



Practice Tests



Video Training



Flash Cards



Study Planner



Review Exercises

# CCNP

## Enterprise Advanced Routing

### ENARSI 300-410

2nd Edition

[ciscopress.com](http://ciscopress.com)

**RAYMOND LACOSTE**  
**BRAD EDGEWORTH, CCIE® NO. 31574**

FREE SAMPLE CHAPTER |



# CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide

## Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book's companion website, including practice test software, review exercises, video training, Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to [ciscopress.com/register](http://ciscopress.com/register).
2. Enter the **print book ISBN: 9780138217525**.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated with the book listing under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at [PearsonTestPrep.com](http://PearsonTestPrep.com). Simply choose Pearson IT Certification as your product group and log into the site with the same credentials you used to register your book. Click the **Activate New Product** button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to [pearsonitp.echelp.org](http://pearsonitp.echelp.org).

*This page intentionally left blank*

# **CCNP Enterprise Advanced Routing**

**ENARSI 300-410**

**Official Cert Guide,  
Second Edition**

**RAYMOND LACOSTE**

**BRAD EDGEWORTH, CCIE No. 31574**

**Cisco Press**

# CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide, Second Edition

Raymond Lacoste, Brad Edgeworth

Copyright© 2024 Cisco Systems, Inc.

Published by:

Cisco Press

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit [www.pearson.com/permissions](http://www.pearson.com/permissions).

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

**\$PrintCode**

Library of Congress Control Number: 2023911481

ISBN-13: 978-0-13-821752-5

ISBN-10: 0-13-821752-1

## Warning and Disclaimer

This book is designed to provide information about Implementing Cisco Enterprise Advanced Routing and Services (ENARSI 300-410). 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.

Figure credit: Figure 7-1 Wireshark

## Special Sales

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

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

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

## Feedback Information

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

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

We greatly appreciate your assistance.

**Vice President, IT Professional:** Mark Taub

**Alliances Manager, Cisco Press:** Jaci Featherly; James Risler

**Director, ITP Product Management:** Brett Bartow

**Managing Editor:** Sandra Schroeder

**Development Editor:** Ellie C. Bru

**Senior Project Editor:** Mandie Frank

**Copy Editor:** Kitty Wilson

**Technical Editor:** Hector Mendoza, Jr

**Editorial Assistant:** Cindy Teeters

**Designer:** Chuti Prasertsith

**Composition:** Codemantra

**Indexer:** Erika Millen

**Proofreader:** Barbara Mack



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

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

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, visit [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner in a partnership relationship between Cisco and any other company. (1110R)

## Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where

- Everyone has an equitable and lifelong opportunity to succeed through learning
- Our educational products and services are inclusive and represent the rich diversity of learners
- Our educational content accurately reflects the histories and experiences of the learners we serve
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview)

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

Please contact us with concerns about any potential bias at <https://www.pearson.com/report-bias.html>.

## About the Authors

**Raymond Lacoste** has dedicated his career to developing the skills of those interested in IT. In 2001, he began to mentor hundreds of IT professionals pursuing their Cisco certification dreams. This role led to teaching Cisco courses full time. Raymond is currently a master instructor for Cisco Enterprise Routing and Switching, AWS, ITIL, and CyberSecurity at StormWind Studios. Raymond treats all technologies as an escape room, working to uncover every mystery in the protocols he works with. Along this journey, Raymond has passed more than 120 exams, and his office wall includes certificates from Microsoft, Cisco, ISC2, ITIL, AWS, and CompTIA. If you were visualizing Raymond's office, you'd probably expect the usual network equipment, certifications, and awards. Those certainly take up space, but they aren't his pride and joy. Most impressive, at least to Raymond, is his gemstone and mineral collection; once he starts talking about it, he just can't stop. Who doesn't get excited by a wondrous barite specimen in a pyrite matrix? Raymond presently resides with his wife and two children in eastern Canada, where they experience many adventures together.

**Brad Edgeworth**, CCIE No. 31574 (R&S and SP), is an SD-WAN technical solutions architect at Cisco Systems. Brad is a distinguished speaker at Cisco Live, where he has presented on various topics. Before joining Cisco, Brad worked as a network architect and consultant for various Fortune 500 companies. Brad's expertise is based on enterprise and service provider environments, with an emphasis on architectural and operational simplicity. Brad holds a bachelor of arts degree in computer systems management from St. Edward's University in Austin, Texas. Brad can be found on Twitter as @BradEdgeworth.

## About the Technical Reviewer

**Hector Mendoza, Jr.**, CCIE No. 10687 (R&S, SP, and Security), has spent the past 14 years at Cisco Systems and is currently a solutions integration architect supporting large SP customers. Prior to this proactive role in CX, he spent nearly a decade providing reactive support in High Touch Technical Services in the Security Group, where he provided escalation support for some of the largest customers for Cisco. A four-time Cisco Live speaker and an Alpha reviewer of Cisco Security courseware, Hector is a huge advocate of continuing education and knowledge sharing. Hector has a passion for technology, enjoys solving complex problems, and loves working with customers. In his spare time, he tech reviews his esteemed colleagues' Cisco Press books.

## Dedications

**Raymond Lacoste:**

This book (just like the first edition) is dedicated to my wife, Melanie, who has dedicated her life to making me a better person, which is the hardest job in the world. Thank you, Melanie, for being the most amazing wife and mother in the world.

**Brad Edgeworth:**

This book is dedicated to my daughter, Teagan. Hopefully you'll want to learn what is written inside of this text. Until then, enjoy your youth.

## Acknowledgments

### **Raymond Lacoste:**

As with the first edition of this book, a huge thank you goes out to Brad for joining me on this writing adventure. Putting our knowledge together to create this work of art was the best decision. Thank you so much for sharing this with me.

Thank you to my wife and children, for allowing me to avoid many family adventures while this book was being developed and supporting me though the entire process. Love you guys!

Finally, thank you to the entire team at Cisco Press, as well as their families and friends, who work extremely hard to produce high-quality training material.

### **Brad Edgeworth:**

To Raymond and Brett, thanks for letting me write this book. I am privileged to be able to share my knowledge with others, and I'm grateful. To the rest of the Cisco Press team, thanks for taking my block of stone and turning it into a work of art.

To the technical editor: Hector, thank you for the time and expertise.

Many people within Cisco have shared their knowledge with me and taken a chance on me with various projects over the years. For that I'm forever indebted.

## Contents at a Glance

	Introduction	xxxv
Chapter 1	IPv4/IPv6 Addressing and Routing Review	2
Chapter 2	EIGRP	72
Chapter 3	Advanced EIGRP	106
Chapter 4	Troubleshooting EIGRP for IPv4	138
Chapter 5	EIGRPv6	188
Chapter 6	OSPF	222
Chapter 7	Advanced OSPF	260
Chapter 8	Troubleshooting OSPFv2	314
Chapter 9	OSPFv3	370
Chapter 10	Troubleshooting OSPFv3	392
Chapter 11	BGP	426
Chapter 12	Advanced BGP	480
Chapter 13	BGP Path Selection	524
Chapter 14	Troubleshooting BGP	556
Chapter 15	Route Maps and Conditional Forwarding	620
Chapter 16	Route Redistribution	648
Chapter 17	Troubleshooting Redistribution	674
Chapter 18	VRF, MPLS, and MPLS Layer 3 VPNs	724
Chapter 19	DMVPN Tunnels	766
Chapter 20	Securing DMVPN Tunnels	820
Chapter 21	Troubleshooting ACLs and Prefix Lists	842
Chapter 22	Infrastructure Security	866
Chapter 23	Device Management and Management Tools Troubleshooting	890
Chapter 24	Final Preparation	944

Chapter 25 *ENARSI 300-410* Exam Updates 954

Appendix A Answers to the “Do I Know This Already?” Quiz Questions 958

Glossary 972

Index 990

**Online Elements**

Appendix B Command Reference Exercises

Appendix C Command Reference Exercises Answer Key

Appendix D Study Planner

# Contents

Introduction xxxv

## Chapter 1 IPv4/IPv6 Addressing and Routing Review 2

“Do I Know This Already?” Quiz 3

Foundation Topics 7

IPv4 Addressing 7

IPv4 Addressing Issues 7

Determining IP Addresses Within a Subnet 10

DHCP for IPv4 11

Reviewing DHCP Operations 11

Potential DHCP Troubleshooting Issues 16

DHCP Troubleshooting Commands 17

IPv6 Addressing 19

IPv6 Addressing Review 19

*EUI-64* 20

IPv6 SLAAC, Stateful DHCPv6, and Stateless DHCPv6 22

SLAAC 22

Stateful DHCPv6 27

Stateless DHCPv6 28

DHCPv6 Operation 29

DHCPv6 Relay Agents 30

Packet-Forwarding Process 31

Reviewing the Layer 3 Packet-Forwarding Process 31

Troubleshooting the Packet-Forwarding Process 35

Administrative Distance 38

Data Structures and the Routing Table 39

Sources of Routing Information 39

Static Routes 41

IPv4 Static Routes 42

IPv6 Static Routes 46

Trouble Tickets 48

IPv4 Addressing and Addressing Technologies Trouble Tickets 48

Trouble Ticket 1-1 48

Trouble Ticket 1-2 50

IPv6 Addressing Trouble Tickets	53
Trouble Ticket 1-3	54
Trouble Ticket 1-4	57
Static Routing Trouble Tickets	61
Trouble Ticket 1-5	61
Trouble Ticket 1-6	64
Exam Preparation Tasks	66
Review All Key Topics	66
Define Key Terms	68
Use the Command Reference to Check Your Memory	68

## **Chapter 2 EIGRP 72**

“Do I Know This Already?” Quiz	72
Foundation Topics	74
EIGRP Fundamentals	74
Autonomous Systems	75
EIGRP Terminology	75
Topology Table	76
EIGRP Neighbors	77
<i>Inter-Router Communication</i>	78
Forming EIGRP Neighbors	79
EIGRP Configuration Modes	80
Classic Configuration Mode	80
EIGRP Named Mode	80
EIGRP Network Statement	81
Sample Topology and Configuration	83
Confirming Interfaces	84
Verifying EIGRP Neighbor Adjacencies	85
Displaying Installed EIGRP Routes	86
Router ID	87
Passive Interfaces	88
Authentication	91
<i>Keychain Configuration</i>	92
<i>Enabling Authentication on the Interface</i>	92
Path Metric Calculation	94
Wide Metrics	96
Metric Backward Compatibility	98

	Interface Delay Settings	99
	Custom K Values	100
	Load Balancing	100
	References in This Chapter	102
	Exam Preparation Tasks	102
	Review All Key Topics	103
	Define Key Terms	103
	Use the Command Reference to Check Your Memory	103
<b>Chapter 3</b>	<b>Advanced EIGRP</b>	<b>106</b>
	“Do I Know This Already?” Quiz	106
	Foundation Topics	108
	Failure Detection and Timers	108
	Convergence	109
	Stuck in Active	112
	Route Summarization	114
	Interface-Specific Summarization	114
	Summary Discard Routes	116
	Summarization Metrics	117
	Automatic Summarization	118
	WAN Considerations	119
	EIGRP Stub Router	119
	Stub Site Functions	121
	IP Bandwidth Percentage	125
	Split Horizon	126
	Route Manipulation	129
	Route Filtering	129
	Traffic Steering with EIGRP Offset Lists	132
	References in This Chapter	135
	Exam Preparation Tasks	135
	Review All Key Topics	135
	Define Key Terms	136
	Use the Command Reference to Check Your Memory	136
<b>Chapter 4</b>	<b>Troubleshooting EIGRP for IPv4</b>	<b>138</b>
	“Do I Know This Already?” Quiz	138
	Foundation Topics	141
	Troubleshooting EIGRP for IPv4 Neighbor Adjacencies	141

Interface Is Down	142
Mismatched Autonomous System Numbers	142
Incorrect Network Statement	144
Mismatched K Values	145
Passive Interface	146
Different Subnets	148
Authentication	148
ACLs	150
Timers	151
Troubleshooting EIGRP for IPv4 Routes	151
Bad or Missing network Command	152
Better Source of Information	154
Route Filtering	157
Stub Configuration	158
Interface Is Shut Down	160
Split Horizon	161
Troubleshooting Miscellaneous EIGRP for IPv4 Issues	162
Feasible Successors	162
Discontiguous Networks and Autosummarization	165
Route Summarization	167
Load Balancing	168
EIGRP for IPv4 Trouble Tickets	169
Trouble Ticket 4-1	169
Trouble Ticket 4-2	177
Trouble Ticket 4-3	180
Exam Preparation Tasks	184
Review All Key Topics	184
Define Key Terms	185
Use the Command Reference to Check Your Memory	185

## **Chapter 5 EIGRPv6 188**

“Do I Know This Already?” Quiz	188
Foundation Topics	191
EIGRPv6 Fundamentals	191
EIGRPv6 Inter-Router Communication	191
EIGRPv6 Configuration	191
<i>EIGRPv6 Classic Mode Configuration</i>	191

	<i>EIGRPv6 Named Mode Configuration</i>	192
	<i>EIGRPv6 Verification</i>	193
	IPv6 Route Summarization	195
	Default Route Advertising	196
	Route Filtering	197
	Troubleshooting EIGRPv6 Neighbor Issues	197
	Interface Is Down	198
	Mismatched Autonomous System Numbers	198
	Mismatched K Values	198
	Passive Interfaces	198
	Mismatched Authentication	199
	Timers	200
	Interface Not Participating in Routing Process	200
	ACLs	201
	Troubleshooting EIGRPv6 Routes	201
	Interface Not Participating in the Routing Process	201
	Better Source of Information	201
	Route Filtering	201
	Stub Configuration	202
	Split Horizon	203
	Troubleshooting Named EIGRP	204
	EIGRPv6 and Named EIGRP Trouble Tickets	209
	Trouble Ticket 5-1	209
	Trouble Ticket 5-2	213
	Exam Preparation Tasks	218
	Review All Key Topics	218
	Define Key Terms	219
	Use the Command Reference to Check Your Memory	219
<b>Chapter 6</b>	<b>OSPF</b>	<b>222</b>
	“Do I Know This Already?” Quiz	222
	Foundation Topics	225
	OSPF Fundamentals	225
	Areas	226
	Inter-Router Communication	228
	Router ID	229
	OSPF Hello Packets	229

Neighbors	230
Requirements for Neighbor Adjacency	230
OSPF Configuration	232
OSPF Network Statement	232
Interface-Specific Configuration	233
Passive Interfaces	233
Sample Topology and Configuration	233
Confirmation of Interfaces	235
Verification of OSPF Neighbor Adjacencies	237
Viewing OSPF Installed Routes	238
External OSPF Routes	240
Default Route Advertisement	241
The Designated Router and Backup Designated Router	242
Designated Router Elections	244
DR and BDR Placement	245
OSPF Network Types	246
Broadcast	247
Nonbroadcast	247
Point-to-Point Networks	248
Point-to-Multipoint Networks	249
Loopback Networks	253
Failure Detection	254
Hello Timer	255
Dead Interval Timer	255
Verifying OSPF Timers	255
Authentication	255
References in This Chapter	257
Exam Preparation Tasks	258
Review All Key Topics	258
Define Key Terms	258
Use the Command Reference to Check Your Memory	258
<b>Chapter 7 Advanced OSPF</b>	<b>260</b>
“Do I Know This Already?” Quiz	260
Foundation Topics	262
Link-State Advertisements	262
LSA Sequences	264

LSA Age and Flooding	264
LSA Types	264
<i>LSA Type 1: Router Link</i>	264
<i>LSA Type 2: Network Link</i>	269
<i>LSA Type 3: Summary Link</i>	271
<i>LSA Type 5: External Routes</i>	277
<i>LSA Type 4: ASBR Summary</i>	279
<i>LSA Type 7: NSSA External Summary</i>	281
<i>LSA Type Summary</i>	283
OSPF Stubby Areas	284
Stub Areas	284
Totally Stubby Areas	287
Not-So-Stubby Areas	289
Totally NSSAs	292
OSPF Path Selection	294
Link Costs	295
Intra-area Routes	295
Inter-area Routes	296
External Route Selection	297
E1 and N1 External Routes	297
E2 and N2 External Routes	297
Equal-Cost Multipathing	298
Summarization of Routes	298
Summarization Fundamentals	299
Inter-area Summarization	301
Configuration of Inter-area Summarization	301
External Summarization	303
Discontiguous Network	305
Virtual Links	307
References in This Chapter	310
Exam Preparation Tasks	310
Review All Key Topics	310
Define Key Terms	311
Use the Command Reference to Check Your Memory	311
<b>Chapter 8 Troubleshooting OSPFv2</b>	<b>314</b>
“Do I Know This Already?” Quiz	314
Foundation Topics	317

Troubleshooting OSPFv2 Neighbor Adjacencies	317
Interface Is Down	319
Interface Not Running the OSPF Process	319
Mismatched Timers	321
Mismatched Area Numbers	322
Mismatched Area Type	323
Different Subnets	324
Passive Interface	325
Mismatched Authentication Information	326
ACLs	327
MTU Mismatch	328
Duplicate Router IDs	330
Mismatched Network Types	330
Troubleshooting OSPFv2 Routes	332
Interface Not Running the OSPF Process	333
Better Source of Information	334
Route Filtering	337
Stub Area Configuration	339
Interface Is Shut Down	341
Wrong Designated Router Elected	341
Duplicate Router IDs	344
Troubleshooting Miscellaneous OSPFv2 Issues	346
Tracking OSPF Advertisements Through a Network	346
Route Summarization	348
Discontiguous Areas	350
Load Balancing	352
Default Route	353
OSPFv2 Trouble Tickets	353
Trouble Ticket 8-1	353
Trouble Ticket 8-2	361
Trouble Ticket 8-3	364
Exam Preparation Tasks	366
Review All Key Topics	366
Define Key Terms	367
Use the Command Reference to Check Your Memory	367

<b>Chapter 9</b>	<b>OSPFv3</b>	<b>370</b>
	“Do I Know This Already?” Quiz	370
	Foundation Topics	371
	OSPFv3 Fundamentals	371
	OSPFv3 Link-State Advertisement	372
	OSPFv3 Communication	373
	OSPFv3 Configuration	374
	OSPFv3 Verification	377
	The Passive Interface	378
	IPv6 Route Summarization	379
	Network Type	380
	OSPFv3 Authentication	381
	OSPFv3 Link-Local Forwarding	383
	OSPFv3 LSA Flooding Scope	384
	References in This Chapter	390
	Exam Preparation Tasks	390
	Review All Key Topics	390
	Define Key Terms	391
	Use the Command Reference to Check Your Memory	391
<b>Chapter 10</b>	<b>Troubleshooting OSPFv3</b>	<b>392</b>
	“Do I Know This Already?” Quiz	392
	Foundation Topics	394
	Troubleshooting OSPFv3 for IPv6	394
	OSPFv3 Troubleshooting Commands	395
	OSPFv3 Trouble Tickets	401
	Trouble Ticket 10-1	401
	Trouble Ticket 10-2	404
	Troubleshooting OSPFv3 Address Families	408
	OSPFv3 AF Trouble Ticket	418
	Trouble Ticket 10-3	419
	Exam Preparation Tasks	423
	Review All Key Topics	423
	Define Key Terms	424
	Use the Command Reference to Check Your Memory	424
<b>Chapter 11</b>	<b>BGP</b>	<b>426</b>
	“Do I Know This Already?” Quiz	426
	Foundation Topics	428

BGP Fundamentals	428
Autonomous System Numbers (ASNs)	428
BGP Sessions	429
Path Attributes	429
Loop Prevention	430
Address Families	430
Inter-Router Communication	430
<i>BGP Messages</i>	431
<i>BGP Neighbor States</i>	432
Basic BGP Configuration	435
Verification of BGP Sessions	437
Route Advertisement	440
Receiving and Viewing Routes	443
Understanding BGP Session Types and Behaviors	448
iBGP	448
<i>iBGP Full Mesh Requirement</i>	450
<i>Peering Using Loopback Addresses</i>	451
eBGP	453
eBGP and iBGP Topologies	454
Next-Hop Manipulation	456
iBGP Scalability Enhancements	457
<i>Route Reflectors</i>	457
<i>Confederations</i>	462
Multiprotocol BGP for IPv6	465
IPv6 Configuration	466
IPv6 over IPv4	471
References in This Chapter	475
Exam Preparation Tasks	476
Review All Key Topics	476
Define Key Terms	477
Use the Command Reference to Check Your Memory	477
<b>Chapter 12 Advanced BGP</b>	<b>480</b>
“Do I Know This Already?” Quiz	480
Foundation Topics	482
Route Summarization	482
Aggregate Addresses	482
The Atomic Aggregate Attribute	488

Route Aggregation with AS_SET	489
IPv6 Summarization	492
BGP Route Filtering and Manipulation	493
Distribute List Filtering	495
Prefix List Filtering	496
AS_Path Filtering	497
<i>Regular Expressions (Regex)</i>	497
<i>AS_Path ACLs</i>	503
Route Maps	505
Clearing BGP Connections	507
BGP Communities	507
Enabling BGP Community Support	508
Well-Known Communities	508
<i>The No_Advertise BGP Community</i>	509
<i>The No_Export BGP Community</i>	510
<i>The Local AS (No_Export_SubConfed) BGP Community</i>	511
Conditionally Matching BGP Communities	512
Setting Private BGP Communities	514
Maximum Prefix	516
Configuration Scalability	517
IOS XE Peer Groups	517
IOS XE Peer Templates	518
References in This Chapter	519
Exam Preparation Tasks	520
Review All Key Topics	520
Define Key Terms	520
Use the Command Reference to Check Your Memory	521
<b>Chapter 13 BGP Path Selection</b>	<b>524</b>
“Do I Know This Already?” Quiz	524
Foundation Topics	526
Understanding BGP Path Selection	526
BGP Best Path	527
Weight	528
Local Preference	532
<i>Phase I: Initial BGP Edge Route Processing</i>	535
<i>Phase II: BGP Edge Evaluation of Multiple Paths</i>	536
<i>Phase III: Final BGP Processing State</i>	538

Locally Originated in the Network or Aggregate Advertisement	538
Accumulated Interior Gateway Protocol (AIGP)	539
Shortest AS_Path	540
Origin Type	542
Multi-Exit Discriminator	545
<i>Missing MED Behavior</i>	548
<i>Always Compare MED</i>	549
<i>BGP Deterministic MED</i>	549
eBGP over iBGP	550
Lowest IGP Metric	551
Prefer the Oldest EBGP Session	551
Router ID	551
Minimum Cluster List Length	552
Lowest Neighbor Address	552
BGP Multipath	553
Exam Preparation Tasks	554
Review All Key Topics	554
Define Key Terms	554
Use the Command Reference to Check Your Memory	554

## **Chapter 14 Troubleshooting BGP 556**

“Do I Know This Already?” Quiz	557
Foundation Topics	559
Troubleshooting BGP Neighbor Adjacencies	559
Interface Is Down	561
Layer 3 Connectivity Is Broken	561
Path to the Neighbor Is Through the Default Route	562
Neighbor Does Not Have a Route to the Local Router	563
Incorrect neighbor Statement	564
BGP Packets Sourced from the Wrong IP Address	564
ACLs	566
The TTL of the BGP Packet Expires	568
Mismatched Authentication	570
Misconfigured Peer Groups	570
Timers	572
Troubleshooting BGP Routes	573

Missing or Bad network mask Command	575
Next-Hop Router Not Reachable	577
BGP Split-Horizon Rule	579
Better Source of Information	580
Route Filtering	582
Troubleshooting BGP Path Selection	588
Understanding the Best-Path Decision-Making Process	588
Private Autonomous System Numbers	591
Using debug Commands	592
Troubleshooting BGP for IPv6	593
BGP Trouble Tickets	598
Trouble Ticket 14-1	598
Trouble Ticket 14-2	604
Trouble Ticket 14-3	610
MP-BGP Trouble Ticket	614
Trouble Ticket 14-4	615
Exam Preparation Tasks	617
Review All Key Topics	617
Define Key Terms	618
Use the Command Reference to Check Your Memory	618
<b>Chapter 15 Route Maps and Conditional Forwarding</b>	<b>620</b>
“Do I Know This Already?” Quiz	620
Foundation Topics	622
Conditional Matching	622
Access Control Lists (ACLs)	622
<i>Standard ACLs</i>	622
<i>Extended ACLs</i>	623
<i>Prefix Matching</i>	624
<i>Prefix Lists</i>	626
<i>IPv6 Prefix Lists</i>	627
Route Maps	627
Conditional Matching	629
Complex Matching	630
Optional Actions	631
Continue	631
Conditional Forwarding of Packets	632

PBR Configuration	633
Local PBR	635
Trouble Tickets	637
Trouble Ticket 15-1	638
Trouble Ticket 15-2	641
Trouble Ticket 15-3	643
Exam Preparation Tasks	645
Review All Key Topics	646
Define Key Terms	646
Use the Command Reference to Check Your Memory	646

## **Chapter 16 Route Redistribution 648**

“Do I Know This Already?” Quiz	648
Foundation Topics	650
Redistribution Overview	650
Redistribution Is Not Transitive	651
Sequential Protocol Redistribution	653
Routes Must Exist in the RIB	653
Seed Metrics	655
Protocol-Specific Configuration	656
Source-Specific Behaviors	657
<i>Connected Networks</i>	657
<i>BGP</i>	657
Destination-Specific Behaviors	658
<i>EIGRP</i>	658
<i>EIGRP-to-EIGRP Redistribution</i>	661
<i>OSPF</i>	663
<i>OSPF-to-OSPF Redistribution</i>	666
<i>OSPF Forwarding Address</i>	667
<i>BGP</i>	670
Reference in This Chapter	672
Exam Preparation Tasks	672
Review All Key Topics	672
Define Key Terms	673
Use the Command Reference to Check Your Memory	673

<b>Chapter 17</b>	<b>Troubleshooting Redistribution</b>	<b>674</b>
	“Do I Know This Already?” Quiz	674
	Foundation Topics	677
	Troubleshooting Advanced Redistribution Issues	677
	Troubleshooting Suboptimal Routing Caused by Redistribution	678
	Troubleshooting Routing Loops Caused by Redistribution	679
	Troubleshooting IPv4 and IPv6 Redistribution	687
	Route Redistribution Review	687
	Troubleshooting Redistribution into EIGRP	689
	Troubleshooting Redistribution into OSPF	694
	Troubleshooting Redistribution into BGP	699
	Troubleshooting Redistribution with Route Maps	702
	Redistribution Trouble Tickets	702
	Trouble Ticket 17-1	703
	Trouble Ticket 17-2	708
	Trouble Ticket 17-3	711
	Trouble Ticket 17-4	717
	Exam Preparation Tasks	721
	Review All Key Topics	722
	Define Key Terms	722
	Command Reference to Check Your Memory	723
<b>Chapter 18</b>	<b>VRF, MPLS, and MPLS Layer 3 VPNs</b>	<b>724</b>
	“Do I Know This Already?” Quiz	724
	Foundation Topics	727
	Implementing and Verifying VRF-Lite	727
	VRF-Lite Overview	728
	Creating and Verifying VRF Instances	728
	An Introduction to MPLS Operations	747
	MPLS LIB and LFIB	748
	Label Switching Routers	748
	Forwarding Equivalence Class (FEC)	749
	Label-Switched Path	749
	Labels	750
	Label Distribution Protocol	751
	Label Switching	752

Penultimate-Hop Popping	753
MPLS LDP Features	754
MPLS Traffic Engineering	755
An Introduction to MPLS Layer 3 VPNs	755
MPLS Layer 3 VPNs	756
MPLS Layer 3 VPNv4 Addresses, RDs, and RTs	757
MPLS Layer 3 VPN Label Stack	759
Reference in This Chapter	762
Exam Preparation Tasks	762
Review All Key Topics	762
Define Key Terms	763
Use the Command Reference to Check Your Memory	763

## **Chapter 19 DMVPN Tunnels 766**

“Do I Know This Already?” Quiz	766
Foundation Topics	769
Generic Routing Encapsulation (GRE) Tunnels	769
GRE Tunnel Configuration	769
GRE Sample Configuration	771
Next Hop Resolution Protocol (NHRP)	774
Dynamic Multipoint VPN (DMVPN)	776
Phase 1: Spoke-to-Hub	777
Phase 2: Spoke-to-Spoke	777
Phase 3: Hierarchical Tree Spoke-to-Spoke	777
DMVPN Phase Comparison	777
DMVPN Configuration	779
DMVPN Hub Configuration	780
DMVPN Spoke Configuration for DMVPN Phase 1 (Point-to-Point)	782
Viewing DMVPN Tunnel Status	784
Viewing the NHRP Cache	787
DMVPN Configuration for Phase 3 DMVPN (Multipoint)	792
IP NHRP Authentication	794
Unique IP NHRP Registration	794
Spoke-to-Spoke Communication	795
Forming Spoke-to-Spoke Tunnels	796
NHRP Routing Table Manipulation	800
NHRP Routing Table Manipulation with Summarization	802

Problems with Overlay Networks	806
Recursive Routing Problems	806
Outbound Interface Selection	808
Front Door Virtual Routing and Forwarding (FVRF)	808
<i>Configuring Front Door VRF (FVRF)</i>	809
<i>FVRF Static Routes</i>	810
DMVPN Failure Detection and High Availability	810
DMVPN Hub Redundancy	811
IPv6 DMVPN Configuration	811
IPv6-over-IPv6 Sample Configuration	813
IPv6 DMVPN Verification	816
References in This Chapter	817
Exam Preparation Tasks	817
Review All Key Topics	817
Define Key Terms	818
Use the Command Reference to Check Your Memory	818
<b>Chapter 20 Securing DMVPN Tunnels</b>	<b>820</b>
“Do I Know This Already?” Quiz	820
Foundation Topics	821
Elements of Secure Transport	821
IPsec Fundamentals	823
Security Protocols	824
<i>Authentication Header</i>	824
<i>Encapsulating Security Payload (ESP)</i>	824
Key Management	825
Security Associations	825
ESP Modes	825
<i>DMVPN Without IPsec</i>	826
<i>DMVPN with IPsec in Transport Mode</i>	826
<i>DMVPN with IPsec in Tunnel Mode</i>	827
IPsec Tunnel Protection	827
Pre-Shared Key Authentication	827
<i>IKEv2 Keyring</i>	828
<i>IKEv2 Profile</i>	829
<i>IPsec Transform Set</i>	831
<i>IPsec Profile</i>	832
<i>Encrypting the Tunnel Interface</i>	833

*IPsec Packet Replay Protection* 833

*Dead Peer Detection* 834

*NAT Keepalives* 834

*Complete IPsec DMVPN Configuration with Pre-Shared Authentication* 835

Verifying Encryption on DMVPN Tunnels 836

IKEv2 Protection 838

References in This Chapter 839

Exam Preparation Tasks 840

Review All Key Topics 840

Define Key Terms 840

Use the Command Reference to Check Your Memory 840

## **Chapter 21 Troubleshooting ACLs and Prefix Lists 842**

“Do I Know This Already?” Quiz 842

Foundation Topics 845

Troubleshooting IPv4 ACLs 845

Reading an IPv4 ACL 846

Using an IPv4 ACL for Filtering 848

Using a Time-Based IPv4 ACL 848

Troubleshooting IPv6 ACLs 850

Reading an IPv6 ACL 850

Using an IPv6 ACL for Filtering 851

Troubleshooting Prefix Lists 852

Reading a Prefix List 853

Prefix List Processing 854

Trouble Tickets 855

Trouble Ticket 21-1: IPv4 ACL Trouble Ticket 855

Trouble Ticket 21-2: IPv6 ACL Trouble Ticket 858

Trouble Ticket 21-3: Prefix List Trouble Ticket 861

Exam Preparation Tasks 863

Review All Key Topics 863

Define Key Terms 864

Use the Command Reference to Check Your Memory 864

## **Chapter 22 Infrastructure Security 866**

“Do I Know This Already?” Quiz 866

Foundation Topics 869

Cisco IOS AAA Troubleshooting	869
Troubleshooting Unicast Reverse Path Forwarding (uRPF)	874
Troubleshooting Control Plane Policing (CoPP)	875
Creating ACLs to Identify the Traffic	876
Creating Class Maps to Define a Traffic Class	878
Creating Policy Maps to Define a Service Policy	880
Applying the Service Policy to the Control Plane	883
CoPP Summary	885
IPv6 First-Hop Security	885
Binding Table	885
IPv6 Snooping	886
Router Advertisement (RA) Guard	886
DHCPv6 Guard	886
Source Guard	887
Destination Guard	887
Prefix Guard	887
Exam Preparation Tasks	887
Review All Key Topics	887
Define Key Terms	888
Use the Command Reference to Check Your Memory	888
Use the IPv6 Features Table to Check Your Memory	889

## **Chapter 23 Device Management and Management Tools Troubleshooting 890**

“Do I Know This Already?” Quiz	890
Foundation Topics	893
Device Management Troubleshooting	893
Console Access Troubleshooting	893
vty Access Troubleshooting	894
<i>Telnet</i>	895
<i>SSH</i>	897
<i>Password Encryption Levels</i>	898
Remote Transfer Troubleshooting	899
<i>TFTP</i>	899
<i>HTTP(S)</i>	900
<i>FTP</i>	901
<i>SCP</i>	902

Management Tools Troubleshooting	903
Syslog Troubleshooting	904
SNMP Troubleshooting	906
Cisco IOS IP SLA Troubleshooting	910
Object Tracking Troubleshooting	917
NetFlow and Flexible NetFlow Troubleshooting	919
Bidirectional Forwarding Detection (BFD)	927
Cisco DNA Center Assurance	929
Exam Preparation Tasks	939
Review All Key Topics	939
Define Key Terms	940
Use the Command Reference to Check Your Memory	940

## **Chapter 24 Final Preparation 944**

Advice About the Exam Event	944
Think About Your Time Budget Versus Numbers of Questions	944
A Suggested Time-Check Method	945
Miscellaneous Pre-Exam Suggestions	946
Exam-Day Advice	946
Reserve the Hour After the Exam in Case You Fail	947
Take Practice Exams	948
<i>Advice on How to Answer Exam Questions</i>	949
Assessing Whether You Are Ready to Pass (and the Fallacy of Exam Scores)	950
Study Suggestions After Failing to Pass	951
Other Study Tasks	952
Final Thoughts	953

## **Chapter 25 ENARSI 300-410 Exam Updates 954**

The Purpose of This Chapter	954
About Possible Exam Updates	954
Impact on You and Your Study Plan	955
News About the Next Exam Release	956
Updated Technical Content	956

**Appendix A** Answers to the “Do I Know This Already?” Quiz Questions 958

**Glossary** 972

**Index** 990

**Online Elements**

**Appendix B** Command Reference Exercises

**Appendix C** Command Reference Exercises Answer Key

**Appendix D** Study Planner

## Icons Used in This Book



ASA  
Firewall



LAN  
Segment



Serial



Switched  
Circuit



Radio  
Tower



Routing  
Domain



Router



Workgroup Switch  
Color/Subdued



Web Server



Workstation  
(Sun)



Optical Cross-  
Connect



File/Application  
Server

## 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

Congratulations! If you are reading this Introduction, then you have probably decided to obtain your Cisco CCNP Enterprise certification. Obtaining a Cisco certification will ensure that you have a solid understanding of common industry protocols along with Cisco's device architecture and configuration. Cisco has a high market share of routers and switches, with a global footprint.

