Special Sales

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

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

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

Feedback Information

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

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

We greatly appreciate your assistance.

Editor-in-Chief: Mark Taub
Technical Editors: Hector Mendoza, Jr, Russ Long
Alliances Manager, Cisco Press: Arzou Gol
Editorial Assistant: Cindy Teeters
Director, Product Manager: Brett Bartow
Designer: Chuti Prasertsith
Managing Editor: Sandra Schroeder
Composition: codeMantra
Development Editor: Marianne Bartow
Indexer: Cheryl Ann Lenser
Project Editor: Mandie Frank
Proofreader: Abigail Bass
Copy Editor: Kitty Wilson
Credits

Figure 7-1 Screenshot of wireshark ©2019 wireshark
Contents at a Glance

Introduction xxxi

Chapter 1 IPv4/IPv6 Addressing and Routing Review 2
Chapter 2 EIGRP 70
Chapter 3 Advanced EIGRP 106
Chapter 4 Troubleshooting EIGRP for IPv4 138
Chapter 5 EIGRPv6 188
Chapter 6 OSPF 222
Chapter 7 Advanced OSPF 258
Chapter 8 Troubleshooting OSPFv2 310
Chapter 9 OSPFv3 364
Chapter 10 Troubleshooting OSPFv3 386
Chapter 11 BGP 420
Chapter 12 Advanced BGP 474
Chapter 13 BGP Path Selection 514
Chapter 14 Troubleshooting BGP 546
Chapter 15 Route Maps and Conditional Forwarding 610
Chapter 16 Route Redistribution 640
Chapter 17 Troubleshooting Redistribution 668
Chapter 18 VRF, MPLS, and MPLS Layer 3 VPNs 718
Chapter 19 DMVPN Tunnels 748
Chapter 20 Securing DMVPN Tunnels 802
Chapter 21 Troubleshooting ACLs and Prefix Lists 824
Chapter 22 Infrastructure Security 846
Chapter 23  Device Management and Management Tools Troubleshooting  868
Chapter 24  Final Preparation  912
Appendix A  Answers to the “Do I Know This Already?” Quiz Questions  922
Appendix B  CCNP Enterprise Advanced Routing ENARSI 300-410 Official Certification Guide Exam Updates  932
  Glossary  934
  Index  952

Online Elements
  Glossary
Appendix C  Command Reference Exercises
Appendix D  Command Reference Exercises Answer Key
Appendix E  Study Planner
Contents

Introduction xxxi

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 18
IPv6 Addressing Review 19
EUI-64 20
IPv6 SLAAC, Stateful DHCPv6, and Stateless DHCPv6 22
SLAAC 22
Stateful DHCPv6 26
Stateless DHCPv6 28
DHCPv6 Operation 29
DHCPv6 Relay Agents 29
Packet-Forwarding Process 30
Reviewing the Layer 3 Packet-Forwarding Process 30
Troubleshooting the Packet-Forwarding Process 34
Routing Information Sources 38
Data Structures and the Routing Table 38
Sources of Routing Information 39
Static Routes 41
IPv4 Static Routes 41
IPv6 Static Routes 45
Trouble Tickets 47
IPv4 Addressing and Addressing Technologies Trouble Tickets 47
Trouble Ticket 1-1 48
Trouble Ticket 1-2 49
IPv6 Addressing Trouble Tickets 53
Trouble Ticket 1-3 53
Trouble Ticket 1-4 56
Chapter 2  EIGRP  70

“Do I Know This Already?” Quiz  70

Foundation Topics  73

EIGRP Fundamentals  73

Autonomous Systems  73

EIGRP Terminology  74

Topology Table  75

EIGRP Neighbors  76

Inter-Router Communication  76

Forming EIGRP Neighbors  77

EIGRP Configuration Modes  78

Classic Configuration Mode  78

EIGRP Named Mode  79

EIGRP Network Statement  80

Sample Topology and Configuration  81

Confirming Interfaces  83

Verifying EIGRP Neighbor Adjacencies  84

Displaying Installed EIGRP Routes  85

Router ID  86

Passive Interfaces  87

Authentication  91

Keychain Configuration  91

Enabling Authentication on the Interface  91

Path Metric Calculation  93

Wide Metrics  96

Metric Backward Compatibility  98

Interface Delay Settings  98

Custom K Values  99

Load Balancing  99

References in This Chapter  102

Exam Preparation Tasks  102
Chapter 3  Advanced EIGRP  106

“Do I Know This Already?” Quiz  106
Foundation Topics  108
Failure Detection and Timers  108
  Convergence  109
  Stuck in Active  112
Route Summarization  113
  Interface-Specific Summarization  114
  Summary Discard Routes  116
  Summarization Metrics  116
  Automatic Summarization  117
WAN Considerations  118
  EIGRP Stub Router  118
  Stub Site Functions  121
  IP Bandwidth Percentage  125
  Split Horizon  126
Route Manipulation  128
  Route Filtering  129
  Traffic Steering with EIGRP Offset Lists  132
References in This Chapter  134
Exam Preparation Tasks  135
Review All Key Topics  135
Complete Tables and Lists from Memory  135
Define Key Terms  135
Use the Command Reference to Check Your Memory  135

Chapter 4  Troubleshooting EIGRP for IPv4  138

“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 160
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 190
EIGRPv6 Fundamentals 190
  
  EIGRPv6 Inter-Router Communication 191
  EIGRPv6 Configuration 191
  
  **EIGRPv6 Classic Mode Configuration** 191
  **EIGRPv6 Named Mode Configuration** 192
  **EIGRPv6 Verification** 192
  
  IPv6 Route Summarization 195
  Default Route Advertising 196
  Route Filtering 196
Troubleshooting EIGRPv6 Neighbor Issues 197
  Interface Is Down 198
Duplicate Router IDs 325
Mismatches Network Types 326
Troubleshooting OSPFv2 Routes 327
Interface Not Running the OSPF Process 328
Better Source of Information 329
Route Filtering 332
Stub Area Configuration 335
Interface Is Shut Down 336
Wrong Designated Router Elected 336
Duplicate Router IDs 340
Troubleshooting Miscellaneous OSPFv2 Issues 341
Tracking OSPF Advertisements Through a Network 341
Route Summarization 343
Discontiguous Areas 345
Load Balancing 347
Default Route 348
OSPFv2 Trouble Tickets 348
Trouble Ticket 8-1 349
Trouble Ticket 8-2 356
Trouble Ticket 8-3 359
Exam Preparation Tasks 361
Review All Key Topics 361
Define Key Terms 362
Use the Command Reference to Check Your Memory 362

Chapter 9  OSPFv3 364
“Do I Know This Already?” Quiz 364
Foundation Topics 365
OSPFv3 Fundamentals 365
OSPFv3 Link-State Advertisement 366
OSPFv3 Communication 367
OSPFv3 Configuration 368
OSPFv3 Verification 371
The Passive Interface 372
IPv6 Route Summarization 373
Network Type 374
OSPFv3 Authentication 375
OSPFv3 Link-Local Forwarding 377
OSPFv3 LSA Flooding Scope 378
Chapter 10 Troubleshooting OSPFv3 386

“Do I Know This Already?” Quiz 386

Foundation Topics 388

Troubleshooting OSPFv3 for IPv6 388

OSPFv3 Troubleshooting Commands 389

OSPFv3 Trouble Tickets 395

Trouble Ticket 10-1 395

Trouble Ticket 10-2 398

Troubleshooting OSPFv3 Address Families 402

OSPFv3 AF Trouble Ticket 412

Trouble Ticket 10-3 412

Exam Preparation Tasks 416

Review All Key Topics 416

Define Key Terms 417

Use the Command Reference to Check Your Memory 417

Chapter 11 BGP 420

“Do I Know This Already?” Quiz 420

Foundation Topics 422

BGP Fundamentals 422

Autonomous System Numbers (ASNs) 422

BGP Sessions 423

Path Attributes 423

Loop Prevention 423

Address Families 423

Inter-Router Communication 424

BGP Messages 425

BGP Neighbor States 426

Basic BGP Configuration 428

Verification of BGP Sessions 431

Prefix Advertisement 433

Receiving and Viewing Routes 436

Understanding BGP Session Types and Behaviors 441

iBGP 441
Chapter 12 Advanced BGP  474

“Do I Know This Already?” Quiz  474
Foundation Topics  476
Route Summarization  476
  Aggregate Addresses  476
  The Atomic Aggregate Attribute  481
  Route Aggregation with AS_SET  483
BGP Route Filtering and Manipulation  486
  Distribution List Filtering  487
  Prefix List Filtering  488
  AS_Path Filtering  489
  Regular Expressions (Regex)  489
  AS_Path ACLs  495
  Route Maps  497
  Clearing BGP Connections  499
BGP Communities  499
  Enabling BGP Community Support  500
  Well-Known Communities  500
  The No_Advertise BGP Community  501
  The No_Export BGP Community  502
  The Local-AS (No_Export_SubConfed) BGP Community  503
Chapter 13  BGP Path Selection  514

“Do I Know This Already?” Quiz  515

Foundation Topics  516

Understanding BGP Path Selection  516

BGP Best Path  517

Weight  519

Local Preference  522

Phase I: Initial BGP Edge Route Processing  525

Phase II: BGP Edge Evaluation of Multiple Paths  526

Phase III: Final BGP Processing State  527

Locally Originated in the Network or Aggregate Advertisement  528

Accumulated Interior Gateway Protocol (AIGP)  528

Shortest AS Path  530

Origin Type  532

Multi- Exit Discriminator  534

Missing MED Behavior  537

Always Compare MED  538

BGP Deterministic MED  538

eBGP over iBGP  540

Lowest IGP Metric  540

Prefer the Oldest EBGP Path  541

Router ID  541

Minimum Cluster List Length  541

Lowest Neighbor Address  541

BGP Equal-Cost Multipath  542

Exam Preparation Tasks  543
Chapter 14 Troubleshooting BGP 546

“Do I Know This Already?” Quiz 547

Foundation Topics 549

Troubleshooting BGP Neighbor Adjacencies 549
  Interface Is Down 551
  Layer 3 Connectivity Is Broken 551
  Path to the Neighbor Is Through the Default Route 552
  Neighbor Does Not Have a Route to the Local Router 553
  Incorrect neighbor Statement 553
  BGP Packets Sourced from the Wrong IP Address 554

ACLs 555
  The TTL of the BGP Packet Expires 557
  Mismatched Authentication 559
  Misconfigured Peer Groups 560
  Timers 561

Troubleshooting BGP Routes 562
  Missing or Bad network mask Command 564
  Next-Hop Router Not Reachable 566
  BGP Split-Horizon Rule 568
  Better Source of Information 569
  Route Filtering 572

Troubleshooting BGP Path Selection 577
  Understanding the Best-Path Decision-Making Process 577
  Private Autonomous System Numbers 581
  Using debug Commands 581

Troubleshooting BGP for IPv6 583

BGP Trouble Tickets 587
  Trouble Ticket 14-1 588
  Trouble Ticket 14-2 593
  Trouble Ticket 14-3 600

MP-BGP Trouble Ticket 604
  Trouble Ticket 14-4 604

Exam Preparation Tasks 607

Review All Key Topics 607
Define Key Terms 608
Use the Command Reference to Check Your Memory 608

