, 207
 switchport trunk native vlan command, 207
 switchport trunk native vlan vlan-id command, 205
 switchport voice vlan command, 198-199, 207
 switchport voice vlan vlan-id command, 200
 system ID extensions, 243-246

T

T1. See leased-line WAN
tables
- ARP tables, 77, 378-379
- IP routing tables, 70-72, 388-389
- MAC address tables, 111-124, 214-215

system ID extensions, 243-246

unknown unicast frames, 114
tagging (VLAN), 181-182
TCP (Transmission Control Protocol), 20-21
TCP/IP (Transmission Control Protocol/Internet Protocol)
application layer, 19-20
data encapsulation terminology, 27-28
data-link layer, 25-26
history of, 16-17
HTTP, 19-20
IPv4, 22-25, 68-78, 140-144
network layer, 22-25
ARP, 77
DNS, 76-77
routing, 68-72
testing connectivity, 78
OSI, compared, 29
overview, 18
physical layer, 25-26
RFC, 18
transport layer, 20-22
Telnet, 90-91, 129, 432-434
terminal history size command, 145, 149
test etherchannel load-balance EXEC command, 255
testing
IPv4 connectivity, 78
LAN neighbors, 425-426
reverse routes, 423-425
WAN neighbors, 427
three-area OSPF (Open Shortest Path First), 460
time stamps, 661
timers
Hello/dead mismatches, troubleshooting, 512-513
Hello messages, 455
STP, 226-227
TKIP (Temporal Key Integrity Protocol), 660-661
topologies
AP noninfrastructure modes, 620-622
STP, 223-225
WLAN, 614-622
traceroute command, 428-432, 587
traffic flows, BSS, 615
transmitters, communication, 613
transmitting
frames, IP routing, 376
optimizing transmit power, 642
transport input all command, 139
transport input command, 138, 148, 356
transport input none command, 139
transport input ssh command, 139
transport input telnet ssh command, 139
transport layer (TCP/IP), 20-22
troubleshooting
EtherChannels, 251-253
Ethernet LAN, 166-168
Hello/dead timers, 512-513
interfaces, 162-168
IP routing
ping command, 419-429
SSH, 432-434
Telnet, 432-434
traceroute command, 428-432
Layer 3 EtherChannels, 413-414
Layer 3 (multilayer) switch SVI, 404-406
native VLAN, 205
neighbor adjacencies, 510-516
OSPF
mismatched MTU settings, 515
mismatched network types, 515-516
neighbor adjacencies, 510-516
shutting down processes, 513-514
ping command, 419-429, 587
RID, 511
ROAS, 400-401
SSH, 432-434
static IPv6 routes, 595-598
static routes, 385-386
Telnet, 432-434
traceroute command, 428-432, 587
VLAN, 201-205
trunking
802.1Q, 182
administrative mode, 191
configuration, 191-195
dynamic auto mode, 191
dynamic desirable mode, 191
ISL, 182
overview, 180-181
type of, 191
VLAN
mismatched native VLAN, 205
mismatched trunking operational states, 202-203
supported VLAN list on trunks, 203-205
tagging, 181-182
VTP, 189-190
TTL (Time To Live), 429
TTL Exceeded (Time-to-Live Exceeded), 429-431
tunneling, CAPWAP, 639-640
two-switch topology, 123-124

UDP (User Datagram Protocol), 20
unabbreviated addresses (IPv6), 530
undebug all command, 104
undefined VLAN, troubleshooting, 201-202
unicast addresses, 50-52, 290, 322, 540, 556-564
unidirectional communication, 613
unified architectures. See centralized architectures
unique local addresses, 542, 551-553
universal addresses, 51
unknown addresses (IPv6), 574
unknown unicast frames, 114
URI (Universal Resource Identifiers), 20
URL (Uniform Resource Locators), 20
USB ports, 89
User Datagram Protocol (UDP), 20
user EXEC mode, 91-93
user mode
external authentication servers, 135-136
passwords, 130-135
usernames, 133-135, 147
users, segregating into logical networks, 676
UTP (Unshielded Twisted-Pair) cables, 37
cabling pinouts, 42-49
overview, 39-40
UTP Ethernet links, 40-41
uWGB (Universal Workgroup Bridges), 621
V