Professional certifications have been an important part of the computing industry for many years and will continue to become more important. Many reasons exist for these certifications, but the most popularly cited reason is credibility. All other considerations held equal, a certified employee/consultant/job candidate is considered more valuable than one who is not certified.

Cisco provides three primary levels of certifications: Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP), and Cisco Certified Internetwork Expert (CCIE). Cisco announced changes to all three levels of certification in February 2020 and those changes still apply to the most recent exam updates. The announcement included many changes, but these are the most notable:

- The exams now include additional topics, such as programming.
- The CCNA certification is not a prerequisite for obtaining the CCNP certification. CCNA specializations are not offered anymore.
- The exams test a candidate's ability to configure and troubleshoot network devices as well as to answer multiple-choice questions.
- The CCNP is obtained by taking and passing a Core exam and a Concentration exam, such as the Implementing Cisco Enterprise Advanced Routing and Services (ENARSI).

So, if you are a CCNP Enterprise candidate you need to take and pass the CCNP and CCIE Enterprise Core ENCOR v1.1 350-401 examination. Then you need to take and pass one of the following Concentration exams to obtain your CCNP Enterprise:

- 300-410 ENARSI to obtain Implementing Cisco Enterprise Advanced Routing and Services
- 300-415 ENSDWI to obtain Implementing Cisco SD-WAN Solutions
- 300-420 ENSLD to obtain Designing Cisco Enterprise Networks
- 300-425 ENWLSD to obtain Designing Cisco Enterprise Wireless Networks
- 300-430 ENWLSI to obtain Implementing Cisco Enterprise Wireless Networks
- 300-435 ENAUTO to obtain Automating Cisco Enterprise Solutions
- 300-440 ENCC to obtain Designing and Implementing Cloud Connectivity

## Goals and Methods

The most important and somewhat obvious goal of this book is to help you pass the CCNP Implementing Cisco Enterprise Advanced Routing and Services (ENARSI) 300-410 exam. In fact, if the primary objective of this book were different, then the book's title would be misleading; however, the methods used in this book to help you pass the exam are designed to also make you much more knowledgeable about how to do your job.

One key methodology used in this book is to help you discover the exam topics that you need to review in more depth, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. This book does not try to help you pass by memorization but helps you truly learn and understand the topics. The ENARSI 300-410 exam covers foundation topics in the CCNP certification, and the knowledge contained within is vitally important for a truly skilled routing/switching engineer or specialist. This book would do you a disservice if it didn't attempt to help you learn the material. To that end, the book will help you pass the exam by:

- Helping you discover which test topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises and scenarios that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the companion website

## Who Should Read This Book?

This book is not designed to be a general networking topics book, although it can be used for that purpose. This book is intended to tremendously increase your chances of passing the ENARSI 300-410 exam. Although other objectives can be achieved from using this book, the book is written with one goal in mind: to help you pass the exam.

So why should you want to pass the ENARSI 300-410 exam? Because it's one of the milestones toward getting the CCNP Enterprise certification, which is no small feat. What would getting the CCNP Enterprise certification mean to you? A raise, a promotion, recognition? How about enhancing your resume? Demonstrating that you are serious about continuing the learning process and that you're not content to rest on your laurels? Pleasing your reseller-employer, who needs more certified employees for a higher discount from Cisco? You might have one of these reasons for getting the CCNP Enterprise certification or one of many others.

## Strategies for Exam Preparation

The strategy you use for taking the ENARSI 300-410 exam might be slightly different from strategies used by other readers, depending on the skills, knowledge, and experience you have already obtained. For instance, if you have attended the CCNP

Implementing Cisco Enterprise Advanced Routing and Services (ENARSI) 300-410 course, you might take a different approach than someone who has learned routing through on-the-job training.

Regardless of the strategy you use or the background you have, this book is designed to help you get to the point where you can pass the exam with the least amount of time required. For instance, there is no need for you to practice or read about IP addressing and subnetting if you fully understand it already. However, many people like to make sure that they truly know a topic and thus read over material that they already know. Several book features will help you gain the confidence you need to be convinced that you know some material already and to also help you know what topics you need to study more.

## The Companion Website for Online Content Review

All the electronic review elements, as well as other electronic components of the book, exist on this book's companion website.

### 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](http://www.ciscopress.com) and registering your book. To do so, simply go to [ciscopress.com/register](http://ciscopress.com/register) and enter the ISBN of the print book: 9780138217525. 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:

- You can get your access code by registering the print ISBN (9780138217525) on [ciscopress.com/register](http://ciscopress.com/register). Make sure to use the print book ISBN regardless of whether you purchased an eBook or the print book. Once you register the book, your access code will be populated on your account page under the Registered Products tab. Instructions for how to redeem the code are available on the book's companion website by clicking the Access Bonus Content link.
- 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 [ciscopress.com](http://ciscopress.com) click Account to see details of your account, and click the digital purchases tab.

**NOTE** After you register your book, your code can always be found in your account under the Registered Products tab.

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 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 [pearsonstestprep.com](http://pearsonstestprep.com), log in using the same credentials used to register your book or purchase the Premium Edition, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

## How This Book Is Organized

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

The chapters cover the following topics:

- **Chapter 1, "IPv4/IPv6 Addressing and Routing Review":** This chapter provides a review of IPv4 and IPv6 addressing, DHCP, and routing, as well as details about how to troubleshoot these topics.
- **Chapter 2, "EIGRP":** This chapter explains the underlying mechanics of the EIGRP routing protocol, the path metric calculations, and how to configure EIGRP.
- **Chapter 3, "Advanced EIGRP":** This chapter explains a variety of advanced concepts, such as failure detection, network summarization, router filtering, and techniques to optimize WAN sites.
- **Chapter 4, "Troubleshooting EIGRP for IPv4":** This chapter focuses on how to troubleshoot EIGRP neighbor adjacency issues as well as EIGRP route issues.
- **Chapter 5, "EIGRPv6":** This chapter explains how EIGRP advertises IPv6 networks and guides you through configuring, verifying, and troubleshooting EIGRPv6.
- **Chapter 6, "OSPF":** This chapter explains the core concepts of OSPF, the exchange of routes, OSPF network types, failure detection, and OSPF authentication.
- **Chapter 7, "Advanced OSPF":** This chapter expands on Chapter 6 by explaining the OSPF database and how it builds the topology. It also explains OSPF path selection, router summarization, and techniques to optimize an OSPF environment.

- **Chapter 8, “Troubleshooting OSPFv2”:** This chapter explores how to troubleshoot OSPFv2 neighbor adjacency issues as well as route issues.
- **Chapter 9, “OSPFv3”:** This chapter explains how the OSPF protocol has changed to accommodate support of the IPv6 protocol.
- **Chapter 10, “Troubleshooting OSPFv3”:** This chapter explains how to troubleshoot issues that may arise with OSPFv3.
- **Chapter 11, “BGP”:** This chapter explains the core concepts of BGP, its path attributes, and configuration for IPv4 and IPv6 network prefixes.
- **Chapter 12, “Advanced BGP”:** This chapter expands on Chapter 11 by explaining BGP communities and configuration techniques for routers with lots of BGP peerings.
- **Chapter 13, “BGP Path Selection”:** This chapter explains the BGP path selection process, how BGP identifies the best BGP path, and methods for load balancing across equal paths.
- **Chapter 14, “Troubleshooting BGP”:** This chapter explores how you can identify and troubleshoot issues related to BGP neighbor adjacencies, BGP routes, and BGP path selection. It also covers MP-BGP (BGP for IPv6).
- **Chapter 15, “Route Maps and Conditional Forwarding”:** This chapter explains route maps, concepts for selecting a network prefix, and how packets can be conditionally forwarded out different interfaces for certain network traffic.
- **Chapter 16, “Route Redistribution”:** This chapter explains the rules of redistribution, configuration for route redistribution, and behaviors of redistribution based on the source or destination routing protocol.
- **Chapter 17, “Troubleshooting Redistribution”:** This chapter focuses on how to troubleshoot issues related to redistribution, including configuration issues, suboptimal routing issues, and routing loop issues.
- **Chapter 18, “VRF, MPLS, and MPLS Layer 3 VPNs”:** This chapter explores how to configure and verify VRF and introduces MPLS operations and MPLS Layer 3 VPNs.
- **Chapter 19, “DMVPN Tunnels”:** This chapter covers GRE tunnels, NHRP, DMVPN, and techniques to optimize a DMVPN deployment.
- **Chapter 20, “Securing DMVPN Tunnels”:** This chapter explains the importance of securing network traffic on the WAN and techniques for deploying IPsec tunnel protection for DMVPN tunnels.
- **Chapter 21, “Troubleshooting ACLs and Prefix Lists”:** This chapter shows how to troubleshoot issues related to IPv4 and IPv6 access control lists and prefix lists.
- **Chapter 22, “Infrastructure Security”:** This chapter covers how to troubleshoot AAA issues, uRPF issues, and CoPP issues. In addition, it introduces various IPv6 first-hop security features.

- **Chapter 23, “Device Management and Management Tools Troubleshooting”:** This chapter explores how to troubleshoot issues that you might experience with local or remote access, remote transfers, syslog, SNMP, IP SLA, Object Tracking, NetFlow, and Flexible NetFlow. In addition, it introduces the troubleshooting options available with Cisco DNA Center Assurance.
- **Chapter 24, “Final Preparation”:** This chapter provides tips and strategies for studying for the ENARSI 300-410 exam.
- **Chapter 25, “ENARSI 300-410 Exam Updates”:** This chapter provides information about how book updates will be handled if and when Cisco decides to make changes to the ENARSI 300-410 exam.

## Certification Exam Topics and This Book

The questions for each certification exam are a closely guarded secret. However, we do know which topics you must know to *successfully* complete the ENARSI 300-410 v1.1 exam. Cisco publishes them as an exam blueprint. Table I-1 lists the exam topics from the blueprint along with references to the book chapters that cover each topic. These are the same topics you should be proficient in when working with enterprise technologies in the real world.

**Table I-1** Enterprise Core Topics and Chapter References

Implementing Cisco Enterprise Advanced Routing (ENARSI) (300-410) Exam Topic	Chapter(s) in Which Topic Is Covered
<b>1.0 Layer 3 Technologies</b>	
1.1 Troubleshoot administrative distance (all routing protocols)	1
1.2 Troubleshoot route map for any routing protocol (attributes, tagging, filtering)	17
1.3 Troubleshoot loop prevention mechanisms (filtering, tagging, split horizon, route poisoning)	17
1.4 Troubleshoot redistribution between any routing protocols or routing sources	16, 17
1.5 Troubleshoot manual and auto-summarization with any routing protocol	3, 4, 5, 7, 8, 9, 10, 12
1.6 Configure and verify policy-based routing	15
1.7 Configure and verify VRF-Lite	18
1.8 Describe Bidirectional Forwarding Detection	23
1.9 Troubleshoot EIGRP (classic and named mode; VRF and global)	4, 5
1.9.a Address families (IPv4, IPv6)	2, 3, 4, 5
1.9.b Neighbor relationship and authentication	2, 4, 5
1.9.c Loop-free path selections (RD, FD, FC, successor, feasible successor, stuck in active)	3, 4
1.9.d Stubs	4

<b>Implementing Cisco Enterprise Advanced Routing (ENARSI) (300-410) Exam Topic</b>	<b>Chapter(s) in Which Topic Is Covered</b>
1.9.e Load balancing (equal and unequal cost)	2
1.9.f Metrics	2
1.10 Troubleshoot OSPF (v2/v3)	6, 7, 8, 9, 10
1.10.a Address families (IPv4, IPv6)	8, 10
1.10.b Neighbor relationship and authentication	6, 8, 10
1.10.c Network types, area types, and router types	8, 10
1.10.c (i) Point-to-point, multipoint, broadcast, nonbroadcast	6, 8, 10
1.10.c (ii) Area type: backbone, normal, transit, stub, NSSA, totally stub	7, 8, 10
1.10.c (iii) Internal router, backbone router, ABR, ASBR	6, 8, 10
1.10.c (iv) Virtual link	7, 8
1.10.d Path preference	7
1.11 Troubleshoot BGP (Internal and External, unicast, and VRF-Lite)	11, 12, 13, 14
1.11.a Address families (IPv4, IPv6)	10, 14
1.11.b Neighbor relationship and authentication (next-hop, mulithop, 4-byte AS, private AS, route refresh, synchronization, operation, peer group, states and timers)	10, 14
1.11.c Path preference (attributes and best-path)	13, 14
1.11.d Route reflector (excluding multiple route reflectors, confederations, dynamic peer)	10
1.11.e Policies (inbound/outbound filtering, path manipulation)	11, 14
<b>2.0 VPN Technologies</b>	
2.1 Describe MPLS operations (LSR, LDP, label switching, LSP)	18
2.2 Describe MPLS Layer 3 VPN	18
2.3 Configure and verify DMVPN (single hub)	19, 20
2.3.a GRE/mGRE	19
2.3.b NHRP	19
2.3.c IPsec	20
2.3.d Dynamic neighbor	19
2.3.e Spoke-to-spoke	19
<b>3.0 Infrastructure Security</b>	
3.1 Troubleshoot device security using IOS AAA (TACACS+, RADIUS, local database)	22
3.2 Troubleshoot router security features	21,22
3.2.a IPv4 access control lists (standard, extended, time-based)	21
3.2.b IPv6 traffic filter	21
3.2.c Unicast reverse path forwarding (uRPF)	22

<b>Implementing Cisco Enterprise Advanced Routing (ENARSI) (300-410) Exam Topic</b>	<b>Chapter(s) in Which Topic Is Covered</b>
3.3 Troubleshoot control plane policing (CoPP) (Telnet, SSH, HTTP(S), SNMP, EIGRP, OSPF, BGP)	22
3.4 Describe IPv6 First Hop Security features (RA Guard, DHCP Guard, binding table, ND inspection/snooping, Source Guard)	22
<b>4.0 Infrastructure Services</b>	
4.1 Troubleshoot device management	23
4.1.a Console and VTY	23
4.1.b Telnet, HTTP, HTTPS, SSH, SCP	23
4.1.c (T)FTP	23
4.2 Troubleshoot SNMP (v2c, v3)	23
4.3 Troubleshoot network problems using logging (local, syslog, debugs, conditional debugs, timestamps)	23
4.4 Troubleshoot IPv4 and IPv6 DHCP (DHCP client, IOS DHCP server, DHCP relay, DHCP options)	1
4.5 Troubleshoot network performance issues using IP SLA (jitter, tracking objects, delay, connectivity)	23
4.6 Troubleshoot NetFlow (v5, v9, flexible NetFlow)	23
4.7 Troubleshoot network problems using Cisco DNA Center assurance (connectivity, monitoring, device health, network health)	23

Each version of the exam can have topics that emphasize different functions or features, and some topics can be rather broad and generalized. The goal of this book is to provide the most comprehensive coverage to ensure that you are well prepared for the exam. Although some chapters might not address specific exam topics, they provide a foundation that is necessary for a clear understanding of important topics.

It is also important to understand that this book is a “static” reference, whereas the exam topics are dynamic. Cisco can and does change the topics covered on certification exams often.

This exam guide should not be your only reference when preparing for the certification exam. You can find a wealth of information at Cisco.com that covers each topic in great detail. If you think that you need more detailed information on a specific topic, read the Cisco documentation that focuses on that topic.

Note that as technologies continue to evolve, Cisco reserves the right to change the exam topics without notice. Although you can refer to the list of exam topics in Table I-1, always check Cisco.com to verify the actual list of topics to ensure that you are prepared before taking the exam. You can view the current exam topics on any current Cisco certification exam by visiting <https://www.cisco.com/c/en/us/training-events/training-certifications/next-level-certifications.html>. In addition, you should keep up to date on future exam changes by using the Cisco Certification Road Map at <https://learningnetwork>.

[cisco.com/s/cisco-certification-roadmaps](http://cisco.com/s/cisco-certification-roadmaps). Also note that, if needed, Cisco Press might post additional preparatory content on the web page associated with this book: <http://www.ciscopress.com/title/9780138217525>. It's a good idea to check the website a couple weeks before taking your exam to be sure that you have up-to-date content.

## Learning in a Lab Environment

This book is an excellent self-study resource for learning the technologies. However, reading is not enough, and any network engineer can tell you that you must implement a technology to fully understand it. We encourage you to re-create the topologies and technologies and follow the examples in this book.

A variety of resources are available for practicing the concepts in this book. Look online for the following:

- Cisco VIRL (Virtual Internet Routing Lab) provides a scalable, extensible network design and simulation environment. For more information about VIRL, see <https://learningnetwork.cisco.com/s/virl>.
- Cisco dCloud provides a huge catalog of demos, training, and sandboxes for every Cisco architecture. It offers customizable environments and is free. For more information, see <https://dcloud.cisco.com>.
- Cisco Devnet provides many resources on programming and programmability, along with free labs. For more information, see <https://developer.cisco.com>.

*This page intentionally left blank*



## CHAPTER 2

# EIGRP

### This chapter covers the following topics:

- **EIGRP Fundamentals:** This section explains how EIGRP establishes a neighborhood with other routers and how routes are exchanged with other routers.
- **EIGRP Configuration Modes:** This section defines the two methods of configuring EIGRP with a baseline configuration.
- **Path Metric Calculation:** This section explains how EIGRP calculates the path metric to identify the best and alternate loop-free paths.

*Enhanced Interior Gateway Routing Protocol (EIGRP)* is an enhanced distance vector routing protocol commonly found in enterprise networks. EIGRP is a derivative of Interior Gateway Routing Protocol (IGRP) but includes support for variable-length subnet masking (VLSM) and metrics capable of supporting higher-speed interfaces. Initially, EIGRP was a Cisco proprietary protocol, but it was released to the Internet Engineering Task Force (IETF) through RFC 7868, which was ratified in May 2016.

This chapter explains the underlying mechanics of the EIGRP routing protocol and the path metric calculations, and it demonstrates how to configure EIGRP on a router. This is the first of several chapters in the book that discuss EIGRP:

- **Chapter 2, “EIGRP”:** This chapter describes the fundamental concepts of EIGRP.
- **Chapter 3, “Advanced EIGRP”:** This chapter describes EIGRP’s failure detection mechanisms and techniques to optimize the operations of the routing protocol. It also includes topics such as route filtering and traffic manipulation.
- **Chapter 4, “Troubleshooting EIGRP for IPv4”:** This chapter reviews common problems with the routing protocols and the methodology to troubleshoot EIGRP from an IPv4 perspective.
- **Chapter 5, “EIGRPv6”:** This chapter demonstrates how IPv4 EIGRP concepts carry over to IPv6 and the methods used to troubleshoot common problems.

## “Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the “Exam Preparation Tasks” section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 2-1 lists the major headings in this chapter and their corresponding “Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quiz Questions.”

**Table 2-1** “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
EIGRP Fundamentals	1–6
EIGRP Configuration Modes	7–9
Path Metric Calculation	10

**CAUTION** The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of self-assessment. Giving yourself credit for an answer that you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. EIGRP uses protocol number \_\_\_\_ for inter-router communication.
  - a. 87
  - b. 88
  - c. 89
  - d. 90
2. How many packet types does EIGRP use for inter-router communication?
  - a. Three
  - b. Four
  - c. Five
  - d. Six
  - e. Seven
3. Which of the following are not required to match in order to form an EIGRP adjacency?
  - a. Metric K values
  - b. Primary subnet
  - c. Hello and hold timers
  - d. Authentication parameters
4. What is an EIGRP successor?
  - a. The next-hop router for the path with the lowest path metric for a destination prefix
  - b. The path with the lowest metric for a destination prefix
  - c. The router selected to maintain the EIGRP adjacencies for a broadcast network
  - d. A route that satisfies the feasibility condition where the reported distance is less than the feasible distance

5. What attributes does the EIGRP topology table contain? (Choose all that apply.)
  - a. Destination network prefix
  - b. Hop count
  - c. Total path delay
  - d. Maximum path bandwidth
  - e. List of EIGRP neighbors
6. What destination addresses does EIGRP use when feasible? (Choose two.)
  - a. IP address 224.0.0.9
  - b. IP address 224.0.0.10
  - c. IP address 224.0.0.8
  - d. MAC address 01:00:5E:00:00:0A
  - e. MAC address 0C:15:C0:00:00:01
7. Which of the following techniques can be used to initialize the EIGRP process? (Choose two.)
  - a. Use the interface command **ip eigrp as-number ipv4 unicast**.
  - b. Use the global configuration command **router eigrp as-number**.
  - c. Use the global configuration command **router eigrp process-name**.
  - d. Use the interface command **router eigrp as-number**.
8. True or false: The EIGRP router ID (RID) must be configured for EIGRP to be able to establish neighborship.
  - a. True
  - b. False
9. True or false: When using MD5 authentication between EIGRP routers, the keychain sequence numbers used on the routers can be different, as long as the password is the same.
  - a. True
  - b. False
10. Which value can be modified on a router to manipulate the path taken by EIGRP but does not have an impact on other routing protocols, like OSPF?
  - a. Interface bandwidth
  - b. Interface MTU
  - c. Interface delay
  - d. Interface priority

## Foundation Topics

### EIGRP Fundamentals

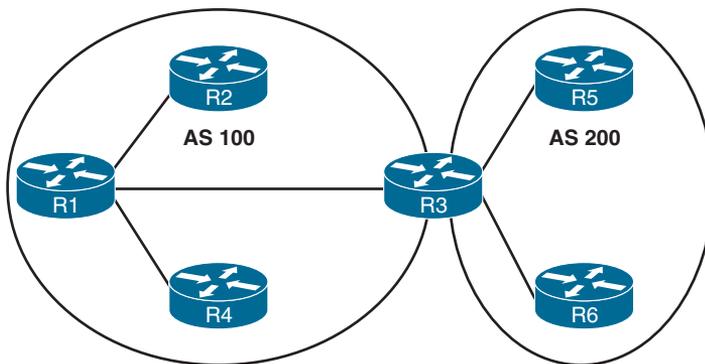
EIGRP overcomes the deficiencies of other distance vector routing protocols, such as Routing Information Protocol (RIP), with features such as unequal-cost load balancing, support for networks 255 hops away, and rapid convergence features. EIGRP uses a *diffusing update*

*algorithm (DUAL)* to identify network paths and provides for fast convergence using precalculated loop-free backup paths. Most distance vector routing protocols use hop count as the metric for routing decisions. However, a route-selection algorithm that uses only hop count for path selection does not take into account link speed and total delay. EIGRP adds logic to the route-selection algorithm to use factors other than hop count alone.

## Autonomous Systems

A router can run multiple EIGRP processes. Each process operates under the context of an autonomous system, which represents a common routing domain. Routers within the same domain use the same metric calculation formula and exchange routes only with members of the same *autonomous system (AS)*. Do not confuse an EIGRP autonomous system with a Border Gateway Protocol (BGP) autonomous system.

In Figure 2-1, EIGRP AS 100 consists of R1, R2, R3, and R4, and EIGRP AS 200 consists of R3, R5, and R6. Each EIGRP process correlates to a specific autonomous system and maintains an independent EIGRP topology table. R1 does not have knowledge of routes from AS 200 because it is different from its own autonomous system, AS 100. R3 is able to participate in both autonomous systems and, by default, does not transfer routes learned from one autonomous system into a different autonomous system.

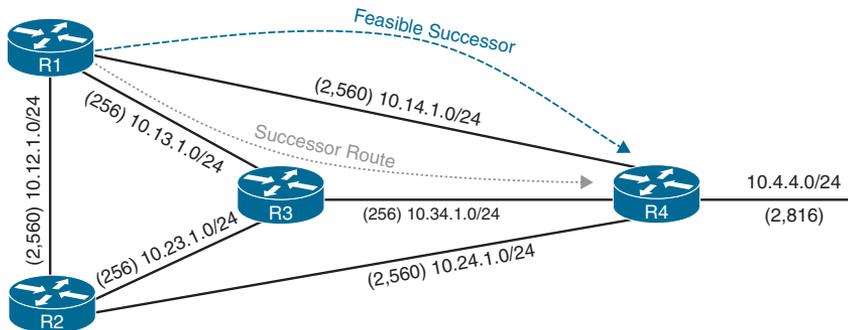


**Figure 2-1** EIGRP Autonomous Systems

EIGRP uses *protocol-dependent modules (PDMs)* to support multiple network protocols, such as IPv4, IPv6, AppleTalk, and IPX. EIGRP is written so that the PDM is responsible for the functions to handle the route selection criteria for each communication protocol. In theory, new PDMs can be written as new communication protocols are created. Current implementations of EIGRP support only IPv4 and IPv6.

## EIGRP Terminology

This section explains some of the core concepts of EIGRP, along with the path selection process. Figure 2-2 is a reference topology for this section, showing R1 calculating the best path and alternative loop-free paths to the 10.4.4.0/24 network. A value in parentheses represents the link's calculated metric for a segment based on bandwidth and delay.



**Figure 2-2** EIGRP Reference Topology

Table 2-2 defines important terms related to EIGRP and correlates them to Figure 2-2.

**Key Topic**

**Table 2-2** EIGRP Terminology

Term	Definition
<i>Successor route</i>	The route with the lowest path metric to reach a destination. The successor route for R1 to reach 10.4.4.0/24 on R4 is R1→R3→R4.
<i>Successor</i>	The first next-hop router for the successor route. R1's successor for 10.4.4.0/24 is R3.
<i>Feasible distance (FD)</i>	The metric value for the lowest path metric to reach a destination. The feasible distance is calculated locally using the formula shown in the "Path Metric Calculation" section, later in this chapter. The FD calculated by R1 for the 10.4.4.0/24 destination network is 3328 (that is, 256 + 256 + 2816).
<i>Reported distance (RD)</i>	Distance reported by a router to reach a destination. The reported distance value is the feasible distance for the advertising router. R3 advertises the 10.4.4.0/24 destination network to R1 and R2 with an RD of 3072. R4 advertises the 10.4.4.0/24 destination network to R1, R2, and R3 with an RD of 2816.
<i>Feasibility condition</i>	For a route to be considered a backup route, the RD received for that route must be less than the FD calculated locally. This logic guarantees a loop-free path.
<i>Feasible successor</i>	A route that satisfies the feasibility condition is maintained as a backup route. The feasibility condition ensures that the backup route is loop free. The route R1→R4 is the feasible successor because the RD of 2816 is lower than the FD of 3328 for the R1→R3→R4 path.

**Key Topic**

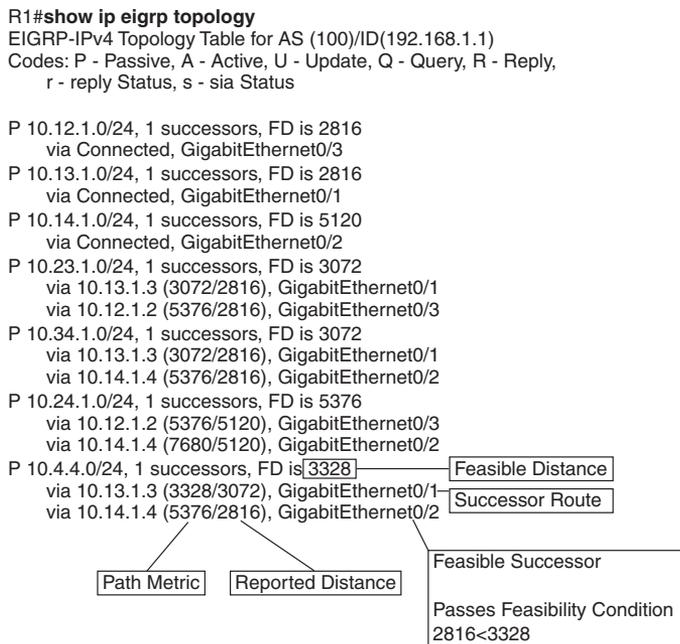
**Topology Table**

EIGRP contains a *topology table*, which makes it different from a true distance vector routing protocol. EIGRP's topology table is a vital component of DUAL and contains information to identify loop-free backup routes. The topology table contains all the network prefixes advertised within an EIGRP autonomous system. Each entry in the table contains the following:

- Network prefix
- EIGRP neighbors that have advertised that prefix
- Metrics from each neighbor (reported distance and hop count)
- Values used for calculating the metric (load, reliability, total delay, and minimum bandwidth)

The command **show ip eigrp topology [all-links]** provides the topology table. By default, only the successor and feasible successor routes are displayed, but the optional **all-links** keyword shows the paths that did not pass the feasibility condition.

Figure 2-3 shows the topology table for R1 from Figure 2-2. This section focuses on the 10.4.4.0/24 network when explaining the topology table.



**Figure 2-3** EIGRP Topology Output

Examine the 10.4.4.0/24 prefix and notice that R1 calculates an FD of 3328 for the successor route. The successor (upstream router) advertises the successor route with an RD of 3072. The second path entry has a metric of 5376 and has an RD of 2816. Because 2816 is less than 3328, the second entry passes the feasibility condition, which means the second entry is classified as the feasible successor for the 10.4.4.0/24 prefix.

The 10.4.4.0/24 route is passive (P), which means the topology is stable. During a topology change, routes go into an active (A) state when computing a new path.

## EIGRP Neighbors

Unlike a number of routing protocols—such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Intermediate System-to-Intermediate System (IS-IS)—EIGRP does not rely on periodic advertisement of all the network prefixes in an autonomous

system. EIGRP neighbors exchange the entire routing table when forming an adjacency, and they advertise incremental updates only as topology changes occur within a network. The neighbor adjacency table is vital for tracking neighbor status and the updates sent to each neighbor.

### Inter-Router Communication

EIGRP uses five different packet types to communicate with other routers, as shown in Table 2-3. EIGRP uses IP protocol number (88) and uses multicast packets where possible; it uses unicast packets when necessary. Communication between routers is done with multicast using the group address 224.0.0.10 or the MAC address 01:00:5e:00:00:0a when possible.

#### Key Topic

**Table 2-3** EIGRP Packet Types

Opcode Value	Packet Type	Function
1	Update	Used to transmit routing and reachability information with other EIGRP neighbors
2	Request	Used to get specific information from one or more neighbors
3	Query	Sent out to search for another path during convergence
4	Reply	Sent in response to a query packet
5	Hello	Used for discovery of EIGRP neighbors and for detecting when a neighbor is no longer available

**NOTE** EIGRP uses multicast packets to reduce bandwidth consumed on a link; that is, it uses one packet to reach multiple devices. While broadcast packets are used in the same general way, all nodes on a network segment process broadcast packets, whereas with multicast, only nodes listening for the particular multicast group process the multicast packets.

EIGRP uses *Reliable Transport Protocol (RTP)* to ensure that packets are delivered in order and to ensure that routers receive specific packets. A sequence number is included in each EIGRP packet. The sequence value zero does not require a response from the receiving EIGRP router; all other values require an ACK packet that includes the original sequence number.

Ensuring that packets are received makes the transport method reliable. All update, query, and reply packets are deemed reliable, and hello and ACK packets do not require acknowledgment and could be unreliable.

If the originating router does not receive an ACK packet from the neighbor before the retransmit timeout expires, it notifies the non-acknowledging router to stop processing its multicast packets. The originating router sends all traffic by unicast until the neighbor is fully synchronized. Upon complete synchronization, the originating router notifies the destination router to start processing multicast packets again. All unicast packets require acknowledgment. EIGRP retries up to 16 times for each packet that requires confirmation, and it resets the neighbor relationship when the neighbor reaches the retry limit of 16.

**NOTE** In the context of EIGRP, do not confuse RTP with the Real-Time Transport Protocol (RTP), which is used for carrying audio or video over an IP network. EIGRP's RTP allows for confirmation of packets while supporting multicast. Other protocols that require reliable connection-oriented communication, such as TCP, cannot use multicast addressing.

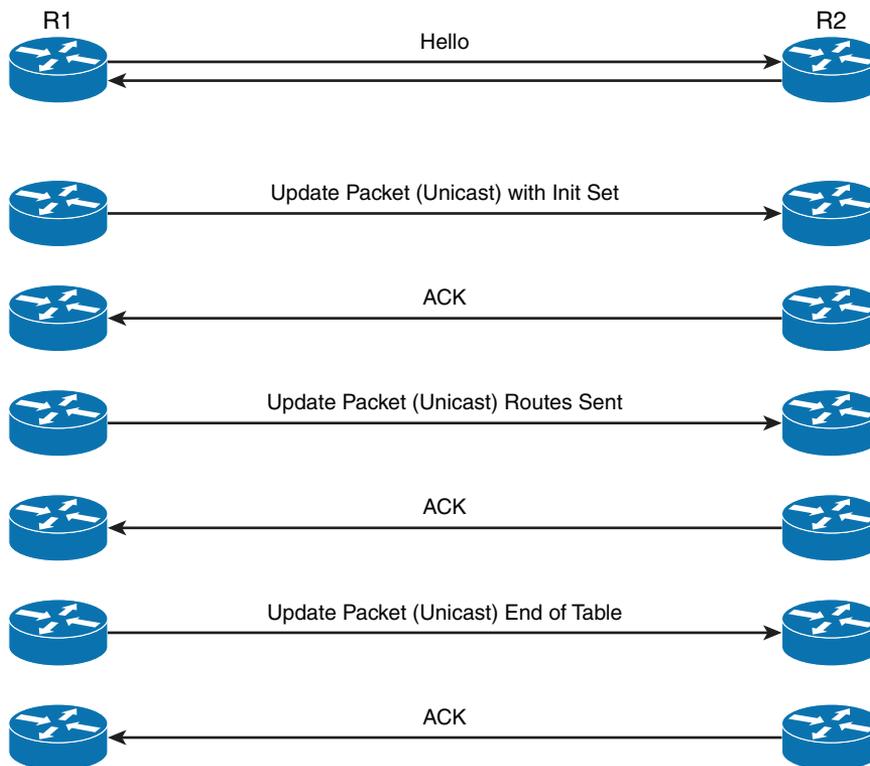
**Key Topic**

## Forming EIGRP Neighbors

Unlike other distance vector routing protocols, EIGRP requires a neighbor relationship to form before routes are processed and added to the Routing Information Base (RIB). Upon hearing an EIGRP hello packet, a router attempts to become the neighbor of the other router. The following parameters must match for the two routers to become neighbors:

- Metric formula K values
- Primary subnet matches
- Autonomous system number (ASN) matches
- Authentication parameters

Figure 2-4 shows the process EIGRP uses for forming neighbor adjacencies.