Chapter 15  Route Maps and Conditional Forwarding 610
“Do I Know This Already?” Quiz 610
Foundation Topics 612
Conditional Matching 612
   Access Control Lists (ACLs) 612
   Standard ACLs 612
   Extended ACLs 613
Prefix Matching 614
   Prefix Lists 617
IPv6 Prefix Lists 617
Route Maps 618
   Conditional Matching 619
   Multiple Conditional Match Conditions 620
Complex Matching 621
Optional Actions 621
Continue 622
Conditional Forwarding of Packets 623
   PBR Configuration 624
Local PBR 626
Trouble Tickets 628
   Trouble Ticket 15-1 629
   Trouble Ticket 15-2 632
   Trouble Ticket 15-3 634
Exam Preparation Tasks 636
Review All Key Topics 637
Define Key Terms 637
Use the Command Reference to Check Your Memory 637

Chapter 16  Route Redistribution 640
“Do I Know This Already?” Quiz 640
Foundation Topics 641
Redistribution Overview 641
Redistribution Is Not Transitive 643
Sequential Protocol Redistribution 645
Routes Must Exist in the RIB 645
Seed Metrics 647
Chapter 17 Troubleshooting Redistribution

“Do I Know This Already?” Quiz

Foundation Topics

Troubleshooting Advanced Redistribution Issues

Troubleshooting Suboptimal Routing Caused by Redistribution

Troubleshooting Routing Loops Caused by Redistribution

Troubleshooting IPv4 and IPv6 Redistribution

Route Redistribution Review

Troubleshooting Redistribution into EIGRP

Troubleshooting Redistribution into OSPF

Troubleshooting Redistribution into BGP

Troubleshooting Redistribution with Route Maps

Redistribution Trouble Tickets

Trouble Ticket 17-1

Trouble Ticket 17-2

Trouble Ticket 17-3

Trouble Ticket 17-4

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Use the Command Reference to Check Your Memory
Chapter 18  VRF, MPLS, and MPLS Layer 3 VPNs  718
“Do I Know This Already?” Quiz  718
Foundation Topics  720
Implementing and Verifying VRF-Lite  720
VRF-Lite Overview  721
Creating and Verifying VRF Instances  721
An Introduction to MPLS Operations  734
MPLS LIB and LFIB  734
Label Switching Routers  735
Label-Switched Path  736
Labels  736
Label Distribution Protocol  737
Label Switching  738
Penultimate Hop Popping  739
An Introduction to MPLS Layer 3 VPNs  739
MPLS Layer 3 VPNs  740
MPLS Layer 3 VPNv4 Address  741
MPLS Layer 3 VPN Label Stack  743
Reference in This Chapter  745
Exam Preparation Tasks  745
Review All Key Topics  745
Define Key Terms  746
Use the Command Reference to Check Your Memory  746

Chapter 19  DMVPN Tunnels  748
“Do I Know This Already?” Quiz  748
Foundation Topics  750
Generic Routing Encapsulation (GRE) Tunnels  750
GRE Tunnel Configuration  751
GRE Sample Configuration  753
Next Hop Resolution Protocol (NHRP)  756
Dynamic Multipoint VPN (DMVPN)  758
Phase 1: Spoke-to-Hub  759
Phase 2: Spoke-to-Spoke  759
Phase 3: Hierarchical Tree Spoke-to-Spoke  759
DMVPN Phase Comparison  760
DMVPN Configuration  761
DMVPN Hub Configuration  762
DMVPN Spoke Configuration for DMVPN Phase 1 (Point-to-Point)  764
Chapter 20  Securing DMVPN Tunnels  802

“Do I Know This Already?” Quiz  802

Foundation Topics  803

Elements of Secure Transport  803

IPsec Fundamentals  805

Security Protocols  806

Authentication Header  806

Encapsulating Security Payload (ESP)  806

Key Management  806

Security Associations  806

ESP Modes  807

DMVPN Without IPsec  808

DMVPN with IPsec in Transport Mode  808
Chapter 21 Troubleshooting ACLs and Prefix Lists 824

“Do I Know This Already?” Quiz 824

Foundation Topics 827

Troubleshooting IPv4 ACLs 827

Reading an IPv4 ACL 827

Using an IPv4 ACL for Filtering 829

Using a Time-Based IPv4 ACL 829

Troubleshooting IPv6 ACLs 830

Reading an IPv6 ACL 831

Using an IPv6 ACL for Filtering 832

Troubleshooting Prefix Lists 833

Reading a Prefix List 833

Prefix List Processing 835

Trouble Tickets 836

Trouble Ticket 21-1: IPv4 ACL Trouble Ticket 836

Trouble Ticket 21-2: IPv6 ACL Trouble Ticket 839

Trouble Ticket 21-3: Prefix List Trouble Ticket 842

Exam Preparation Tasks 844
Chapter 22 Infrastructure Security 846
“Do I Know This Already?” Quiz 846
Foundation Topics 849
Cisco IOS AAA Troubleshooting 849
Troubleshooting Unicast Reverse Path Forwarding (uRPF) 852
Troubleshooting Control Plane Policing (CoPP) 854
Creating ACLs to Identify the Traffic 854
Creating Class Maps to Define a Traffic Class 856
Creating Policy Maps to Define a Service Policy 859
Applying the Service Policy to the Control Plane 861
CoPP Summary 863
IPv6 First-Hop Security 863
Router Advertisement (RA) Guard 863
DHCPv6 Guard 864
Binding Table 864
IPv6 Neighbor Discovery Inspection/IPv6 Snooping 864
Source Guard 864
Exam Preparation Tasks 864
Review All Key Topics 865
Define Key Terms 865
Use the Command Reference to Check Your Memory 865

Chapter 23 Device Management and Management Tools Troubleshooting 868
“Do I Know This Already?” Quiz 868
Foundation Topics 871
Device Management Troubleshooting 871
Console Access Troubleshooting 871
vty Access Troubleshooting 872
Telnet 872
SSH 874
Password Encryption Levels 875
Remote Transfer Troubleshooting 875
TFTP 875
HTTP(S) 876
SCP 877
Chapter 24  Final Preparation  912

Advice About the Exam Event  912
  Think About Your Time Budget Versus Numbers of Questions  912
  A Suggested Time-Check Method  913
  Miscellaneous Pre-Exam Suggestions  914
  Exam-Day Advice  914
  Reserve the Hour After the Exam in Case You Fail  915
  Take Practice Exams  916

Advice on How to Answer Exam Questions  917
  Assessing Whether You Are Ready to Pass (and the Fallacy of Exam Scores)  918
  Study Suggestions After Failing to Pass  919
  Other Study Tasks  920
  Final Thoughts  921

Appendix A  Answers to the “Do I Know This Already?” Quiz Questions  922

Appendix B  CCNP Enterprise Advanced Routing ENARSI 300-410 Official Certification Guide Exam Updates  932

Glossary  934

Index  952
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 master instructor for Cisco Enterprise Routing and Switching, AWS, and ITIL 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 110 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 a systems architect at Cisco Systems. He 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 and consistency. 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 Reviewers

Hector Mendoza, Jr., 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, he 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.

Russ Long was introduced to computers and networking at a very young age, when he tried to save the world from digital monsters and aliens, an endeavor that keeps him busy to this day. Russ started his career in enterprise-level IT work splicing fiber-optic networks in the Pacific Northwest. His career has taken a long and winding path from there: from systems administrator, to IT consultant and computer shop owner, to IT instructor. Roughly the last decade of his career has focused solely on instruction and consulting in IT environments. Some of his favorite topics include Cisco routing and switching, real-world security, storage solutions, and virtualization.
Dedications

Raymond Lacoste:
This book 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. I know that you want to write a book with wizards and princesses, but I don't know how to do that. However, these are your words in a book:

I can speak in Spanish, English, French, Chinese, and Parseltongue!

—Teagan Edgeworth
Acknowledgments

Raymond Lacoste:
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.

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!

To Russ Long, a long-time friend and a man whom I can trust. Thank you for finding my mistakes before the readers do. You have always been there to make me look my best. (The R&R Show for life!)

To Hector Mendoza, Jr.: I don’t know you personally, but you found those little things that make a huge difference to the readers, and for that I thank you!

To Brett Bartow, thanks for trusting us to put this book together and put our knowledge on paper.

To MJB, thank you for keeping me on task and making sure nothing slipped through the cracks.

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 editors: Hector and Russ, thank you for finding our mistakes before everyone else found them. If any slipped by, I completely blame the both of you.

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. Special gratitude goes to Craig Smith, Aaron Foss, Ramiro Garza Rios, Vinit Jain, Richard Furr, David Prall, Dustin Schuemann, Tyson Scott, Denise Fishbourne, Tyler Creek, and Mohammad Ali.
Icons Used in This Book

ASA
Firewall

LAN
Segment

Serial

Switched
Circuit

Radio
Tower

Routing
Domain

Router

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 certifications:

Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP), and Cisco Certified Internetwork Expert (CCIE).

Cisco announced changes to all three certifications to take effect in February 2020. The announcement included many changes, but these are the most notable:

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

CCNP Enterprise candidates need to take and pass the CCNP and CCIE Enterprise CoreENCOR 350-401 examination. Then they need to take and pass one of the following Concentration exams to obtain their CCNP Enterprise:

- 300-410 ENARSI to obtain Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)
- 300-415 ENSDWI to obtain Implementing Cisco SD-WAN Solutions (SDWAN300)
- 300-420 ENSLD to obtain Designing Cisco Enterprise Networks (ENSLD)
- 300-425 ENWLSD to obtain Designing Cisco Enterprise Wireless Networks (ENWLSD)
- 300-430 ENWLSI to obtain Implementing Cisco Enterprise Wireless Networks (ENWLSI)
- 300-435 ENAUTO to obtain Implementing Automation for Cisco Enterprise Solutions (ENAUTO)
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 using the following methods:

- 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 already have 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 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.

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 troubleshooting 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 you can troubleshooting 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 relating 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 you to 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.