verifying
Data VLAN, 198-199
EtherChannel configuration before adding interfaces, 251-253
Ethernet switching, 116
IPv4 on switch, 143-144
Layer 3 (multilayer) switch SVI, 403-404
OSPF
  configuration, 479-480
  operation, 475-478
OSPFv2 interface configuration, 485-486
ROAS, 398-400
static unicast address configuration, 558-560
Voice VLAN, 198-199
virtual interfaces (controllers), 674
VLAN (Virtual Local Area Networks)
  AP, 635, 668
  configuration, 185-195, 198-199
  Data VLAN, 197-199
  default VLAN, 186
  disabled VLAN, troubleshooting, 201-202
dynamic interface ID, 678
hopping, 205
ID, 180
interfaces, 402
IP telephony, 196-200
LAN trunking, 182
mapping, 673
native VLAN, 183, 205, 398
overview, 179-180
PVST+, 242-243
routing, 183-184, 395-414
split-MAC architecture, 640
supported VLAN list on trunks, 203-205
switches, 140
tagging, 181-182
troubleshooting
disabled VLAN, 201-202
  supported VLAN list on trunks, 203-205
trunking, 202-205
undefined VLAN, 201-202
trunking, 180-182, 189-195
VLAN ID, 180
Voice VLAN, 197-199
  vlan command, 185, 198, 207
  vlan number command, 201
VLSM (Variable Length Subnet Masks), 275
voice switches, 196
VTP (VLAN Trunking Protocol), 189-190
  vtp mode command, 207
  vtp mode off command, 190
  vtp mode transparent command, 190
W - X - Y - Z

WAN (Wide Area Networks), 32, 60
  Ethernet WAN, 65-68
    enterprise networks, 350
    point-to-point network type (OSPF), 506-508
  leased-line WAN, 61-65
neighbors, testing, 427
Serial WAN, enterprise networks, 350
waves
  continuous pattern, 623
cycles, 625
electric/magnetic, 624
electromagnetic, 624
frequency, 625-627
propagation with idealistic antenna, 624
WebAuth (Web Authentication), 657
WEP (Wired Equivalent Privacy), 657
WGB (Workgroup Bridges), 621
wildcard masks, 473-475
wired LAN, See Ethernet, LAN
wired networks, 612-613
wireless band frequencies, 627
wireless LAN, 32
wireless networks
  802.11 standard, 628-629
  waves, 625
  wired networks, compared, 612-613
  WPA, 662-663
  WPA2, 662-663
  WPA3, 662-663
WLAN (Wireless Local Area Networks)
  802.11 WLAN, 614
  advanced settings, 684-685
  AP, 668-669
  BSS, 614-616
  client session timeouts, 684
  configuration, 675
    advanced settings, 684-685
    controller configuration, 685
    dynamic interfaces, 678
    QoS, 683-684
    RADIUS servers, 676
    security, 681-682
  creating, 679-681
  defined, 675
  DS, 616-618
  dynamic interfaces, creating, 678
  ESS, 618
  IBSS, 619
  limiting, 676
  listings of, displaying, 679
  management access, allowing, 685
  mesh networks, 622
  outdoor bridges, 621-622
  QoS, 683-684
  RADIUS server, configuration, 676
  repeaters, 620-621
  security, 681-684
  too many, creating, 676
  topologies, 614-622
  user segregation into logical networks, 676
  WGB, 621
  WLC, 669-675
WLC (Wireless LAN Controllers)
  activities, 642
  centralized, 642-643
  cloud-based architectures, 643
  dynamic interfaces, 674-675
  embedded deployments, 644
  interfaces, 673-675
  LAP, 639-640
  management interfaces, 674
  Mobility Express WLC deployments, 645
  ports, 672-673
  redundancy management, 674
  service port interfaces, 674
  virtual interfaces, 674
  WLAN, 669-675
  working interfaces, defined, 217
WPA (Wi-Fi Protected Access), 662-663
WPA2 (Wi-Fi Protected Access version 2), 662-663
WPA3 (Wi-Fi Protected Access version 3), 662-663
write erase command, 104