**Figure 2-4** EIGRP Neighbor Adjacency Process from R1's Perspective

## EIGRP Configuration Modes

This section describes the two methods of EIGRP configuration: classic mode and named mode.

### Classic Configuration Mode

With *classic EIGRP configuration mode*, most of the configuration takes place in the EIGRP process, but some settings are configured under the interface configuration submode. This can add complexity for deployment and troubleshooting as users must scroll back and forth between the EIGRP process and individual network interfaces. Some of the settings that are set individually are hello advertisement interval, split-horizon, authentication, and summary route advertisements.

#### Key Topic

Classic configuration requires the initialization of the routing process with the global configuration command **router eigrp as-number** to identify the ASN and initialize the EIGRP process. The second step is to identify the network interfaces with the command **network ip-address [wildcard-mask]**. The **network** statement is explained in the following sections.

#### Key Topic

### EIGRP Named Mode

*EIGRP named mode* configuration was released to overcome some of the difficulties network engineers have with classic EIGRP autonomous system configuration, including scattered configurations and unclear scope of commands.

EIGRP named configuration provides the following benefits:

- All the EIGRP configuration occurs in one location.
- It supports current EIGRP features and future developments.
- It supports multiple address families (including virtual routing and forwarding [VRF] instances). EIGRP named configuration is also known as *multi-address family configuration mode*.
- Commands are clear in terms of the scope of their configuration.

EIGRP named mode provides a hierarchical configuration and stores settings in three subsections:

- **Address Family:** This submode contains settings that are relevant to the global EIGRP AS operations, such as selection of network interfaces, EIGRP K values, logging settings, and stub settings.
- **Interface:** This submode contains settings that are relevant to the interface, such as hello advertisement interval, split-horizon, authentication, and summary route advertisements. In actuality, there are two methods of the EIGRP interface section's configuration. Commands can be assigned to a specific interface or to a *default* interface, in which case those settings are placed on all EIGRP-enabled interfaces. If there is a conflict between the default interface and a specific interface, the specific interface takes priority over the default interface.

- **Topology:** This submode contains settings regarding the EIGRP topology database and how routes are presented to the router's RIB. This section also contains route redistribution and administrative distance settings.

EIGRP named configuration makes it possible to run multiple instances under the same EIGRP process. The process for enabling EIGRP interfaces on a specific instance is as follows:

- Step 1.** Initialize the EIGRP process by using the command **router eigrp *process-name***. (If a number is used for *process-name*, the *number* does not correlate to the autonomous system number.)
- Step 2.** Initialize the EIGRP instance for the appropriate address family with the command **address-family {IPv4 | IPv6} {unicast | vrf *vrf-name*} autonomous-system *as-number***.
- Step 3.** Enable EIGRP on interfaces by using the command **network *network wildcard-mask***.

## EIGRP Network Statement

Both configuration modes use a **network** statement to identify the interfaces that EIGRP will use. The **network** statement uses a wildcard mask, which allows the configuration to be as specific or ambiguous as necessary.

**NOTE** The two styles of EIGRP configuration are independent. Using the configuration options from classic EIGRP autonomous system configuration does not modify settings on a router running EIGRP named configuration.

The syntax for the **network** statement, which exists under the EIGRP process, is **network *ip-address [wildcard-mask]***. The optional *wildcard-mask* can be omitted to enable interfaces that fall within the classful boundaries for that **network** statement.

A common misconception is that the **network** statement adds prefixes to the EIGRP topology table. In reality, the **network** statement identifies the interface to enable EIGRP on, and it adds the interface's connected network to the EIGRP topology table. EIGRP then advertises the topology table to other routers in the EIGRP autonomous system.

EIGRP does not add an interface's secondary connected network to the topology table. For secondary connected networks to be installed in the EIGRP routing table, they must be redistributed into the EIGRP process. Chapter 16, "Route Redistribution," provides additional coverage of route redistribution.

To help illustrate the concept of the wildcard mask, Table 2-4 provides a set of IP addresses and interfaces for a router. The following examples provide configurations to match specific scenarios.

**Table 2-4** Table of Sample Interface and IP Addresses

Router Interface	IP Address
Gigabit Ethernet 0/0	10.0.0.10/24
Gigabit Ethernet 0/1	10.0.10.10/24
Gigabit Ethernet 0/2	192.0.0.10/24
Gigabit Ethernet 0/3	192.10.0.10/24

The configuration in Example 2-1 enables EIGRP only on interfaces that explicitly match the IP addresses in Table 2-4.

**Example 2-1** *EIGRP Configuration with Explicit IP Addresses*

```
Router eigrp 1
  network 10.0.0.10 0.0.0.0
  network 10.0.10.10 0.0.0.0
  network 192.0.0.10 0.0.0.0
  network 192.10.0.10 0.0.0.0
```

Example 2-2 shows the EIGRP configuration using **network** statements that match the subnets used in Table 2-4. Setting the last octet of the IP address to 0 and changing the wildcard mask to 255 cause the **network** statements to match all IP addresses within the /24 network range.

**Example 2-2** *EIGRP Configuration with an Explicit Subnet*

```
Router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 10.0.10.0 0.0.0.255
  network 192.0.0.0 0.0.0.255
  network 192.10.0.0 0.0.0.255
```

The following snippet shows the EIGRP configuration using **network** statements for interfaces that are within the 10.0.0.0/8 or 192.0.0.0/8 network ranges:

```
router eigrp 1
  network 10.0.0.0 0.255.255.255
  network 192.0.0.0 0.255.255.255
```

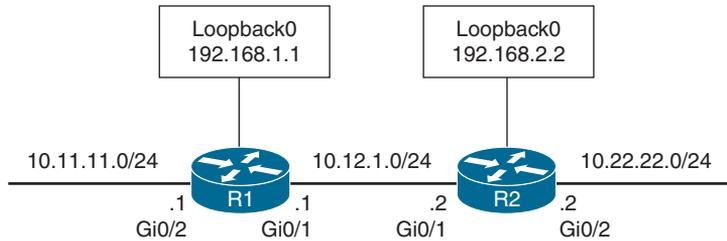
The following snippet shows the configuration to enable all interfaces with EIGRP:

```
router eigrp 1
  network 0.0.0.0 255.255.255.255
```

**NOTE** A key topic with wildcard **network** statements is that large ranges simplify configuration; however, they may possibly enable EIGRP on interfaces where not intended.

## Sample Topology and Configuration

Figure 2-5 shows a sample topology for demonstrating EIGRP configuration in classic mode for R1 and named mode for R2.



**Figure 2-5** EIGRP Sample Topology

R1 and R2 enable EIGRP on all of their interfaces. R1 configures EIGRP using multiple specific network interface addresses, and R2 enables EIGRP on all network interfaces with one command. Example 2-3 provides the configuration that is applied to R1 and R2.

### Example 2-3 Sample EIGRP Configuration

#### R1 (Classic Configuration)

```
interface Loopback0
  ip address 192.168.1.1 255.255.255.255
!
interface GigabitEthernet0/1
  ip address 10.12.1.1 255.255.255.0
!
interface GigabitEthernet0/2
  ip address 10.11.11.1 255.255.255.0
!
router eigrp 100
  network 10.11.11.1 0.0.0.0
  network 10.12.1.1 0.0.0.0
  network 192.168.1.1 0.0.0.0
```

#### R2 (Named Mode Configuration)

```
interface Loopback0
  ip address 192.168.2.2 255.255.255.255
!
interface GigabitEthernet0/1
  ip address 10.12.1.2 255.255.255.0
!
interface GigabitEthernet0/2
  ip address 10.22.22.2 255.255.255.0
!
router eigrp EIGRP-NAMED
  address-family ipv4 unicast autonomous-system 100
    network 0.0.0.0 255.255.255.255
```

As mentioned earlier, EIGRP named mode has three configuration submodes. The configuration in Example 2-3 uses only the EIGRP address-family submode section, which uses the **network** statement. The EIGRP topology base submode is created automatically with the command **topology base** and exited with the command **exit-af-topology**. Settings for the topology submode are listed between those two commands.

Example 2-4 demonstrates the slight difference in how the configuration is stored on the router between EIGRP classic and named mode configurations.

#### Example 2-4 Comparison of EIGRP Configuration Mode Structures

```
R1# show run | section router eigrp
router eigrp 100
  network 10.11.11.1 0.0.0.0
  network 10.12.1.1 0.0.0.0
  network 192.168.1.1 0.0.0.0

R2# show run | section router eigrp
router eigrp EIGRP-NAMED
!
address-family ipv4 unicast autonomous-system 100
!
  topology base
  exit-af-topology
  network 0.0.0.0
exit-address-family
```

**NOTE** The EIGRP interface submode configurations contain the command **af-interface interface-id** or **af-interface default**, with any specific commands listed immediately. The EIGRP interface submode configuration is exited with the command **exit-af-interface**. This is demonstrated later in this chapter.

### Confirming Interfaces

Upon configuring EIGRP, it is a good practice to verify that only the intended interfaces are running EIGRP. The command **show ip eigrp interfaces** *[interface-id [detail] | detail]* shows active EIGRP interfaces. Appending the optional **detail** keyword provides additional information, such as authentication, EIGRP timers, split horizon, and various packet counts.

Example 2-5 demonstrates R1's non-detailed EIGRP interface and R2's detailed information for the Gi0/1 interface.

#### Example 2-5 Verifying EIGRP Interfaces

```
R1# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(100)

```

Interface	Peers	Xmit Queue Un/Reliable	PeerQ Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Gi0/2	0	0/0	0/0	0	0/0	0	0

Gi0/1	1	0/0	0/0	10	0/0	50	0
Lo0	0	0/0	0/0	0	0/0	0	0

```

R2# show ip eigrp interfaces gi0/1 detail
EIGRP-IPv4 VR(EIGRP-NAMED) Address-Family Interfaces for AS(100)
      Xmit Queue  PeerQ      Mean  Pacing Time  Multicast  Pending
Interface Peers  Un/Reliable Un/Reliable SRTT   Un/Reliable  Flow Timer Routes
Gi0/1      1      0/0        0/0      1583   0/0         7912      0
  Hello-interval is 5, Hold-time is 15
  Split-horizon is enabled
  Next xmit serial <none>
  Packetized sent/expedited: 2/0
  Hello's sent/expedited: 186/2
  Un/reliable mcasts: 0/2  Un/reliable ucasts: 2/2
  Mcast exceptions: 0  CR packets: 0  ACKs suppressed: 0
  Retransmissions sent: 1  Out-of-sequence rcvd: 0
  Topology-ids on interface - 0
  Authentication mode is not set
  Topologies advertised on this interface: base
  Topologies not advertised on this interface:

```

Table 2-5 provides a brief explanation to the key fields shown with the EIGRP interfaces.

**Table 2-5** EIGRP Interface Fields

Field	Description
Interface	Interfaces running EIGRP.
Peers	Number of peers detected on the interface.
Xmt Queue Un/Reliable	Number of unreliable/reliable packets remaining in the transmit queue. The value zero is an indication of a stable network.
Mean SRTT	Average time for a packet to be sent to a neighbor and a reply from that neighbor to be received, in milliseconds.
Multicast Flow Timer	Maximum time (seconds) that the router sent multicast packets.
Pending Routes	Number of routes in the transmit queue that need to be sent.

## Verifying EIGRP Neighbor Adjacencies

Each EIGRP process maintains a table of neighbors to ensure that they are alive and processing updates properly. If EIGRP didn't keep track of neighbor states, an autonomous system could contain incorrect data and could potentially route traffic improperly. EIGRP must form a neighbor relationship before a router advertises update packets containing network prefixes.

The command `show ip eigrp neighbors [interface-id]` displays the EIGRP neighbors for a router. Example 2-6 shows the EIGRP neighbor information obtained using this command.

**Example 2-6** *EIGRP Neighbor Confirmation*

```

R1# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                Interface           Hold Uptime      SRTT   RTO  Q  Seq
                               (sec)            (ms)            Cnt  Num
0   10.12.1.2                Gi0/1              13 00:18:31     10   100  0  3

```

Table 2-6 provides a brief explanation of the key fields shown in Example 2-6.

**Table 2-6** EIGRP Neighbor Columns

Field	Description
Address	IP address of the EIGRP neighbor
Interface	Interface the neighbor was detected on
Holdtime	Time left to receive a packet from this neighbor to ensure that it is still alive
SRTT	Time for a packet to be sent to a neighbor and a reply to be received from that neighbor, in milliseconds
RTO	Timeout for retransmission (waiting for ACK)
Q Cnt	Number of packets (update/query/reply) in queue for sending
Seq Num	Sequence number that was last received from this router

**Displaying Installed EIGRP Routes**

You can see EIGRP routes that are installed into the RIB by using the command **show ip route eigrp**. EIGRP routes that originate within the autonomous system have an administrative distance (AD) of 90 and are indicated in the routing table with a D. Routes that originate from outside the autonomous system are external EIGRP routes. External EIGRP routes have an AD of 170 and are indicated in the routing table with D EX. Placing external EIGRP routes into the RIB with a higher AD acts as a loop-prevention mechanism.

Example 2-7 displays the EIGRP routes from the sample topology in Figure 2-5. The metric for the selected route is the second number in brackets.

**Example 2-7** *EIGRP Routes for R1 and R2*

```

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

```

```
Gateway of last resort is not set
```

```

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D       10.22.22.0/24 [90/3072] via 10.12.1.2, 00:19:25, GigabitEthernet0/1
      192.168.2.0/32 is subnetted, 1 subnets
D       192.168.2.2 [90/2848] via 10.12.1.2, 00:19:25, GigabitEthernet0/1

```

```
R2# show ip route eigrp
```

```
! Output omitted for brevity
```

```
Gateway of last resort is not set
```

```

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D       10.11.11.0/24 [90/15360] via 10.12.1.1, 00:20:34, GigabitEthernet0/1
      192.168.1.0/32 is subnetted, 1 subnets
D       192.168.1.1 [90/2570240] via 10.12.1.1, 00:20:34, GigabitEthernet0/1

```

**NOTE** The metrics for R2’s routes are different from the metrics from R1’s routes. This is because R1’s classic EIGRP mode uses classic metrics, and R2’s named mode uses wide metrics by default. This topic is explained in depth in the “Path Metric Calculation” section, later in this chapter.

## Router ID

The router ID (RID) is a 32-bit number that uniquely identifies an EIGRP router and is used as a loop-prevention mechanism. The RID can be set dynamically, which is the default, or manually.

The algorithm for dynamically choosing the EIGRP RID uses the highest IPv4 address of any *up* loopback interfaces. If there are not any *up* loopback interfaces, the highest IPv4 address of any active *up* physical interfaces becomes the RID when the EIGRP process initializes.

IPv4 addresses are commonly used for the RID because they are 32 bits and are maintained in dotted-decimal format. You use the command `eigrp router-id router-id` to set the RID, as demonstrated in Example 2-8, for both classic and named mode configurations.

### Example 2-8 Static Configuration of EIGRP Router ID

```

R1(config)# router eigrp 100
R1(config-router)# eigrp router-id 192.168.1.1

```

---

```

R2(config)# router eigrp EIGRP-NAMED
R2(config-router)# address-family ipv4 unicast autonomous-system 100
R2(config-router-af)# eigrp router-id 192.168.2.2

```



## Passive Interfaces

Some network topologies must advertise a network segment into EIGRP but need to prevent neighbors from forming adjacencies with other routers on that segment. This might be the case, for example, when advertising access layer networks in a campus topology. In such a scenario, you need to put the EIGRP interface in a passive state. Passive EIGRP interfaces do not send out or process EIGRP hellos, which prevents EIGRP from forming adjacencies on those interfaces.

To configure an EIGRP interface as passive, you use the command `passive-interface interface-id` under the EIGRP process for classic configuration. Another option is to configure all interfaces as passive by default with the command `passive-interface default` and then use the command `no passive-interface interface-id` to allow an interface to process EIGRP packets, preempting the global `passive interface` default configuration.

Example 2-9 demonstrates making R1's Gi0/2 interface passive and also the alternative option of making all interfaces passive but setting Gi0/1 as non-passive.

### Example 2-9 *Passive EIGRP Interfaces for Classic Configuration*

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# router eigrp 100
R1(config-router)# passive-interface gi0/2

R1(config)# router eigrp 100
R1(config-router)# passive-interface default
04:22:52.031: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.12.1.2
(GigabitEthernet0/1) is down: interface passive
R1(config-router)# no passive-interface gi0/1
*May 10 04:22:56.179: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.12.1.2
(GigabitEthernet0/1) is up: new adjacency
```

For a named mode configuration, you place the `passive-interface` state on `af-interface default` for all EIGRP interfaces or on a specific interface with the `af-interface interface-id` section. Example 2-10 shows how to set the Gi0/2 interface as passive while allowing the Gi0/1 interface to be active, using both configuration strategies.

### Example 2-10 *Passive EIGRP Interfaces for Named Mode Configuration*

```
R2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# router eigrp EIGRP-NAMED
R2(config-router)# address-family ipv4 unicast autonomous-system 100
R2(config-router-af)# af-interface gi0/2
R2(config-router-af-interface)# passive-interface

R2(config)# router eigrp EIGRP-NAMED
R2(config-router)# address-family ipv4 unicast autonomous-system 100
```

```

R2(config-router-af)# af-interface default
R2(config-router-af-interface)# passive-interface
04:28:30.366: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.12.1.1
(GigabitEthernet0/1) is down: interface passiveex
R2(config-router-af-interface)# exit-af-interface
R2(config-router-af)# af-interface gi0/1
R2(config-router-af-interface)# no passive-interface
R2(config-router-af-interface)# exit-af-interface
*May 10 04:28:40.219: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.12.1.1
(GigabitEthernet0/1) is up: new adjacency

```

Example 2-11 shows what the named mode configuration looks like with some settings (that is, `passive-interface` and `no passive-interface`) placed under the `af-interface default` and `af-interface interface-id` settings.

### Example 2-11 Viewing the EIGRP Interface Settings with Named Mode

```

R2# show run | section router eigrp
router eigrp EIGRP-NAMED
!
address-family ipv4 unicast autonomous-system 100
!
af-interface default
  passive-interface
exit-af-interface
!
af-interface GigabitEthernet0/1
  no passive-interface
exit-af-interface
!
topology base
exit-af-topology
network 0.0.0.0
exit-address-family

```

A passive interface does not appear in the output of the command `show ip eigrp interfaces` even though it was enabled. Connected networks for passive interfaces are still added to the EIGRP topology table so that they are advertised to neighbors.

Example 2-12 shows that the Gi0/2 interface on R1 no longer appears; compare this to Example 2-5, where it does exist.

### Example 2-12 `show ip eigrp interfaces` Output

```

R1# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(100)

```

Interface	Peers	Xmit Queue Un/Reliable	PeerQ Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Gi0/1	1	0/0	0/0	9	0/0	50	0

To accelerate troubleshooting of passive interfaces, as well as other settings, use the command **show ip protocols**, which provides a lot of valuable information about all the routing protocols. With EIGRP, it displays the EIGRP process identifier, the ASN, *K values* that are used for path calculation, RID, neighbors, AD settings, and all the passive interfaces.

Example 2-13 provides sample output for both classic and named mode instances on R1 and R2.

### Example 2-13 *show ip protocols Output*

```
R1# show ip protocols
! Output omitted for brevity
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(100)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    Soft SIA disabled
    NSF-aware route hold timer is 240
    Router-ID: 192.168.1.1
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    10.11.11.1/32
    10.12.1.1/32
    192.168.1.1/32
  Passive Interface(s):
    GigabitEthernet0/2
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.12.1.2         90           00:21:35
  Distance: internal 90 external 170
```

```
R2# show ip protocols
! Output omitted for brevity
Routing Protocol is "eigrp 100"
```

```

Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default networks flagged in outgoing updates
Default networks accepted from incoming updates
EIGRP-IPv4 VR(EIGRP-NAMED) Address-Family Protocol for AS(100)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0 K6=0
  Metric rib-scale 128
  Metric version 64bit
  Soft SIA disabled
  NSF-aware route hold timer is 240
  Router-ID: 192.168.2.2
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 4
    Maximum hopcount 100
    Maximum metric variance 1
    Total Prefix Count: 5
    Total Redist Count: 0

Automatic Summarization: disabled
Maximum path: 4
Routing for Networks:
  0.0.0.0
  Passive Interface(s):
    GigabitEthernet0/2
    Loopback0
Routing Information Sources:
  Gateway          Distance      Last Update
  10.12.1.1         90           00:24:26
Distance: internal 90 external 170

```



## Authentication

Authentication is a mechanism for ensuring that only authorized routers are eligible to become EIGRP neighbors. It is possible for someone to add a router to a network and introduce invalid routes accidentally or maliciously. Authentication prevents such scenarios from happening. A precomputed password hash is included with all EIGRP packets, and the receiving router decrypts the hash. If the passwords do not match for a packet, the router discards the packet.

EIGRP encrypts the password by using Message Digest 5 (MD5) authentication and the keychain function. The hash consists of the key number and a password. EIGRP authentication encrypts just the password rather than the entire EIGRP packet.

**NOTE** Keychain functionality allows a password to be valid for a specific time, so passwords can change at preconfigured times. Restricting the key sequence to a specific time is beyond the scope of this book. For more information, see Cisco.com.

To configure EIGRP authentication, you need to create a keychain and then enable EIGRP authentication on the interface. The following sections explain the steps.

### Keychain Configuration

Keychain creation is accomplished with the following steps:

- Step 1.** Create the keychain by using the command `key chain key-chain-name`.
- Step 2.** Identify the key sequence by using the command `key key-number`, where *key-number* can be anything from 0 to 2147483647.
- Step 3.** Specify the preshared password by using the command `key-string password`.

**NOTE** Be careful not to use a space after the password because the password, including any trailing space, will be used for computing the hash.

### Enabling Authentication on the Interface

When using classic configuration, authentication must be enabled on the interface under the interface configuration submode. The following commands are used in the interface configuration submode:

```
ip authentication key-chain eigrp as-number key-chain-name
ip authentication mode eigrp as-number md5
```

The named mode configuration places the configurations under the EIGRP interface submode, under `af-interface default` or `af-interface interface-id`. Named mode configuration supports MD5 or *Hashed Message Authentication Code-Secure Hash Algorithm-256 (HMAC-SHA-256)* authentication. MD5 authentication involves the following commands:

```
authentication key-chain eigrp key-chain-name
authentication mode md5
```

HMAC-SHA-256 authentication involves the command `authentication mode hmac-sha-256 password`.

Example 2-14 demonstrates MD5 configuration on R1 with classic EIGRP configuration and on R2 with named mode configuration. Remember that the hash is computed using the key sequence number and key string, which must match on the two nodes.

**Example 2-14** *Configuring EIGRP Authentication*

```

R1(config)# key chain EIGRPKEY
R1(config-keychain)# key 2
R1(config-keychain-key)# key-string CISCO
R1(config)# interface gi0/1
R1(config-if)# ip authentication mode eigrp 100 md5
R1(config-if)# ip authentication key-chain eigrp 100 EIGRPKEY

R2(config)# key chain EIGRPKEY
R2(config-keychain)# key 2
R2(config-keychain-key)# key-string CISCO
R2(config-keychain-key)# router eigrp EIGRP-NAMED
R2(config-router)# address-family ipv4 unicast autonomous-system 100
R2(config-router-af)# af-interface default
R2(config-router-af-interface)# authentication mode md5
R2(config-router-af-interface)# authentication key-chain EIGRPKEY

```

The command **show key chain** provides verification of the keychain. Example 2-15 shows that each key sequence provides the lifetime and password.

**Example 2-15** *Verifying Keychain Settings*

```

R1# show key chain
Key-chain EIGRPKEY:
  key 2 -- text "CISCO"
    accept lifetime (always valid) - (always valid) [valid now]
    send lifetime (always valid) - (always valid) [valid now]

```

The EIGRP interface detail view provides verification of EIGRP authentication on a specific interface. Example 2-16 shows detailed EIGRP interface output.

**Example 2-16** *Verifying EIGRP Authentication*

```

R1# show ip eigrp interface detail
EIGRP-IPv4 Interfaces for AS(100)

Interface Peers Xmit Queue PeerQ Mean Pacing Time Multicast Pending
           Un/Reliable Un/Reliable SRTT Un/Reliable Flow Timer Routes
Gi0/1      0      0/0      0/0    0      0/0      50      0

Hello-interval is 5, Hold-time is 15
Split-horizon is enabled
Next xmit serial <none>
Packetized sent/expedited: 10/1
Hello's sent/expedited: 673/12

```

```

Un/reliable mcasts: 0/9 Un/reliable ucasts: 6/19
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
Retransmissions sent: 16 Out-of-sequence rcvd: 1
Topology-ids on interface - 0
Authentication mode is md5, key-chain is "EIGRPKEY"

```

## Key Topic

## Path Metric Calculation

Metric calculation is a critical component for any routing protocol. EIGRP uses multiple factors to calculate the metric for a path. Metric calculation uses *bandwidth* and *delay* by default but can include interface load and reliability, too. Figure 2-6 shows the EIGRP classic metric formula.

$$\text{Metric} = 256 * \left[ (K_1 * \text{BW} + \frac{K_2 * \text{BW}}{256 - \text{Load}} + K_3 * \text{Delay}) * \frac{K_5}{K_4 + \text{Reliability}} \right]$$

**Figure 2-6** EIGRP Metric Formula

EIGRP uses K values to define which factors the formula uses and the impact associated with a factor when calculating the metric. A common misconception is that the K values directly apply to bandwidth, load, delay, or reliability; this is not accurate. For example,  $K_1$  and  $K_2$  both reference bandwidth (BW).

BW represents the slowest link in the path, scaled to a 10 Gbps link ( $10^7$ ). Link speed correlates to the configured interface bandwidth on an interface and is measured in kilobits per second (Kbps). Delay is the total measure of delay in the path, measured in tens of microseconds ( $\mu\text{s}$ ).

Taking these definitions into consideration, look at the formula for classic EIGRP metrics in Figure 2-7.

$$\text{Metric} = 256 * \left[ \left( K_1 * \frac{10^7}{\text{Min. Bandwidth}} + \frac{K_2 * \text{Min. Bandwidth}}{256 - \text{Load}} + \frac{K_3 * \text{Total Delay}}{10} \right) * \frac{K_5}{K_4 + \text{Reliability}} \right]$$

**Figure 2-7** EIGRP Classic Metric Formula with Definitions

**NOTE** RFC 7868 states that if  $K_5 = 0$ , then the reliability quotient is defined to be 1. This is not demonstrated in Figure 2-7 but is shown in the simpler formula in Figure 2-8.

By default,  $K_1$  and  $K_3$  each has a value of 1, and  $K_2$ ,  $K_4$ , and  $K_5$  are all set to 0. Figure 2-8 places default K values into the formula and shows a streamlined version of the formula.

## Key Topic

The EIGRP update packet includes path attributes associated with each prefix. The EIGRP path attributes can include hop count, cumulative delay, minimum bandwidth link speed, and RD. The attributes are updated each hop along the way, allowing each router to independently identify the shortest path.

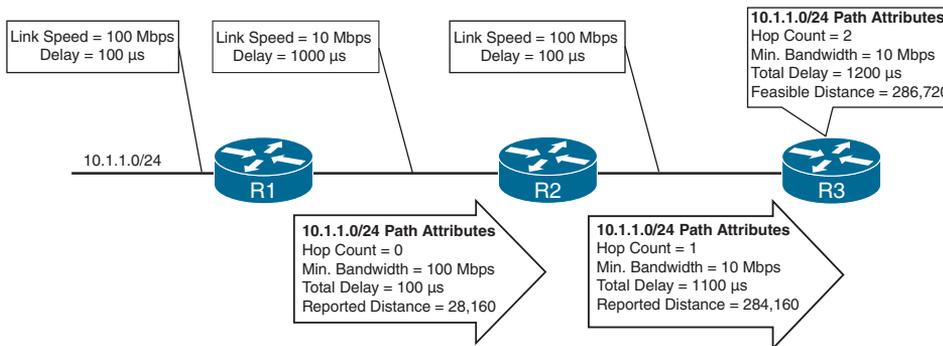
$$\text{Metric} = 256 * \left[ \left( 1 * \frac{10^7}{\text{Min. Bandwidth}} + \frac{0 * \text{Min. Bandwidth}}{256 - \text{Load}} + \frac{1 * \text{Total Delay}}{10} \right) * \frac{0}{0 + \text{Reliability}} \right]$$

↓  
Equals

$$\text{Metric} = 256 * \left( \frac{10^7}{\text{Min. Bandwidth}} + \frac{\text{Total Delay}}{10} \right)$$

**Figure 2-8** EIGRP Classic Metric Formula with Default K Values

Figure 2-9 shows the information in the EIGRP update packets for the 10.1.1.0/24 network propagating through the autonomous system. Notice that the hop count increments, minimum bandwidth decreases, total delay increases, and the RD changes with each EIGRP update.



**Figure 2-9** EIGRP Attribute Propagation

Table 2-7 shows for some common network types the link speed, delay, and EIGRP metric, based on the streamlined formula in Figure 2-8.

**Table 2-7** Default EIGRP Interface Metrics for Classic Metrics

Interface Type	Link Speed (Kbps)	Delay	Metric
Serial	64	20,000 μs	40,512,000
T1	1544	20,000 μs	2,170,031
Ethernet	10,000	1000 μs	281,600
FastEthernet	100,000	100 μs	28,160
GigabitEthernet	1,000,000	10 μs	2816
TenGigabitEthernet	10,000,000	10 μs	512

Using the topology from Figure 2-2, the metrics from R1 and R2 for the 10.4.4.0/24 network are calculated using the formula in Figure 2-10. The link speed for both routers is 1 Gbps,

and the total delay is 30  $\mu$ s (10  $\mu$ s for the 10.4.4.0/24 link, 10  $\mu$ s for the 10.34.1.0/24 link, and 10  $\mu$ s for the 10.13.1.0/24 link).

$$\text{Metric} = 256 * \left( \frac{10^7}{1,000,000} + \frac{30}{10} \right) = 3,328$$

**Figure 2-10** *Calculating EIGRP Metrics with Default K Values*

If you are unsure of the EIGRP metrics, you can query the parameters for the formula directly from EIGRP's topology table by using the command `show ip eigrp topology network/prefix-length`.

Example 2-17 shows R1's topology table output for the 10.4.4.0/24 network. Notice that the output includes the successor route, any feasible successor paths, and the EIGRP state for the prefix. Each path contains the EIGRP attributes minimum bandwidth, total delay, interface reliability, load, and hop count.

**Example 2-17** *EIGRP Topology for a Specific Prefix*

```
R1# show ip eigrp topology 10.4.4.0/24
! Output omitted for brevity
EIGRP-IPv4 Topology Entry for AS(100)/ID(10.14.1.1) for 10.4.4.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 3328
Descriptor Blocks:
  10.13.1.3 (GigabitEthernet0/1), from 10.13.1.3, Send flag is 0x0
    Composite metric is (3328/3072), route is Internal
    Vector metric:
      Minimum bandwidth is 1000000 Kbit
      Total delay is 30 microseconds
      Reliability is 252/255
      Load is 1/255
      Minimum MTU is 1500
      Hop count is 2
      Originating router is 10.34.1.4
  10.14.1.4 (GigabitEthernet0/2), from 10.14.1.4, Send flag is 0x0
    Composite metric is (5376/2816), route is Internal
    Vector metric:
      Minimum bandwidth is 1000000 Kbit
      Total delay is 110 microseconds
      Reliability is 255/255
      Load is 1/255
      Minimum MTU is 1500
      Hop count is 1
      Originating router is 10.34.1.4
```

## Wide Metrics

The original EIGRP specifications measured delay in 10-microsecond ( $\mu$ s) units and bandwidth in kilobits per second, which did not scale well with higher-speed interfaces. In

Table 2-7, notice that the delay is the same for the GigabitEthernet and TenGigabitEthernet interfaces.

Example 2-18 provides some metric calculations for common LAN interface speeds. Notice that there is not a differentiation between an 11 Gbps interface and a 20 Gbps interface. The composite metric stays at 256, despite the different bandwidth rates.

**Example 2-18** *Metric Calculation for Common LAN Interface Speeds*

<p><b>GigabitEthernet:</b>  Scaled Bandwidth = 10,000,000 / 1,000,000  Scaled Delay = 10 / 10  Composite Metric = 10 + 1 * 256 = 2816</p>
<p><b>10 GigabitEthernet:</b>  Scaled Bandwidth = 10,000,000 / 10,000,000  Scaled Delay = 10 / 10  Composite Metric = 1 + 1 * 256 = 512</p>
<p><b>11 GigabitEthernet:</b>  Scaled Bandwidth = 10,000,000 / 11,000,000  Scaled Delay = 10 / 10  Composite Metric = 0 + 1 * 256 = 256</p>
<p><b>20 GigabitEthernet:</b>  Scaled Bandwidth = 10,000,000 / 20,000,000  Scaled Delay = 10 / 10  Composite Metric = 0 + 1 * 256 = 256</p>

EIGRP includes support for a second set of metrics, known as *wide metrics*, that addresses the issue of scalability with higher-capacity interfaces. Just as EIGRP scaled by 256 to accommodate IGRP, EIGRP wide metrics scale by 65,536 to accommodate higher-speed links. This provides support for interface speeds up to 655 Tbps ( $65,536 \times 10^7$ ) without any scalability issues.

Figure 2-11 shows the explicit EIGRP wide metrics formula. Notice that an additional K value ( $K_6$ ) is included that adds an extended attribute to measure jitter, energy, or other future attributes.



$$\text{Wide Metric} = 65,536 * \left[ (K_1 * \text{BW} + \frac{K_2 * \text{BW}}{256 - \text{Load}} + K_3 * \text{Latency} + K_6 * \text{Extended}) * \frac{K_5}{K_4 + \text{Reliability}} \right]$$

**Figure 2-11** *EIGRP Wide Metrics Formula*

Latency is the total interface delay measured in picoseconds ( $10^{12}$ ) instead of in microseconds ( $10^6$ ). Figure 2-12 shows an updated formula that takes into account the conversions in latency and scalability.

$$\text{Wide Metric} = 65,536 * \left[ \left( \frac{K_1 * 10^7}{\text{Min. Bandwidth}} + \frac{K_2 * 10^7}{256 - \text{Load}} + \frac{K_3 * \text{Latency}}{10^6} + K_6 * \text{Extended} \right) * \frac{K_5}{K_4 + \text{Reliability}} \right]$$

**Figure 2-12** EIGRP Wide Metrics Formula with Definitions

The interface delay varies from router to router, depending on the following logic:

- If the interface's delay was specifically set, the value is converted to picoseconds. Interface delay is always configured in tens of microseconds and is multiplied by  $10^7$  for picosecond conversion.
- If the interface's bandwidth was specifically set, the interface delay is configured using the classic default delay, converted to picoseconds. The configured bandwidth is not considered when determining the interface delay. If delay was configured, this step is ignored.
- If the interface supports speeds of 1 Gbps or less and does not contain bandwidth or delay configuration, the delay is the classic default delay, converted to picoseconds.
- If the interface supports speeds over 1 Gbps and does not contain bandwidth or delay configuration, the interface delay is calculated by  $10^{13}/\text{interface bandwidth}$ .

The EIGRP classic metrics exist only with EIGRP classic configuration, and EIGRP wide metrics exist only in EIGRP named mode. The metric style used by a router is identified with the command **show ip protocols**. If a  $K_6$  metric is present, the router is using wide-style metrics.

Example 2-19 shows the commands to verify the operational mode of EIGRP on R1 and R2. It shows that R1 does not have a  $K_6$  metric and is using EIGRP classic metrics. R2 has a  $K_6$  metric and is using EIGRP wide metrics.

**Example 2-19** Verifying EIGRP Metric Style