The last chapter, Chapter 24, “Final Preparation,” provides tips and strategies for studying for 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 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

<table>
<thead>
<tr>
<th>Implementing Cisco Enterprise Advanced Routing (ENARSI) (300-410) Exam Topic</th>
<th>Chapter(s) in Which Topic Is Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Layer 3 Technologies</td>
<td></td>
</tr>
<tr>
<td>1.1 Troubleshoot administrative distance (all routing protocols)</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Troubleshoot route map for any routing protocol (attributes, tagging, filtering)</td>
<td>17</td>
</tr>
<tr>
<td>1.3 Troubleshoot loop prevention mechanisms (filtering, tagging, split horizon, route poisoning)</td>
<td>17</td>
</tr>
<tr>
<td>1.4 Troubleshoot redistribution between any routing protocols or routing sources</td>
<td>16, 17</td>
</tr>
<tr>
<td>1.5 Troubleshoot manual and auto-summarization with any routing protocol</td>
<td>3, 4, 5, 7, 8, 9, 10, 12</td>
</tr>
<tr>
<td>1.6 Configure and verify policy-based routing</td>
<td>15</td>
</tr>
<tr>
<td>1.7 Configure and verify VRF-Lite</td>
<td>18</td>
</tr>
<tr>
<td>1.8 Describe Bidirectional Forwarding Detection</td>
<td>23</td>
</tr>
<tr>
<td>1.9 Troubleshoot EIGRP (classic and named mode)</td>
<td>4, 5</td>
</tr>
<tr>
<td>1.9.a Address families (IPv4, IPv6)</td>
<td>2, 3, 4, 5</td>
</tr>
<tr>
<td>1.9.b Neighbor relationship and authentication</td>
<td>2, 4, 5</td>
</tr>
<tr>
<td>1.9.c Loop-free path selections (RD, FD, FC, successor, feasible successor, stuck in active)</td>
<td>3, 4</td>
</tr>
<tr>
<td>1.9.d Stubs</td>
<td>4</td>
</tr>
<tr>
<td>1.9.e Load balancing (equal and unequal cost)</td>
<td>2</td>
</tr>
<tr>
<td>1.9.f Metrics</td>
<td>2</td>
</tr>
<tr>
<td>1.10 Troubleshoot OSPF (v2/v3)</td>
<td>6, 7, 8, 9, 10</td>
</tr>
<tr>
<td>1.10.a Address families (IPv4, IPv6)</td>
<td>8, 10</td>
</tr>
<tr>
<td>1.10.b Neighbor relationship and authentication</td>
<td>6, 8, 10</td>
</tr>
<tr>
<td>Implementing Cisco Enterprise Advanced Routing</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>(ENARSI) (300-410) Exam Topic</td>
<td></td>
</tr>
<tr>
<td>Chapter(s) in Which Topic Is Covered</td>
<td></td>
</tr>
<tr>
<td>1.10.c Network types, area types, and router types</td>
<td>8, 10</td>
</tr>
<tr>
<td>1.10.c (i) Point-to-point, multipoint, broadcast, nonbroadcast</td>
<td>6, 8, 10</td>
</tr>
<tr>
<td>1.10.c (ii) Area type: backbone, normal, transit, stub, NSSA, totally stub</td>
<td>7, 8, 10</td>
</tr>
<tr>
<td>1.10.c (iii) Internal router, backbone router, ABR, ASBR</td>
<td>6, 8, 10</td>
</tr>
<tr>
<td>1.10.c (iv) Virtual link</td>
<td>7, 8</td>
</tr>
<tr>
<td>1.10.d Path preference</td>
<td>7</td>
</tr>
<tr>
<td>1.11 Troubleshoot BGP (Internal and External)</td>
<td>11, 12, 13, 14</td>
</tr>
<tr>
<td>1.11.a Address families (IPv4, IPv6)</td>
<td>10, 14</td>
</tr>
<tr>
<td>1.11.b Neighbor relationship and authentication (next-hop, multihop, 4-byte AS, private AS, route refresh, synchronization, operation, peer group, states and timers)</td>
<td>10, 14</td>
</tr>
<tr>
<td>1.11.c Path preference (attributes and best-path)</td>
<td>13, 14</td>
</tr>
<tr>
<td>1.11.d Route reflector (excluding multiple route reflectors, confederations, dynamic peer)</td>
<td>10</td>
</tr>
<tr>
<td>1.11.e Policies (inbound/outbound filtering, path manipulation)</td>
<td>11, 14</td>
</tr>
<tr>
<td>2.0 VPN Technologies</td>
<td></td>
</tr>
<tr>
<td>2.1 Describe MPLS operations (LSR, LDP, label switching, LSP)</td>
<td>18</td>
</tr>
<tr>
<td>2.2 Describe MPLS Layer 3 VPN</td>
<td>18</td>
</tr>
<tr>
<td>2.3 Configure and verify DMVPN (single hub)</td>
<td>19, 20</td>
</tr>
<tr>
<td>2.3.a GRE/mGRE</td>
<td>19</td>
</tr>
<tr>
<td>2.3.b NHRP</td>
<td>19</td>
</tr>
<tr>
<td>2.3.c IPsec</td>
<td>20</td>
</tr>
<tr>
<td>2.3.d Dynamic neighbor</td>
<td>19</td>
</tr>
<tr>
<td>2.3.e Spoke-to-spoke</td>
<td>19</td>
</tr>
<tr>
<td>3.0 Infrastructure Security</td>
<td></td>
</tr>
<tr>
<td>3.1 Troubleshoot device security using IOS AAA (TACACS+, RADIUS, local database)</td>
<td>22</td>
</tr>
<tr>
<td>3.2 Troubleshoot router security features</td>
<td></td>
</tr>
<tr>
<td>3.2.a IPv4 access control lists (standard, extended, time-based)</td>
<td>21</td>
</tr>
<tr>
<td>3.2.b IPv6 traffic filter</td>
<td>21</td>
</tr>
<tr>
<td>3.2.c Unicast reverse path forwarding (uRPF)</td>
<td>22</td>
</tr>
<tr>
<td>3.3 Troubleshoot control plane policing (CoPP) (Telnet, SSH, HTTP(S), SNMP, EIGRP, OSPF, BGP)</td>
<td>22</td>
</tr>
<tr>
<td>3.4 Describe IPv6 First Hop Security features (RA Guard, DHCP Guard, binding table, ND inspection/snooping, Source Guard)</td>
<td>22</td>
</tr>
<tr>
<td>4.0 Infrastructure Services</td>
<td></td>
</tr>
<tr>
<td>4.1 Troubleshoot device management</td>
<td>23</td>
</tr>
<tr>
<td>4.1.a Console and VTY</td>
<td>23</td>
</tr>
</tbody>
</table>
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.

### 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 the reader 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 http://virl.cisco.com.

- 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 http://dcloud.cisco.com.

- Cisco Devnet provides many resources on programming and programmability, along with free labs. For more information, see http://developer.cisco.com.
CHAPTER 2

EIGRP

This chapter covers the following topics:

■ EIGRP Fundamentals: This section explains how EIGRP establishes a neighborship 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 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

<table>
<thead>
<tr>
<th>Foundation Topics Section</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIGRP Fundamentals</td>
<td>1–6</td>
</tr>
<tr>
<td>EIGRP Configuration Modes</td>
<td>7–9</td>
</tr>
<tr>
<td>Path Metric Calculation</td>
<td>10</td>
</tr>
</tbody>
</table>

**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 is not required to match 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. The EIGRP process is initialized by which of the following technique? (Choose two.)
   a. Using the interface command \texttt{ip eigrp as-number ipv4 unicast}
   b. Using the global configuration command \texttt{router eigrp as-number}
   c. Using the global configuration command \texttt{router eigrp process-name}
   d. Using the interface command \texttt{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 key-chain sequence number 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 impacts on other routing protocols, like OSPF?
    a. Interface bandwidth
    b. Interface MTU
    c. Interface delay
    d. Interface priority
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. Using hop count for path selection does not take into account link speed and total delay. EIGRP adds logic to the route-selection algorithm that uses factors besides hop count.

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. Do not confuse an EIGRP autonomous system with a Border Gateway Protocol (BGP) autonomous system.

In Figure 2-1, EIGRP autonomous system (AS) 100 consists of R1, R2, R3, 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 used as a reference topology for R1 calculating the best path and alternative loop-free paths to the 10.4.4.0/24 network. The values in parentheses represent the link's calculated metric for a segment based on bandwidth and delay.

![Figure 2-2 EIGRP Reference Topology](image)

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successor route</td>
<td>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.</td>
</tr>
<tr>
<td>Successor</td>
<td>The first next-hop router for the successor route. The successor for 10.4.4.0/24 is R3.</td>
</tr>
<tr>
<td>Feasible distance (FD)</td>
<td>The metric value for the lowest-metric path to reach a destination. The feasible distance is calculated locally using the formula shown in the &quot;Path Metric Calculation&quot; section, later in this chapter. The FD calculated by R1 for the 10.4.4.0/24 network is 3328 (that is, 256 + 256 + 2816).</td>
</tr>
<tr>
<td>Reported distance (RD)</td>
<td>Distance reported by a router to reach a prefix. The reported distance value is the feasible distance for the advertising router. R3 advertises the 10.4.4.0/24 prefix with an RD of 3072. R4 advertises the 10.4.4.0/24 to R1 and R2 with an RD of 2816.</td>
</tr>
<tr>
<td>Feasibility condition</td>
<td>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.</td>
</tr>
<tr>
<td>Feasible successor</td>
<td>A route with 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.</td>
</tr>
</tbody>
</table>
Topography 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 10.4.0.0/24 network when explaining the topology table.

Figure 2-3  EIGRP Topology Output
Examine the network 10.4.4.0/24 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 3072, the second entry passes the feasibility condition and classifies the second entry as the feasible successor for the 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**

EIGRP does not rely on periodic advertisement of all the network prefixes in an autonomous system, which is done with routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Intermediate System-to-Intermediate System (IS-IS). 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 its own 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.

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

**NOTE** EIGRP uses multicast packets to reduce bandwidth consumed on a link (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.

**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.
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 set individually are hello advertisement interval, split-horizon, authentication, and summary route advertisements.

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 [mask]`. The network statement is explained in the following sections.
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 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 [mask]`. The optional `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 the networks 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>
<thead>
<tr>
<th>Table 2-4</th>
<th>Table of Sample Interface and IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router Interface</td>
<td>IP Address</td>
</tr>
<tr>
<td>Gigabit Ethernet 0/0</td>
<td>10.0.0.10/24</td>
</tr>
<tr>
<td>Gigabit Ethernet 0/1</td>
<td>10.10.10.24</td>
</tr>
<tr>
<td>Gigabit Ethernet 0/2</td>
<td>192.0.0.10/24</td>
</tr>
<tr>
<td>Gigabit Ethernet 0/3</td>
<td>192.10.10.24</td>
</tr>
</tbody>
</table>

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 10.0.10.20 0.0.0.0
    network 192.0.0.20 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 causes the network statements to match all IP addresses within the /24 network range.

**Example 2-2  EIGRP Configuration with 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 unintended interfaces.

**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.

![EIGRP Sample Topology](image-url)
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 from 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  Named Mode Configuration Structure

<table>
<thead>
<tr>
<th>Command</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1# show run</td>
<td>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</td>
</tr>
<tr>
<td>R2# show run</td>
<td>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</td>
</tr>
</tbody>
</table>

**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]]` 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  Verification of EIGRP Interfaces

<table>
<thead>
<tr>
<th>Command</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1# show ip eigrp interfaces EIGRP-IPv4 Interfaces for AS(100) Xmit Queue PeerQ Mean Pacing Time Multicast Pending Interface Peers Un/Reliable Un/Reliable SRTT Un/Reliable Flow Timer Routes G10/2 0 0/0 0/0 0 0/0 0 0 G10/1 1 0/0 0/0 10 0/0 50 0 Lo0 0 0/0 0/0 0 0/0 0 0</td>
<td>R2# show ip eigrp interfaces gi0/1 detail</td>
</tr>
</tbody>
</table>
Table 2-5 provides a brief explanation to the key fields shown with the EIGRP interfaces.