```
R1# show ip protocols | include AS|K
EIGRP-IPv4 Protocol for AS(100)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0

R2# show ip protocols | include AS|K
EIGRP-IPv4 VR(EIGRP-NAMED) Address-Family Protocol for AS(100)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0, K6=0
```

## Metric Backward Compatibility

EIGRP wide metrics were designed with backward compatibility in mind. EIGRP wide metrics set  $K_1$  and  $K_3$  to a value of 1 and set  $K_2$ ,  $K_4$ ,  $K_5$ , and  $K_6$  to 0, which allows backward compatibility because the K value metrics match with classic metrics. As long as  $K_1$  through  $K_5$  are the same and  $K_6$  is not set, the two metric styles allow adjacency between routers.

EIGRP is able to detect when peering with a router is using classic metrics, and it *unscales* the metric by using the formula in Figure 2-13.

$$\text{Unscaled Bandwidth} = \left( \frac{\text{EIGRP Bandwidth} * \text{EIGRP Classic Scale}}{\text{Scaled Bandwidth}} \right)$$

**Figure 2-13** Formula for Calculating Unscaled EIGRP Metrics

This conversion results in loss of clarity if routes pass through a mixture of classic metric and wide metric devices. An end result of this intended behavior is that paths learned from wide metric peers always look better than paths learned from classic peers. Using a mixture of classic metric and wide metric devices could lead to suboptimal routing, so it is best to keep all devices operating with the same metric style.

2

## Interface Delay Settings

If you do not remember the delay values from Table 2-7, you can query the values dynamically by using the command `show interface interface-id`. The output displays the EIGRP interface delay, in microseconds, after the DLY field. Example 2-20 provides sample output of the command on R1 and R2. The output shows that both interfaces have a delay of 10  $\mu$ s.

**Example 2-20** Verifying EIGRP Interface Delay

```
R1# show interfaces gigabitEthernet 0/1 | i DLY
    MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
R2# show interfaces gigabitEthernet 0/1 | i DLY
    MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
```

EIGRP delay is set on an interface-by-interface basis, allowing for manipulation of traffic patterns flowing through a specific interface on a router. Delay is configured with the interface parameter command `delay tens-of-microseconds` under the interface.

Example 2-21 demonstrates the modification of the delay on R1 to 100, increasing the delay to 1000  $\mu$ s on the link between R1 and R2. To ensure consistent routing, modify the delay on R2's Gi0/1 interface as well. Afterward, you can verify the change.

**Example 2-21** Configuring Interface Delay

```
R1# configure terminal
R1(config)# interface gi0/1
R1(config-if)# delay 100
R1(config-if)# do show interface Gigabit0/1 | i DLY
    MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 1000 usec,
```

**NOTE** Bandwidth modification with the interface parameter command `bandwidth bandwidth` has a similar effect on the metric calculation formula but can impact other routing protocols, such as OSPF, at the same time. Modifying the interface delay only impacts EIGRP.



## Custom K Values

If the default metric calculations are insufficient, you can change them to modify the path metric formula. K values for the path metric formula are set with the command **metric weights TOS K1 K2 K3 K4 K5 [K6]** under the EIGRP process. *TOS* always has a value of 0, and *K6* is used for named mode configurations.

To ensure consistent routing logic in an EIGRP autonomous system, the K values must match between EIGRP neighbors to form an adjacency and exchange routes. The K values are included as part of the EIGRP hello packet. The K values are displayed with the **show ip protocols** command, as demonstrated with the sample topology in Example 2-13. Notice that both routers are using the default K values, with R1 using classic metrics and R2 using wide metrics.

## Load Balancing

EIGRP allows multiple successor routes (with the same metric) to be installed into the RIB. Installing multiple paths into the RIB for the same prefix is called *equal-cost multipathing (ECMP)*. At the time of this writing, the default maximum ECMP setting is four routes. You change the default ECMP setting with the command **maximum-paths maximum-paths** under the EIGRP process in classic mode and under the topology base submode in named mode.

Example 2-22 shows the configuration for changing the maximum paths on R1 and R2 so that classic and named mode configurations are visible.

### Example 2-22 Changing the EIGRP Maximum Paths

```
R1# show run | section router eigrp
router eigrp 100
maximum-paths 6
network 0.0.0.0

R2# show run | section router eigrp
router eigrp EIGRP-NAMED
!
address-family ipv4 unicast autonomous-system 100
!
topology base
maximum-paths 6
exit-af-topology
network 0.0.0.0
eigrp router-id 192.168.2.2
exit-address-family
```



EIGRP supports unequal-cost load balancing, which allows installation of both successor routes and feasible successors into the EIGRP RIB. To use unequal-cost load balancing with EIGRP, change EIGRP's *variance multiplier*. The EIGRP *variance value* is the feasible distance (FD) for a route multiplied by the EIGRP variance multiplier. Any feasible successor's FD with a metric below the EIGRP variance value is installed into the RIB. EIGRP installs

multiple routes where the FD for the routes is less than the EIGRP variance value up to the maximum number of ECMP routes, as discussed earlier.

Dividing the feasible successor metric by the successor route metric provides the variance multiplier. The variance multiplier is a whole number, and any remainders should always round up.

Using the topology shown in Figure 2-2 and output from the EIGRP topology table in Figure 2-3, the minimum EIGRP variance multiplier can be calculated so that the direct path from R1 to R4 can be installed into the RIB. The FD for the successor route is 3328, and the FD for the feasible successor is 5376. The formula provides a value of about 1.6 and is always rounded up to the nearest whole number to provide an EIGRP variance multiplier of 2. Figure 2-14 shows the calculation.

$$\frac{\text{Feasible Successor FD}}{\text{Successor Route FD}} \leq \text{Variance Multiplier}$$

$$\frac{5376}{3328} \leq 1.6$$

$$2 = \text{Variance Multiplier}$$

**Figure 2-14** EIGRP Variance Multiplier Formula

The command `variance multiplier` configures the variance multiplier under the EIGRP process for classic configuration and under the topology base submode in named mode. Example 2-23 provides a sample configuration for each configuration mode.

### Example 2-23 Configuring EIGRP Variance

```
R1 (Classic Configuration)
router eigrp 100
 variance 2
 network 0.0.0.0

R1 (Named Mode Configuration)
router eigrp EIGRP-NAMED
 !
 address-family ipv4 unicast autonomous-system 100
 !
 topology base
  variance 2
 exit-af-topology
 network 0.0.0.0
 exit-address-family
```

Example 2-24 shows how to verify that both paths were installed into the RIB. Notice that the metrics for the paths are different. One path metric is 3328, and the other path metric is 5376. To see the traffic load-balancing ratios, you use the command `show ip route network`, as demonstrated in the second output. The load-balancing traffic share is highlighted.

### Example 2-24 Verifying Unequal-Cost Load Balancing

```
R1# show ip route eigrp | begin Gateway
Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
D       10.4.4.0/24 [90/5376] via 10.14.1.4, 00:00:03, GigabitEthernet0/2
          [90/3328] via 10.13.1.3, 00:00:03, GigabitEthernet0/1