### Table 2-5 EIGRP Interface Fields

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

### Verifying EIGRP Neighbor Adjacencies

Each EIGRP process maintains a table of neighbors to ensure that they are alive and processing updates properly. Without keeping track of a neighbor state, 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 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  G10/1        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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>IP address of the EIGRP neighbor</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface the neighbor was detected on</td>
</tr>
<tr>
<td>Holdtime</td>
<td>Time left to receive a packet from this neighbor to ensure that it is still alive</td>
</tr>
<tr>
<td>SRTT</td>
<td>Time for a packet to be sent to a neighbor and a reply to be received from that neighbor, in milliseconds</td>
</tr>
<tr>
<td>RTO</td>
<td>Timeout for retransmission (waiting for ACK)</td>
</tr>
<tr>
<td>Q Cnt</td>
<td>Number of packets (update/query/reply) in queue for sending</td>
</tr>
<tr>
<td>Seq Num</td>
<td>Sequence number that was last received from this router</td>
</tr>
</tbody>
</table>

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 originating 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
```
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

<table>
<thead>
<tr>
<th>Sample Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1(config)# router eigrp 100</td>
</tr>
<tr>
<td>R2(config-router)# eigrp router-id 192.168.1.1</td>
</tr>
<tr>
<td>R2(config-router)# router eigrp EIGRP-NAMED</td>
</tr>
<tr>
<td>R2(config-router)# address-family ipv4 unicast autonomous-system 100</td>
</tr>
<tr>
<td>R2(config-router-af)# eigrp router-id 192.168.2.2</td>
</tr>
</tbody>
</table>
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 that interface.

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**

```bash
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)# 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**

```bash
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
```
Example 2-11 shows what the named mode configuration looks like with some settings (i.e. passive-interface or no passive-interface) placed under the af-interface default or the af-interface interface-id setting.

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

```
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
(GigabitEthernet0/1) is down: interface passive
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
(GigabitEthernet0/1) is up: new adjacency
```

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  Passive Interfaces do not Appear

To accelerate troubleshooting of passive interfaces, and other settings, the command `show ip protocols` 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  IP Protocols Output

```plaintext
R1# show ip protocols
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:

<table>
<thead>
<tr>
<th>Gateway</th>
<th>Distance</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.12.1.2</td>
<td>90</td>
<td>00:21:35</td>
</tr>
</tbody>
</table>

Distance: internal 90 external 170

R2# show ip protocols

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:

<table>
<thead>
<tr>
<th>Gateway</th>
<th>Distance</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.12.1.1</td>
<td>90</td>
<td>00:24:26</td>
</tr>
</tbody>
</table>

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 a Message Digest 5 (MD5) authentication, using 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 that 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 the `af-interface default` or the `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
```

The 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  EIGRP Authentication Configuration**

```
R1(config)#
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)#
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  Verification of 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 provides detailed EIGRP interface output.
## Example 2-16  Verification of EIGRP Authentication

<table>
<thead>
<tr>
<th>Interface</th>
<th>Peers</th>
<th>Xmit Queue</th>
<th>PeerQ</th>
<th>Mean</th>
<th>Pacing Time</th>
<th>Multicast Pending</th>
<th>Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/1</td>
<td>0</td>
<td>0/0</td>
<td>0/0</td>
<td>0</td>
<td>0/0</td>
<td>0</td>
<td>50</td>
</tr>
</tbody>
</table>

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"

---

### 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. The formula shown in Figure 2-6 illustrates the EIGRP classic metric formula.

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

**Figure 2-6  EIGRP Classic 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 is collected from the configured interface bandwidth on an interface. Delay is the total measure of delay in the path, measured in tens of microseconds (μs).

The EIGRP formula is based on the IGRP metric formula, except the output is multiplied by 256 to change the metric from 24 bits to 32 bits. Taking these definitions into consideration, the formula for EIGRP is shown in Figure 2-7.

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

**Figure 2-7  EIGRP Classic Metric Formula with Definitions**
By default, $K_1$ and $K_3$ have a value of 1, and $K_2$, $K_4$, and $K_5$ are set to 0. Figure 2-8 places default K values into the formula and shows a streamlined version of the formula.

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

Equals

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

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

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.

Figure 2-9 shows the information in the EIGRP update packets for the 10.1.1.0/24 prefix 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 some of the common network types, link speeds, delay, and EIGRP metric, using the streamlined formula from Figure 2-7.
Table 2-7  Default EIGRP Interface Metrics for Classic Metrics

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>Link Speed (Kbps)</th>
<th>Delay (μs)</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial</td>
<td>64</td>
<td>20,000</td>
<td>40,512,000</td>
</tr>
<tr>
<td>T1</td>
<td>1544</td>
<td>20,000</td>
<td>2,170,031</td>
</tr>
<tr>
<td>Ethernet</td>
<td>10,000</td>
<td>1000</td>
<td>281,600</td>
</tr>
<tr>
<td>FastEthernet</td>
<td>100,000</td>
<td>100</td>
<td>28,160</td>
</tr>
<tr>
<td>GigabitEthernet</td>
<td>1,000,000</td>
<td>10</td>
<td>2816</td>
</tr>
<tr>
<td>TenGigabitEthernet</td>
<td>10,000,000</td>
<td>10</td>
<td>512</td>
</tr>
</tbody>
</table>

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 μs (10 μs for the 10.4.4.0/24 link, 10 μs for the 10.34.1.0/24 link, and 10 μs for the 10.13.1.0/24 link).

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

Figure 2-10  EIGRP Classic Metric Formula 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  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
```
Wide Metrics

The original EIGRP specifications measured delay in 10-microsecond (μs) units and bandwidth in kilobytes 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**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Scaled Bandwidth</th>
<th>Scaled Delay</th>
<th>Composite Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet</td>
<td>10,000,000 / 1,000,000</td>
<td>10 / 10</td>
<td>2816</td>
</tr>
<tr>
<td>10 GigabitEthernet</td>
<td>10,000,000 / 10,000,000</td>
<td>10 / 10</td>
<td>512</td>
</tr>
<tr>
<td>11 GigabitEthernet</td>
<td>10,000,000 / 11,000,000</td>
<td>10 / 10</td>
<td>256</td>
</tr>
<tr>
<td>20 GigabitEthernet</td>
<td>10,000,000 / 20,000,000</td>
<td>10 / 10</td>
<td>256</td>
</tr>
</tbody>
</table>

EIGRP includes support for a second set of metrics, known as *wide metrics*, that addresses the issue of scalability with higher-capacity interfaces. The original formula referenced in Figure 2-6 is known as *EIGRP classic metrics*. 

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
Chapter 2: EIGRP

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.

$$\text{Wide Metric} = \left( K_1 \times \text{BW} + \frac{K_3 \times \text{Latency}}{256 - \text{Load}} + K_6 \times \text{Extended} \right) \times \frac{K_5}{K_4 + \text{Reliability}} $$

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

Just as EIGRP scaled by 256 to accommodate IGRP, EIGRP wide metrics scale by 65,535 to accommodate higher-speed links. This provides support for interface speeds up to 655 terabits per second ($65,535 \times 10^7$) without any scalability issues. 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.

$$\text{Wide Metric} = 65,535 \times \left( \frac{K_1 \times 10^7}{\text{Min. Bandwidth}} + \frac{K_2 \times 10^7}{\text{Min. Bandwidth} + \frac{K_3 \times \text{Latency}}{256 - \text{Load} + \frac{K_6 \times \text{Extended}}{10^{-6}}} \right) \times \frac{K_5}{K_4 + \text{Reliability}} $$

**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 $10^{13}$/interface bandwidth.

The EIGRP classic metrics exist only with EIGRP classic configuration, while 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 verifies the operational mode of EIGRP on R1 and R2. 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**  Verification of 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 to the formula in Figure 2-13.

Unscaled Bandwidth = \( \frac{EIGRP Bandwidth \times EIGRP Classic Scale}{Scaled Bandwidth} \)

**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.

**Interface Delay Settings**

If you do not remember the delay values from Table 2-7, the values can be dynamically queried with the command `show interface interface-id`. The output displays the EIGRP interface delay, in microseconds, after the DL Y field. Example 2-20 provides sample output of the command on R1 and R2. Both interfaces have a delay of 10.

**Example 2-20**  Verification of 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 μs 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  Interface Delay Configuration

```text
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. The TOS value always has a value of 0, and the K₆ value 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) routing. At the time of this writing, the default maximum ECMP 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

Key Topic

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 multiplier 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.

\[
\text{Feasible Successor FD} \leq \| \text{Variance Multiplier} \|
\]

\[
\begin{align*}
5376 & \leq 1.6 \\
3328 & = 2
\end{align*}
\]

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 both configuration modes.

**Example 2-23  EIGRP Variance Configuration**

<table>
<thead>
<tr>
<th>R1</th>
<th>(Classic Configuration)</th>
<th>R1</th>
<th>(Named Mode Configuration)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>router eigrp 100</td>
<td></td>
<td>router eigrp EIGRP-NAMED</td>
</tr>
<tr>
<td></td>
<td>variance 2</td>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td>network 0.0.0.0</td>
<td></td>
<td>address-family ipv4 unicast autonomous-system 100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>!</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>topology base</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>variance 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exit-af-topology</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>network 0.0.0.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exit-address-family</td>
</tr>
</tbody>
</table>

Example 2-24 provides a brief verification 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  Verification of 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
    Redirecting 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
```
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>
<thead>
<tr>
<th>Table 2-8</th>
<th>Key Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Topic Element</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Paragraph</td>
<td>EIGRP terminology</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Topology table</td>
</tr>
<tr>
<td>Table 2-3</td>
<td>EIGRP packet types</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Forming EIGRP neighbors</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Classic configuration mode</td>
</tr>
<tr>
<td>Paragraph</td>
<td>EIGRP named mode</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Passive interfaces</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Authentication</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Path metric calculation</td>
</tr>
<tr>
<td>Paragraph</td>
<td>EIGRP attribute propagation</td>
</tr>
<tr>
<td>Figure 2-11</td>
<td>EIGRP wide metrics formula</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Custom K values</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Unequal-cost load balancing</td>
</tr>
</tbody>
</table>
Complete Tables and Lists from Memory

There are no memory tables in this chapter.

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, EIGRP classic configuration, EIGRP named mode configuration, passive interface, K values, wide metrics, variance value

Use the Command Reference to Check Your Memory

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, cover the right side of Table 2-9 with a piece of paper, read the description on the left side, and then see how much of the command you can remember.