R1# show ip route 10.4.4.0
Routing entry for 10.4.4.0/24
  Known via "eigrp 100", distance 90, metric 3328, type internal
  Redistributing via eigrp 100
  Last update from 10.13.1.3 on GigabitEthernet0/1, 00:00:35 ago
  Routing Descriptor Blocks:
  * 10.14.1.4, from 10.14.1.4, 00:00:35 ago, via GigabitEthernet0/2
    Route metric is 5376, traffic share count is 149
    Total delay is 110 microseconds, minimum bandwidth is 1000000 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 1
  10.13.1.3, from 10.13.1.3, 00:00:35 ago, via GigabitEthernet0/1
    Route metric is 3328, traffic share count is 240
    Total delay is 30 microseconds, minimum bandwidth is 1000000 Kbit
    Reliability 254/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 2
```

## References in This Chapter

Edgeworth, Brad, Foss, Aaron, and Garza Rios, Ramiro, *IP Routing on Cisco IOS, IOS XE, and IOS XR*, Cisco Press, 2014.

RFC 7868, *Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP)*, D. Savage, J. Ng, S. Moore, D. Slice, P. Paluch, and R. White. <http://tools.ietf.org/html/rfc7868>, May 2016.

Cisco, *Cisco IOS Software Configuration Guides*, <http://www.cisco.com>.

## Exam Preparation Tasks

As mentioned in the section “How to Use This Book” in the Introduction, you have a couple choices for exam preparation: the exercises here, Chapter 24, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep software.

## Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 2-8 lists these key topics and the page number on which each is found.

**Table 2-8** Key Topics

Key Topic Element	Description	Page Number
Paragraph	EIGRP terminology	76
Paragraph	Topology table	76
Table 2-3	EIGRP packet types	78
Paragraph	Forming EIGRP neighbors	79
Paragraph	Classic configuration mode	80
Paragraph	EIGRP named mode	80
Paragraph	Passive interfaces	88
Paragraph	Authentication	91
Paragraph	Path metric calculation	94
Paragraph	EIGRP attribute propagation	94
Figure 2-11	EIGRP wide metrics formula	97
Paragraph	Custom K values	100
Paragraph	Unequal-cost load balancing	100

## Define Key Terms

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

autonomous system (AS), successor route, successor, feasible distance, reported distance, feasibility condition, feasible successor, topology table, classic EIGRP configuration mode, EIGRP named mode configuration, passive interface, K values, wide metrics, variance value

## Use the Command Reference to Check Your Memory

The ENARSI 300-410 exam focuses on the practical, hands-on skills that networking professionals use. Therefore, you should be able to identify the commands needed to configure, verify, and troubleshoot the topics covered in this chapter.

This section includes the most important configuration and verification commands covered in this chapter. It might not be necessary to memorize the complete syntax of every command, but you should be able to remember the basic keywords that are needed.

To test your memory of the commands in Table 2-9, go to the companion website and download Appendix B, “Command Reference Exercises.” Fill in the missing commands in the tables based on each command description. You can check your work by downloading Appendix C, “Command Reference Exercise Answer Key,” from the companion website.

**Table 2-9** Command Reference

Task	Command Syntax
Initialize EIGRP in a classic configuration.	<b>router eigrp</b> <i>as-number</i> <b>network</b> <i>network wildcard-mask</i>
Initialize EIGRP in a named mode configuration.	<b>router eigrp</b> <i>process-name</i> <b>address-family</b> { <i>ipv4</i>   <i>ipv6</i> } { <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> } <b>autonomous-system</b> <i>as-number</i> <b>network</b> <i>network wildcard-mask</i>
Define the EIGRP router ID.	<b>eigrp router-id</b> <i>router-id</i>
Configure an EIGRP-enabled interface to prevent neighbor adjacencies.	Classic: <b>(EIGRP process)</b> <b>passive-interface</b> <i>interface-id</i>  Named mode: <b>af-interface</b> { <b>default</b>   <i>interface-id</i> } <b>passive-interface</b>
Configure a keychain for EIGRP MD5 authentication.	<b>key chain</b> <i>key-chain-name</i> <b>key</b> <i>key-number</i> <b>key-string</b> <i>password</i>
Configure MD5 authentication for an EIGRP interface.	Classic: <b>(EIGRP process)</b> <b>ip authentication key-chain eigrp</b> <i>as-number</i> <i>key-chain-name</i> <b>ip authentication mode eigrp</b> <i>as-number</i> <b>md5</b>  Named mode: <b>af-interface</b> { <b>default</b>   <i>interface-id</i> } <b>authentication key-chain eigrp</b> <i>key-chain-name</i> <b>authentication mode md5</b>
Configure SHA authentication for EIGRP named mode interfaces.	Named mode: <b>af-interface</b> { <b>default</b>   <i>interface-id</i> } <b>authentication mode hmac-sha-256</b> <i>password</i>
Modify the interface delay for an interface.	<b>delay</b> <i>tens-of-microseconds</i>
Modify the EIGRP K values.	<b>metric weights</b> <i>TOS K<sub>1</sub> K<sub>2</sub> K<sub>3</sub> K<sub>4</sub> K<sub>5</sub> [K<sub>6</sub>]</i>
Modify the default number of EIGRP maximum paths that can be installed into the RIB.	<b>maximum-paths</b> <i>maximum-paths</i>
Modify the EIGRP variance multiplier for unequal-cost load balancing.	<b>variance</b> <i>multiplier</i>
Display the EIGRP-enabled interfaces.	<b>show ip eigrp interface</b> [{ <i>interface-id</i> [ <b>detail</b> ]   <b>detail</b> }]
Display the EIGRP topology table.	<b>show ip eigrp topology</b> [ <b>all-links</b> ]
Display the configured EIGRP keychains and passwords.	<b>show key chain</b>
Display the IP routing protocol information configured on the router.	<b>show ip protocols</b>

*This page intentionally left blank*



# Index

## Symbols

---

- \* (asterisk), 497, 503, 507
- > (best-path symbol), 454
- [ ] (brackets), 497, 500–501
- ^ (caret), 497, 499–500
- [^] (caret in brackets), 497, 501
- \$ (dollar sign), 497, 500
- (hyphen), 497, 501
- () (parentheses), 497, 502
- . (period), 497, 502
- | (pipe), 497, 502
- + (plus sign), 497, 502
- ? (question mark), 497, 503
- \_ (underscore), 497, 498–499
- 2-Way state
  - OSPF (Open Shortest Path First), 230
  - OSPFv2 (Open Shortest Path First version 2), 318

## A

---

- AAA (authentication, authorization, and accounting)
  - definition of, 866. *See also* authentication
  - troubleshooting
    - authentication*, 871–873
    - authorization*, 873–874
    - verification of configuration*, 869–871
- aaa authentication login VTY\_ACCESS group RADIUSMETHOD local command, 870
- aaa authorization console command, 874
- aaa authorization exec command, 873
- aaa group server radius RADIUSMETHOD command, 870
- aaa group server tacacs+ TACACSMETHOD command, 870
- aaa new-model command, 869, 871
- ABRs (area border routers), 227, 264, 395, 695–696
- acacs server TACSRV1 command, 870
- access control lists. *See* ACLs (access control lists)
- access-class command, 848
- access-list command, 623
- accounting, 869. *See also* AAA (authentication, authorization, and accounting)
- Accumulated Interior Gateway Protocol (AIGP), 539–540, 588
- ACEs (access control entries), 622
- Acknowledgment packets (EIGRPv6), 191
- ACL-ALLOW, 495
- ACLs (access control lists)
  - AS\_Path, 503–505
  - BGP (Border Gateway Protocol), 566–567
  - components of, 622

CoPP (Control Plane Policing), 876–878

extended, 623–625

IPv4

- importance of*, 845
- packet filtering with*, 848
- reading*, 846–847
- time-based*, 848–850
- trouble ticket*, 845, 855–857

IPv6

- importance of*, 850
- packet filtering with*, 851–852
- reading*, 850–851
- trouble ticket*, 858–861

MPLS (Multiprotocol Label Switching), 754

named ACL configuration mode, 857

OSPFv2 (Open Shortest Path First version 2), 327–328

standard, 622–623

troubleshooting, 150–151, 201

**Active state (BGP), 434**

**AD (administrative distance), 38–41**

- BGP (Border Gateway Protocol), 154, 448, 580–582
- data structures and routing table, 39
- EIGRP (Enhanced Interior Gateway Routing Protocol), 86, 682–683
- OSPF (Open Shortest Path First), 238
- sources of routing information, 39–41

**Adaptive Security Appliance (ASA), 822**

**additive keyword, 515**

**address command, 828**

**address families, troubleshooting**

- BGP (Border Gateway Protocol), 430, 593
- OSPFv3 (Open Shortest Path First version 3)

- debug ospfv3 command*, 418
- default-information originate command*, 422
- sample configuration*, 408–410
- show ip protocols command*, 410–411
- show ip route ospfv3 command*, 418
- show ipv6 protocols command*, 410–411
- show ipv6 route command*, 420
- show ipv6 route ospf command*, 418
- show ospfv3 command*, 411–413
- show ospfv3 database command*, 415–418
- show ospfv3 interface brief command*, 413
- show ospfv3 interface command*, 413–414
- show ospfv3 ipv6 command*, 421
- show ospfv3 neighbor command*, 414
- show run | section router ospfv3 command*, 422
- trouble ticket*, 419–423

**address family identifier (AFI), 430**

**Address Resolution Protocol. *See* ARP (Address Resolution Protocol)**

**address-family [ipv4 | ipv6] [unicast | multicast] command, 81, 374, 442, 728**

**address-family [ipv4 | ipv6] vrf command, 741, 746**

**address-family command, 436, 730, 809**

**address-family ipv6 autonomous-system command, 192**

**address-family ipv6 command, 813**

**addressing**

- BGP (Border Gateway Protocol)
  - aggregate addresses*, 482–488
  - aggregation with suppression*, 485–488
  - atomic aggregate attribute*, 488–489
  - VRF-Lite configuration*, 746
- forwarding addresses, 667–670
- IPv4. *See* IPv4 (Internet Protocol version 4)
- IPv6. *See* IPv6 (Internet Protocol version 6)
- loopback addresses, 451–453
- MAC (media access control), 43–44
- OSPF (Open Shortest Path First), 745–746
- VPNv4, 757–759
- adjacency tables, 35
- Adj-RIB-in table, 440
- Adj-RIB-out table, 440, 447
- administrative distance. *See* AD (administrative distance)
- ADV Router field (OSPF LSDB), 265
- Advanced Encryption Standard (AES), 831
- ADVERTISE message, 29, 30
- advertisement tracking, 346–348
- Advertising Router field
  - Type 3 LSA (summary LSA), 275
  - Type 5 LSA (external LSA), 279
  - Type 7 LSA (NSSA external LSA), 283
- AES (Advanced Encryption Standard), 831
- AFI (address family identifier), 430
- af-interface command, 88, 89, 125, 128, 192
- af-interface default command, 84, 89, 92, 108, 125, 128, 192
- AFs. *See* address families, troubleshooting
- AGE field (OSPF LSDB), 265
- aggregate addresses (BGP), 482–488
- aggregate-address command, 482, 485, 489–490, 492, 573
- aggregation, route. *See* route aggregation
- AH (Authentication Header), 381
- AI Analytics, Cisco DNA Center Assurance, 937–938
- AIGP (Accumulated Interior Gateway Protocol), 539–540, 588
- all keyword, 456
- AllDRouters, 228, 373
- AllSPFRouters, 228, 373
- always-compare-med feature, 549
- any keyword, 829
- Any Transport over MPLS (AToM), 751
- APIPA (Automatic Private IP Addressing) address, 15–16
- area *area-id* authentication message-digest command, 255
- area *area-id* nssa [default-information-originate] command, 290
- area *area-id* nssa no-summary command, 293
- area *area-id* range command, 301
- area *area-id* stub command, 286, 409
- area *area-id* stub no-summary command, 288
- area *area-id* virtual-link command, 307–308
- area border routers (ABRs), 227, 264, 395, 695–696
- area flooding scope, 384
- area ID, 227
- area numbers, mismatched, 322–323
- area range command, 349

- area types, mismatched, 323–324
- areas, OSPF, 226–227
- ARP (Address Resolution Protocol), 248
  - cache, 32–33, 43–46
  - proxy, 44–46
- AS (Sub-AS) peering, 550
- AS confederations
  - confederation identifier, 462
  - configuration, 462–465
  - definition of, 462
  - topology, 462
- AS field (BGP), 438
- AS\_CONFED\_SEQUENCE, 464, 540
- AS\_Path filtering, 430, 497–505
  - AS\_Path ACLs, 503–505
  - AS\_Path length, 540–542
  - overview of, 497
  - regular expressions
    - asterisk (\*)*, 497, 503
    - BGP table for regex queries*, 498
    - brackets ([ ])*, 497, 500–501
    - caret (^)*, 497, 499–500
    - caret in brackets ([^])*, 497, 501
    - dollar sign (\$)*, 497, 500
    - hyphen (-)*, 497, 501
    - parentheses ()*, 497, 502
    - period (.)*, 497, 502
    - pipe (|)*, 497, 502
    - plus sign (+)*, 497, 502
    - question mark (?)*, 497, 503
    - regex reference topology*, 497
    - table of*, 497–503
    - underscore (\_)*, 497, 498–499
- AS\_SET, 489–491
- ASA (Adaptive Security Appliance), 822
- ASBRs (autonomous system boundary routers), 240, 277, 279–281, 347, 372, 395, 678–679
- AS-external LSAs (link-state advertisements), 373
- ASNs (autonomous number systems), 428–429, 591
- ASs (autonomous systems), 428
- assessing exam readiness, C25.0122-C25.0136
- asterisk (\*), 497, 503, 507
- ATM, 247
- AToM (Any Transport over MPLS), 751
- atomic aggregate attribute, 488–489
- Attempt state (OSPF), 230, 318
- authentication. *See also* AAA (authentication, authorization, and accounting)
  - BGP (Border Gateway Protocol), 570
  - certificate-based, 824
  - definition of, 869
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 88–91, 148–150, 199–200
  - HMAC-SHA-256 (Hashed Message Authentication Code-Secure Hash Algorithm-256), 92
  - IP NHRP, 794–795
  - MD5 (Message Digest 5), 91, 255–256, 326, 570
  - NHRP (Next Hop Resolution Protocol), 776
  - null, 326
  - origin, 824
  - OSPF (Open Shortest Path First), 253–254, 255–257
  - OSPFv2 (Open Shortest Path First version 2), 326–327

OSPFv3 (Open Shortest Path First version 3), 381–383  
 plaintext, 255, 326  
 pre-shared key, 824, 827–836  
   *complete IPsec DMVPN configuration*, 834  
   *DPD (Dead Peer Protection)*, 834  
   *IKEv2*, 828–830, 838–839  
   *IPsec packet replay protection*, 833–834  
   *IPsec profiles*, 832–833  
   *IPsec transform set*, 831–832  
   *NAT (Network Address Translation) keepalives*, 834  
   *tunnel interface encryption*, 833  
 SHA (Secure Hash Algorithm), 831  
 troubleshooting, 873–874  
 verification of, 836–838

authentication headers, 381, 824

authentication local {pre-share | rsa-sig} command, 829

authentication mode hmac-sha-256 command, 92

authentication remote {pre-share | rsa-sig} command, 829

authorization, 869–871. *See also* AAA (authentication, authorization, and accounting)

authorization exec default command, 874

autoconfiguration, MPLS (Multiprotocol Label Switching), 755

auto-cost reference-bandwidth command, 295

Automatic Private IP Addressing (APIPA) address, 15–16

automatic route summarization (EIGRP), 118

autonomous number systems (ASNs), 428–429

autonomous system boundary routers (ASBRs), 240, 277, 347, 372, 395, 678–679

autonomous system flooding scope, 384

autonomous system numbers, 142–143, 191, 198

autonomous systems (ASs), 75, 428, 526

autosummarization, 165–168

auto-summary command, 118

## B

---

backbone area, 227, 273

backup designated routers. *See* BDRs (backup designated routers)

backward compatibility, EIGRP (Enhanced Interior Gateway Routing Protocol) metrics, 98–99

bandwidth  
   EIGRP (Enhanced Interior Gateway Routing Protocol), 125–126  
   path metric calculation and, 94–96

bandwidth command, 781, 783

bandwidth-percent command, 125

BDRs (backup designated routers)  
   OSPF (Open Shortest Path First)  
     *concept of*, 242–243  
     *elections*, 244–245  
     *placement*, 245–246  
   OSPFv2 (Open Shortest Path First version 2), 341–344  
   OSPFv3 (Open Shortest Path First version 3), 373

best-path algorithm, BGP, 87  
   AS\_Path length, 540–542  
   AIGP (Accumulated Interior Gateway Protocol), 539–540

- best-path decision-making process, 588–591
- eBGP versus iBGP, 550
- local preference, 532–538
  - bgp default local-preference command*, 532
  - BGP edge evaluation of multiple paths*, 536–538
  - BGP tables after local preference modification*, 534–535
  - configuration*, 533–534
  - final BGP processing state*, 538
  - set local-preference command*, 532
  - topology*, 533
- locally originated route, 538
- lowest IGP metric, 551
- lowest neighbor address, 552
- MED (multi-exit discriminator)
  - always-compare-med feature*, 549
  - BGP deterministic MED*, 549–550
  - configuration*, 542–545
  - missing MED behavior*, 548–549
- minimum cluster list length, 552
- oldest (established) BGP session, 548
- origin type, 542–545
- overview of, 527–528
- path attribute classifications, 528
- RID (router ID), 551
- weight, 528–532
- bestpath keyword, 531
- best-path symbol (>), 454
- best-path-reason keyword, 531
- BFD (Bidirectional Forwarding Detection), 927–928
- bfd interface command, 928
- bfd interval command, 928
- BGP (Border Gateway Protocol), 553**
  - AS\_Path attribute, 430
  - address families, 430, 593
  - ASNs (autonomous number systems), 428–429, 591
  - ASs (autonomous systems), 428
  - best-path algorithm
    - AS\_Path length*, 540–542
    - AIGP (Accumulated Interior Gateway Protocol)*, 539–540
    - eBGP over iBGP*, 550
    - local preference*, 532–538
    - local route origination*, 538
    - lowest IGP metric*, 551
    - lowest neighbor address*, 552
    - MED (multi-exit discriminator)*, 545–550
    - minimum cluster list length*, 552
    - oldest (established) BGP session*, 548
    - Origin type*, 542–545
    - overview of*, 527–528
    - path attribute classifications*, 528
    - RID (router ID)*, 551
    - weight*, 528–532
  - communities
    - conditionally matching*, 512–514
    - enabling*, 508
    - extended*, 508
    - formats*, 508
    - local AS*, 511–512
    - new format*, 508
    - No\_Advertise*, 509–510
    - No\_Export*, 510–511
    - No\_Export\_SubConfed*, 511–512
    - overview of*, 507–508
    - private*, 514–516

- configuration
  - example of*, 436–437
  - required components*, 435
  - route advertisement*, 440–443
  - route receiving and viewing*, 443–448
  - simple eBGP topology*, 436–437
  - steps for*, 435–436
- configuration scalability
  - IOS XE peer groups*, 517–518
  - IOS XE peer templates*, 518–519
- connection collisions, 567
- definition of, 426
- eBGP (external BGP), 448
  - AD (administrative distance)*, 580–582
  - iBGP (internal BGP) compared to*, 453–454
  - next-hop manipulation*, 456–457
  - route verification*, 580–582
  - topologies*, 454–455
- ECMP (equal-cost multipathing), 553
- FSM (finite-state machine), 432
- iBGP (internal BGP), 429, 448–453
  - AD (administrative distance)*, 448, 580–582
  - benefits of*, 448–450
  - confederations*, 462–465
  - definition of*, 448
  - eBGP (external BGP) compared to*, 453–454
  - full mesh requirement*, 450
  - next-hop manipulation*, 456–457
  - peering using loopback addresses*, 451–453
  - prefix advertisement behavior*, 449
  - route reflectors*, 457–461
  - split horizon*, 579–580
  - topologies*, 454–455
- inter-router communication, 430–435
  - messages*, 431–432
  - neighbor states*, 432–435, 563
  - single- and multi-hop sessions*, 430–431
- loop prevention, 430
- maximum prefix, 516–517
- MP-BGP (Multiprotocol BGP)
  - IPv6 configuration*, 466–471
  - IPv6 over IPv4*, 471–475
  - topology*, 465–466, 593
- network selection, 623–625
- PAs (path attributes), 429
- path selection
  - best-path decision-making process*, 588–591
  - debug commands*, 592–593
  - private autonomous systems numbers*, 591
- port numbers, 567
- prefix attributes, 446
- redistribution
  - connected networks*, 657
  - nontransitive nature of*, 651–652
  - overview of*, 650–651
  - RIB (Routing Information Base) and*, 653–655
  - seed metrics*, 655–656, 688
  - sequential protocol redistribution*, 653
  - source-specific behaviors*, 657–658
  - trouble ticket: users in BGP autonomous system unable to access IPv4 resources*, 717–721
  - troubleshooting*, 699–702

## route filtering and manipulation

- AS\_Path*, 497–505
- AS\_Path ACLs*, 503–505
- BGP route processing logic*, 493–494
- clearing of BGP connections*, 507
- distribute list*, 495–496, 586–587
- overview of*, 493–495
- prefix list*, 496
- receiving and viewing*, 443–448
- reference BGP table*, 494–495
- regular expressions*, 497–503
- RIB (Routing Information Base) failures, verifying*, 582
- route advertisement*, 440–443
- route maps*, 505–507

## route refresh, 507

## route summarization

- aggregate addresses*, 482–488
- aggregation with suppression*, 485–488
- atomic aggregate attribute*, 488–489
- IPv6 summarization*, 492–493
- overview of*, 482
- route aggregation with AS\_SET*, 489–491

## sessions

- definition of*, 429
- summary fields*, 438
- verification of*, 437–440

## split-horizon rule, 579–580

## synchronization, 450

## tables and table fields, 440, 445

## timers, 572–573

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

## VRF-Lite configuration, 746

**BGP (Border Gateway Protocol) troubleshooting**

## benefits of, 556

## BGP for IPv6, 593–598

- MP-BGP configuration*, 594–598

- MP-BGP topology*, 593–594

## MP-BGP (Multiprotocol BGP), 593–598

- configuration*, 594–598

- MP-BGP topology*, 593–594

## neighbor adjacencies

- ACLs (access control lists)*, 566–567

- BGP packets sourced from wrong IP address*, 564–566

- incorrect neighbor statement*, 564

- interface is down*, 561

- Layer 3 connectivity is broken*, 561–562

- misconfigured peer groups*, 570–571

- mismatched authentication*, 570

- neighbor lacks route to local router*, 563

- neighbor verification*, 559–560

- overview of*, 559–561

- path to neighbor is through default route*, 562–563

- timers*, 572–573

- TTL (time to live) expiration*, 568–570

## path selection

- best-path decision-making process*, 588–591

- debug commands*, 592–593

- private autonomous systems numbers*, 591

- routes
    - examining in routing table, 573–574*
    - missing or bad network mask command, 575–576*
    - next-hop router not reachable, 577–579*
    - route filtering, 582–587*
    - split-horizon rule, 579–580*
  - trouble ticket: link between R1 and R3 not forwarding traffic to BGP AS 65501, 598–604
    - connectivity, verifying, 598–599*
    - neighbor adjacency verification, 602–603*
    - route confirmation, 603–604*
    - route examination, 599–602*
    - route verification, 602*
  - trouble ticket: MP-BGP default route not being learned, 615–617
  - trouble ticket: traffic out of autonomous system flowing through R3 and across backup link, 610–614
  - trouble ticket: users in 10.1.1.0/26 and 10.1.1.64/26 unable to access resources at 10.1.5.5, 604–610
    - advertised routes, 607*
    - BGP configuration on R1, 608*
    - BGP filters, 607*
    - BGP table, examining, 605–606*
    - connectivity, verifying, 604*
    - neighbor verification, 606*
    - prefix lists, 607–609*
    - route advertisement, 609–610*
  - bgp always-compare-med command, 549**
  - bgp bestpath med missing-as-worst command, 548**
  - bgp confederation identifier command, 462**
  - bgp confederation peers command, 464**
  - bgp default local-preference command, 532**
  - bgp deterministic-med command, 550**
  - BGP MED attribute, 464**
  - bgp redistribute-internal command, 658, 671, 699**
  - bgp router-id command, 435**
  - Bidirectional Forwarding Detection (BFD), 927–928**
  - binding table, IPv6 First-Hop Security, 885**
  - Border Gateway Protocol. *See* BGP (Border Gateway Protocol)**
  - boundary routers, 678, 687**
  - brackets ([ ]), 497, 500–501**
    - “brain dumps” 952
  - branch routers. *See* spoke routers**
  - Branch site, OSPFv3 trouble tickets**
    - Branch receiving inter-area routes other than default route, 401–404
    - Branch users unable to access IPv6-enabled resources on Internet, 419–423
    - Branch users unable to access resources outside Branch office, 404–408
    - topology, 401
  - broadcast networks, 246, 247, 331**
- 
- C**
- cache, NHRP (Next Hop Resolution Protocol), 787–791**
    - examples of, 789–791
    - NHRP mapping entries, 788
    - NHRP message flags, 788–789

- cache format record command, 924
- caret (^), 497, 499–500
- caret in brackets ([^]), 497, 501
- CE (customer edge) routers, 756
- CEF (Cisco Express Forwarding), 34–35, 927
- certificate-based authentication, 824
- Checksum field (OSPF LSDB), 265
- Cisco Adaptive Security Appliance (ASA), 822
- Cisco Certification Roadmap, 955
- Cisco dCloud, 952
- Cisco Devnet, 952
- Cisco DNA Center Assurance, 929–940
  - accessing, 929
  - AI Analytics, 937–938
  - Client Health page, 933–934
  - Command Runner, 938–940
  - Device 360 and Client 360 pages, 933–937
  - Issues and Events page, 938–939
  - Network Health page, 931–932
  - Network Time Travel, 937
  - Overall Health page, 930–931
  - overview of, 929
  - Path Trace, 936–937
- Cisco Express Forwarding (CEF), 34–35, 927
- Cisco IOS IP SLA troubleshooting, 910–917
  - debug ip sla trace 2 command, 916–917
  - IP SLA icmp-echo probe configuration, 911
  - IP SLA UDP-JITTER probe configuration, 911–912
  - show ip sla application command, 912–913
  - show ip sla configuration command, 913–914
  - show ip sla responder command, 915–916
  - show ip sla statistics command, 914–915
  - source and responder topology, 910–911
- Cisco Learning Network, 953
- Cisco nondisclosure agreement (NDA), 948
- Cisco VIRL (Virtual Internet Routing Lab), 952
- class maps, 878–880
- classic configuration mode (EIGRP), 80
- classic EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 191–192
- classic metric formula, EIGRP (Enhanced Interior Gateway Routing Protocol), 94–96
- classless networks, troubleshooting, 708–711
- clear bgp command, 507
- clear bgp ipv4 unicast \* soft out command, 609, 614
- clear ip bgp command, 507
- clear ip dhcp binding \* command, 17
- clear ip dhcp conflict \* command, 17
- clear ip nhrp command, 803
- clear ip ospf process command, 330
- clear line command, 895
- Client 360 page, Cisco DNA Center Assurance, 933–937
- Client Health page, Cisco DNA Center Assurance, 933–934
- clients, DHCP (Dynamic Host Configuration Protocol) for IPv4, 14–15
- Cluster List attribute (BGP), 461

- cluster list length, 552
- cluster-id attribute, 552
- C-network, 755
- collectors, NetFlow, 919
- command af-interface command, 84
- Command Runner, Cisco DNA Center Assurance, 938–940
- communication
  - BGP (Border Gateway Protocol), 430–435
    - messages*, 431–432
    - neighbor states*, 432–435, 563
    - single- and multi-hop sessions*, 430–431
  - EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 191
  - OSPF (Open Shortest Path First), 228
  - OSPFv3 (Open Shortest Path First version 3), 373–374
- communities, BGP (Border Gateway Protocol)
  - conditionally matching, 512–514
  - enabling, 508
  - extended, 508
  - formats, 508
  - local AS, 511–512
  - new format, 508
  - No\_Advertise, 509–510
  - No\_Export, 510–511
  - No\_Export\_SubConfed, 511–512
  - overview of, 507–508
  - private, 514–516
- COMMUNITY-CHECK, 514
- complex matching, 631–632
- component routes
  - definition of, 114–115
  - route summarization
    - automatic*, 118
    - hierarchical nature of*, 114
    - interface-specific*, 114–116
    - metrics*, 117
    - summary discard routes*, 116–117
- conditional forwarding
  - overview of, 634–635
  - PBR (policy-based routing)
    - configuration*, 635–637
    - local*, 637–639
  - trouble tickets: traffic routing from 10.1.4.0/24 to 10.1.1.0/24
    - topology*, 639
    - trouble ticket 15–1*, 639–643
    - trouble ticket 15–2*, 643–645
    - trouble ticket 15–3*, 645–646
- conditional matching
  - ACLs (access control lists). *See* ACLs (access control lists)
  - BGP (Border Gateway Protocol) communities, 512–514
  - prefix matching
    - prefix lists*, 627–628
    - prefix match specifications*, 625–627
  - route maps
    - complex matching*, 631–632
    - components of*, 628–629
    - conditional match options*, 629–631
    - continue keyword*, 634
    - multiple conditional match conditions*, 631
    - optional actions*, 632–634
    - processing order*, 628
- confederation identifier, 462
- confederations, iBGP (internal BGP), 462
  - configuration, 462–465

- definition of, 462
- topology, 462
- configuration.** *See also troubleshooting*
  - AAA (authentication, authorization, and accounting)
    - authentication*, 871–873
    - authorization*, 873–874
    - troubleshooting*, 869–874
  - ACLs (access control lists). *See* ACLs (access control lists)
  - BFD (Bidirectional Forwarding Detection), 927–928
  - BGP (Border Gateway Protocol). *See* BGP (Border Gateway Protocol)
  - Cisco DNA Center Assurance
    - accessing*, 929
    - Network Health page*, 931–932
    - Overall Health page*, 930–931
    - overview of*, 929
  - Cisco IOS IP SLA
    - debug ip sla trace 2 command*, 916–917
    - IP SLA icmp-echo probe configuration*, 911–912
    - IP SLA UDP-JITTER probe configuration*, 911–912
    - show ip sla application command*, 912–913
    - show ip sla configuration command*, 913–914
    - show ip sla responder command*, 915–916
    - show ip sla statistics command*, 914–915
    - source and responder topology*, 911
  - class maps, 878–880
  - DMVPN (Dynamic Multipoint Virtual Private Network) tunnels
    - front door VRF (FVRF)*, 809–810
    - on hub routers*, 780–781
    - IP NHRP authentication*, 794–795
    - overview of*, 779–780
    - for phase 3 DMVPN (multipoint)*, 792–793
    - on spoke routers*, 782–784
  - EIGRP (Enhanced Interior Gateway Routing Protocol)
    - AD (administrative distance)*, 41, 154, 682–683
    - authentication*, 88–91
    - classic configuration mode*, 80
    - failure detection and timers*, 108–114
    - installed routes, displaying*, 86–87
    - interfaces*, 84–85
    - IP bandwidth percentage*, 125–126
    - named configuration mode*, 80–81
    - neighbor adjacencies*, 85–86
    - network statement*, 81–82, 144–145
    - passive interfaces*, 88–91
    - RID (router ID)*, 87–88
    - route filtering*, 129–132
    - route summarization*, 114–118
    - sample topology and configuration*, 83–84
    - split horizon*, 126–129
    - stub feature*, 158–160
    - stub routers*, 119–121
    - stub site functions*, 121–125
    - traffic steering with offset lists*, 132–135
  - EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6)

- classic mode*, 191–192
  - named mode*, 192
  - verification of*, 193–195
- Flexible NetFlow, 923–927
- GRE (Generic Routing Encapsulation) tunnels, 769–774
  - path verification*, 774
  - routing table with GRE tunnel*, 773–774
  - routing table without GRE tunnel*, 770
  - sample configuration*, 771–772
  - steps for*, 770–771
  - topology*, 769–770
  - tunnel parameters*, 773
- IPv4
  - AD (administrative distance)*, 38–41
  - APIPA (Automatic Private IP Addressing) address*, 15–16
  - DHCP (Dynamic Host Configuration Protocol)*, 11–18
  - overview of*, 2–3, 7
  - packet-forwarding process*, 31–38
  - static routes*, 42–46, 61–64
  - structure of*, 7–10
  - subnets*, 10–11
  - verification of*, 9–10
- IPv6
  - AD (administrative distance)*, 38–41
  - DHCPv6 messages*, 29–30
  - DHCPv6 relay agents*, 30–31
  - example of*, 19
  - IEEE EUI-64 standard*, 20–22
  - IPv6 over IPv4*, 471–475
  - MP-BGP (Multiprotocol BGP)*, 466–471
  - overview of*, 3, 19–20
  - packet-forwarding process*, 31–38
  - SLAAC (stateless address autoconfiguration)*, 22–27
  - stateful DHCPv6*, 27–28
  - stateless DHCPv6*, 28–29
  - static routes*, 46–48, 64–66
  - verification of*, 19–20
- IPv6 DMVPN (Dynamic Multipoint Virtual Private Network)
  - correlation of IPv4-to-IPv6 transport protocol commands*, 812
  - display commands*, 813
  - DMVPN tunnel technique and*, 812
  - IPv6 DMVPN verification*, 816–817
  - IPv6-over-IPv6 sample configuration*, 813–815
  - tunneled protocol commands*, 811–812
- NetFlow, 919–923
- Object Tracking, 917–919
- OSPF (Open Shortest Path First)
  - confirmation of interfaces*, 235–237
  - default route advertisement*, 241–242
  - discontiguous networks*, 305–306
  - distribute lists*, 683–684
  - external OSPF routes*, 240–241
  - installed routes, displaying*, 238–239
  - interface columns*, 237
  - interface-specific*, 233

- neighbor adjacencies*, 237–238
- network statement*, 232–233, 234
- network types*, 246–254
- overview of*, 232
- route tags*, 684–686
- sample topology and configuration*, 233–235
- stubby areas*, 284–294, 339–340
- virtual links*, 307–309
- OSPF (Open Shortest Path First) route summarization
  - external summarization*, 303–305
  - impact on SPF topology calculation*, 299–301
  - inter-area summarization*, 301–303
  - LSA reduction through area segmentation*, 298–299
  - topology example with summarization*, 300–301
- OSPFv3 (Open Shortest Path First version 3)
  - address families. See address families, troubleshooting*
  - authentication*, 381–383
  - IPv6 addressing*, 375–376
  - IPv6 route summarization*, 379–380
  - link-local forwarding*, 383–384
  - network type*, 380–381
  - process for*, 374
  - topology*, 374–375
  - verification of*, 377–378
- PBR (policy-based routing), 635–637, 638
- policy maps, 880–882
- redistribution
  - BGP topology and configuration*, 670–672
  - commands*, 656–657
  - EIGRP topology and configuration*, 658–661
  - EIGRP-to-EIGRP mutual redistribution*, 661–663
  - OSPF forwarding address*, 667–670
  - OSPF topology and configuration*, 663–666
  - OSPF-to-OSPF mutual redistribution*, 666–667
  - protocol-specific*, 656–657
- SCP (Secure Copy Protocol), 902–903
- SNMP (Simple Network Management Protocol), 906–910
- static routes
  - IPv4*, 42–46, 61–64
  - IPv6*, 46–48, 64–66
- stubby areas, 339–340
  - not-so-stubby-areas (NSSAs)*, 289–292
  - overview of*, 284
  - stub areas*, 284–287
  - totally not-so-stubby-areas (NSSAs)*, 292–294
  - totally stubby areas*, 287–289
- syslog, 904–905
- VRF-Lite
  - EIGRP configuration for multiple VRF instances*, 741
  - EIGRP neighbors*, 742–743
  - EIGRP routes in VRF routing table*, 743–744
  - instance creation*, 728–730
  - interface assignment*, 730–731
  - interface IPv4 and IPv6 addresses*, 733–734

- interface participation in EIGRP processes*, 741–742
  - IPv4 global routing table, 735
  - IPv4 VRF routing tables, 735–736
  - MP-BGPv4 address families for multiple VRF instances, 746
  - OSPFv3 address families for multiple VRF instances, 745–746
  - overview of, 728
  - RED VRF instance routing table, 741
  - route distinguishers, 746–747
  - route targets, 747
  - subinterfaces on R1, 732–733
  - VRF connectivity, 744–745
  - VRF instances on R1, 733–734
  - VRF instances on R2, 736–738
  - VRF instances on R3, 738–740
  - CONFIRM message, 30
  - Connect state (BGP), 433–434
  - connected network redistribution, 657
  - connection collisions (BGP), 567
  - ConnectRetry timer, 433
  - console access, troubleshooting, 893–894
  - continue keyword, 634
  - control plane, 35, 883–885
  - convergence, EIGRP (Enhanced Interior Gateway Routing Protocol), 109–112
  - CoPP (Control Plane Policing), 875–885
    - definition of, 866
    - troubleshooting
      - ACL (*access control list*) configuration, 876–878
      - class map configuration, 878–880
      - overview of, 875–876, 885
      - policy map configuration, 880–882
      - service policy applied to control plane interface, 883–885
  - copy command, 900, 901, 902, 903
  - crypto ikev2 cookie-challenge command, 838
  - crypto ikev2 dpd command, 834
  - crypto ikev2 keyring command, 828
  - crypto ikev2 limit command, 838
  - crypto ikev2 profile command, 829
  - crypto ipsec profile command, 832
  - crypto ipsec security-association replay window-size command, 834
  - crypto ipsec transform-set command, 831–832
  - crypto isakmp nat keepalive command, 834
  - crypto key generate rsa modulus command, 897
  - custom K values, EIGRP (Enhanced Interior Gateway Routing Protocol) metrics, 100
  - customer edge (CE) routers, 756
- ## D
- 
- data availability, 822
  - data confidentiality, 822, 824
  - data integrity, 822, 824
  - data plane, 35
  - database description (DBD) packets, 228
  - Database description packet (OSPFv3), 374
  - DBD (database description) packets, 228

- dCloud, 952
- dead interval timer, 255
- Dead Peer Protection (DPD), 834
- debug aaa authentication command, 873
- debug aaa protocol local command, 873
- debug eigrp packet command, 906
- debug eigrp packet hello command, 906
- debug eigrp packets command
  - authentication, 150
  - incorrect network statement, 145
  - mismatched autonomous system numbers, 143
  - passive interfaces, 146–147
- debug ip bgp command, 592, 593
- debug ip bgp updates command, 593
- debug ip dhcp server events command, 18
- debug ip dhcp server packet command, 18
- debug ip http client all command, 901
- debug ip nat translations command, 906
- debug ip ospf adj command, 323, 327
- debug ip ospf hello command, 321–322, 324
- debug ip policy command, 638–639, 643
- debug ip routing command, 592, 681
- debug ip scp command, 903
- debug ip sla trace 2 command, 916–917
- debug ipv6 ospf hello command, 406
- debug ospfv3 command, 418
- debug radius authentication command, 873
- debugging. *See* troubleshooting
- DECLINE message, 30
- DECnet, 769
- deep packet inspection (DPI), 754
- default route advertisement
  - EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 196
  - OSPF (Open Shortest Path First), 241–242
  - OSPFv2 (Open Shortest Path First version 2) troubleshooting, 353
- default-information originate command, 241, 290, 353, 422, 422
- default-metric command, 549, 658, 659, 679, 688, 706
- delay, path metric calculation and, 94–96, 99–100
- deny ipv6 any any log command, 850–851
- deny statements, 130
- deny tcp any any eq bgp command, 567
- designated routers (DRs)
  - OSPF (Open Shortest Path First)
    - concept of*, 242–243
    - elections*, 244–245
    - placement*, 245–246
  - OSPFv2 (Open Shortest Path First version 2), 341–344
  - OSPFv3 (Open Shortest Path First version 3), 373
- Destination Guard, 887
- destination protocols, 651
- destination-specific redistribution behaviors
  - EIGRP (Enhanced Interior Gateway Routing Protocol)
    - EIGRP-to-EIGRP mutual redistribution*, 661–663
    - topology and configuration*, 658–661

- OSPF (Open Shortest Path First)
  - BGP topology and configuration*, 670–672
  - OSPF forwarding address*, 667–670
  - OSPF-to-OSPF mutual redistribution*, 666–667
  - topology and configuration*, 663–666
- Device 360 page, Cisco DNA Center Assurance, 933–937
- device LSAs (link-state advertisements), 373
- device management troubleshooting
  - console access, 893–894
  - overview of, 893
  - remote transfer, 899–903
    - FTP (File Transfer Protocol)*, 901–902
    - HTTP (Hypertext Transfer Protocol)*, 900–901
    - HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer)*, 900–901
    - SCP (Secure Copy Protocol)*, 902–903
    - TFTP (Trivial File Transfer Protocol)*, 899–900
  - vtty access, 894–899
    - password encryption levels*, 898–899
    - SSH (Secure Shell)*, 897–898
    - Telnet*, 895–897
- Devnet, 952
- DHCP (Dynamic Host Configuration Protocol) for IPv4, 2
  - clients, 14–15
  - DHCP-assigned IP addresses, verifying, 15–16
  - DORA process, 11–12
    - messages, 14
    - purpose of, 11
    - relay agents, 12–14
    - servers, 15
    - troubleshooting commands, 17–18
    - troubleshooting issues, 16–17
- dhcp option (ip address command), 14
- DHCPACK message, 14
- DHCPDECLINE message, 14
- DHCPDISCOVER message, 12, 14, 15–16
- DHCPINFORM message, 14
- DHCPNAK message, 14
- DHCPOFFER message, 12, 14
- DHCPRELEASE message, 14
- DHCPREQUEST message, 12, 14
- DHCPv6 (Dynamic Host Configuration Protocol version 6)
  - DHCPv6 Guard, 886
  - messages, 29–30
  - relay agents, 30–31
  - stateful, 27–28
  - stateless, 28–29
- diffusing update algorithm (DUAL), 74–75, 108, 109–111, 129, 655
- Digital Subscriber Line (DSL), 11–12
- Dijkstra's shortest path first (SPF) algorithm, 225, 294, 314, 392. *See also* OSPF (Open Shortest Path First)
- discard route, 116–117
- discontiguous networks
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 165–167
  - OSPF (Open Shortest Path First), 305–306
  - OSPFv2 (Open Shortest Path First version 2), 350–352

- distance bgp command, 683
- distance command, 682, 683
- distance eigrp command, 682–683
- distance ospf command, 683
- distribute list filtering, 495–496, 586–587
- distribute-list command, 129–132
- distribute-list prefix-list command, 201–202
- distribution list filtering (EIGRP), 129–132
- divide-and-conquer method, 31
- DMVPN (Dynamic Multipoint Virtual Private Network) tunnel security. *See also* DMVPN (Dynamic Multipoint Virtual Private Network) tunnels
- data availability, 822
- data confidentiality, 822, 824
- data integrity, 822, 824
- ESP modes, 825–827
- IKEv2 protection, 838–839
- key management, 824
- overview of, 821–823
- perfect forward secrecy, 824
- pre-shared key authentication, 827–836
  - complete IPsec DMVPN configuration, 834*
  - DPD (Dead Peer Protection), 834*
  - IKEv2 keyring, 828–829*
  - IKEv2 profile, 829–830*
  - IPsec packet replay protection, 833–834*
  - IPsec profiles, 832–833*
  - IPsec transform set, 831–832*
  - NAT (Network Address Translation) keepalives, 834*
  - tunnel interface encryption, 833*
  - SAs (security associations), 825*
  - secure transport, elements of, 821–823*
  - security protocols, 824*
  - verification of, 836–838*
- DMVPN (Dynamic Multipoint Virtual Private Network) tunnels, 34, 862–863. *See also* DMVPN (Dynamic Multipoint Virtual Private Network) tunnel security
- benefits of, 776–777
- configuration
  - on hub routers, 780–781*
  - IP NHRP authentication, 794–795*
  - overview of, 779–780*
  - for phase 3 DMVPN (multipoint), 792–793*
  - on spoke routers, 782–784*
- default-metric command, 766
- failure detection and high availability, 810–811
- GRE (Generic Routing Encapsulation)
  - configuration, 769–774*
  - definition of, 769*
  - mGRE (Multipoint GRE), 769*
- hub redundancy, 811
- IPv6 DMVPN configuration
  - correlation of IPv4-to-IPv6 transport protocol commands, 812*
  - display commands, 813*
  - DMVPN tunnel technique and, 812*
  - IPv6 DMVPN verification, 816–817*
  - IPv6-over-IPv6 sample configuration, 813–815*
  - tunneled protocol commands, 811–812*

- NHRP (Next Hop Resolution Protocol)
    - cache, viewing, 787–791*
    - holdtime, 810*
    - messages, 774–776*
    - NHRP mapping with spoke-to-hub traffic, 798–800*
    - NHSs (next-hop servers), 774–776*
    - shortcuts, 777*
    - timeout, 810–811*
    - unique IP NHRP registration, 794–795*
  - overlay networks, 806–810
    - definition of, 769*
    - front door VRF (FVRF), 808–810*
    - outbound interface selection, 808*
    - recursive routing problems, 806–807*
  - phases of, 777–778
  - split horizon and, 128
  - spoke-to-spoke communication
    - initiation of traffic between spoke routers, 795*
    - NHRP mapping with spoke-to-hub traffic, 798–800*
    - NHRP routing table manipulation, 800–806*
    - spoke-to-spoke tunnel formation, 796–800*
  - tunnel status, viewing, 784–787
  - DNS lookup, 8
  - dollar sign (\$), 497, 500
  - DORA process, 11–12
  - Down state
    - GRE (Generic Routing Encapsulation), 771
    - OSPF (Open Shortest Path First), 230
    - OSPFv2 (Open Shortest Path First version 2), 318
  - DPD (Dead Peer Protection), 834
  - DPI (deep packet inspection), 754
  - DROTHERs, 237
  - DRs (designated routers)
    - OSPF (Open Shortest Path First)
      - concept of, 242–243*
      - elections, 244–245*
      - placement, 245–246*
    - OSPFv2 (Open Shortest Path First version 2), 341–344
    - OSPFv3 (Open Shortest Path First version 3), 373
  - DSL (Digital Subscriber Line), 11–12
  - DUAL (diffusing update algorithm), 74–75, 108, 109–111, 129, 655
  - duplicate IP addresses, 17
  - duplicate router IDs, 330, 344–346
  - Dynamic Host Configuration Protocol (DHCP), 2
  - Dynamic Multipoint Virtual Private Network. *See* DMVPN (Dynamic Multipoint Virtual Private Network) tunnels
- 
- ## E
- E1 external routes, OSPF (Open Shortest Path First), 297
  - E2 external routes, OSPF (Open Shortest Path First), 297–298
  - EAP (Extensible Authentication Protocol), 825
  - earplugs, 946
  - eBGP (external BGP), 448, 553. *See also* BGP (Border Gateway Protocol) troubleshooting
  - AD (administrative distance), 580–582
    - in BGP best-path algorithm, 550

- iBGP (internal BGP) compared to, 453–454
- multipath, 553
- next-hop manipulation, 456–457
- route verification, 580–582
- topologies, 454–455
- ECMP (equal-cost multipathing), 298, 553
- edge LSRs (label switching routers), 748–749
- edge routes, BGP (Border Gateway Protocol)
  - BGP edge evaluation of multiple paths, 536–538
  - final BGP processing state, 538
  - initial BGP edge route processing, 535–536
- EGP (Exterior Gateway Protocol), 556
- egress LSRs (label switching routers), 748–749
- EIGRP (Enhanced Interior Gateway Routing Protocol), 83–84
  - autonomous system numbers, 191
  - autonomous systems, 75
  - configuration
    - AD (administrative distance)*, 41, 154, 682–683
    - authentication*, 91–94
    - classic configuration mode*, 80
    - installed routes, displaying*, 86–87
    - interfaces*, 84–85
    - named configuration mode*, 80–81
    - neighbor adjacencies*, 85–86
    - network statement*, 81–82, 144–145
    - passive interfaces*, 88–91
    - RID (router ID)*, 87–88
    - sample topology and configuration*, 83–84
  - definition of, 72
  - DUAL (diffusing update algorithm), 74–75
  - failure detection and timers, 108–109
    - configuration*, 113–114
    - convergence*, 109–112
    - hello timer*, 108–109
    - hold timer*, 108–109
    - SIA (stuck in active) queries*, 112–114
  - GRE (Generic Routing Encapsulation)
    - configuration and, 771–773
  - hello packets, 108, 180–184
  - named mode, 771
  - neighbors, 77–79
    - forming*, 79
    - inter-router communication*, 78–79
  - packet types, 78
  - path metric calculation
    - classic metric formula*, 94–96
    - custom K values*, 100
    - interface delay settings*, 99
    - load balancing*, 100–102
    - metric backward compatibility*, 98–99
    - wide metrics*, 96–98
  - PDMs (protocol-dependent modules), 75
  - redistribution
    - connected networks*, 657
    - EIGRP-to-EIGRP mutual redistribution*, 661–663
    - nontransitive nature of*, 651–652
    - overview of*, 650–651
    - RIB (Routing Information Base) and*, 653–655

- seed metrics*, 655–656, 688
- sequential protocol redistribution*, 653
- topology and configuration*, 658–661
- troubleshooting*, 689–694
- reverse routes
  - definition of*, 127
  - split horizon*, 126–129
- route manipulation
  - definition of*, 129
  - route filtering*, 129–132
  - traffic steering with offset lists*, 132–135
- route summarization
  - automatic*, 118
  - hierarchical nature of*, 114
  - interface-specific*, 114–116
  - metrics*, 117
  - summary discard routes*, 116–117
- terminology for, 75–76
- topology table, 76–77
- troubleshooting. *See* EIGRP (Enhanced Interior Gateway Routing Protocol) troubleshooting
- variance value/variance multiplier, 100–102
- VRF-Lite configuration
  - EIGRP configuration for multiple VRF instances*, 741
  - EIGRP neighbors*, 742–743
  - EIGRP routes in VRF routing table*, 743–744
  - interface participation in EIGRP processes*, 741–742
- WAN considerations
  - EIGRP stub routers*, 119–121
  - IP bandwidth percentage*, 125–126
  - split horizon*, 126–129, 161–162
  - stub site functions*, 121–125
- EIGRP (Enhanced Interior Gateway Routing Protocol) troubleshooting**
  - autosummarization, 165–168
  - discontiguous networks, 165–167
  - feasible successors, 161–162
  - load balancing, 168–169
  - neighbor adjacencies
    - ACLs (access control lists)*, 150–151
    - authentication*, 148–150
    - different subnets*, 148
    - incorrect network statement*, 144–145
    - interface is down*, 142
    - mismatched autonomous system numbers*, 142–143
    - mismatched K values*, 145–146
    - overview of*, 141–151
    - passive interface feature*, 146–148
    - timers*, 151
- routes
  - bad or missing network command*, 152–154
  - better source of information*, 154–157
  - interface is shut down*, 160
  - missing*, 151–152
  - route filtering*, 157–158
  - split horizon*, 161–162
  - stub configuration*, 158–160
- trouble tickets: users in 10.1.1.0/24
  - unable to access resources in 10.1.3.0/24, 169–184
  - trouble ticket 4–1*, 169–176

- trouble ticket 4–2, 177–180*
  - trouble ticket 4–3, 180–184*
- trouble tickets: users unable to access resources outside their LAN, 215
- eigrp router-id command, 87, 192, 192**
- eigrp stub command, 120–121, 158, 212–213**
- eigrp stub-site command, 124**
- EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6)**
  - classic, 191–192
  - configuration
    - classic mode, 191–192*
    - named mode, 192*
    - verification of, 193–195*
  - default route advertising, 196
  - definition of, 188
  - inter-router communication, 191
  - IPv6 route summarization, 195–196
  - named
    - configuration, 192*
    - trouble ticket: users unable to access resources outside their LAN, 213–218*
    - troubleshooting, 204–209*
- neighbor issues, troubleshooting
  - ACLs (access control lists), 201*
  - interface not participating in routing process, 200*
  - IPv6 interface status, 198*
  - mismatched authentication, 199–200*
  - mismatched autonomous system numbers, 198*
  - mismatched K values, 198*
  - neighbor verification, 197–198*
  - passive interfaces, 198–199*
  - timers, 200*
- packet types, 191
- route filtering, 197
- route troubleshooting, 201–204
  - AD (administrative distance) verification, 201*
  - interface not participating in routing process, 201*
  - route filtering, 201–202*
  - split horizon, 203–204*
  - stub configuration, 202–203*
- trouble ticket: users unable to access Internet, 209–213
  - link-local address verification, 211*
  - neighbor adjacencies, 210–211*
  - ping command, 209–210*
  - route verification, 210*
- trouble ticket: users unable to access resources outside their LAN, 213–218
  - configuration modification, 217*
  - configuration review, 215–217*
  - EIGRP-learned routes verification, 217*
  - IPv4 routing tables, 214–215*
  - learned IPv6 route verification, 211–212*
  - link-local address verification, 211*
  - neighbor adjacencies, 210–211*
  - ping command, 209–210, 213–218*
  - route filtering, 212–213*
  - route verification, 210, 213*
- elections, DR/BDR, 244–245
- ENARSI 300–410 exam preparation.**
  - See exam preparation*
- ENARSI\_BGP\_FILTER, 613**
- ENARSI\_IBGP\_NEIGHBORS, 613**

- encapsulating interface, DMVPN (Dynamic Multipoint Virtual Private Network) hub configuration, 780
- Encapsulating Security Payload (ESP), 381, 824, 825–827
- encapsulation failure, 45
- encapsulation overhead for tunnels, 771
- encryption. *See also* IPsec, DMVPN tunnel protection
  - AES (Advanced Encryption Standard), 831
  - IPsec
    - authentication*, 824
    - data availability*, 822
    - data confidentiality*, 822, 824
    - data integrity*, 822, 824
    - elements of*, 821–823
    - ESP modes*, 825–827
    - IKEv2 protection*, 838–839
    - key management*, 824, 825
    - overview of*, 821–823
    - perfect forward secrecy*, 824
    - pre-shared key authentication*, 827–836
    - SAs (security associations)*, 825
    - security protocols*, 824
    - SPI (Security Parameter Index)*, 381–382
    - tunnel protection*, 827–839
    - verification of*, 836–838
  - password encryption levels, 898–899
- entropy label, 754
- equal-cost multipathing (ECMP), 298, 553
- error messages, NHRP (Next Hop Resolution Protocol), 775
- ESP (Encapsulating Security Payload), 381, 824, 825–827
- Established state (BGP), 435
- eui-64 keyword, ipv6 address command, 21–22
- EUI-64 standard, 20–22
- exam preparation
  - assessing exam readiness, C25.0122-C25.0136
  - exam updates, 954–956
  - exam-day advice, 956-C25.0083
  - failed attempts
    - note-taking after*, C25.0068-C25.0083
    - study suggestions after*, C25.0138-C25.0146
  - final thoughts on, C25.0163-C25.0165
  - practice exams
    - exam scores*, C25.0122-C25.0136
    - tips for*, C25.0085-C25.0120
  - pre-exam suggestions, 954–956
  - resources, 952–953
  - study tasks, C25.0148-C25.0161
- Exchange state
  - OSPF (Open Shortest Path First), 230
  - OSPFv2 (Open Shortest Path First version 2), 319
- exec command, 894
- exec-timeout command, 894
- exit-af-interface command, 84
- exit-af-topology command, 84
- explicit NULL label, 755
- ExStart state
  - OSPF (Open Shortest Path First), 230
  - OSPFv2 (Open Shortest Path First version 2), 318
- extended BGP (Border Gateway Protocol) communities, 508
- extended IPv4 ACLs (access control lists), 846–847

Extensible Authentication Protocol (EAP), 825

Exterior Gateway Protocol (EGP), 556

external BGP (Border Gateway Protocol) sessions. *See* eBGP (external BGP)

external LSAs (link-state advertisements), 277–279

external OSPF (Open Shortest Path First), 240–241

  E1 and N1 external routes, 297

  E2 and N2 external routes, 297–298

External Route Tag field

  Type 5 LSA (external LSA), 279

  Type 7 LSA (NSSA external LSA), 283

external summarization, OSPF (Open Shortest Path First), 303–305

## F

---

failed exam attempts

  note-taking after, C25.0068-C25.0083

  study suggestions after, C25.0138-C25.0146

failure detection

  DMVPN (Dynamic Multipoint Virtual Private Network) tunnels, 810–811

  EIGRP (Enhanced Interior Gateway Routing Protocol)

*convergence*, 109–112

*hello timer*, 108–109

*hold timer*, 108–109

*SIA (stuck in active) queries*, 112–114

  OSPF (Open Shortest Path First), 254–255

FD (feasible distance), 76, 100–101, 109, 162–165

feasibility conditions, 76

feasible successors, 76, 162–165

FEC (forwarding equivalence class), 749

FIB (Forwarding Information Base), 35

File Transfer Protocol (FTP), 901–902

filtering of routes

  with ACLs (access control lists), 848

  BGP (Border Gateway Protocol), 582–587

*AS\_Path*, 497–505

*BGP route processing logic*, 493–494

*clearing of BGP connections*, 507

*distribute list*, 495–496, 586–587

*overview of*, 493–495

*prefix list*, 496

*reference BGP table*, 494–495

*regular expressions*, 497–503

*route maps*, 505–507

  EIGRP (Enhanced Interior Gateway Routing Protocol), 129–132, 157–158

  EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 197, 201–202

  OSPFv2 (Open Shortest Path First version 2), 337–339

**FILTERROUTES**, 519

finite-state machine (FSM), 432

First-Hop Security (IPv6), 885–887

  binding table, 885

  definition of, 866

  Destination Guard, 887

  DHCPv6 Guard, 886

  IPv6 snooping, 886

  Prefix Guard, 887

  RA (router advertisement) Guard, 886

  Source Guard, 887

Flexible NetFlow troubleshooting, 923–927

floating static routes, 918–919

flooding

- LSA (link-state advertisement), 264
- OSPF (Open Shortest Path First), 264–265, 277
- OSPFv3 (Open Shortest Path First version 3) configuration, 384–390

flow, definition of, 919

flow cache, 919

flow monitors, 924–927

flow records, 923–924

forward transit NHS record, 775

forwarding address, OSPF (Open Shortest Path First), 667–670

forwarding equivalence class (FEC), 749

Forwarding Information Base (FIB), 35

forwarding process, 31–38. *See also* conditional forwarding

- basic routing, 31–35
- basic routing topology, 31–32
- troubleshooting, 35–38
  - show adjacency detail command*, 38
  - show ip arp command*, 37
  - show ip cef command*, 37
  - show ip cef exact-route command*, 37
  - show ip nbrp command*, 38
  - show ip route command*, 35–36

Frame Relay, 128, 247–248

FSM (finite-state machine), 432

FTP (File Transfer Protocol), 901–902

full mesh requirement, iBGP (internal BGP), 450

Full state

- OSPF (Open Shortest Path First), 230

OSPFv2 (Open Shortest Path First version 2), 319

FVRF (front door VRF), 808–810. *See also* VRF (virtual routing and forwarding)

- configuration, 809–810
- definition of, 808
- static routes, 810

## G

---

gateway command, 130

global OSPFv3 settings, 395–396

GRE (Generic Routing Encapsulation) tunnels, 766, 826–827

- configuration, 769–774
  - path verification*, 774
  - routing table with GRE tunnel*, 773–774
  - routing table without GRE tunnel*, 770
  - sample configuration*, 771–772
  - steps for*, 770–771
  - topology*, 769–770
  - tunnel parameters*, 773
- definition of, 769
- mGRE (Multipoint GRE), 769

groups, peer, 517–518, 570–571

## H

---

hairpinning, 792

hashed message authentication code (HMAC), 898

Hashed Message Authentication Code-Secure Hash Algorithm-256 (HMAC-SHA-256), 92

HDLC (High-Level Data Link Control), 34

- headers, authentication, 824
  - headquarters/data center routers. *See* hub routers
  - Hello packets
    - EIGRP (Enhanced Interior Gateway Routing Protocol), 78, 180–184
    - EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 191
    - OSPF (Open Shortest Path First), 228, 229
    - OSPFv3 (Open Shortest Path First version 3), 374
  - Hello timer, 108–109, 255
  - hello-interval command, 108
  - hierarchical tree spoke-to-spoke phase, DMVPN, 777
  - high availability, 810–811
  - High-Level Data Link Control (HDLC), 34
  - high-order bit count, 624
  - high-order bit pattern, 624
  - HMAC (hashed message authentication code), 898
  - HMAC-SHA-256 (Hashed Message Authentication Code-Secure Hash Algorithm-256), 92
  - Hold timer, 108–109
  - holdtime (NHRP), 810
  - hold-time command, 108
  - hostname command, 897
  - hosts, SNMP (Simple Network Management Protocol), 910
  - how ospfv3 interface brief command, 377–378
  - how policy-map command, 882
  - HTTP (Hypertext Transfer Protocol), 900–901
  - HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer), 900–901
  - hub redundancy, 811
  - hub routers, 780–781
  - hub-and-spoke topology, 126–129
  - Hypertext Transfer Protocol (HTTP), 900–901
  - Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS), 900–901
  - hyphen (-), 497, 501
- 
- IANA (Internet Assigned Numbers Authority), 228, 429
  - iBGP (internal BGP), 429, 448–453. *See also* BGP (Border Gateway Protocol) troubleshooting
    - AD (administrative distance), 448, 580–582
    - benefits of, 448–450
    - in BGP best-path algorithm, 550
    - confederations
      - confederation identifier*, 462
      - configuration*, 462–465
      - definition of*, 462
      - topology*, 462
    - definition of, 448
    - eBGP (external BGP) compared to, 453–454
    - full mesh requirement, 450
    - multipath, 553
    - next-hop manipulation, 456–457
    - peering using loopback addresses, 451–453
    - prefix advertisement behavior, 449
    - route reflectors
      - configuration*, 459–461
      - loop prevention*, 461
      - route reflector clients*, 457

- split horizon, 579–580
- topologies, 454–455
- ICMP (Internet Control Message Protocol)**, 32–33, 847
- identity local address command**, 829
- Idle state (BGP)**, 433, 563
- IEEE EUI-64 standard**, 20–22
- IETF (Internet Engineering Task Force)**, 72
- IGP (Interior Gateway Protocol)**, 222, 551, 688
- igp-metric keyword**, 539
- IGRP (Interior Gateway Routing Protocol)**, 72
- IKE (Internet Key Exchange)**, 825
- IKEv2 (Internet Key Exchange version 2)**, 838–839
  - DMVPN (Dynamic Multipoint Virtual Private Network) tunnel security, 838–839
  - keyring, 828–829
  - profiles, 829–830
- implicit deny**, 846
- implicit deny any**
  - IPv4 ACLs (access control lists), 846
  - IPv6 ACLs (access control lists), 850
  - prefix list processing, 854, 862
- implicit message flag (NHRP)**, 788
- implicit NULL label**, 754–755
- inbound label binding filtering**, 754
- include-connected keyword**, 690, 695, 715
- INFORMATION-REQUEST message**, 30
- infrastructure security**
  - AAA (authentication, authorization, and accounting) troubleshooting, 866
  - CoPP (Control Plane Policing)
    - ACL (*access control list*) configuration, 876–878
    - class map configuration, 878–880
    - definition of, 866
    - overview of, 875–876, 885
    - policy map configuration, 880–882
    - service policy applied to control plane interface, 883–885
- IPv6 First-Hop Security, 885–887
- troubleshooting, 869–874
- uRPF (Unicast Reverse Path Forwarding)
  - definition of, 866
  - troubleshooting, 874–875
- ingress LSRs (label switching routers)**, 748–749
- inherit peer-policy command**, 519
- inherit peer-session command**, 519
- Init state**
  - OSPF (Open Shortest Path First), 230
  - OSPFv2 (Open Shortest Path First version 2), 318
- InQ field (BGP)**, 438
- installed routes, displaying**
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 86–87
  - OSPF (Open Shortest Path First), 238–239
- instances, VRF (virtual routing and forwarding)**. *See* VRF-Lite configuration
- inter-area router LSAs (link-state advertisements)**, 372, 373, 373
- inter-area routes**, 238, 296, 301–303
- interface delay settings, EIGRP (Enhanced Interior Gateway Routing Protocol) metrics**, 99
- Interface field (EIGRP)**, 85

**interface status**

- BGP (Border Gateway Protocol), 561
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 84–85, 142
  - OSPF (Open Shortest Path First), 245
  - OSPFv2 (Open Shortest Path First version 2), 319
- interface tunnel command**, 770, 780, 782, 792
- interface-specific configuration**
- EIGRP (Enhanced Interior Gateway Routing Protocol), 114–116
  - OSPF (Open Shortest Path First), 233
  - Interior Gateway Protocol (IGP), 222, 688
  - Interior Gateway Routing Protocol (IGRP), 72
- intermediate LSRs (label switching routers)**, 748–749
- Intermediate System-to-Intermediate System (IS-IS)**, 372, 426, 755
- internal BGP (Border Gateway Protocol)**. *See* iBGP (internal BGP)
- Internet Assigned Numbers Authority (IANA)**, 228, 429
- Internet Control Message Protocol**. *See* ICMP (Internet Control Message Protocol)
- Internet Engineering Task Force (IETF)**, 72
- Internet Key Exchange**. *See* IKE (Internet Key Exchange); IKEv2 (Internet Key Exchange version 2)
- inter-router communication**
- BGP (Border Gateway Protocol), 430–435
    - messages*, 431–432
    - neighbor states*, 432–435, 563
    - single- and multi-hop sessions*, 430–431
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 78–79
  - EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 191
  - OSPF (Open Shortest Path First), 228
- intra-area routes**, 238, 295–296
- intra-area-prefix LSAs (link-state advertisements)**, 373
- IOS XE peer groups**, 517–518
- IOS XE peer templates**, 518–519
- ip access-group command**, 848
- ip access-list extended command**, 623
- ip access-list standard command**, 622
- ip address command**, 14, 770, 780, 782, 809
- ip as-path access-list command**, 504
- ip bandwidth-percent eigrp command**, 125
- ip bgp summary command**, 438
- ip bgp-community new-format command**, 508
- ip cef command**, 927
- ip community-list command**, 513
- ip default next-hop command**, 641
- ip dhcp excluded-address command**, 15
- ip dhcp pool command**, 15
- ip flow egress command**, 921
- ip flow ingress command**, 919, 921
- ip flow monitor command**, 926
- ip flow-cache entries command**, 922–923
- ip flow-cache timeout active command**, 922–923
- ip flow-cache timeout inactive command**, 922–923
- ip flow-export destination command**, 920, 921
- ip flow-export source command**, 919, 921

- ip flow-export version [5 | 9] command, 921
- ip ftp client password command, 902
- ip ftp client username command, 902
- ip ftp source-interface command, 902
- ip hello-interval eigrp command, 108
- ip helper-address command, 12, 13, 52
- ip hold-time eigrp command, 108
- ip http client password command, 901
- ip http client source-interface command, 901
- ip http client username command, 901
- ip local policy command, 637
- ip low monitor command, 926
- ip mtu command, 771, 781, 783, 792
- ip next-hop command, 642
- ip nhrp authentication command, 794
- ip nhrp holdtime command, 810
- ip nhrp map command, 783
- ip nhrp map multicast command, 783
- ip nhrp map multicast dynamic command, 781
- ip nhrp network-id command, 781, 782, 792
- ip nhrp nhs command, 782–783, 792
- ip nhrp redirect command, 781, 792, 797
- ip nhrp registration no-unique command, 795
- ip nhrp registration timeout command, 811
- ip nhrp shortcut command, 792
- ip ospf area command, 366
- ip ospf authentication command, 255
- ip ospf authentication message-digest command, 255–256
- ip ospf authentication-key command, 255
- ip ospf command, 233, 319–320
- ip ospf cost command, 295
- ip ospf hello-interval command, 255, 359
- ip ospf message-digest-key command, 255–256
- ip ospf mtu-ignore command, 330
- ip ospf network broadcast command, 247
- ip ospf network non-broadcast command, 247
- ip ospf network point-to-point command, 249
- ip ospf priority command, 246
- ip policy route-map command, 646
- ip prefix-list command, 609, 627
- ip radius source-interface command, 873
- ip route command, 42
- ip route vrf command, 810
- ip scp server enable command, 903
- IP SLA (Internet Protocol Service Level Agreement) troubleshooting
  - debug ip sla trace 2 command, 916–917
  - IP SLA icmp-echo probe configuration, 911
  - IP SLA UDP-JITTER probe configuration, 911–912
  - show ip sla application command, 912–913
  - show ip sla configuration command, 913–914
  - show ip sla responder command, 915–916
  - show ip sla statistics command, 914–915
  - source and responder topology, 910–911
- ip ssh version {1 | 2} command, 897
- ip summary-address command, 115

- `ip tacacs source-interface` command, 873
- `ip tcp adjust-mss` command, 781, 783, 792
- `ip tftp source-interface` command, 900
- `ip verify notification threshold` command, 875
- `ip verify unicast reverse-path` command, 875
- `ip verify unicast source reachable-via` command, 874–875
- `ip vrf` command, 728–729, 734
- `ip vrf forwarding` command, 730–731, 870
- `ipconfig /all` command, 20–21, 22–23
- `ipconfig` command
  - IPv4 addressing, 9–10, 11, 49–50, 51–52
  - IPv6 addressing, 19–20, 26, 54–55, 58
- IPsec, DMVPN tunnel protection
  - data availability, 822
  - data confidentiality, 822, 824
  - data integrity, 822, 824
  - ESP modes, 825–827
  - IKEv2 protection, 838–839
  - key management, 824
  - overview of, 821–823
  - perfect forward secrecy, 824
  - pre-shared key authentication, 827–836
  - SAs (security associations), 825
  - secure transport, elements of, 821–823
  - security protocols, 824
  - SPI (Security Parameter Index), 381–382
  - verification of, 836–838
- IPv4 (Internet Protocol version 4)**
  - ACLs (access control lists)
    - importance of, 845*
    - packet filtering with, 848*
    - reading, 846–847*
    - time-based, 848–850*
    - trouble ticket, 855–857*
  - AD (administrative distance), 38–41
    - data structures and routing table, 39*
    - sources of routing information, 39–41*
  - APIPA (Automatic Private IP Addressing) address, 15–16
  - authentication headers, 824
  - BGP packets sourced from wrong IP address, 564–566
  - determining within subnet, 10–11
  - DHCP (Dynamic Host Configuration Protocol)
    - clients, 14–15*
    - DHCP-assigned IP addresses, verifying, 15–16*
    - DORA process, 11–12*
    - messages, 14*
    - purpose of, 11*
    - relay agents, 12–14*
    - servers, 15*
    - troubleshooting commands, 17–18*
    - troubleshooting issues, 16–17*
  - EIGRP for. *See* EIGRP (Enhanced Interior Gateway Routing Protocol)
  - IP bandwidth percentage, 125–126
  - IPv6 over IPv4, 471–475
  - NHRP (Next Hop Resolution Protocol), 794–795
  - overview of, 2–3, 7
  - packet-forwarding process, 31–38
    - basic routing, 31–35*
    - basic routing topology, 31–32*
    - troubleshooting, 35–38*

- prefix lists, 627
  - processing*, 854–855
  - purpose of*, 852
  - reading*, 853–854
  - trouble ticket*, 861–863
- redistribution
  - into BGP*, 699–702
  - into EIGRP*, 689–694
  - into OSPF*, 694–699
  - with route maps*, 702
  - route redistribution review*, 687–689
  - trouble ticket: users in IPv4 Branch unable to access resources outside Branch office*, 703–707
  - trouble ticket: users unable to access resources in classless network*, 708–711
  - troubleshooting targets for*, 689
- routing tables, 214–215
- static routes, 42–46, 61–64
- structure of, 7–10
- subnets, 10–11
- trouble tickets
  - IPv4 static routes*, 61–64
  - PC1 not able to access resources on 192.0.2.1*, 48–53
  - topology*, 48
  - users in IPv4 Branch unable to access resources outside Branch office*, 703–707
  - users unable to access resources in classless network*, 708–711
- unique IP NHRP registration, 794–795
- verification of, 9–10
- VRF-Lite configuration, 733–734
  - IPv4 global routing table*, 735
  - IPv4 VRF routing tables*, 735–736

**IPv6 (Internet Protocol version 6).** *See also EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6)*

- ACLs (access control lists)
  - importance of*, 850
  - packet filtering with*, 851–852
  - reading*, 850–851
  - trouble ticket*, 858–861
- AD (administrative distance), 38–41
  - data structures and routing table*, 39
  - sources of routing information*, 39–41
- BGP (Border Gateway Protocol)
  - troubleshooting
    - MP-BGP configuration*, 594–598
    - MP-BGP topology*, 593–594
- DHCPv6 messages, 29–30
- DHCPv6 relay agents, 30–31
- DMVPN (Dynamic Multipoint Virtual Private Network) configuration
  - correlation of IPv4-to-IPv6 transport protocol commands*, 812
  - display commands*, 813
  - DMVPN tunnel technique and*, 812
  - IPv6 DMVPN verification*, 816–817
  - IPv6-over-IPv6 sample configuration*, 813–815
  - tunneled protocol commands*, 811–812
- example of, 19
- First-Hop Security, 866, 885–887
  - binding table*, 885
  - Destination Guard*, 887
  - DHCPv6 Guard*, 886
  - IPv6 snooping*, 886

- Prefix Guard*, 887
- RA (router advertisement) Guard*, 886
- Source Guard*, 887
- IEEE EUI-64 standard, 20–22
- interface verification, 198
- IPv6-over-IPv6, 813–815
- link-local addresses, 23
- MP-BGP (Multiprotocol BGP)
  - configuration*, 594–598
  - IPv6 configuration*, 466–471
  - IPv6 over IPv4*, 471–475
  - MP-BGP topology*, 593–594
  - topology*, 465–466
- neighbor discovery messages, 886
- OSPFv3 (Open Shortest Path First version 3) configuration
  - authentication*, 381–383
  - IPv6 addressing*, 375–376
  - IPv6 route summarization*, 379–380
  - link-local forwarding*, 383–384
  - network type*, 380–381
  - process for*, 374
  - topology*, 374–375
  - verification of*, 377–378
- OSPFv3 (Open Shortest Path First version 3) troubleshooting
  - debug ipv6 ospf hello command*, 406
  - overview of*, 394–395
  - show cdp neighbors detail command*, 406
  - show ipv6 interface command*, 400
  - show ipv6 ospf command*, 395–396, 402–403
  - show ipv6 ospf database command*, 398–399
  - show ipv6 ospf interface brief command*, 396, 405–406
  - show ipv6 ospf interface command*, 397, 406–407
  - show ipv6 ospf neighbor command*, 397, 405
  - show ipv6 protocols command*, 395
  - show ipv6 route command*, 405
  - show ipv6 route ospf command*, 399–400, 401–402, 404
  - trouble ticket: Branch receiving inter-area routes other than default*, 401–404
  - trouble ticket: Branch users unable to access resources outside Branch office*, 404–408
- overview of, 3, 19–20
- packet-forwarding process, 31–38
  - basic routing*, 31–35
  - basic routing topology*, 31–32
  - troubleshooting*, 35–38
- prefix lists, 627–628
  - processing*, 854–855
  - purpose of*, 852
  - reading*, 853–854
  - trouble ticket*, 861–863
- redistribution
  - into BGP*, 699–702
  - into EIGRP*, 689–694
  - into OSPF*, 694–699
  - with route maps*, 702
  - route redistribution review*, 687–689
  - trouble ticket: IPv6 users unable to access resources*, 711–717
  - trouble ticket: users in BGP autonomous system unable to access IPv4 resources*, 717–721

- troubleshooting targets for*, 689
- route summarization, 195–196, 492–493
- SLAAC (stateless address autoconfiguration), 22–27
- snooping, 886
- stateful DHCPv6, 27–28
- stateless DHCPv6, 28–29
- static routes, 46–48, 64–66
- trouble tickets
  - Branch receiving inter-area routes other than default*, 401–404
  - Branch users unable to access resources outside Branch office*, 404–408
  - IPv6 users unable to access resources*, 711–717
  - PC1 not able to access resources on 2001:db8:d::1*, 54–61
  - users in BGP autonomous system unable to access IPv4 resources*, 717–721
- verification of, 19–20
- VRF-Lite configuration, 733–734
- ipv6 access-class command, 851
- ipv6 address autoconfig command, 23
- ipv6 address command, 21–22, 59, 60, 782, 809
- ipv6 cef command, 927
- ipv6 dhcp guard attach-policy command, 886
- ipv6 dhcp relay destination command, 31
- ipv6 dhcp server command, 27
- ipv6 eigrp command, 192
- ipv6 mtu command, 811
- ipv6 nd other-config-flag command, 28–29
- ipv6 nd ra suppress all command, 56
- ipv6 nd rguard attach-policy command, 886
- ipv6 nhrp authentication command, 812
- ipv6 nhrp holdtime command, 812
- ipv6 nhrp network-id command, 811
- ipv6 nhrp nhs command, 811
- ipv6 nhrp redirect command, 811
- ipv6 nhrp registration no-unique command, 812
- ipv6 nhrp registration timeout command, 812
- ipv6 nhrp shortcut command, 811
- ipv6 ospf command, 376
- ipv6 prefix-list command, 628
- ipv6 route command, 46, 65–66
- ipv6 route vrf command, 812
- ipv6 router eigrp command, 192
- ipv6 router ospf command, 376
- ipv6 summary-address eigrp command, 195
- ipv6 tcp adjust-mss command, 811
- ipv6 traffic-filter command, 851
- ipv6 unicast-routing command, 374
- IS-IS (Intermediate System-to-Intermediate System), 372, 426, 755
- Issues and Events page, Cisco DNA Center Assurance, 938–939

## J-K

---

- K values, 145–146, 198
- keepalive command, 771
- keepalives, 771, 834
- key chain command, 92
- key command, 92
- key management, 825
- keychains, 92
- keyring local command, 829

keyrings, 828–829  
key-string command, 92

## L

---

L2VPN (Layer 2 Virtual Private Network), split horizon and, 128  
label bindings, 750  
Label Distribution Protocol (LDP), 750, 751–752, 753, 754–755, 759  
Label Forwarding Information Base (LFIB), 748  
Label Information Base (LIB), 748, 753  
label stack, MPLS Layer 3 VPNs, 759–761  
label switching, 752–753. *See also* MPLS (Multiprotocol Label Switching)  
label switching routers (LSRs), 748–749  
label-switched path (LSP), 749  
latency, 97  
Layer 2 Virtual Private Network (L2VPN), 128  
Layer 3 packet-forwarding process  
  basic routing, 31–35  
  data structures, 35  
  troubleshooting, 561–562  
    *show adjacency detail command*, 38  
    *show ip arp command*, 37  
    *show ip cef command*, 37  
    *show ip cef exact-route command*, 37  
    *show ip nbrp command*, 38  
    *show ip route command*, 35–36  
Layer 3-to-Layer 2 mapping table, 34  
LDP (Label Distribution Protocol), 750, 751–752, 753, 754–755, 759

leak-map option, summary-address command, 115  
learned IPv6 route verification, 211–212  
level 5 encryption, 898–899  
level 7 encryption, 898–899  
level 8 encryption, 898–899  
LFIB (Label Forwarding Information Base), 748  
LIB (Label Information Base), 748, 753  
link costs, OSPF (Open Shortest Path First), 295  
Link Count field (OSPF LSDB), 265  
Link ID field  
  OSPF LSDB, 265  
  Type 3 LSA (summary LSA), 275  
  Type 5 LSA (external LSA), 279  
  Type 7 LSA (NSSA external LSA), 283  
link LSAs (link-state advertisements), 373  
link-local addresses, 23, 211  
link-local flooding scope, 384  
link-local forwarding, 383–384  
link-state acknowledgment packets, 228, 374  
link-state advertisement. *See* LSA (link-state advertisement)  
link-state database. *See* LSDB (link-state database)  
link-state request (LSR) packets, 228, 374  
link-state update (LSU) packets, 228, 374  
lists  
  access control. *See* ACLs (access control lists)  
  distribute, 495–496, 586–587  
  distribution, 129–132

- offset, 132–135
- prefix, 496
  - IPv4*, 627
  - IPv6*, 627–628
  - processing*, 854–855
  - purpose of*, 852
  - reading*, 853–854
  - trouble ticket*, 861–863
- load balancing
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 100–102, 168–169
  - OSPFv2 (Open Shortest Path First version 2), 352–353
- Loading state
  - OSPF (Open Shortest Path First), 230
  - OSPFv2 (Open Shortest Path First version 2), 319
- local AS BGP community, 511–512
- local PBR (policy-based routing), 637–639
- local preference, in BGP best-path algorithm, 532–538, 588
  - bgp default local-preference command, 532
  - BGP edge evaluation of multiple paths, 536–538
  - BGP tables after local preference modification, 534–535
  - configuration, 533–534
  - final BGP processing state, 538
  - set local-preference command, 532
  - topology, 533
- local route origination, 538
- LOCAL\_PREF attribute, 464
- locally originated route, in BGP best-path algorithm, 538
- LocPrf field (BGP), 445
- Loc-RIB table, 440
- log keyword, 877, 895
- logging buffered command, 904
- logging synchronous command, 894, 896
- login authentication command, 871, 872, 894, 895, 897
- login command, 895, 897
- login local command, 895, 897
- log-input keyword, 877
- longer-prefixes option (show ip route command), 36
- lookup, DNS, 8
- loop prevention
  - BGP (Border Gateway Protocol), 430
  - route reflectors, 461
- loopback addresses, 451–453, 565
- loopback interfaces, MPLS (Multiprotocol Label Switching), 752
- loopback networks, 246, 253–254