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

Table 2-9 Command Reference

<table>
<thead>
<tr>
<th>Task</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initialize EIGRP in classic configuration</td>
<td><code>router eigrp as-number</code> network network mask</td>
</tr>
<tr>
<td>Initialize EIGRP in named mode configuration</td>
<td><code>router eigrp process-name</code> address-family `{ipv4</td>
</tr>
<tr>
<td>Define the EIGRP router ID</td>
<td><code>eigrp router-id router-id</code></td>
</tr>
</tbody>
</table>
| Configure an EIGRP-enabled interface to prevent neighbor adjacencies | Classic:  `passive-interface interface-id`   
Named Mode:  `af-interface {default | interface-id}` passive-interface |
<p>| Configure a keychain for EIGRP MDS authentication| <code>key chain key-chain-name</code> key key-number key-string password |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure MD5 authentication for an EIGRP interface</td>
<td><strong>Classic:</strong> (EIGRP Process)</td>
</tr>
<tr>
<td></td>
<td><code>ip authentication key-chain eigrp as-number</code></td>
</tr>
<tr>
<td></td>
<td><code>key-chain-name</code></td>
</tr>
<tr>
<td></td>
<td><code>ip authentication mode eigrp as-number md5</code></td>
</tr>
<tr>
<td></td>
<td><strong>Named Mode:</strong> `af-interface {default</td>
</tr>
<tr>
<td></td>
<td><code>interface-id}</code></td>
</tr>
<tr>
<td></td>
<td><code>authentication key-chain eigrp</code></td>
</tr>
<tr>
<td></td>
<td><code>key-chain-name</code></td>
</tr>
<tr>
<td></td>
<td><code>authentication mode md5</code></td>
</tr>
<tr>
<td>Configure SHA authentication for EIGRP named mode interfaces</td>
<td><strong>Named Mode:</strong> `af-interface {default</td>
</tr>
<tr>
<td></td>
<td><code>interface-id}</code></td>
</tr>
<tr>
<td></td>
<td><code>authentication mode hmac-sha-256 password</code></td>
</tr>
<tr>
<td>Modify the interface delay for an interface</td>
<td><code>delay tens-of-microseconds</code></td>
</tr>
<tr>
<td>Modify the EIGRP K values</td>
<td><code>metric weights TOS K₁ K₂ K₃ K₄ K₅[K₆]</code></td>
</tr>
<tr>
<td>Modify the default number of EIGRP maximum paths that can be installed into the RIB</td>
<td><code>maximum-paths maximum-paths</code></td>
</tr>
<tr>
<td>Modify the EIGRP variance multiplier for unequal-cost load balancing</td>
<td><code>variance multiplier</code></td>
</tr>
<tr>
<td>Display the EIGRP-enabled interfaces</td>
<td><code>show ip eigrp interface [{interface-id</code></td>
</tr>
<tr>
<td>Display the EIGRP topology table</td>
<td>`[detail]</td>
</tr>
<tr>
<td>Display the configured EIGRP keychains and passwords</td>
<td><code>show ip eigrp topology [all-links]</code></td>
</tr>
<tr>
<td>Display the IP routing protocol information configured on the router</td>
<td><code>show key chain</code></td>
</tr>
<tr>
<td></td>
<td><code>show ip protocols</code></td>
</tr>
</tbody>
</table>
**SYMBOLS**

* (asterisk) regular expression, 495  
[] (brackets) regular expression, 493  
^ (caret) regular expression, 491–492  
[^] (caret in brackets) regular expression, 493  
$ (dollar sign) regular expression, 492  
- (hyphen) regular expression, 493  
() (parentheses) regular expression, 494  
. (period) regular expression, 494  
| (pipe) regular expression, 494  
+ (plus sign) regular expression, 494  
? (question mark) regular expression, 495  
_ (underscore) regular expression, 490–491

**A**

AAA (authentication, authorization, accounting), troubleshooting, 849–852  
aaa authentication login CONSOLE ACCESS group TACACSMETHOD local command, 850  
aaa authentication login local command, 866  
aaa authentication login VTY ACCESS group RADIUSMETHOD local command, 850  
aaa group server radius RADIUSMETHOD command, 849–850  
aaa group server tacacs+ TACACSMETHOD command, 850  
aaa new-model command, 849, 866  
Accumulated Interior Gateway Protocol (AIGP), 528–529  
ACLs (access control lists)  
BGP, 555–557  
BGP AS_Path filtering, 495–497  
creating for traffic identification, 854–856  
EIGRP interfaces, troubleshooting, 150–151  
EIGRPv6, 201  
extended ACLs, 613–614  
IPv4 ACLs, troubleshooting, 827–830, 836–838  
IPv6 ACLs, troubleshooting, 830–833, 839–842  
opportunistic overview, 612  
OSPFv2 interfaces, troubleshooting, 323  
standard ACLs, 612–613  
Active state (BGP), 427  
address command, 822  
address families  
BGP, 423–424  
OSPFv3, troubleshooting, 402–416  
address-family afi safi command, 472  
address-family command, 103  
address-family ipv4 vrf autonomous-system command, 730
address-family ipv6 autonomous-system as-number command, 220
address-family ipv6 command, 795
administrative distance (AD), 39–41
modifying
    in BGP, 677
    in EIGRP, 676
    in OSPF, 676–677
verifying
    in BGP, 569–571
    in EIGRPv6, 201
    in OSPFv2, 329–332
aggregate addresses (BGP), 476–481
aggregate-address as-set command, 483–485
aggregate-address command, 464, 476, 479, 512
aggregate-address prefix command, 512
area 23 stub command, 402–403
area authentication command, 257
area command, 308
area nssa command, 288, 308
area nssa no-summary command, 291, 308
area range command, 298, 344, 374, 385
area stub command, 308
area stub no-summary command, 285, 308
area virtual-link command, 304, 308
areas
    OSPF, 226–228
    OSPFv2
        mismatched numbers, 317–318
        mismatched type, 319–320
ARP cache
    MAC address lookups, 43
    proxy ARP disabled, 45
    proxy ARP enabled, 44–45
AS _Path filtering (BGP), 489–497
    ACLs, 495–497
    regular expressions, 489–495
AS _Path length (BGP), 530–532
AS_SET (BGP), 483–485
ASNs (autonomous system numbers), 422, 581
asterisk (*) regular expression, 495
atomic aggregate attribute (BGP), 481–483
authentication
    BGP, mismatched, 559–560
    EIGRP, 91–93
        enabling, 91–93
        keychain configuration, 91
        troubleshooting, 148–150
    EIGRPv6, verifying, 199–200
    NHRP, 775
    OSPF, 253–255
    OSPFv2, 321–322
    OSPFv3, 375–377
    pre-shared key authentication, 808–817
        configuring, 816–817
        dead peer detection, 815
        IKEv2 keyring, 809–810
        IKEv2 profile, 810–811
        NAT keepalives, 815
        packet replay protection, 814–815
        profile, 813–814
        transform set, 812–813
        tunnel interface encryption, 814
authentication headers, 806
authentication key-chain eigrp key-chain-name command, 104
authentication local pre-share command, 822
authentication mode hmac-sha-256 command, 92, 104
authentication mode md5 command, 104
authentication remote pre-share command, 822
auto-cost reference-bandwidth command, 257, 292, 308
automatic route summarization, 117–118
discontiguous networks and, 165–166
autonomous system numbers (ASNs), 422, 581
autonomous systems
BGP, 422
EIGRP, 73
mismatched numbers, 142–143
EIGRPv6, mismatched numbers, 198
auto-summary command, 118

B

bandwidth percentage, 125
bandwidth-percent command, 125
BDR (backup designated router)
elections, 243–244, 336–339
operational overview, 242–243
placement, 244
BFD (Bidirectional Forwarding Detection), troubleshooting, 900–901
bfd interface command, 901
bfd interval command, 901
BGP (Border Gateway Protocol)
ACLs, 555–557
address families, 423–424
administrative distance, modifying, 677
ASNs, 422, 581
authentication, mismatched, 559–560
autonomous systems, 422
communities, 499–500
conditional matching, 504–506
enabling, 500
private, 506–507
well-known, 500–504
configuring, 428–430
interfaces, status of, 551
inter-router communication, 424–428
loop prevention, 423
MP-BGP, 458–459
configuring, 459–464
IPv6 over IPv4, 466–470
route summarization, 464–466
troubleshooting, 583–587, 604–606
neighbors
status of, 426–428
troubleshooting, 549–562, 587–604
network selection, 614
next-hop manipulation, 449–450
packet types, 425–426
path attributes, 423, 439, 517–518
path selection, 516–517
AIGP, 528–529
best path, 517–518, 577–581
eBGP over iBGP, 540
equal-cost multipathing, 542–543
local origination, 528
local preference, 522–528
lowest IGP metric, 540
lowest neighbor address, 541–542
MED, 534–539
minimum cluster list length, 541
oldest established, 541
origin type, 532–534
RID (router ID), 541
shortest AS_Path, 530–532
troublesbooting, 577–583, 587–604
weight, 519–522
prefix advertisement, 433–436
route filtering, 486–487
   AS_Path, 489–497
distribute lists, 487–488
prefix lists, 488–489
troublesbooting, 572–577
route maps, 497–499
route summarization, 476
   with AS_SET, 483–485
aggregate addresses, 476–481
atomic aggregate attribute, 481–483
routes
   administrative distance, 569–571
default, 552
local, 553
maximum prefix, 507–508
next-hop addresses, 566–568
processing, 436–441
sources, 554–555
split horizon, 568–569
troublesbooting, 562–577, 587–604
scalability, 509
   IOS peer groups, 509–510, 560–561
   IOS peer templates, 510–511
sessions
   clearing connections, 499
eBGP, 446–447
iBGP, 441–446, 450–458
topologies, 447–449
types of, 423, 441
timers, 561–562
TTL (time to live), 557–559
verifying, 431–433
bgp always-compare-med command, 538, 544
bgp bestpath med missing-as-worst command, 537, 544
bgp confederation identifier command, 472
bgp confederation peers command, 455, 472
bgp default local-preference command, 522
bgp deterministic-med command, 539, 544
bgp redistribute-internal command, 663, 666, 693
bgp router-id command, 472
Bidirectional Forwarding Detection (BFD), troubleshooting, 900–901
binding table, 864
Border Gateway Protocol. See BGP (Border Gateway Protocol)
boundary routers, 680
brackets ([]) regular expression, 493
broadcast networks (OSPF), 245

C

cache (NHRP), viewing, 769–773
caret (^) regular expression, 491–492
caret in brackets ([^]) regular expression, 493
Cisco DNA Center Assurance, troubleshooting, 901–908
Cisco IOS AAA, troubleshooting, 849–852
Cisco IOS IP SLA, troubleshooting, 885–891
class maps, creating, 856–858
classic configuration mode
  EIGRP, 78
  EIGRPv6, 191–192
classic metric formula (EIGRP), 93–96
clear bgp command, 499, 513
clear ip bgp command, 499
clear ip dhcp conflict command, 17
clear ip flow stats command, 896
clear ip nhrp command, 785
clear ip ospf process command, 257, 325
clearing BGP connections, 499
clients (DHCP), 14–15
cluster list length attribute (BGP), 541
communities (BGP), 499–500
  conditional matching, 504–506
  enabling, 500
  private, 506–507
  well-known, 500–504
complex matching, 621
conditional matching
  with ACLs
    extended ACLs, 613–614
    operational overview, 612
    standard ACLs, 612–613
  BGP communities, 504–506
  commands, 619–620
  complex matching, 621
  multiple conditions, 620–621
  with prefix lists, 614–618
conditional packet forwarding. See PBR (policy-based routing)
confederations (BGP), 454–458
configuration modes
  EIGRP
    classic, 78
    named, 79
  EIGRPv6
    classic, 191–192
    named, 192, 204–208, 213–218
configuring
  BGP, 428–430
  DHCP relay agents, 12–13
  DHCP servers, 15
  DHCPv6, 27
  DHCPv6 relay agents, 29–30
  DMVPN, 761–762
    hub routers, 762–764
    IPv6, 793–797
    for phase 2, 777–782
    for phase 3, 773–775
    spoke routers, 764–766
  EIGRP, 81–83
  EIGRPv6, 191–195
  FVRF, 790–791
  GRE tunnels, 751–756
  IPsec DMVPN with pre-shared authentication, 816–817
  keychains, 91
  local PBR, 627
  MP-BGP, 459–464
  OSPF, 232
    examples, 233–235
    interarea route summarization, 298–300
    interface-specific, 233
    network statement, 232–233
OSPFv2 stub areas, 335
OSPFv3, 368–372
PBR, 624–626
route redistribution, 648–649
route reflectors, 452–454
VRF instances, 721–734
Connect state (BGP), 427
connected networks
route redistribution, 649
verifying connectivity, 551
console access, troubleshooting, 871–872
continue keyword, 622–623
convergence (EIGRP), 109–111
CoPP (Control Plane Policing), troubleshooting, 854–863
ACL creation, 854–856
class map creation, 856–858
policy map creation, 859–860
service policy application, 861–863
crypt ipsec profile command, 822
crypto ikev2 dpd on-demand command, 815
crypto ikev2 keyring command, 822
crypto ikev2 limit command, 819
crypto ikev2 profile command, 822
crypto ipsec security-association replay window-size command, 815, 822
crypto ipsec transform-set command, 822
crypto isakmp nat keepalive command, 822
custom K values
EIGRP, 99, 145–146
EIGRPv6, 198

data availability, 804
data confidentiality, 803
data integrity, 803
data structures, routing tables and, 38–39
deaf interval timers (OSPF), 252
deaf peer detection, 815
debug aaa authentication command, 852, 866
debug aaa protocol local command, 852, 866
debug commands, 880–881
debug eigrp packet command, 145, 147
debug eigrp packets command, 143, 150, 187, 221
debug ip bgp command, 582, 609
debug ip bgp updates command, 582–583, 609
debug ip dhcp server events command, 17–18
debug ip dhcp server packet command, 18
debug ip ospf adj command, 318, 322, 363
debug ip ospf events command, 363
debug ip ospf hello command, 317, 320, 363
debug ip ospf packet command, 363
debug ip policy command, 628
debug ip routing command, 581, 609, 674–675
debug ip sla trace 2 command, 890–891
debug ospf adj command, 418
debug ospf events command, 418
debug ospf hello command, 418
debug ospf packet command, 418

deploy ospfv3 adj command, 418

deploy ospfv3 command, 412

deploy ospfv3 events command, 418

deploy ospfv3 hello command, 418

deploy ospfv3 packet command, 418

deploy radius authentication command, 852, 866

deploy tacacs authentication command, 852

default gateways, verifying, 26

default route advertising
  EIGRPv6, 196
  OSPF, 241–242
  OSPFv2, 348

default routes (BGP), 552

default-information originate command, 241, 257, 348

default-metric command, 544, 651, 666

delay command, 104

delay settings (EIGRP), 98–99

deny ipv6 any any log command, 831

designated router (DR)
  elections, 243–244, 336–339
  operational overview, 242–243
  placement, 244

destination protocols for redistribution
  BGP, 662–664, 693–695
  EIGRP, 650–655, 683–688
  OSPF, 655–662, 688–693

DHCP (Dynamic Host Configuration Protocol), 11
  clients, 14–15

DHCPv6
  message types, 29
  operational overview, 29

relay agents, 29–30

stateful, 26–27

stateless, 28

message types, 14

operational overview, 11–16

relay agent configuration, 12–13

servers, 15

troubleshooting, 16–18

commands, 17–18

issues, 16–17

verifying, 16

DHCPv6
  message types, 29
  operational overview, 29
  relay agents, 29–30
  stateful, 26–27
  stateless, 28

DHCPv6 Guard, 864

discard routes (EIGRP), 116

discontiguous networks
  autosummarization and, 165–166
  OSPF, 302–303
  OSPFv2, 345–347

distance bgp command, 677

distance eigrp command, 676

distance ospf command, 676

 distribute lists
  in BGP, 487–488
  in OSPF, 677

distribute-list command, 129, 136

distribute-list prefix-list command, 201

DMVPN (Dynamic Multipoint Virtual Private Network)
  benefits, 758
  configuring, 761–762

hub routers, 762–764

for phase 2, 777–782
EIGRP (Enhanced Interior Gateway Routing Protocol) 959

for phase 3, 773–775
spoke routers, 764–766
failure detection, 792
high availability, 792
hub redundancy, 793
IPv6
  configuring, 793–797
  verifying, 797–798
NHRP cache, viewing, 769–773
phases, 759
  comparison, 760–761
  hierarchical tree spoke-to-spoke (phase 3), 759, 773–775
  spoke-to-hub (phase 1), 759, 764–766
  spoke-to-spoke (phase 2), 759, 777–782
security
  IKEv2 protection, 819–820
  IPsec in transport mode, 808
  IPsec in tunnel mode, 808
  pre-shared key authentication, 808–817
  verifying encryption, 817–819
  without IPsec, 808
  tunnel status, verifying, 766–769
dollar sign ($) regular expression, 492
DORA process, 11–12
DR (designated router)
  elections, 243–244, 336–339
  operational overview, 242–243
  placement, 244
Dynamic Host Configuration Protocol. See DHCP (Dynamic Host Configuration Protocol)
Dynamic Multipoint Virtual Private Network. See DMVPN (Dynamic Multipoint Virtual Private Network)

E

eBGP (external BGP), 423, 441
  iBGP versus, 446–447
  path selection, 540
topologies, 447–449
EIGRP (Enhanced Interior Gateway Routing Protocol), 73
  administrative distance, modifying, 676
  authentication, 91–93
    enabling, 91–93
    keychain configuration, 91
    troubleshooting, 148–150
  autonomous systems, 73
    mismatched numbers, 142–143
  bandwidth percentage, 125
  configuration modes
    classic, 78
    named, 79
  configuring, 81–83
  convergence, 109–111
discontiguous networks, 165–166
  failure detection, 108–109
  feasible successors, 162–165
  interfaces
    ACLs, 150–151
    delay settings, 98–99
    passive, 87–90, 146–147
    status of, 142, 160
    subnets, 148
    verifying, 83–84
  metrics
    backward compatibility, 98
    classic formula, 93–96
    custom K values, 99, 145–146
    interface delay settings, 98–99
EIGRP (Enhanced Interior Gateway Routing Protocol)