- loops, routing. *See* routing loops caused by redistribution, troubleshooting
- loose mode, uRPF (Unicast Reverse Path Forwarding), 874
- lowest IGP metric, 551
- LSA (link-state advertisement)
  - LSDB (link-state database), 262–263, 372, 387–390
    - displaying*, 398–399
    - fields*, 265
    - verification of*, 415–418
  - OSPF (Open Shortest Path First), 225
    - ABRs (area border routers)*, 264
    - age and flooding*, 264
    - overview of*, 262–264
    - reference topology*, 264
    - sequences*, 264
    - summary of types of*, 283
    - Type 1 LSA (router LSA)*, 264–269

- Type 2 LSA (network LSA), 269–271
  - Type 3 LSA (summary LSA), 271–276
  - Type 4 LSA (ASBR summary LSA), 279–281
  - Type 5 LSA (external LSA), 277–279, 679
  - Type 7 LSA (NSSA external LSA), 281–283
  - OSPFv2 (Open Shortest Path First version 2), 346–348
  - OSPFv3 (Open Shortest Path First version 3), 372–373
    - flooding scope, 384–390
    - Options field, 386
    - types of, 372–373
    - verification of, 398–399
    - viewing, 385–387
  - LSDB (link-state database), 262–263, 372, 387–390
    - displaying, 398–399
    - fields, 265
    - verification of, 415–418
  - LSP (label-switched path), 749
  - LSR (link-state request) packets, 228, 374
  - LSRs (label switching routers), 748–749
  - LSU (link-state update) packets, 228, 374
- M**
- 
- MAC (media access control) addresses, 43–44
  - management tools troubleshooting
    - BFD (Bidirectional Forwarding Detection), 927–928
    - Cisco DNA Center Assurance
      - accessing, 929
      - AI Analytics, 937–938
      - Client Health page, 933–934
      - Command Runner, 938–940
      - Device 360 and Client 360 pages, 933–937
      - Issues and Events page, 938–939
      - Network Health page, 931–932
      - Network Time Travel, 937
      - Overall Health page, 930–931
      - overview of, 929
      - Path Trace, 936–937
  - Cisco IOS IP SLA
    - debug ip sla trace 2 command, 916–917
    - IP SLA icmp-echo probe configuration, 911
    - IP SLA UDP-JITTER probe configuration, 911–912
    - show ip sla application command, 912–913
    - show ip sla configuration command, 913–914
    - show ip sla responder command, 915–916
    - show ip sla statistics command, 914–915
    - source and responder topology, 910–911
  - Flexible NetFlow, 923–927
  - NetFlow, 919–924
  - Object Tracking, 917–919
  - SNMP (Simple Network Management Protocol), 906–910
    - syslog, 904–906
  - maps, route. *See* route maps
  - match command, 635, 690, 878–879
  - match fvrf command, 829
  - match identity remote address command, 829

- match interface command, 656
- match route-type command, 656
- matching, conditional. *See* conditional matching
- maximum paths, 168–169
- maximum prefix, BGP (Border Gateway Protocol), 516–517
- maximum segment size (MSS), 781
- maximum transmission unit (MTU), 117, 328–330, 658, 771
- maximum-paths command, 100, 168, 298, 553
- maximum-paths ibgp command, 757
- max-in-negotiation-sa keyword, 838
- max-sa keyword, 838
- MD5 (Message Digest 5), 91, 255–256, 326, 570
- Mean SRTT field (EIGRP), 85
- MED (multi-exit discriminator), 438, 588
  - always-compare-med feature, 549
  - BGP deterministic MED, 549–550
  - configuration, 542–545
  - missing MED behavior, 548–549
- Message Digest 5 (MD5), 91, 255–256, 326, 570
- messages
  - BGP (Border Gateway Protocol), 431–432
  - DHCP (Dynamic Host Configuration Protocol) for IPv4, 14
  - DHCPv6 (Dynamic Host Configuration Protocol version 6), 29–30
  - NHRP (Next Hop Resolution Protocol), 774–776
    - message extensions*, 775
    - redirect*, 777
    - types of*, 775
- Metric field (BGP), 445
  - Type 3 LSA (summary LSA), 275
  - Type 5 LSA (external LSA), 279
  - Type 7 LSA (NSSA external LSA), 283
- metric keyword, 664, 690, 694, 699, 706
- Metric Type field (BGP), 279
- metric weights command, 100
- metrics, EIGRP (Enhanced Interior Gateway Routing Protocol)
  - classic metric formula, 94–96
  - custom K values, 100
  - interface delay settings, 99
  - load balancing, 100–102
  - metric backward compatibility, 98–99
  - redistribution troubleshooting and, 678–679
  - route summarization, 117
  - wide metrics, 96–98
- metric-type keyword, 241, 664, 694
- mGRE (Multipoint GRE), 769
- minimum hold time, 572
- misconfigured peer groups, 570–571
- mismatched area numbers, 322–323
- mismatched area type, 323–324
- mismatched authentication, 199–200, 570
- mismatched autonomous system numbers, 142–143, 198
- mismatched K values, 145–146, 198
- mismatched timers, 321–322
- missing MED behavior, 548–549
- mode {transport | tunnel} command, 832
- modes, ESP (Encapsulating Security Payload), 825–827
- MP-BGP (Multiprotocol BGP)
  - IPv6 configuration, 466–471

- IPv6 over IPv4, 471–475
- topology, 465–466, 593
- troubleshooting
  - MP-BGP configuration*, 594–598
  - MP-BGP topology*, 593–594
- MP-BGPv4 address families, 746
- MP-IBGP (Multiprotocol-Interior Border Gateway Protocol), 757
- MPLS (Multiprotocol Label Switching), 747, 752–753, 754
  - FEC (forwarding equivalence class), 749
  - label placement and format, 749–750
  - LDP (Label Distribution Protocol), 751–752, 754–755
  - LFIB (Label Forwarding Information Base), 748
  - LIB (Label Information Base), 748
  - LSP (label-switched path), 749
  - LSRs (label switching routers), 748–749
  - MPLS Layer 3 VPNs
    - architecture*, 756–757
    - CE (customer edge) routers*, 756
    - label stack*, 759–761
    - PE (provider edge) routers*, 756
    - RD (route distinguishers)*, 757–759
    - RTs (route targets)*, 757–759
    - VPNv4 addresses*, 757–759
  - PHP (penultimate-hop popping), 753–754
  - TE (Traffic Engineering), 755
- `mpls ldp neighbor` command, 751
- `mpls ldp router-id` command, 752
- MsgRcvd field (BGP), 438
- MsgSent field (BGP), 438
- MSS (maximum segment size), 781
- MTU (maximum transmission unit), 117, 328–330, 658, 771
- multi-address family configuration mode (EIGRP), 80–81
- Multicast Flow Timer field (EIGRP), 85
- multi-exit discriminator. *See* MED (multi-exit discriminator)
- multi-hop sessions, BGP (Border Gateway Protocol), 430–431
- multipath BGP (Border Gateway Protocol), 553
- multiple-exit discriminator (MED), 438
- Multipoint Frame Relay networks, 34
- Multipoint GRE (mGRE), 769
- multipoint redistribution
  - routing loops, 679–686
    - distribute list to control OSPF routes*, 683–684
    - EIGRP AD configuration*, 682–683
    - route tags*, 684–686
    - routing topology*, 679–680
    - sample scenario for*, 679–682
  - suboptimal routing, 678–679
- multiprocess redistribution, 666–667
- Multiprotocol BGP. *See* MP-BGP (Multiprotocol BGP)
- Multiprotocol Label Switching. *See* MPLS (Multiprotocol Label Switching)
- Multiprotocol-Interior Border Gateway Protocol (MP-IBGP), 757
- mutual redistribution, 650–651, 661–663

## N

---

- NA (neighbor advertisement), 850
- named configuration mode, 80–81, 857

**named EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 771**

configuration, 192

trouble ticket: users unable to access resources outside their LAN, 213–218

*configuration modification, 217**configuration review, 215–217**EIGRP-learned routes verification, 217**interfaces and IPv4 addresses, 215**IPv4 routing tables, 214–215**ping command, 213–218*

troubleshooting, 204–209

**NAT (Network Address Translation), 776, 825, 834, 845****NBMA (nonbroadcast multi-access), 247, 331, 372****NDP (Neighbor Discovery Protocol), 850****neighbor 2001:DB8::2 activate command, 616****neighbor 2001:DB8::2 remote-as 65502 command, 616****neighbor addresses, 552****neighbor adjacencies, troubleshooting**

BGP (Border Gateway Protocol), 602–603

*ACLs (access control lists), 566–567**BGP packets sourced from wrong IP address, 564–566**incorrect neighbor statement, 564**interface is down, 561**Layer 3 connectivity is broken, 561–562**misconfigured peer groups, 570–571**mismatched authentication, 570**neighbor lacks route to local router, 563**neighbor verification, 559–560**overview of, 559–561**path to neighbor is through default route, 562–563**timers, 572–573**TTL (time to live) expiration, 568–570***EIGRP (Enhanced Interior Gateway Routing Protocol), 141–151***ACLs (access control lists), 150–151**authentication, 148–150**different subnets, 148**incorrect network statement, 144–145**interface is down, 142**mismatched autonomous system numbers, 142–143**mismatched K values, 145–146**overview of, 141–151**passive interface feature, 146–148**timers, 151***EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 210–211****OSPF (Open Shortest Path First), 230–232, 237–238****OSPFv2 (Open Shortest Path First version 2)***ACLs (access control lists), 327–328**adjacency states, 318–319**different subnets, 324–325**duplicate router IDs, 330*

- interface is down*, 319
- interface not running OSPF process*, 319–321
- mismatched area numbers*, 322–323
- mismatched area type*, 323–324
- mismatched authentication information*, 326–327
- mismatched network types*, 330–332
- mismatched timers*, 321–322
- MTU mismatch*, 328–330
- neighbor verification*, 317
- overview of*, 317–319
- passive interfaces*, 325–326
- neighbor advertisement (NA), 850
- Neighbor Discovery Protocol (NDP), 850
- Neighbor field (BGP), 438
- neighbor *group-name* peer-group command, 518
- neighbor ID. *See* RID (router ID)
- neighbor *ip\_address* activate command, 594
- neighbor *ip\_address* distribute-list command, 586
- neighbor *ip\_address* ebgp-multihop [*TTL*] command, 569
- neighbor *ip\_address* filter-list command, 586
- neighbor *ip\_address* next-hop-self command, 578
- neighbor *ip\_address* peer-group command, 571
- neighbor *ip\_address* prefix-list command, 586
- neighbor *ip\_address* remote-as *as\_number* command, 564, 565
- neighbor *ip\_address* remove-private-as command, 591
- neighbor *ip\_address* route-map command, 586
- neighbor *ip\_address* transport connection-mode {*active* | *passive*} command, 567
- neighbor *ip\_address* update-source command, 565
- neighbor *ip-address* activate command, 436
- neighbor *ip-address* aigp command, 539
- neighbor *ip-address* distribute-list {*acl-number* | *acl-name*} {*in* | *out*} command, 495
- neighbor *ip-address* filter-list *acl-number* {*in* | *out*} command, 504
- neighbor *ip-address* maximum-prefix *prefix-count* [*warning-percentage*] [*restart time*] [*warning-only*] command, 516
- neighbor *ip-address* next-hop-self [*all*] command, 456
- neighbor *ip-address* password *password* command, 436
- neighbor *ip-address* prefix-list *prefix-list-name* {*in* | *out*} command, 496
- neighbor *ip-address* remote-as *as-number* command, 435
  - neighbor *ip-address* route-map *route-map-name* {*in* | *out*}505
- neighbor *ip-address* route-reflector-client command, 459
- neighbor *ip-address* send-community [*standard* | *extended* | *both*] command, 508
- neighbor *ip-address* timers keepalive holdtime [*minimum-holdtime*] command, 436
- neighbor *ip-address* update-source *interface-id* command, 435–436, 452

- neighbor *ip-address* weight *weight* command, 529
- neighbor *ipv6\_address* activate command, 596
- neighbor *ipv6\_address* remote-as command, 596
- neighbor remote-as command, 564, 565–566, 603
- neighbor solicitation (NS), 850
- neighbor states, 268, 432–435, 563
- NetFlow, 919–924
- Network Address Translation. *See* NAT (Network Address Translation)
- network area command, 366
- network command, 317
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 152–154, 160
  - OSPFv2 (Open Shortest Path First version 2), 319–320
- Network field (BGP), 445
- Network Health page, Cisco DNA Center Assurance, 931–932
- network layer reachability information (NLRI), 430, 524
- network LSAs (link-state advertisements), 269–271, 373
- network mask command, 440, 573, 575–576, 605–606
- Network Mask field
  - Type 3 LSA (summary LSA), 275
  - Type 5 LSA (external LSA), 279
  - Type 7 LSA (NSSA external LSA), 283
- network selection, BGP (Border Gateway Protocol), 623–625
- network statement, 80–82, 84, 234
  - BGP (Border Gateway Protocol), 440–441
  - MP-BGP (Multiprotocol BGP), 467
  - OSPF (Open Shortest Path First), 232–233
  - troubleshooting, 144–145
- Network Time Protocol (NTP), 27, 905
- Network Time Travel, Cisco DNA Center Assurance, 937
- network types
  - OSPF (Open Shortest Path First)
    - broadcast*, 246, 247
    - loopback*, 246, 253–254
    - nonbroadcast*, 246, 247–248
    - overview of*, 246
    - point-to-multipoint*, 246–253
    - point-to-point*, 246, 248–249
  - OSPFv2 troubleshooting, 330–332
  - OSPFv3 (Open Shortest Path First version 3), 380–381
- networks
  - discontiguous, 165–167, 305–306
  - overlay, 806–810
    - definition of*, 769
    - front door VRF (FVRF)*, 808–810
    - outbound interface selection*, 808
    - recursive routing problems*, 806–807
  - point-to-point, 269
  - stub, 269
  - transit, 268
- Next Hop field (BGP), 445
- Next Hop Resolution Protocol. *See* NHRP (Next Hop Resolution Protocol)
- next-hop manipulation, 577–579
- next-hop override routing table, 801–802
- next-hop router, 577–579
- next-hop servers (NHSs), 774
- next-hop-self feature, 456
- nho message flag (NHRP), 789
- nhop message flag (NHRP), 789

- NHRP (Next Hop Resolution Protocol)**
- cache, viewing, 787–791
    - examples of*, 789–791
    - NHRP mapping entries*, 788
    - NHRP message flags*, 788–789
  - holdtime, 810
  - IP NHRP authentication, 794–795
  - messages, 774–776
    - message extensions*, 775
    - redirect*, 777
    - types of*, 775
  - NHRP mapping with spoke-to-hub traffic, 798–800
  - NHRP routing table manipulation, 800–806
    - example of*, 800–801
    - next-hop override routing table*, 801–802
    - with summarization*, 802–806
  - NHSs (next-hop servers), 774
  - shortcuts, 777
  - timeout, 810–811
  - unique IP NHRP registration, 794–795
  - NHSs (next-hop servers)**, 774
  - NLRI (network layer reachability information)**, 430, 524
  - no auto-summary command**, 118, 165–166
  - no bgp default ipv4-unicast command**, 436–437
  - no eigrp stub command**, 212–213
  - no exec command**, 894
  - no exec-timeout command**, 894
  - no ip helper-address 172.16.1.100 command**, 52
  - no ip ospf hello-interval 11 command**, 359
  - no ip split-horizon command**, 162
  - no ip split-horizon eigrp command**, 128, 162
  - no ipv6 address 2001:db8:a:a::1/60 command**, 60
  - no ipv6 nd ra suppress all command**, 56
  - no ipv6 ospf network non-broadcast command**, 408
  - no neighbor 2001:DB8::2 activate command**, 616
  - no passive-interface command**, 88–89, 217, 233, 378
  - no service timestamps command**, 905
  - no shutdown command**, 750
  - no split-horizon command**, 128
  - No\_Advertise BGP community**, 509–510
  - No\_Export BGP community**, 510–511
  - No\_Export\_SubConfed BGP community**, 511–512
  - nonbroadcast multi-access (NBMA)**, 38, 247, 331, 372
  - nonbroadcast networks**, 246, 247–248
  - nondisclosure agreement (NDA)**, 948
  - normal-time questions**, 945
  - no-summary keyword**, 288, 293
  - NOTIFICATION messages (BGP)**, 432
  - not-so-stubby-areas**. *See* NSSAs (not-so-stubby-areas)
  - NS (neighbor solicitation)**, 850
  - NSSA external LSAs (link-state advertisements)**, 281–283
  - nssa-only option**, 694
  - NSSAs (not-so-stubby-areas)**, 289–292, 373, 395
  - NTP (Network Time Protocol)**, 27, 905
  - NULL**
    - authentication, 326
    - explicit/implicit, 754–755

## O

---

- object identifiers (OIDs), 908**
- Object Tracking**
  - floating static routes, 918–919
  - troubleshooting, 917–918
- offset lists, 132–135**
- offset-list command, 132**
- OIDs (object identifiers), 908**
- OPEN messages (BGP), 431–432**
- Open Shortest Path First. *See* OSPF (Open Shortest Path First)**
- OpenConfirm state (BGP), 434**
- OpenSent state (BGP), 434**
- optional transitive BGP path attributes, 429, 528**
- Options field, OSPFv3 LSAs, 386**
- origin authentication, 824**
- origin type, BGP (Border Gateway Protocol), 542–545**
- Originator attribute (BGP), 461**
- OSI model, Layer 3 packet-forwarding process**
  - basic routing, 32–35
  - basic routing topology, 31
  - data structures, 35
  - troubleshooting, 35–38
- OSPF (Open Shortest Path First), 373. *See also* OSPFv2 (Open Shortest Path First version 2); OSPFv3 (Open Shortest Path First version 3)**
  - ABRs (area border routers), 227
  - areas, 226–227
  - ASBRs (autonomous system boundary routers), 240, 277, 279–281, 347, 372, 395, 678–679
  - authentication, 253–254, 255–257
  - configuration
    - confirmation of interfaces, 235–237*
    - default route advertisement, 241–242*
    - distribute lists, 683–684*
    - external OSPF routes, 240–241*
    - installed routes, displaying, 238–239*
    - interface columns, 237*
    - interface-specific, 233*
    - neighbor adjacencies, 237–238*
    - network statement, 232–233, 234*
    - network types, 246–254*
    - overview of, 232*
    - route tags, 684–686*
    - sample topology and configuration, 233–235*
  - definition of, 222
  - discontiguous networks, 305–306
  - distribute lists, 683–684
  - DR (designated router)/BDR (backup designated router)
    - concept of, 242–243*
    - elections, 244–245*
    - interface priority, 245*
    - placement, 245–246*
  - failure detection and timers, 254–255
  - Hello packets, 229
  - inter-router communication, 228
  - LSA (link-state advertisement), 225
    - ABRs (area border routers), 264*
    - age and flooding, 264*
    - LSDb (link-state database), 262–263, 265*
    - overview of, 262–264*
    - reference topology, 264*
    - sequences, 264*
    - summary of types of, 283*

- Type 1 LSA (router LSA), 264–269
- Type 2 LSA (network LSA), 269–271
- Type 3 LSA (summary LSA), 271–276
- Type 4 LSA (ASBR summary LSA), 279–281
- Type 5 LSA (external LSA), 277–279
- Type 7 LSA (NSSA external LSA), 281–283
- neighbor adjacencies
  - debugging*, 231–232
  - forming*, 231
  - neighbor adjacencies*, 237–238
  - requirements for*, 230–231
- neighbor states, 230
- network types
  - broadcast*, 246, 247
  - loopback*, 246, 253–254
  - nonbroadcast*, 246, 247–248
  - overview of*, 246
  - point-to-multipoint*, 246–253
  - point-to-point*, 246, 248–249
- packet types, 228
- path selection
  - ECMP (equal-cost multipathing)*, 298
  - external routes*, 297–298
  - inter-area routes*, 296
  - intra-area routes*, 295–296
  - link costs*, 295
  - overview of*, 294–295
- redistribution
  - BGP topology and configuration*, 670–672
  - connected networks*, 657
  - nontransitive nature of*, 651–652
  - OSPF forwarding address*, 667–670
  - OSPF-to-OSPF mutual redistribution*, 666–667
  - overview of*, 650–651
  - RIB (Routing Information Base) and*, 653–655
  - seed metrics*, 655–656, 688
  - sequential protocol redistribution*, 653
  - topology and configuration*, 663–666
  - troubleshooting*, 694–699
- RID (router ID), 229
- route tags, 684–686
- SPF trees, 225–226
- stubby areas
  - not-so-stubby-areas*, 289–292
  - overview of*, 284
  - stub areas*, 284–287
  - totally not-so-stubby-areas*, 292–294
  - totally stubby areas*, 287–289
- summarization of routes
  - external summarization*, 303–305
  - impact on SPF topology calculation*, 299–301
  - inter-area summarization*, 301–303
  - LSA reduction through area segmentation*, 298–299
  - topology example with summarization*, 300–301
- virtual links, 307–309
- VLSM (variable-length subnet masking), 222
- VRF-Lite configuration, 745–746
- OSPFv2 (Open Shortest Path First version 2)

- advertisement tracking, 346–348
  - default routes, 353
  - discontiguous areas, 350–352
  - DRs (designated routers), 341–344
  - load balancing, 352–353
  - LSA (link-state advertisement), 346–348
  - neighbor adjacencies, troubleshooting
    - ACLs (access control lists)*, 327–328
    - adjacency states*, 318–319
    - different subnets*, 324–325
    - duplicate router IDs*, 330
    - interface is down*, 319
    - interface not running OSPF process*, 319–321
    - mismatched area numbers*, 322–323
    - mismatched area type*, 323–324
    - mismatched authentication information*, 326–327
    - mismatched network types*, 330–332
    - mismatched timers*, 321–322
    - MTU mismatch*, 328–330
    - neighbor verification*, 317
    - overview of*, 317–319
    - passive interfaces*, 325–326
  - OSPFv3 compared to, 371–372
  - route summarization, 348–350
  - route troubleshooting
    - better source of information*, 334–337
    - duplicate router IDs*, 344–346
    - interface not running OSPF process*, 333–334
    - overview of*, 332–333
    - route filtering*, 337–339
    - stub area configuration*, 339–340
    - wrong designated router elected*, 341–344
  - stub areas, 339–340
  - transit areas, 350
  - trouble ticket: routers R1 and R2
    - not forming neighbor adjacency, 364–366
  - trouble ticket: users in 10.1.1.0/24
    - not able to access resources in 192.168.1.0/24
      - ticket 8–1*, 353–361
      - ticket 8–2*, 361–364
  - virtual links, 350–352
- OSPFv3 (Open Shortest Path First version 3), 420**
- address families troubleshooting
    - debug ospfv3 command*, 418
    - default-information originate command*, 422
    - sample configuration*, 408–410
    - show ip protocols command*, 410–411
    - show ip route ospfv3 command*, 418
    - show ipv6 protocols command*, 410–411
    - show ipv6 route command*, 420
    - show ipv6 route ospf command*, 418
    - show ospfv3 command*, 411–413
    - show ospfv3 database command*, 415–418
    - show ospfv3 interface brief command*, 413
    - show ospfv3 interface command*, 413–414
    - show ospfv3 ipv6 command*, 421
    - show ospfv3 neighbor command*, 414

- show run | section router ospfv3*  
command, 422
- trouble ticket: Branch users*  
unable to access IPv6-  
enabled resources on Internet,  
419–423
- communication and packet types,  
373–374
- configuration
  - authentication, 381–383
  - IPv6 addressing, 375–376
  - IPv6 route summarization,  
379–380
  - link-local forwarding, 383–384
  - network type, 380–381
  - process for, 374
  - topology, 374–375
  - verification of, 377–378
- interface tunnel command, 409
- LSA (link-state advertisement),  
372–373
  - flooding scope, 384–390
  - Options field, 386
  - types of, 372–373
  - verification of, 398–399
  - viewing, 385–387
- LSDB (link-state database), 372,  
387–390, 398–399, 415–418
- OSPFv2 compared to, 371–372
- OSPFv3 for IPv6 troubleshooting
  - debug ipv6 ospf hello* command,  
406
  - overview of, 394–395
  - show cdp neighbors detail*  
command, 406
  - show ipv6 interface* command,  
400
  - show ipv6 ospf* command, 395–  
396, 402–403
  - show ipv6 ospf database*  
command, 398–399
  - show ipv6 ospf interface brief*  
command, 396, 405–406
  - show ipv6 ospf interface*  
command, 397, 406–407
  - show ipv6 ospf neighbor*  
command, 397, 405
  - show ipv6 protocols* command,  
395
  - show ipv6 route* command, 405
  - show ipv6 route ospf* command,  
399–400, 401–402, 404
  - topology, 401
  - trouble ticket: Branch receiving*  
inter-area routes other than  
default, 401–404
  - trouble ticket: Branch users*  
unable to access resources  
outside Branch office,  
404–408
- overview of, 370
- route verification, 399–400, 420
- ospfv3 authentication command, 381
- ospfv3 command, 745
- ospfv3 encryption command, 381
- ospfv3 network {point-to-point |  
point-to-multipoint broadcast |  
nonbroadcast} command, 380
- outbound interface selection, 808
- OutQ field (BGP), 438
- Overall Health page, Cisco DNA  
Center Assurance, 930–931
- overlay networks, 724, 806–810. *See*  
also VPNs (virtual private networks)
  - definition of, 769
  - front door VRF (FVRF)
    - configuration, 809–810
    - definition of, 808
    - static routes, 810

outbound interface selection, 808  
recursive routing problems, 806–807

## P

---

P2P (point-to-point) networks, 246,  
248–249, 269, 331, 771

packet replay protection, IPsec,  
833–834

### packet types

EIGRP (Enhanced Interior Gateway  
Routing Protocol), 78, 108

EIGRPv6 (Enhanced Interior Gateway  
Routing Protocol version 6), 191

OSPF (Open Shortest Path First), 228

OSPFv3 (Open Shortest Path First  
version 3), 373–374

### packet-forwarding process, 31–38

basic routing, 31–35

basic routing topology, 31–32

troubleshooting, 35–38

*show adjacency detail command,*  
38

*show ip arp command,* 37

*show ip cef command,* 37

*show ip cef exact-route  
command,* 37

*show ip nbrp command,* 38

*show ip route command,* 35–36

parentheses (), 497, 502

PAs (path attributes), 429, 524

### passive interfaces

EIGRP (Enhanced Interior Gateway  
Routing Protocol), 88–91, 146–148

OSPFv2 (Open Shortest Path First  
version 2), 325–326

troubleshooting, 198–199

passive-interface command, 88–91,  
217, 233, 378

passive-interface default command,  
88–89, 233, 378

password encryption levels, 898–899

PAT (Port Address Translation), 845

Path and Origin field (BGP), 445

path attributes (PAs), 429, 524

path metric calculation, EIGRP  
(Enhanced Interior Gateway Routing  
Protocol)

classic metric formula, 94–96

custom K values, 100

interface delay settings, 99

load balancing, 100–102

metric backward compatibility, 98–99

wide metrics, 96–98

### path selection

BGP (Border Gateway Protocol)

*best-path decision-making  
process,* 588–591

*debug commands,* 592–593

*private autonomous systems  
numbers,* 591

with longest match, 526–527

OSPF (Open Shortest Path First)

*ECMP (equal-cost multipathing),*  
298

*external routes,* 297–298

*inter-area routes,* 296

*intra-area routes,* 295–296

*link costs,* 295

*overview of,* 294–295

Path Trace, Cisco DNA Center  
Assurance, 936–937

path vector routing protocols, 430. *See  
also* BGP (Border Gateway Protocol)

path verification, GRE (Generic  
Routing Encapsulation) tunnels, 774

payload, ESP (Encapsulating Security  
Payload), 824

- PBR (policy-based routing)**
  - configuration, 635–637, 638
  - local, 637–639
  - overview of, 634–635
- PDMs (protocol-dependent modules),** 75, 188
- PE (provider edge) routers,** 756
- Pearson IT Certification Practice Test (PCPT) exam software,** 948–949
  - exam scores, C25.0122-C25.0136
  - tips for, C25.0085-C25.0120
- peer command,** 828
- peer groups,** 517–518, 570–571
- peer templates,** 518–519
- peer-group command,** 518
- Peers field (EIGRP),** 85
- Pending Routes field (EIGRP),** 85
- penultimate-hop popping (PHP),** 753–754
- perfect forward secrecy,** 824
- period (.),** 497, 502
- periodic rekey,** 824
- permit statements,** 130
- phases, DMVPN (Dynamic Multipoint Virtual Private Network) tunnels,** 777–778
- PHP (penultimate-hop popping),** 753–754
- PID (process ID),** 395
- ping command**
  - BGP (Border Gateway Protocol) troubleshooting, 561, 562, 577, 598–599, 604, 610
  - EIGRP (Enhanced Interior Gateway Routing Protocol) troubleshooting, 169–170, 173–176, 177, 180–181, 184
  - EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 209–210, 213–218
  - FTP (File Transfer Protocol), 901
  - HTTP (Hypertext Transfer Protocol), 900
  - IPv4 (Internet Protocol version 4) troubleshooting, 48–49, 50–51, 53, 855–856
  - IPv6 (Internet Protocol version 6) troubleshooting, 26–27, 54, 57–58, 60–61, 473, 858
  - OSPFv2 (Open Shortest Path First version 2) troubleshooting, 354, 361, 364
  - OSPFv3 (Open Shortest Path First version 3) troubleshooting, 404, 408, 419–420, 422–423
  - redistribution troubleshooting, 711, 712, 717
  - static routing troubleshooting, 61–62, 64
  - VRF-Lite configuration, 740
  - vtv access troubleshooting, 895
- ping vrf command,** 744–745
- pipe (|),** 497, 502
- placement, DR/BDR,** 245–246
- plaintext authentication,** 255, 326
- plus sign (+),** 497, 502
- P-network,** 755
- point-to-multipoint networks,** 246–253, 331
- point-to-point (P2P) networks,** 246, 248–249, 269, 331, 771
- policies, PBR (policy-based routing)**
  - configuration, 635–637
  - local, 637–639
  - overview of, 634–635
- policy maps,** 880–882
- Port Address Translation (PAT),** 845
- port numbers,** 430, 567, 847, 896, 898
- PPP (Point-to-Point Protocol),** 34
- practice exams**

“brain dumps” 952

PCPT (Pearson IT Certification Practice Test) exam software  
*exam scores, C25.0122-C25.0136*  
*tips for, C25.0085-C25.0120*

### pre-exam suggestions

miscellaneous suggestions, 955–956  
 time-check methods, 954–955

### prefix advertisement behavior, 449

### prefix attributes, 446

### Prefix Guard, 887

### prefix keyword, 131

### prefix lists

filtering, 496  
 IPv4, 627  
 IPv6, 627–628  
 processing, 854–855  
 purpose of, 852  
 reading, 853–854  
 trouble ticket: R1 not learning routes, 861–863  
*prefix list review, 862–863*  
*route verification, 862–863*  
*topology, 861*  
 trouble ticket: users in 10.1.1.0/26 and 10.1.1.64/26 network unable to access resources at 10.1.5.5, 607–609

### prefix matching

prefix lists, 627–628  
 prefix match specifications, 625–627

### preparation, exam. *See* exam preparation

### pre-shared key authentication, 824

complete IPsec DMVPN configuration, 834  
 DPD (Dead Peer Protection), 834  
 IKEv2 keyring, 828–829

IKEv2 profile, 829–830

IPsec packet replay protection, 833–834

IPsec profiles, 832–833

IPsec transform set, 831–832

NAT (Network Address Translation) keepalives, 834

tunnel interface encryption, 833

### pre-shared-key command, 828

private autonomous systems numbers, 591

private BGP (Border Gateway Protocol) communities, 514–516

probe state, 811

process ID (PID), 395

### profiles

IKEv2, 829–830

IPsec, 832–833

protocol-dependent modules (PDMs), 75, 188

proxy ARP (Address Resolution Protocol), 44–46

purge messages (NHRP), 775

## Q

---

### QoS (quality of service), 622

DMVPN (Dynamic Multipoint Virtual Private Network) hub configuration, 780

MPLS (Multiprotocol Label Switching), 755

### Query packets

EIGRP (Enhanced Interior Gateway Routing Protocol), 78

EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 191

question mark (?), 497, 503

## R

- RA (router advertisement) Guard, 886
- RADIUS server, 869–874
- radius server RADSRV1 command, 870
- RAs (Router Advertisements), 23–24
- RD (reported distance), 76, 109, 163
- RD (route distinguishers)
  - MPLS Layer 3 VPNs, 757–759
  - VRF-Lite configuration, 746–747
- rd command, 746–747, 758
- Real-Time Transport Protocol (RTP), 79
- REBIND message, 30
- RECONFIGURE message, 30
- records, flow, 923–924
- recursive routing problems, 806–807
- redirect messages (NHRP), 775, 777
- redistribute command, 353, 573, 656, 658, 664, 679, 688, 720
- redistribution
  - commands, 656–657
  - destination protocols, 651
  - destination-specific behaviors
    - BGP topology and configuration*, 670–672
    - EIGRP topology and configuration*, 658–661
    - OSPF forwarding address*, 667–670
    - OSPF topology and configuration*, 663–666
    - OSPF-to-OSPF mutual redistribution*, 666–667
  - mutual, 650–651, 661–663
  - need for, 674
  - nontransitive nature of, 651–652
  - overview of, 650–651
  - protocol-specific configuration, 656–657
  - RIB (Routing Information Base) and, 653–655
  - seed metrics for, 655–656, 688
  - sequential protocol, 653
  - source protocols, 651
  - source-specific behaviors
    - BGP (Border Gateway Protocol)*, 657–658
    - connected networks*, 657
  - troubleshooting. *See* redistribution troubleshooting
- redistribution command, 702
- redistribution troubleshooting, 684–686
  - IPv4 and IPv6 redistribution
    - into BGP*, 699–702
    - into EIGRP*, 689–694
    - into OSPF*, 694–699
    - route redistribution review*, 687–689
    - troubleshooting targets for*, 689
  - with route maps, 702
- routing loops, 679–686
- suboptimal routing, 678–679
- trouble ticket: IPv6 users unable to access resources, 711–717
- trouble ticket: users in BGP autonomous system unable to access IPv4 resources, 717–721
- trouble ticket: users in IPv4 Branch unable to access resources outside Branch office, 703–707
- trouble ticket: users unable to access resources in classless network, 708–711
- redundancy, DMVPN (Dynamic Multipoint Virtual Private Network), 811

- regex. *See* regular expressions
- registration messages (NHS), 775
- regular expressions
  - asterisk (\*), 497, 503
  - BGP table for regex queries, 498
  - brackets ([ ]), 497, 500–501
  - caret (^), 497, 499–500
  - caret in brackets ([^]), 497, 501
  - dollar sign (\$), 497, 500
  - hyphen (-), 497, 501
  - parentheses (), 497, 502
  - period (.), 497, 502
  - pipe (|), 497, 502
  - plus sign (+), 497, 502
  - question mark (?), 497, 503
  - regex reference topology, 497
  - table of, 497
  - underscore (\_), 497, 498–499
- relay agents (DHCP), 12–14, 30–31
- RELAY-FORW message, 30
- RELAY-REPL message, 30
- RELEASE message, 30
- Reliable Transport Protocol (RTP), 78
- remote transfer troubleshooting
  - FTP (File Transfer Protocol), 901–902
  - HTTP (Hypertext Transfer Protocol), 900–901
  - HTTPS (Hypertext Transfer Protocol over Secure Sockets Layer), 900–901
  - SCP (Secure Copy Protocol), 902–903
  - TFTP (Trivial File Transfer Protocol), 899–900
- remote-as statement, 454
- RENEW message, 30
- replay detection, 824, 833–834
- REPLY message, 30
- Reply packets
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 78
  - EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 191
- reported distance (RD), 76, 109, 163
- REQUEST message, 30
- Request packets (EIGRP), 78
- resolution messages (NHRP), 775
- Resource Reservation Protocol (RSVP), 755
- responder address, NHRP (Next Hop Resolution Protocol), 775
- reverse routes, 126–129
- reverse transit NHS record, 775
- RFCs (requests for comments)
  - RFC 1930, 429
  - RFC 1966, 457, 461
  - RFC 2328, 247
  - RFC 2332, 774
  - RFC 2858, 430
  - RFC 4271, 450
  - RFC 4306, 825
  - RFC 5340, 372
  - RFC 6996, 429
  - RFC 7300, 429
  - RFC 7868, 72
- RIB (Routing Information Base), 238
  - failures, verifying, 582
  - NHRP routing table manipulation, 800–802
    - example of, 800–801*
    - next-hop override routing table, 801–802*
    - with summarization, 802–806*
  - redistribution and, 653–655
  - route summarization, 486–488
- rib message flag (NHRP), 788
- RID (router ID), 374

- BGP (Border Gateway Protocol), 435, 551
- EIGRP (Enhanced Interior Gateway Routing Protocol), 87–88
- OSPF (Open Shortest Path First), 229
- OSPFv2 (Open Shortest Path First version 2), 330, 344–346
- verification of, 395
- RIP (Routing Information Protocol), 40, 125**
- route advertisement, 440–443, 609–610**
- route aggregation, 489–491**
- route distinguishers (RD), 746–747, 757–759**
- route filtering**
  - with ACLs (access control lists), 848
  - BGP (Border Gateway Protocol), 582–587
    - AS\_Path*, 497–505
    - BGP route processing logic*, 493–494
    - clearing of BGP connections*, 507
    - distribute list*, 495–496, 586–587
    - overview of*, 493–495
    - prefix list*, 496
    - reference BGP table*, 494–495
    - regular expressions*, 497–503
    - route maps*, 505–507
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 129–132, 157–158
  - EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 197, 201–202
  - OSPFv2 (Open Shortest Path First version 2), 337–339
- route manipulation, EIGRP (Enhanced Interior Gateway Routing Protocol)**
  - definition of, 129
  - route filtering, 129–132
  - traffic steering with offset lists, 132–135
- route maps, 505–507**
  - complex matching, 631–632
  - components of, 628–629
  - conditional match options, 629–631
  - continue keyword, 634
  - multiple conditional match conditions, 631
  - optional actions, 632–634
  - processing order, 628
  - redistribution troubleshooting with, 702
  - trouble tickets: traffic routing from 10.1.4.0/24 to 10.1.1.0/24
    - topology*, 639
    - trouble ticket 15–1*, 639–643
    - trouble ticket 15–2*, 643–645
    - trouble ticket 15–3*, 645–646
- route redistribution. *See* redistribution**
- route reflectors, iBGP (internal BGP) sessions, 457–461**
  - configuration, 459–461
  - loop prevention, 461
  - route reflector clients, 457
- route refresh, 507**
- route summarization**
  - BGP (Border Gateway Protocol)
    - aggregate addresses*, 482–488
    - aggregation with suppression*, 485–488
    - atomic aggregate attribute*, 488–489
    - IPv6 summarization*, 492–493
    - overview of*, 482
    - route aggregation with AS\_SET*, 489–491

- EIGRP (Enhanced Interior Gateway Routing Protocol)
  - automatic*, 118
  - hierarchical nature of*, 114
  - interface-specific*, 114–116
  - metrics*, 117
  - summary discard routes*, 116–117
- OSPF (Open Shortest Path First)
  - external summarization*, 303–305
  - impact on SPF topology calculation*, 299–301
  - inter-area summarization*, 301–303
  - LSA reduction through area segmentation*, 298–299
  - topology example with summarization*, 300–301
- OSPFv2 (Open Shortest Path First version 2), 348–350
- route targets (RTs)**, 747, 757–759
- route troubleshooting**
  - BGP (Border Gateway Protocol)
    - examining in routing table*, 573–574
    - missing or bad network mask command*, 575–576
    - next-hop router not reachable*, 577–579
    - route filtering*, 582–587
    - split-horizon rule*, 579–580
  - EIGRP (Enhanced Interior Gateway Routing Protocol)
    - bad or missing network command*, 152–154
    - better source of information*, 154–157
    - interface is shut down*, 160
    - overview of*, 151–152
    - route filtering*, 157–158
    - split horizon*, 161–162
    - stub configuration*, 158–160
  - OSPFv2 (Open Shortest Path First version 2)
    - better source of information*, 334–337
    - interface not running OSPF process*, 333–334
    - overview of*, 332–333
- route-map** keyword, 628, 635, 689, 690, 699
- Router Advertisements (RAs)**, 23–24
- router bgp** command, 435, 462
- router eigrp** command, 80, 81, 142, 192, 741
- router ID (RID)**. *See* RID (router ID)
- router LSAs (link-state advertisements)**, 264–269
  - flooding, 264–265
  - generic OSPF LSA output for, 265
    - examining*, 266–268
    - neighbor states for*, 268
    - topology*, 266
    - visualization of*, 268–270
- router message flag (NHRP)**, 788
- router ospf** command, 235, 745
- router ospfv3** command, 374
- Router Solicitation (RS) message**, 23
- router-id** command, 229, 330, 374
- route-target export** command, 747, 759
- route-target import** command, 747, 759
- Routing Information Base**. *See* RIB (Routing Information Base)
- Routing Information Protocol (RIP)**, 40, 125, 238
- routing information sources**

- AD (administrative distance) and, 39–41
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 154–157
  - OSPFv2 (Open Shortest Path First version 2), 334–337