**load balancing**, 99–102, 168–169

**wide metrics**, 96–98

multiple VRF instances, configuring, 730–732

neighbors, 76–78

*forming*, 77–78

inter-router communication, 76–77

troubleshooting, 141–151

verifying, 84–85

network statement, 80–81, 144–145, 152–154

packet types, 76

route redistribution, 650–655, 683–688, 697–701

route summarization, 113–114

*automatic*, 117–118

discard routes, 116

interface-specific, 114–116

metrics, 116–117

troubleshooting, 167

router ID (RID), 86

routes

*displaying*, 85–86

filtering, 129–131, 157–158

traffic steering with offset lists, 132–134

troubleshooting, 151–162

split horizon, 126–128, 160–162

stub routers, 118–121, 158–160

stub sites, 121–125

stuck in active (SIA), 112–113

terminology, 74

timers, 108–109, 151

topology tables, 75–76

trouble ticket examples, 169–184

*eigrp router-id command*, 86, 103, 220

*eigrp stub command*, 120, 136, 158

eigrp stub-site command, 123, 136

EIGRP-to-EIGRP redistribution, 653–655

EIGRPv6

ACLs, 201

authentication, verifying, 199–200

autonomous systems, mismatched numbers, 198

configuration modes

*classic*, 191–192

*named*, 192, 204–208, 213–218

interfaces

*passive*, 198–199

*status of*, 198, 201

verifying, 200

inter-router communication, 191

metrics, custom K values, 198

neighbors, troubleshooting, 197–201

route summarization, 195–196

routes

*default route advertising*, 196

filtering, 196–197, 201–202

troubleshooting, 201–203

split horizon, 203

stub routers, 202–203

timers, 200

trouble ticket examples, 208–218

verifying, 192–195

elections, DR and BDR, 243–244, 336–339

enabling

*BGP communities*, 500

EIGRP authentication, 91–93

SLAAC, 23

encapsulation overhead for tunnels, 753

encryption. See IPSec
equal-cost multipathing, 295, 542–543
ESP (Encapsulating Security Payload), 806
ESP modes, 807–808
Established state (BGP), 428
EUI-64 standard, 20–22
exam
    assessing readiness, 918–919
day-of tips, 914–915
failed exam, tips for, 915–916, 919–920
post-exam tips, 915–916
practice exams, 916–918
pre-exam tips, 914
study resources, 920–921
time budget for, 912–914
examples
    2.2.2.2 reachable status confirmation, 602
    10.1.1.0/26 network, determining whether advertised, 564–565
    10.1.3.0/24 in R1’s routing table verification, 180, 184
    10.1.4.0 route verification in OSPF database on R1, 704
    172.16.0.0/20 and 192.168.0.0/16 aggregation configuration, 482
    2001:db8:0:23::/64 network summarization configuration change, 466
    2001:db8:0:23::/64 network summarization verification, 466
    access lists applied to interfaces, verifying, 829
ACLs
    100 configuration verification, 636
    applied to interfaces verification, 151, 323
    blocking BGP packets and R5 neighbor relationship state verification, 556
    configuration for CoPP sample, 854–855
    configuration verification on R1, 837
    entry verification, 151, 323
    verification on Gig0/0 of R1, 841
    verification on Gig2/0 of R1, 840
    verification to secure management access, 873
    verification with show access-list command, 856
    administrative distance (AD)
    change verification for summary route AD, 116
    of IPv6 route verification, 201
    of local summary route to null 0 verification, 345
    route verification in routing table, 571
    advertised BGP route verification, 712
    advertised route verification to R1 neighbors, 599
    advertising non-connected routes configuration, 435–436
    aggregated properties of 192.168.0.0/16, viewing, 485
    aggregation configuration while preserving BGP attributes, 483–484
    area 1 stub area verification on branch, 396
    with no summary LSAs on R1, 397
    on R1, 396
ARP cache on R1 with R2 proxy ARP disabled, 45
ARP cache on R1 with R2 proxy ARP enabled, 44
AS 100 BGP table, 457
AS Path access list configuration, 496
automatic summarization on R1 and R5, 118
autonomous system number verification with show ip protocols, 142–143
BGP
  AS_Path prepending configuration, 531
  atomic aggregate attribute, examining, 483
  attributes for local-AS routes, 503
  attributes for no_advertise routes, 501
  attributes for no_export routes, 502
  best-path decision-making process, 580
  communities for two network prefixes, viewing, 506
  community change verification, 507
  community formats, 500
  confederation configuration, 455–456
  configuration, 430
  configuration on R1, viewing, 605
  configuration source for next-hop-self, 449–450
  configuration source from loopback interfaces, 445–446, 452–454
  configuration verification on R1, 597–598
  configuration verification on R1 and R2, 558
  configuration verification on R2, 713–714
  configuration verification with show ip protocols, 712
distribute list configuration, 487
IPv4 neighbor output, 432–433
for IPv4 redistribution options, 694
IPv4 session summary verification, 431
for IPv6 redistribution options, 694
local preference configuration, 523–524
neighbor verification, 711
neighbor verification with show ipv4 unicast summary, 550
neighbors, viewing for IPv6 capabilities, 461
next hop modification, 585
next hop verification, 585
next-hop issue identification, 566
origin manipulation configuration, 533
path attributes for 10.23.1.0/24 network, viewing, 505
path attributes for 192.168.1.1/32, 448
path attributes for IPv6 route, viewing, 463
prefix for best-path selection, viewing, 521–522
redistribution configuration, 663
regex query for AS 100, 490–491
regex query for AS 300, 492
regex query for AS_100, 491
regex query for AS_100_491
regex query with AS 40, 492
regex query with asterisk, 495
regex query with brackets, 493
regex query with caret, 492
regex query with caret in brackets, 493
regex query with dollar sign, 492
regex query with hyphen, 493
regex query with parenteses, 494
regex query with period, 494
regex query with plus sign, 494
regex query with question mark, 495
route aggregation configuration, 478
route aggregation configuration with suppression, 479–480
route detail verification, 571
route examination in R3 routing table, 591
route examination in R3 table, 591
route examination in routing table, 564
route table, 664
route verification, 570, 664
routes, displaying in IP routing table, 441
routes from R2 (AS 65200), 504
routes with local-AS community, viewing, 504
routes with no_export community, viewing, 503
session verification for IPv6 routes, 467
state verification on R1 and R2, 559
state verification on R2 and route to 5.5.5.5, 553
state verification on R5 with show ipv4 unicast summary, 552
state verification with show ipv4 unicast summary, 551
summary with prefixes, 440
table after origin manipulation, 534
table after phase I processing, 525
table after phase II processing, 527
table after phase III processing, 528
table after weight manipulation, 521
table before application of route map, 497
table examination, 563
table for regex queries, 490
table of routes from multiple sources, 437–438
table verification on route R5 for network 10.1.1.0, 578
tables after AS_Path prepending, 531–532
tables for R1, R2, R3 with aggregation, 478–479
tables for R1, R2, R3 without aggregation, 477
tables for R3 with aggregation and suppression, 480
timer modification to unacceptable values on R1, 562
timer verification, 561
branch receiving only default route verification, 397–398
Cisco IOS AAA configuration verification, 850–851
class map configuration for CoPP sample, 857
class map verification with show class-map command, 858
common LAN interface speeds metric calculation, 96
complete IPsec DMVPN configuration with pre-shared authentication, 816–817
complex matching route maps, 621
conditionally matching BGP communities, 505
confederation NLRI, 458
configuration and status verification of tracking object (down), 892
configuration and status verification of tracking object (up), 891
connected and redistributed entry verification in topology table, 165
connection verification with ping command, 729
connectivity checking between R1 and R3, 468
connectivity from branch to remote network, testing, 398, 402
connectivity test with link-local forwarding, 378
connectivity verification, 412–413, 588
CoPP match-all versus match-any example, 858
crypto IKEv2 limit configuration, 820
debug command output showing successful IP SLA operation, 890
debug command output showing unsuccessful IP SLA operation, 891
debug eigrp packet sample output when autonomous system mismatch exists, 143
debug ip bgp command output, 582
debug ip bgp updates command output, 582–583
debug ip dhcp server events command output, 18
debug ip dhcp server packet command output, 18
debug ip policy output, 633
debug ip routing command output, 581
debug ipv6 ospf hello, 400
debug output when authentication is missing on neighbor, 150
debug output when key IDs or key strings do not match, 150
default gateway configuration verification on PC, 26
default route existence in routing table verification, 552
default route in IPv6 BGP table verification on R1, 606
default route in IPv6 routing table verification on R1, 606
destination unreachable result from ping command on PC, 169, 173, 177, 181, 349
detailed DMVPN tunnel output, 787–788
detailed NHRP mapping with spoke-to-hub traffic, 780–781
detailed output for OSPF type 2 LSAs, 269
detailed output for OSPF type 3 LSAs, 273
detailed output for OSPF type 4 LSAs, 278
detailed output for OSPF type 5 LSAs, 275–276
detailed output for OSPF type 7 LSAs, 280
DHCP
  relay agent configuration, 13
  server configuration, 15
DHCP-assigned IP address verification on PC, 16
DHCPv6
  information verification on R1, 27
  sample configuration on R1, 27
disable split horizon configuration, 128
discard route for loop prevention, 300
distribute list application to neighbor verification, 576
DMVPN
  phase 1 routing table, 772–773
  phase 3 configuration for spokes, 774–775
tunnel status for DMVPN phase 1, viewing, 767–769
DR verification, 338–339
dynamic configured OSPFv3 network type, viewing, 374
EIGRP
  AD manipulation configuration, 676
  authentication configuration, 92
  authentication keychain verification, 149
  authentication verification, 93
  authentication verification on interface, 149
  bandwidth percentage configuration, 125
  bandwidth percentage, viewing, 125
  configuration for multiple VRF instances, 730
  configuration sample, 82
  configuration verification on R1, 703
  configuration with explicit IP addresses, 80
  configuration with explicit subnet, 81
distribute-list command verification, 158
  hello and hold timer value verification, 108–109
  interface delay verification, 98
  interface settings with named mode, viewing, 88
  interface verification, 83–84
  interface verification with show ip eigrp interfaces, 144
  for IPv4 redistributed routes in routing table, examining, 686
  for IPv4 redistribution options, 684
  for IPv6 redistribution options, 684
  maximum paths, changing, 100
  metric style verification, 98
  mutual redistribution configuration, 653–654
  neighbor confirmation, 85
  neighbor stub router verification, 160
  neighbor verification for each VRF instance with show ip eigrp vrf vrf-name neighbors command, 731–732
  neighbor verification on branch, 697
  neighbor verification with show ip eigrp neighbors, 141
  offset list configuration, 133–134
  offset list verification, 134
  redistribution configuration, 651
redistribution with route map configuration, 652
route filtering configuration, 130–131
route filtering verification, 131
route verification, 630
route verification in VRF routing table with show ip route vrf vrf-name eigrp command, 732
router id static configuration, 86
routes for R1 and R2, 85–86
split-horizon configuration verification, 203
stub configuration, 120
stub configuration verification on neighbor router, 203
stub configuration verification on stub router, 202
stub router flags, 124
stub site configuration, 123
summarization configuration, 115
topology for specific prefix, 95–96
topology table for 10.13.1.0/24 network, 647
topology table of redistributed routes, 652
variance configuration, 101
verification for IPv6 redistributed routes, 687–688
verification for IPv6 redistribution with show ipv6 eigrp topology, 687
verification for IPv6 redistribution with show ipv6 protocols, 686–687
EIGRP-learned routes verification, 217
EIGRPv6
authentication verification, 199–200
base configuration, 193–194
configuration verification with show ipv6 protocols, 199
default route injection, 196
distribute list verification, 202
interface verification, 200
neighbor adjacencies verification, 210
neighbor adjacency, 194
neighbor verification, 198
routing table entries, 195–196
summary configuration, 195
ENARSI IPv6 ACL on R1, 841
ENARSI IPv6 ACL on R1 modification, 842
entry verification for 10.1.3.10, 63
established BGP neighbor verification, 711
established BGP session, 427
EUI-64 usage on router interface, 21
EUI-64 verification on router interface, 22
explicit BGP routes and path attributes, viewing, 438–439
extended numbered ACL sample, 828
external EIGRP route verification, 652–653
failed pings
from PC1 to 10.1.3.10 and successful ping to 10.1.3.5, 60–61
from PC1 to 192.0.2.1, 48, 50
from PC1 to 2001:db8:d::1, 26
from PC1 to default gateway, 50
from PC1 to default gateway at 2001:db8:a:a::1, 53–54, 57
from PC1 to web server at 2001:db8:d::1, 53, 57
from PC2 to 192.0.2.1 and default gateway, 50–51
from R1 to 10.1.3.10, 170, 177, 181
from R1 to 192.168.1.10, 349
failed telnet and successful ping from PC1 to 192.0.2.1, 836–837
failed telnet and successful ping from PC2 to 2001:db8:ab::7, 839
failure to connect because of unique registration, 776
filter application verification to neighbor statements, 577 on R5, 575
filtering verification with BGP prefix list, 488–489
Flexible NetFlow
exporter information, viewing, 899
flow monitor cache format records, viewing, 898
flow monitors, viewing, 898
flow records, viewing, 897
Flexible NetFlow-enabled interfaces, viewing, 899
FVRF
configuration example, 791
static default route configuration, 792
general OSPFv3 parameter verification for AFs with show ospfv3, 405–406
generic OSPF LSA output
for type 1 LSAs, 263
for type 2 LSAs, 269
for type 3 LSAs, 271–272
for type 4 LSAs, 277
for type 5 LSAs, 275
for type 7 LSAs, 279
global IPv6 address removal, 377
global RIB for BGP learned IPv6 routes, 463–464
global routing table verification, 724
GRE configuration, 753–754
GRE tunnel parameters display, 755
hub router in DR verification, 339
IKEv2
keyring, 810
profile settings display, 811
sample profile, 811
inbound MED modification configuration, 536
information gathering with ping, 705
initiation of traffic between spoke routers, 777
interarea route summarization verification with show ip ospf, 343–344
interfaces
assignment to VRF instances with ip vrf forwarding command, 722
assignment verification to correct VRF instances, 722
configuration verification on branch, 401
configuration verification on R1, 55, 59
configuration verification on R2, 354
delay configuration, 99
enabled for IPv6 verification, 25
IP address review, 179
IP address verification, 702
IP address, VRF, protocol configuration verification, 724
MTU verification, 324–325
participating in EIGRP process
determination, 178
participation verification in
EIGRP process for each VRF, 731
IOS distribute list to filter default
route, 197
IOS OSPF authentication verification, 255
IP address verification on PC and
router, 10
IP address verification on PC with
ipconfig command, 11
IP helper address verification on
Gig0/0 of R1, 51–52
ip policy route-map configuration
modification, 636
IP protocols output, 89–90
IP SLA ICMP-ECHO probe
configuration example, 886
IP SLA UDP-JITTER probe
configuration example, 886
ipconfig output on PC1, 49, 51
IPsec
DMVPN tunnel protection
verification, 817
profile sample, 813
profile verification, 814
security association verification, 818–819
transform set sample, 813
transform set verification, 813
tunnel protection, enabling, 814
IPv4 addressing
address and mask verification on
router interfaces, 148
addresses of interfaces display, 215
prefix list sample, 834
route verification on R2, 713
routing table display on branch, 214
IPv6 addressing
access lists applied to interfaces,
verifying, 832–833
ACL sample, 832
address generation by SLAAC
verification on PC, 24
address generation by SLAAC
verification on router
interface, 24
address verification on PC1, 54,
56, 57, 59
address verification on PC2, 54,
58
address verification with
ipconfig, 20
address verification with
ipconfig /all, 21
addressing and OSPFv3
configuration, 369–370
BGP aggregation configuration
on R2, 464
BGP configuration, 460
BGP session verification,
461–462
BGP table verification, 587
BGP table, viewing, 462–463
connectivity between R31 and
R41, 798
DMVPN configuration for R31
and R41, 796–797
DMVPN hub configuration on
R11, 795
DMVPN verification, 797–798
interface parameters, displaying, 394
interface status verification, 198
link-local address verification, 210
OSPF neighbor verification, 399
prefix list sample, 618
redistribution on R1 verification, 706–707
route aggregation verification, 465
route exchange configuration over IPv4 BGP session, 466–467
route verification in routing table, 398–399
route verification to 2001:db8:0:3::/64 on R1, 64
router OSPF configuration verification on R1 and branch, 396–397
router OSPF configuration verification on R1 and branch after changes, 397
routes exchanged over IPv4 BGP session, viewing, 468
routing table, displaying on branch, 395–396
routing table verification on R1, 64–65
SLAAC enabling verification with ipconfig /all, 22–23
static route configuration verification on R1, 64
static route verification on R1, 46
summarization, 374
issue solved verification with extended IPv6 ping, 213
issue verification, 600
with extended IPv6 ping, 209
with pings, 594
K value verification with show ip protocols, 146
keychain settings verification, 92
learned IPv6 routes verification on branch, 211
on R1, 211
line usage verification, 873
local and foreign BGP port number verification, 557
local NHRP cache for DMVPN phase 1, 771
local PBR configuration, 627
verification, 627
local preference value modification in route map, 603
local route advertisements with AS_Path ACL verification, 497
LSDB verification with show ospfv3 database, 408–411
MAC address lookup in ARP cache, 43
manually setting IPv6 next hop route map, 469
manually setting IPv6 next hop, viewing IPv6 routes after, 469–470
maximum number of paths for load balancing verification, 348
maximum prefix configuration, 508
maximum prefix violation, 508
mismatched area number identification with debug ip ospf adj, 318
mismatched area type identification with debug ip ospf hello, 320
mismatched authentication information identification with debug ip ospf adj, 322
mismatched timer identification with debug ip ospf hello, 317
missing route verification on R5, 572
missing routes because of EIGRP stub routing, 121–122
modified TTLs of eBGP packet verification, 559
MP-BGP

adjacencies with IPv6 TCP sessions, 587
configuration for IPv6 routes over IPv4 TCP session, 583–584
configuration for IPv6 routes over IPv6 TCP session, 586
IPv6 unicast neighbor adjacencies verification, 584
IPv6 unicast route verification in IPv6 BGP table, 585