  - routing loops caused by redistribution, troubleshooting, 679–686
    - distribute list to control OSPF routes, 683–684
    - EIGRP AD manipulation, 682–683
    - route tags, 684–686
    - routing topology, 679–680
    - sample scenario for, 679–682
  - routing tables
    - BGP (Border Gateway Protocol), 440
      - aggregation*, 483–485
      - examining routes in*, 573–574
      - reference BGP table*, 494–495
      - suppression*, 485–488
    - data structures and, 39
    - without GRE tunnel, 770
    - with GRE tunnel, 773–774
    - IP, 32–35
    - NHRP (Next Hop Resolution Protocol), 800–806
      - next-hop override routing table*, 801–802
      - routing tables, showing*, 800–801
      - with summarization*, 802–806
    - VRF-Lite
      - EIGRP routes in VRF routing table*, 743–744
      - IPv4 global routing table*, 735
      - IPv4 VRF routing tables*, 735–736
      - RED VRF instance routing table*, 741
  - RRs (route reflectors), 457–461
  - RS (Router Solicitation) message, 23
  - RSVP (Resource Reservation Protocol), 755
  - RTP (Real-Time Transport Protocol), 79
  - RTP (Reliable Transport Protocol), 78
  - RTs (route targets), 757–759
- ## S
- 
- SAFI (subsequent address family identifier), 430
  - SAs (security associations), 825, 837–838
  - scalability, BGP (Border Gateway Protocol)
    - iBGP (internal BGP) sessions, 457–461, 462–465
    - IOS XE peer groups, 517–518
    - IOS XE peer templates, 518–519
  - scores, exam, C25.0122-C25.0136
  - SCP (Secure Copy Protocol), 902–903
  - Secure Hash Algorithm (SHA), 831
  - Secure Shell (SSH), 897–898
  - secure transport, IPsec, 821–823
  - security association database (SADB), 833
  - security associations (SAs), 825, 837–838
  - Security Parameter Index (SPI), 381–382
  - seed metrics, 655–656, 678–679, 688
  - Seq # field (OSPF LSDB), 265
  - sequences, LSA (link-state advertisement), 264
  - sequential protocol redistribution, 653
  - server-private name command, 870
  - servers, DHCP (Dynamic Host Configuration Protocol) for IPv4, 15
  - service dhcp command, 13

- service password-encryption
  - command, 898–899
- service policy, 883–885
- service timestamps [debug | log]
  - [datetime | uptime] command, 905
- service-level agreements (SLAs), 755
- sessions. *See* eBGP (external BGP); iBGP (internal BGP)
- set aigp-metric command, 539
- set as-path prepend command, 540, 632, 656
- set commands, 630–634, 635
- set community command, 514
- set community local-as command, 511
- set community no-advertise command, 509
- set community no-export command, 510
- set ikev2-profile command, 832
- set ip next-hop command, 632, 656
- as-set keyword as-set keyword, aggregate-address command, 489–490
- set local-preference command, 532, 632–633, 656
- set metric command, 546, 633, 657, 659
- set origin command, 543, 633, 657
- set tag command, 633
- set transform-set command, 832
- set weight command, 529, 631, 657
- SHA (Secure Hash Algorithm), 831
- shared keyword, 833
- shortcuts, NHRP (Next Hop Resolution Protocol), 777
- shortest path first (SPF) algorithm, 225, 294, 314, 392. *See also* OSPF (Open Shortest Path First)
- show {ip | ipv6} access-list command, 702
- show {ip | ipv6} prefix-list command, 702
- show access-list command, 338, 646, 885
- show access-lists command, 150–151, 158, 327–328, 846, 877–878
- show adjacency detail command, 38
- show bgp *afi safi* community command, 513
- show bgp *afi safi* community local-as command, 512
- show bgp *afi safi* community no-advertise command, 509
- show bgp *afi safi* community no-export, 511
- show bgp *afi safi* detail command, 513
- show bgp *afi safi* neighbors *ip-address* command, 438–440
- show bgp *afi safi* regexp *regex-pattern* command, 497
- show bgp *afi safi* summary command, 437
- show bgp all command, 701
- show bgp command, 443, 445, 446, 447, 531
- show bgp ipv4 unicast command, 444–445, 453, 454, 536, 537–538, 544, 573, 574, 577, 580–583, 588–589, 599, 601–602, 603–604, 605–606, 611, 671–672
- show bgp ipv4 unicast neighbors | i prefix command, 607–608
- show bgp ipv4 unicast neighbors | include BGP command, 568, 717–718
- show bgp ipv4 unicast neighbors command, 559, 567, 587, 721
- show bgp ipv4 unicast neighbors *ip\_address* advertised-routes command, 583–585, 600–601, 607, 607, 609

- show bgp ipv4 unicast neighbors *ip\_address* routes command, 583–584, 599–600, 602
- show bgp ipv4 unicast regexp .\* command, 503
- show bgp ipv4 unicast regexp [4–8]0\_ command, 501
- show bgp ipv4 unicast regexp ^[0–9]+([0–9]+)?\$ command, 503
- show bgp ipv4 unicast regexp ^[13]00\_[^3–8] command, 501
- show bgp ipv4 unicast regexp ^300\_ command, 499–500
- show bgp ipv4 unicast regexp \_.\$ command, 502
- show bgp ipv4 unicast regexp \_4(510)\$ command, 502
- show bgp ipv4 unicast regexp \_40\$ command, 500
- show bgp ipv4 unicast regexp \_100\_ command, 499
- show bgp ipv4 unicast regexp 1[14] command, 501
- show bgp ipv4 unicast regexp (10)+[^ (100)] command, 502
- show bgp ipv4 unicast rib-failure command, 582
- show bgp ipv4 unicast summary command, 447, 559–560, 561, 562–563, 569, 580, 602–603, 606, 717
- show bgp ipv6 unicast | begin Network command, 473, 475
- show bgp ipv6 unicast command, 469–470, 595–596, 615, 616–617
- show bgp ipv6 unicast neighbors command, 468
- show bgp ipv6 unicast summary command, 468–469, 472, 594, 597–598, 616
- show cdp neighbors command, 142, 172, 319, 357, 365
- show cdp neighbors detail command, 406, 703
- show cef interface command, 875
- show class-map command, 880, 885
- show clock command, 849–850, 905
- show crypto ikev2 profile command, 830
- show crypto ikev2 stats command, 839
- show crypto ipsec sa | include spi command, 381–382
- show crypto ipsec sa command, 837
- show debug condition command, 906
- show dmvpn command, 785–786
- show dmvpn detail command, 785, 786–787, 813, 816, 836, 837
- show eigrp address-family ipv4 interfaces command, 206, 215
- show eigrp address-family ipv4 interfaces detail command, 206–207
- show eigrp address-family ipv4 neighbors command, 207, 215
- show eigrp address-family ipv4 topology command, 208–209
- show eigrp address-family ipv6 interfaces command, 206
- show eigrp address-family ipv6 neighbors command, 207
- show eigrp address-family ipv6 topology command, 208–209
- show eigrp protocols command, 205–206
- show flash command, 899–900
- show flow exporter command, 926
- show flow interface command, 926
- show flow monitor command, 923–925, 926
- show flow monitor name command, 924–925
- show flow record command, 923–924
- show interface command, 99, 148

- show interface tunnel command, 773
- show ip access-list command, 586–587
- show ip access-lists command, 856–857
- show ip arp command, 37, 43–46
- show ip bgp command, 573
- show ip bgp neighbors command, 559
- show ip bgp summary command, 559
- show ip cache flow command, 920, 923
- show ip cef command, 37, 927
- show ip cef exact-route command, 37
- show ip dhcp binding command, 17
- show ip dhcp conflict command, 17
- show ip eigrp interface detail command, 93
- show ip eigrp interfaces command, 84, 89, 144, 154, 171, 172, 175, 178
- show ip eigrp interfaces detail command, 84, 109, 126, 148–150, 151, 162
- show ip eigrp neighbors command, 85, 141, 171, 173, 174, 182, 703
- show ip eigrp neighbors detail command, 160
- show ip eigrp topology active command, 112–113
- show ip eigrp topology all-links command, 100, 163–164
- show ip eigrp topology command, 110, 112, 691
  - EIGRP (Enhanced Interior Gateway Routing Protocol) troubleshooting, 154–155, 162–165, 182
  - path metric calculation, 96
  - route redistribution, 655, 660, 662, 705, 706–707
- show ip eigrp vrf command, 741–743
- show ip flow export command, 921–922
- show ip flow interface command, 921
- show ip http client all command, 900
- show ip interface brief command, 142, 172, 179, 215, 319, 561, 708
- show ip interface command, 9–10, 45, 148, 848
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 150–151, 153–154, 161–162
  - OSPFv2 (Open Shortest Path First version 2), 327–328
- show ip nat translations command, 906
- show ip nhrp command, 38, 787, 789–790
- show ip ospf command, 326, 340, 348–349
- show ip ospf database asbr-summary command, 280–281
- show ip ospf database command, 264, 265
  - OSPFv2 (Open Shortest Path First version 2), 335, 338–339, 356–357
  - redistribution troubleshooting, 710–711
  - route redistribution, 695–696, 709
- show ip ospf database external command, 277–278, 664–665, 668, 669
- show ip ospf database network command, 271
- show ip ospf database nssa-external command, 282–283
- show ip ospf database router command, 266–268, 335–336, 362–363
- show ip ospf database summary command, 274–275
- show ip ospf interface brief command, 236, 245, 319–320, 322–323, 329, 357, 365

- show ip ospf interface command, 235–236, 248–255, 321
  - DR (designated router) verification, 342–344
  - mismatched area numbers, 322
  - mismatched authentication information, 326–327
  - mismatched network types, 331–332
  - trouble ticket, 357–359
- show ip ospf neighbor command, 237–238, 317, 328, 351, 355, 357, 364
- show ip ospf virtual-links command, 308–309, 352
- show ip policy command, 639, 641, 646
- show ip prefix-list command, 158, 182–183, 338, 608, 609, 853, 862–863
- show ip protocols command, 98, 100, 114, 206, 410–411, 690
  - BGP (Border Gateway Protocol) troubleshooting, 585–587, 607
  - EIGRP (Enhanced Interior Gateway Routing Protocol) troubleshooting
    - bad or missing network command*, 153
    - discontiguous networks and autosummarization*, 166–167
    - incorrect network statement*, 144–145
    - load balancing*, 168–169
    - mismatched autonomous system numbers*, 142–143
    - mismatched K values*, 145–146
    - passive interfaces*, 89–91, 146–147
    - route filtering*, 158
    - route summarization*, 167–168
    - stub configuration*, 159–160
    - trouble tickets*, 170–171, 178–179, 182–183
- OSPFv2 (Open Shortest Path First version 2) troubleshooting, 320
  - duplicate router IDs*, 330, 344–346
  - interface not running OSPF process*, 320, 333–334
  - load balancing*, 352–353
  - mismatched area type*, 323–324
  - passive interfaces*, 325–326
  - route filtering*, 337–338
  - trouble tickets*, 355
- prefix list trouble ticket, 862
- redistribution troubleshooting, 695, 700–701, 704–705, 718–719, 720–721
- show ip rip database command, 654
- show ip route bgp command, 447, 574
- show ip route command, 43, 116, 214–215, 640
  - AD (administrative distance) verification, 41
  - BGP (Border Gateway Protocol) troubleshooting, 561, 562, 601, 604, 611
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 155–156, 169–170, 174, 175–176, 177–180, 183
  - NHRP (Next Hop Resolution Protocol), 790–791
  - OSPF (Open Shortest Path First), 296, 298
  - OSPFv2 (Open Shortest Path First version 2), 354, 356, 360, 363–364
  - packet-forwarding process troubleshooting, 35–37
  - PBR (policy-based routing), 637
  - prefix list trouble ticket, 862

- route redistribution, 655, 660, 665, 691–692, 696–697, 703, 706, 707, 708–709, 711, 719
- static routing, 62–66
- unequal-cost load balancing, 102
- VRF-Lite configuration, 734
- show ip route eigrp command, 86, 115–116, 118, 122, 130–132, 133–134, 155–157, 662
- show ip route next-hop-override command, 801–802
- show ip route ospf command, 238–239, 241, 302, 303, 304–305, 309, 334, 363, 667
- show ip route ospfv3 command, 418
- show ip route static command, 42
- show ip route vrf command, 734–736, 737–738, 739–741, 743–744
- show ip sla application command, 912–913
- show ip sla configuration command, 913–914
- show ip sla responder command, 915–916
- show ip sla statistics command, 914–915
- show ip ssh command, 897, 898
- show ip vrf command, 730, 731–732
- show ip vrf interfaces command, 733–734
- show ipv6 access-list command, 851, 860–861
- show ipv6 cef command, 927
- show ipv6 dhcp binding command, 28
- show ipv6 dhcp interface command, 28
- show ipv6 dhcp pool command, 28
- show ipv6 eigrp interfaces command, 193, 200, 201
- show ipv6 eigrp interfaces detail command, 199, 200, 203
- show ipv6 eigrp neighbors command, 193, 197–198, 210–211
- show ipv6 eigrp neighbors detail command, 202–203
- show ipv6 eigrp topology command, 211–212, 693, 713–714, 715–716
- show ipv6 interface brief command, 198, 210–211
- show ipv6 interface command, 22, 24–26, 28–29, 55–56, 59, 400, 851, 859–860
- show ipv6 neighbors command, 47
- show ipv6 nhrp [brief | detail] command, 813
- show ipv6 nhrp nhs [detail] command, 813
- show ipv6 nhrp traffic command, 813
- show ipv6 ospf command, 395–396, 402–403
- show ipv6 ospf database command, 398–399, 697–698
- show ipv6 ospf interface brief command, 396, 405–406, 715
- show ipv6 ospf interface command, 397, 406–407
- show ipv6 ospf neighbor command, 397, 405
- show ipv6 prefix-list command, 201–202, 853
- show ipv6 protocols command, 193, 198–199, 200, 201, 202, 206, 395, 410–411, 692–693, 697, 700–701, 713, 715–716
- show ipv6 route bgp command, 471
- show ipv6 route command, 201, 405
  - BGP (Border Gateway Protocol) troubleshooting, 615
  - EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 213
  - OSPFv3 (Open Shortest Path First version 3) troubleshooting, 420

- redistribution troubleshooting, 693–694, 698–699, 712, 714, 716
- VRF-Lite configuration, 734
- show ipv6 route eigrp command, 193, 196
- show ipv6 route ospf command, 378, 399–400, 401–402, 404, 418
- show ipv6 route static command, 47
- show key chain command, 93, 199
- show line vty command, 895
- show logging command, 904–905
- show mpls ldp bindings command, 753
- show ospfv3 command, 411–413
- show ospfv3 database command, 388–390, 415–418
- show ospfv3 database link [self-originate] command, 388
- show ospfv3 database network [self-originate] command, 387–388
- show ospfv3 database router command, 385
- show ospfv3 interface brief command, 413
- show ospfv3 interface command, 377, 379, 382–383, 413–414
- show ospfv3 ipv6 command, 421
- show ospfv3 ipv6 neighbor command, 377
- show ospfv3 neighbor command, 414
- show policy-map command, 885
- show policy-map control-plane [input | output] command, 883–885
- show route-map command, 613–614, 642
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 158
  - OSPFv2 (Open Shortest Path First version 2), 338
  - PBR (policy-based routing), 641, 644
- show run | include ip route command, 63, 364
- show run | include ipv6 route command, 65
- show run | include ipv6 unicast-routing command, 25
- show run | s router bgp command, 569
- show run | section ipv6 router eigrp command, 201–202, 212
- show run | section ipv6 router ospf command, 402
- show run | section router bgp command, 565–566, 608, 612–613, 616, 720
- show run | section router eigrp command, 145, 158, 172, 179, 706, 710
- show run | section router ospf command, 353, 365, 710
- show run | section router ospfv3 command, 422
- show run interface command, 52, 56, 59–60, 407–408
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 148–150
  - OSPFv2 (Open Shortest Path First version 2), 329, 359
- show running-config | section router eigrp command, 215–216
- show running-config flow record command, 923–924
- show running-config interface command, 324, 326
- show snmp host command, 910
- show snmp mib ifmib ifindex detail command, 909
- show snmp user command, 909
- show snmp view command, 910
- show ssh command, 898
- show tcp brief all command, 564
- show tcp brief command, 433

- show time-range AFTERHOURS command, 849
- show track command, 917–918
- show users command, 895
- show version command, 897
- show vrf command, 730, 731–732
- show vrf ipv4 unicast interfaces command, 733–734, 737–738, 739–740
- show vrf ipv6 unicast interfaces command, 733–734
- SIA (stuck in active) queries, 112–114
- Simple Network Management Protocol (SNMP), 906–910
- single-hop sessions, 430–431
- SLAAC (stateless address autoconfiguration), 22–27
- SLAs (service-level agreements), 755
- SNA (Systems Network Architecture), 769
- SNMP (Simple Network Management Protocol), 906–910
- snmp trap ip verify drop-rate command, 875
- snmp-server host command, 907, 908
- snmp-server ifindex persist command, 907, 909
- soft keyword, 507
- SOLICIT message, 29, 30
- source and responder topology, Cisco IOS IP SLA, 910–911
- Source Guard, 887
- source protocols, redistribution, 651
- source-specific redistribution behaviors, 657–658
- Spanning Tree Protocol (STP), 15–16
- SPF (shortest path first) algorithm, 225, 294, 314. *See also* OSPF (Open Shortest Path First)
- SPF trees (SPTs), 225–226
- SPI (Security Parameter Index), 381–382
- split horizon, 203–204
  - BGP (Border Gateway Protocol), 579–580
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 126–129, 161–162
- spoke routers, 782–784
- spoke-to-hub phase, 777
- spoke-to-spoke communication, DMVPN tunnels, 777
  - initiation of traffic between spoke routers, 795
  - NHRP routing table manipulation
    - next-hop override routing table*, 801–802
    - routing tables, showing*, 800–801
    - with summarization*, 802–806
  - spoke-to-spoke tunnel formation, 796–800
- spot-the-difference troubleshooting, 142–143
- SPTs (SPF trees), 225–226
- SSH (Secure Shell), 897–898
- standard ACLs (access control lists), 622–623
- standard IPv4 ACLs (access control lists), 846
- stateful DHCPv6, 27–28
- stateless address autoconfiguration (SLAAC), 22–27
- stateless DHCPv6, 28–29
- State/PfxRcd field (BGP), 438
- states
  - BGP (Border Gateway Protocol), 432–435, 563
  - OSPF (Open Shortest Path First) neighbors, 230

- OSPFv2 (Open Shortest Path First version 2), 318–319
- TCP (Transmission Control Protocol) sessions, 564
- static routes, 3
  - front door VRF (FVRF), 810
  - IPv4, 42–46, 61–64
  - IPv6, 46–48, 64–66
- status, of DMVPN (Dynamic Multipoint Virtual Private Network) tunnels, 784–787
- steering traffic, with EIGRP offset lists, 132–135
- STP (Spanning Tree Protocol), 15–16
- strict mode, uRPF (Unicast Reverse Path Forwarding), 874
- stub configuration
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 158–160
  - EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 202–203
- stub networks, 269
- stub routers
  - configuration, 119–121
  - stub site functions, 121–125
- stubby areas, 395
  - OSPF (Open Shortest Path First), 284–287
    - not-so-stubby-areas (NSSAs)*, 289–292
    - overview of*, 284
    - stub areas*, 284–287
    - totally not-so-stubby-areas (NSSAs)*, 292–294
    - totally stubby areas*, 287–289
  - OSPFv2 (Open Shortest Path First version 2), 339–340
- stub-site wan-interface command, 124
- stuck in active (SIA) queries, 112–114
- study plan
  - assessing exam readiness, C25.0122-C25.0136
  - exam updates, 954–956
  - exam-day advice, 956-C25.0083
  - failed attempts
    - note-taking after*, C25.0068-C25.0083
    - study suggestions after*, C25.0138-C25.0146
  - final thoughts on, C25.0163-C25.0165
  - practice exams
    - exam scores*, C25.0122-C25.0136
    - tips for*, C25.0085-C25.0120
  - pre-exam suggestions, 956
    - miscellaneous suggestions*, 955–956
    - time-check methods*, 954–955
  - resources, 952–953
  - study tasks, C25.0148-C25.0161
- subinterfaces, VRF-Lite configuration, 732–733
- subnet masks, 10–11
- subnets
  - determining IPv4 addresses in, 10–11
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 148
  - IPv4 (Internet Protocol version 4), 10–11
  - OSPFv2 (Open Shortest Path First version 2), 324–325
- subnets keyword, 664, 694–695
- suboptimal routing caused by redistribution, 678–679
- subsequent address family identifier (SAFI), 430
- successors, 76
- summarization of routes. *See* route summarization

summary discard routes, 116–117

summary LSAs (link-state advertisements), 271–276

- conceptual diagram, 273
- examining, 274–275
- fields, 275
- generic OSPF LSA output for, 273–274
- visualization of, 275–276

summary-address command, 115–116, 349

summary-metric command, 117

summary-only keyword, 485

suppression, aggregation with, 485–488

synchronization, BGP (Border Gateway Protocol), 450

syslog, 807, 904–906

Systems Network Architecture (SNA), 769

## T

---

tables, routing. *See* routing tables

TACACS+ server, 869–874

tag keyword, 664

tagged routes, 684–686

TblVer field (BGP), 438

TCAM (Ternary Content Addressable Memory), 886

TCP (Transmission Control Protocol)

- port numbers, 430, 566, 847, 896, 898
- session state, 564

TE (Traffic Engineering), 755

Telnet

- IPv4 ACL (access control list) trouble ticket, 855–856, 857
- IPv6 ACL (access control list) trouble ticket, 858–859, 861

- vty access troubleshooting, 895–897

template peer-policy command, 519

template peer-session command, 518–519

TEMPLATE-CHILD-POLICY, 519

TEMPLATE-PARENT-POLICY, 519

templates, IOS XE peer templates, 518–519

terminal monitor command, 896, 904

terminal no monitor command, 896

Ternary Content Addressable Memory (TCAM), 886

test aaa command, 872

TFTP (Trivial File Transfer Protocol), 27, 899–900

time to live (TTL), 750, 774

- eBGP (external BGP), 453
- packet-forwarding process, 32–33
- TTL expired in transit, 361–362

time-based IPv4 ACLs (access control lists), 848–850

time-burner questions, 945

time-check methods, 954–955

time-exceeded message, 32–33

timeout (NHRP), 810–811

timers

- BGP (Border Gateway Protocol), 572–573
- EIGRP (Enhanced Interior Gateway Routing Protocol)
  - configuration*, 113–114
  - convergence*, 109–112
  - hello timer*, 108–109
  - hold timer*, 108–109
  - SIA (stuck in active) queries*, 112–114
  - timers*, 108–109
  - troubleshooting*, 151, 200
- NetFlow, 923

- OSPF (Open Shortest Path First), 254–255
- OSPFv2 (Open Shortest Path First version 2), 321–322
- timers active-time command, 113**
- topology**
  - BFD (Bidirectional Forwarding Detection), 466
  - BGP (Border Gateway Protocol)
    - confederations, 462*
    - eBGP (external BGP), 454–455*
    - iBGP (internal BGP), 454–455*
    - IPv6 sample topology, 492*
    - Local AS community, 511–512*
    - local preference, 533*
    - MP-BGP (Multiprotocol BGP), 465–466, 593–594*
    - No\_Advertise community, 509*
    - No\_Export community, 510*
    - path selection, 543*
    - regular expressions, 497*
    - route summarization, 482–483*
    - simple eBGP topology, 436–437*
  - EIGRP (Enhanced Interior Gateway Routing Protocol)
    - convergence, 109–112*
    - distribution list filtering, 130*
    - offset list, 132–133*
    - route summarization, 114*
    - sample topology and configuration, 83–84*
    - SIA (stuck in active) queries, 112–114*
  - EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 208–209
  - GRE (Generic Routing Encapsulation) tunnels, 769–770
  - IPv4 (Internet Protocol version 4), 31–32
    - ACL (access control list), 855*
    - trouble tickets, 48*
  - IPv6 (Internet Protocol version 6), 858
  - MP-BGP (Multiprotocol BGP), 593
  - OSPF (Open Shortest Path First)
    - broadcast networks, 247*
    - default route, 241–242*
    - loopback networks, 253–254*
    - LSA (link-state advertisement), 264*
    - nonbroadcast networks, 247–248*
    - point-to-multipoint networks, 249–253*
    - point-to-point (P2P) networks, 248–249*
    - sample topology and configuration, 233–235*
    - topology example with summarization, 300–301*
    - Type 1 LSA (router LSA), 266*
  - OSPFv3 (Open Shortest Path First version 3), 374–375, 401
  - PBR (policy-based routing) trouble tickets, 639
  - prefix list trouble ticket, 861
  - redistribution
    - BGP, 670–672*
    - EIGRP, 658–661*
    - EIGRP-to-EIGRP, 661–663*
    - OSPF, 663–667*
    - routing loops caused by redistribution, 679–680*
    - suboptimal routing caused by redistribution, 678*
  - route verification, 862–863
  - topology base command, 84, 118**

topology table, EIGRP (Enhanced Interior Gateway Routing Protocol), 76–77

totally not-so-stubby-areas (NSSAs), 292–294, 395

totally stubby areas, 287–289, 395

traceroute command

BGP (Border Gateway Protocol), 605, 610, 614

NHRP (Next Hop Resolution Protocol), 791

OSPFv2 (Open Shortest Path First version 2), 362

OSPFv3 (Open Shortest Path First version 3), 420

PBR (policy-based routing), 635

redistribution troubleshooting, 678, 707

static routing trouble tickets, 64–65, 66

Traffic Engineering (TE), 755

traffic steering, 132–135

transform set (IPsec), 831–832

transit areas, 350

transit branch routing, 119–121

transit networks, 268

Transmission Control Protocol. *See* TCP (Transmission Control Protocol)

transport input command, 895

transport input ssh command, 897

transport mode (ESP), 825, 826–827

transport output ssh command, 898

transport output telnet command, 896

Trivial File Transfer Protocol (TFTP), 27, 899–900

trouble tickets. *See also* troubleshooting

BGP (Border Gateway Protocol)

*link between R1 and R3 not forwarding traffic to BGP AS 65501, 598–604*

*MP-BGP default route not being learned, 615–617*

*traffic out of autonomous system flowing through R3 and across backup link, 610–614*

*users in 10.1.1.0/26 and 10.1.1.64/26 unable to access resources at 10.1.5.5, 604–610*

conditional forwarding

*topology, 639*

*trouble tickets, 639–646*

EIGRP (Enhanced Interior Gateway Routing Protocol), 169–176, 177–184

EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 209–218

IPv4 (Internet Protocol version 4)

*PC1 not able to access resources on 192.0.2.1, 48–53*

*static routes, 61–64*

*topology, 48*

*users in IPv4 Branch unable to access resources outside Branch office, 703–707*

*users unable to access resources in classless network, 708–711*

IPv4 ACL (access control list), 855–857

*failed Telnet and successful ping, 855–856*

*named ACL configuration mode, 857*

*packet match verification, 857*

*successful Telnet connection, 857*

*topology, 855*

*verification of ACL*

*configuration, 856–857*

- IPv6 (Internet Protocol version 6)
  - Branch receiving inter-area routes other than default, 401–404*
  - Branch users unable to access resources outside Branch office, 404–408*
  - IPv6 users unable to access resources, 711–717*
  - PC1 not able to access resources on 2001:db8:d::1, 54–61*
  - users in BGP autonomous system unable to access IPv4 resources, 717–721*
- IPv6 ACL (access control list), 858–861
  - ENARSI IPv6 ACL on R1, 860–861*
  - failed Telnet and successful ping, 858–859*
  - successful Telnet connection, 861*
  - topology, 858*
  - verification of ACL configuration, 859–860*
- OSPFv2 (Open Shortest Path First version 2)
  - routers R1 and R2 not forming neighbor adjacency, 364–366*
  - users in 10.1.1.0/24 not able to access resources in 192.168.1.0/24, 353–364*
- OSPFv3 (Open Shortest Path First version 3)
  - Branch receiving inter-area routes other than default, 401–404*
  - Branch users unable to access resources outside Branch office, 404–408*
  - topology, 401*
- prefix list
  - prefix list review, 862–863*
  - route verification, 862–863*
  - topology, 861*
- redistribution
  - IPv6 users unable to access resources, 711–717*
  - users in BGP autonomous system unable to access IPv4 resources, 717–721*
  - users in IPv4 Branch unable to access resources outside Branch office, 703–707*
  - users unable to access resources in classless network, 708–711*
- troubleshooting. *See also* trouble tickets**
  - AAA (authentication, authorization, and accounting), 869–874*
  - BGP (Border Gateway Protocol)*
    - ACLs (access control lists), 566–567*
    - BGP packets sourced from wrong IP address, 564–566*
    - incorrect neighbor statement, 564*
    - interface is down, 561*
    - Layer 3 connectivity is broken, 561–562*
    - misconfigured peer groups, 570–571*
    - mismatched authentication, 570*
    - neighbor lacks route to local router, 563*
    - neighbor verification, 559–560*
    - overview of, 559–561*
    - path to neighbor is through default route, 562–563*
    - timers, 572–573*
    - TTL (time to live) expiration, 568–570*

- Cisco IOS IP SLA, 916–917
- CoPP (Control Plane Policing)
  - ACL (access control list) configuration*, 876–878
  - class map configuration*, 878–880
  - overview of*, 875–876, 885
  - policy map configuration*, 880–882
  - service policy applied to control plane interface*, 883–885
- device management
  - console access*, 893–894
  - overview of*, 893
  - vty access*, 894–899
- DHCP (Dynamic Host Configuration Protocol) for IPv4, 16–18
- DMVPN (Dynamic Multipoint Virtual Private Network) tunnels
  - front door VRF (FVRF)*, 808–810
  - outbound interface selection*, 808
- EIGRP (Enhanced Interior Gateway Routing Protocol)
  - autosummarization*, 165–168
  - better source of information*, 154–157
  - discontiguous networks*, 165–167
  - feasible successors*, 162–165
  - interface is shut down*, 160
  - load balancing*, 168–169
  - neighbor adjacencies*, 141–151
  - neighbor issues*, 197–201
  - overview of*, 151–152
  - route filtering*, 157–158
  - routes*, 151–162, 201–204
  - split horizon*, 161–162
  - stub configuration*, 158–160
  - trouble tickets*, 169–176, 177–184
- EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6)
  - named EIGRPv6*, 204–209
  - trouble ticket: users unable to access Internet*, 209–213
  - trouble ticket: users unable to access resources outside their LAN*, 213–218
- IPv4 (Internet Protocol version 4)
  - IPv4 static routes*, 61–64
  - PC1 not able to access resources on 192.0.2.1*, 48–53
  - trouble tickets topology*, 48
- IPv4 ACLs (access control lists), 846–847
  - importance of*, 845
  - packet filtering*, 848
  - time-based*, 848–850
  - trouble ticket*, 855–857
- IPv6 (Internet Protocol version 6), 64–66
  - trouble ticket 1–3: PC1 not able to access resources on 2001:db8:d::1*, 54–57
  - trouble ticket 1–4: PC1 not able to access resources on 2001:db8:d::1*, 57–61
- IPv6 ACLs (access control lists)
  - importance of*, 850
  - packet filtering*, 851–852
  - reading*, 850–851
  - trouble ticket*, 858–861
- local PBR (policy-based routing), 638–639
- management tools
  - BFD (Bidirectional Forwarding Detection)*, 927–928

- Cisco DNA Center Assurance, 929–940*
- Cisco IOS IP SLA, 910–917*
- Flexible NetFlow, 923–927*
- NetFlow, 919–924*
- Object Tracking, 917–919*
- SNMP (Simple Network Management Protocol), 906–910*
- syslog, 904–906*
- OSPF (Open Shortest Path First), 231–232
- OSPFv2 (Open Shortest Path First version 2)
  - ACLs (access control lists), 327–328*
  - adjacency states, 318–319*
  - advertisement tracking, 346–348*
  - better source of information, 334–337*
  - default routes, 353*
  - different subnets, 324–325*
  - discontiguous areas, 350–352*
  - duplicate router IDs, 330, 344–346*
  - interface is down, 319*
  - interface not running OSPF process, 319–321, 333–334*
  - load balancing, 352–353*
  - mismatched area numbers, 322–323*
  - mismatched area types, 323–324*
  - mismatched authentication information, 326–327*
  - mismatched network types, 330–332*
  - mismatched timers, 321–322*
  - MTU mismatch, 328–330*
  - neighbor verification, 317*
  - overview of, 317–319, 332–333*
  - passive interfaces, 325–326*
  - route filtering, 337–339*
  - route summarization, 348–350*
  - stub area configuration, 339–340*
  - trouble ticket: routers R1 and R2 not forming neighbor adjacency, 364–366*
  - trouble ticket: users in 10.1.1.0/24 not able to access resources in 192.168.1.0/24, 353–364*
  - wrong designated router elected, 341–344*
- OSPFv3 (Open Shortest Path First version 3)
  - debug ipv6 ospf hello command, 406*
  - debug ospfv3 command, 418*
  - default-information originate command, 422*
  - overview of, 394–395*
  - sample configuration, 408–410*
  - show cdp neighbors detail command, 406*
  - show ip protocols command, 410–411*
  - show ip route ospfv3 command, 418*
  - show ipv6 interface command, 400*
  - show ipv6 ospf command, 395–396, 402–403*
  - show ipv6 ospf database command, 398–399*
  - show ipv6 ospf interface brief command, 396, 405–406*
  - show ipv6 ospf interface command, 397, 406–407*
  - show ipv6 ospf neighbor command, 397, 405*

- show ipv6 protocols command*, 395, 410–411
- show ipv6 route command*, 405, 420
- show ipv6 route ospf command*, 399–400, 401–402, 404, 418
- show ospfv3 command*, 411–413
- show ospfv3 database command*, 415–418
- show ospfv3 interface brief command*, 413
- show ospfv3 interface command*, 413–414
- show ospfv3 ipv6 command*, 421
- show ospfv3 neighbor command*, 414
- show run | section router ospfv3 command*, 422
- topology*, 401
- trouble ticket: Branch receiving inter-area routes other than default*, 401–404
- trouble ticket: Branch users unable to access IPv6-enabled resources on Internet*, 419–423
- trouble ticket: Branch users unable to access resources outside Branch office*, 404–408
- overlay networks, 806–810
- packet-forwarding process, 35–38
- prefix lists, 852
  - processing*, 854–855
  - reading*, 853–854
  - trouble ticket*, 861–863
- redistribution
  - into EIGRP*, 689–694
  - into OSPF*, 694–699
  - with route maps*, 702
  - route redistribution review*, 687–689
- routing loops, 679–686
- suboptimal routing, 678–679
- trouble ticket: IPv6 users unable to access resources*, 711–717
- trouble ticket: users in BGP autonomous system unable to access IPv4 resources*, 717–721
- trouble ticket: users in IPv4 Branch unable to access resources outside Branch office*, 703–707
- trouble ticket: users unable to access resources in classless network*, 708–711
- troubleshooting targets for*, 689
- route maps
  - topology*, 639
  - trouble tickets*, 639–646
- uRPF (Unicast Reverse Path Forwarding), 874–875
- TTL (time to live), 750, 774
  - eBGP (external BGP), 453
  - packet-forwarding process, 32–33
  - TTL expired in transit, 361–362, 568–570
- tunnel destination command*, 770, 782
- tunnel key command*, 781, 782, 792
- tunnel keys*, 782, 792
- tunnel mode (ESP)*, 825, 827
- tunnel mode gre multipoint command*, 780, 792
- tunnel mode gre multipoint ipv6 command*, 812, 813
- tunnel protection ipsec profile profile-name [shared] command*, 833
- tunnel source command*, 770, 780, 782, 792

tunnels. *See* DMVPN (Dynamic Multipoint Virtual Private Network) tunnels; GRE (Generic Routing Encapsulation) tunnels

Type 1 LSA (router LSA), 264–269

flooding, 264–265

generic OSPF LSA output for, 265

*examining*, 266–268

*neighbor states for*, 268

*topology*, 266

*visualization of*, 268–270

Type 2 LSA (network LSA), 269–271

Type 3 LSA (summary LSA), 271–276

conceptual diagram, 273

examining, 274–275

fields, 275

generic OSPF LSA output for, 273–274

visualization of, 275–276

Type 4 LSA (ASBR summary LSA), 279–281

Type 5 LSA (external LSA), 277–279, 679

Type 7 LSA (NSSA external LSA), 281–283

## U

---

UDP (User Datagram Protocol), 847

underlay networks. *See* VPNs (virtual private networks)

underscore ( \_ ), 497, 498–499

unequal-cost load balancing, 100–102

Unicast Reverse Path Forwarding. *See* uRPF (Unicast Reverse Path Forwarding)

unique global unicast addressing, 467

unique IP NHRP registration, 794–795

unique message flag (NHRP), 788

Un/Reliable field (EIGRP), 85

up state, GRE (Generic Routing Encapsulation), 771

Update packets

BGP (Border Gateway Protocol), 431, 432

EIGRP (Enhanced Interior Gateway Routing Protocol), 78

EIGRPv6 (Enhanced Interior Gateway Routing Protocol version 6), 191

updates, exam, 954–956

impact on study plan, 955–956

news about, 956

schedule for, 954–955

Up/Down field (BGP), 438

uRPF (Unicast Reverse Path Forwarding), 866, 874–875

used message flag (NHRP), 788

User Datagram Protocol. *See* UDP (User Datagram Protocol)

username admin password 0 letmein command, 869–870

## V

---

variable-length subnet masking (VLSM), 72, 222

variance, 168–169

variance command, 168

variance multiplier, 100–102

variance value, 100–102

vendor private extension (NHRP), 776

views, SNMP (Simple Network Management Protocol), 910

VIRL (Virtual Internet Routing Lab), 952

Virtual Internet Routing Lab (VIRL), 952

virtual links

- OSPF (Open Shortest Path First), 307–309
- OSPFv2, 350–352
- virtual routing and forwarding.**  
  *See* VRF (virtual routing and forwarding)
- VLANs, 15–16
- VLSM (variable-length subnet masking), 72, 222
- VPNs (virtual private networks), 119
  - definition of, 724
  - labels, 759
  - MPLS Layer 3 VPNs
    - architecture*, 756–757
    - CE (customer edge) routers*, 756
    - label stack*, 759–761
    - PE (provider edge) routers*, 756
    - RD (route distinguishers)*, 757–759
    - RTs (route targets)*, 757–759
    - VPNv4 addresses*, 757–759
- VPNv4 addresses, 757–759
- VRF (virtual routing and forwarding).  
  *See also* VRF-Lite configuration
  - definition of, 727
  - front door VRF (FVRF), 808–810
    - configuration*, 809–810
    - definition of*, 808
    - static routes*, 810
- vrf definition command, 728, 734, 809
- vrf forwarding command, 730–731, 809
- VRF mode, uRPF (Unicast Reverse Path Forwarding), 874
- VRF-Lite configuration
  - connections, verifying, 740
  - EIGRP configuration for multiple VRF instances, 741
  - EIGRP neighbors, 742–743
  - EIGRP routes in VRF routing table, 743–744
  - instance creation, 728–730
  - interface assignment, 730–731
  - interface IPv4 and IPv6 addresses, 733–734
  - interface participation in EIGRP processes, 741–742
  - IPv4 global routing table, 735
  - IPv4 VRF routing tables, 735–736
  - MP-BGPv4 address families for multiple VRF instances, 746
  - OSPFv3 address families for multiple VRF instances, 745–746
  - overview of, 728
  - RED VRF instance routing table, 741
  - route distinguishers, 746–747
  - route targets, 747
  - subinterfaces on R1, 732–733
  - VRF connectivity, 744–745
  - VRF instances on R1, 733–734
  - VRF instances on R2, 736–738
  - VRF instances on R3, 738–740
- vty access troubleshooting, 894–899**
  - password encryption levels, 898–899
  - SSH (Secure Shell), 897–898
  - Telnet, 895–897

## W

---

- WANs (wide area networks), EIGRP for
  - IP bandwidth percentage, 125–126
  - split horizon, 126–129, 161–162
  - stub routers, 119–121
  - stub site functions, 121–125
- warning percentage, 516
- warning-only keyword, 516

weight, best-path decision-making process, 528–532, 588

Weight field (BGP), 445

well-known BGP (Border Gateway Protocol) communities

conditionally matching, 512–514

local AS, 511–512

No\_Advertise, 509–510

No\_Export, 510–511

No\_Export\_SubConfed, 511–512

private, 514–516

well-known discretionary path attributes, 429, 528

well-known mandatory path attributes, 429, 528

wide metrics, EIGRP (Enhanced Interior Gateway Routing Protocol), 96–98

## X-Y-Z

---

X.25, 247

Xmt Queue field (EIGRP), 85