MTU mismatch (nbrs column values do not match) symptoms, 324
MTU mismatch (stuck in ExStart/Exchange) symptoms, 324
multiple match variables sample route map, 620
multiprotocol redistribution logic, 644
named ACL configuration mode for numbered ACL modification, 838

named EIGRP
configuration modification, 217
configuration review in running configuration, 215–216
configuration sample, 204
IPv4 interface table display, 215
neighbors verification, 207
process interface details verification, 206–207
process interfaces verification, 206
topology tables verification, 208

named mode configuration structure, 83

neighboring interfaces on same subnet verification, 320

neighbors
activation in address family configuration mode, 606

adjacency between R1 and R3 verification, 592
IPv6 address verification with show cdp neighbors details, 400
relationship verification over virtual link, 347
remote-as command verification on R2, 553
remote-as statement modification, 592
state verification with mismatched authentication, 560
statement and loopback IP address verification on R2, 555
verification with show ip eigrp neighbors command, 173

neighbor-specific view of Adj-RIB-OUT table, 440

NetFlow
information, viewing with show ip cache flow, 893
information, viewing with show ip flow export, 895
information, viewing with show ip flow interface, 895
sample configuration, 895
timers, viewing with show ip cache flow, 896

network, determining whether advertised, 565
network ID verification with show ip interface, 153, 329

network statement
review in running configuration, 179
verification with show ip protocols, 144–145, 153
verification with show run | section router eigrp, 145
network verification in link-state databases, 646
new route map configuration verification, 631, 634
next-hop address modification, 568
next-hop address verification in BGP table, 568
next-hop override routing table, 783–784
next-hop reachability verification, 567
NHRP
  mapping with spoke-to-hub traffic, 781–782
  routing table manipulation, 782–783
NSSA configuration for area 34 routers, 288
optimal routing verification, 662
OSPF
  adjacency debugging output, 231–232
  area authentication verification, 322
  area type determination, 319, 335
  area type determination on ABR, 335
  authentication configuration, 254
  authentication key verification, 322
  configuration for frame relay interfaces, 246
  configuration verification on R1, 703
  configurations for topology example, 234–235
  customized AD configuration, 677
  database verification on R1, 702–703
default information originate configuration, 241
distribute list and prefix list verification, 333
external LSA with forwarding address 0.0.0.0, 660
external LSA with forwarding address 10.123.1.1, 662
external route metrics on R1 and R2, 240
external summarization configuration, 301
forwarding metric, 295
interface area display with show ip ospf interface brief command, 318
interface area display with show ip ospf interface interface_type interface_number command, 318
interface output in brief format, 236
interface output in detail, 235–236
interface parameters of R2 and R3, compared, 353–354
interface state, 244
interface timer display on R1 GigabitEthernet1/0, 317
interface timers, 253
interface verification with show ip ospf interface brief, 315
loopback network type, 251
LSDB from R3, 656–657
multiprocess redistribution, 658–659
neighbor adjacency on hub-and-spoke topology, 250
neighbor output, 237
neighbor verification on P2P interfaces, 248
neighbor verification with show ip ospf neighbor, 313
network type display for loopback interfaces, 252
network type point-to-multipoint verification, 250
network type verification, 326–327
P2P interface verification, 247
point-to-multipoint configuration, 249
point-to-multipoint routing tables, 250–251
priority changes on spokes, 339
redistribution configuration, 656
redistribution into EIGRP verification, 698
redistribution verification, 659
RID verification, 325, 341
route advertisement verification to BGP neighbor, 715
route and LSDB verification after distribute list application, 334
route redistribution verification, 657–658
route types advertised into BGP, verifying, 714
routes installed in RIB, 238
routes installed in routing table, controlling with distribute list, 677
routing table for loopback network types, 252
routing tables for ABR R4, 238
routing tables for R5 and R6, 239
stub configuration for area 34, 283
type 1 LSAs for area 1234, 264–266
virtual link as interface, 305
virtual link configuration, 304
virtual link verification, 305
OSPF-enabled interface verification with show ip protocols, 316, 328
OSPF-enabled interfaces and neighbors verification, 352
OSPFv2
  redistributed routes in routing table, examining, 691
  redistribution options, 688
OSPFv3
  area authentication and encryption, 376
  configuration verification on R2, 415
  configuration with address families, 403
database link, 382
database network, 381
interface authentication and encryption, 376
interface brief iteration, viewing, 372
interface configuration, viewing, 371–372
interface detail verification with show ospfv3 interface, 407–408
interface verification with show ospfv3 interface brief, 407
IPSec verification, 377
LSDB display, 392–393
LSDB summary view, 383–384
neighbor verification with show ospfv3 neighbor, 408
network type, changing, 375
parameter verification on R2, 414–415
passive interface configuration, 373
redistributed route verification, 693
redistribution options, 689
redistribution verification with show ipv6 ospf database, 692
redistribution verification with show ipv6 protocols, 691
routes, displaying in routing table, 394
routes, viewing in IPv6 routing table, 372
verification identification with show ipv6 ospf, 389–390
verification identification with show ipv6 ospf interface brief, 390
verification identification with show ipv6 ospf interface interface_type interface_number, 391
verification identification with show ipv6 ospf neighbor, 391
verification identification with show ipv6 protocols, 389
OSPFv3-enabled interface verification on branch, 399
OSPFv3-enabled interface verification on R1, 399
packet match verification for ACL entry, 838
packet traveling distance before failure, 594–595
packets on correct path confirmation, 632, 634, 636
passive EIGRP interfaces
  for classic configuration, 87
  for named mode configuration, 87–88
passive interfaces
determination, 178–179
do not appear, 89
verification with show ip protocols, 147, 321
password security level verification, 875
path attributes injected into BGP aggregate verification, 484
path selection problems on R3 with automatic summarization, 118
path tracing, 413
path verification from R11 to R31, 756
PBR
debugging, 628
route map application verification, 631, 635
verification with debug commands, 634
peer group configuration example, 509–510, 561
peer template sample configuration, 510–511
phase 1 DMVPN
configuration, 766
trace from R31 to R41, 773
policy application to control plane interface, 861
policy map configuration sample for CoPP, 859
policy map verification with show policy-map command, 860
policy matches verification, 632
policy-based routing configuration, 625
prefix lists
filtering configuration, 488
modification on R1, 598
on R1, reviewing, 843
prefixes with no advertise community display, 501
preventing routes from being reinjected with route tags, 680
private BGP community configuration, 507
problem confirmation with ping, 705
problem solved verification with successful ping, 710
problem verification, 214, 604–605 from R2, 701
with trace to 10.1.1.1, 629, 632, 635
problematic multiprotocol redistribution logi, 643
protocol redistribution
  into BGP verification, 694–695
  into EIGRP for IPv4 verification, 684–685
  into OSPFv2 verification, 689
proxy ARP enabling verification, 44–45
R1
  advertised route verification, 596
  BGP and RIB after aggregation with suppression, 481
  BGP filter verification, 596–597
  BGP neighbor verification, 596
  BGP prefix list filter verification, 597
  BGP table after application of route map, 506
  BGP table verification, 595
  BGP table, with 192.168.0.0/16 discarded, 485
  and branch differences, 400–401
  CDP neighbor verification, 359–360
  configuration as DHCPv6 relay agent, 30
  with correct IP addressing after fixing ip helper-address command, 52
  EIGRP topology review, 707
  GigabitEthernet1/0 configuration verification, 360–361
  interface and subinterface configuration with IP addresses, 723
  IPv6 OSPF interface review, 708
  IPv6 routing table review, 708
  learning about 10.1.3.0/24 determination, 182
  OSPF configuration verification, 360
  OSPF neighbor verification, 359
  OSPF-enabled interface verification, 360
  and R2 serial and OSPF configuration, 247
  to R5 paths demonstrating PBR, 625
  and R5 routing tables after virtual link creation, 306
  route map configuration for inbound AS 65200 routes, 498
  route map to AS 65200 change verification, 499
  routing table for 10.4.4.0/24 network, 293
R1, R2, R4's routing tables before area 34 is converted to NSSA, 287–288
R1, R3, R4's routing tables before area 34 is totally NSSA, 290
R2
BGP and RIB after aggregation with suppression, 480–481
BGP configuration examination, 602–603
BGP table, 457
configuration verification with show ip vrf interfaces command and show ip route vrf command, 726–727
interarea route summarization configuration, 299
knows about 10.1.4.0 network verification, 704
neighbor determination, 183
and R3 BGP table with path attribute loss, 482–483
and R3 routing tables, 241–242
and R4 routing tables, 130
and R4 routing tables before offset, 133
route map examination, 603
routining table for 10.5.5.0/24 network, 626
VRF instance configuration, subinterface assignment to VRF instances, IP address configuration on subinterfaces, 725–726

R3
BGP table, 446
configuration verification with show ip vrf interfaces command and show ip route vrf command, 728–729
configurations required to solve issue, 175
LSAs, viewing in OSPFv3 database, 381
OSPFv3 neighbor identification, 371
and R4 OSPF NSSA routing tables, 289
and R4 routing tables after area 34 is totally NSSA, 291
VRF instance configuration, interface assignment to VRF instances, IP address configuration on interfaces, 727–728

R4
BGP configuration mirror of R2 verification, 555
IPv6 routing table after summarization, 374
IPv6 routing table before summarization, 373
routining table after removal of global IPv6 addresses, 378
routining table after summarization, 116
routining table before summarization, 115
R4, R5, R6 BGP tables after local preference modification, 524
R4, R5, R6 BGP tables after MED modification, 537
R4, R5, R6 BGP tables with med missing-as-worst, 538

R5
BGP configuration examination, 602
BGP table examination, 589, 601
known routes from R2 and R3 confirmation, 593
routining table, 647
R6 discard route verification, 302
R11
routining table with GRE tunnel, 755, 788–789
routining table without GRE tunnel, 752
summarization configuration, 785
RAs

suppression verification on R1, 55, 58–59

unsuppressed verification, 25

received route verification on R5, 573

recursive lookup on R1 for next-hop address, 42

recursive routing syslog messages on R11 for GRE tunnels, 789

RED VRF routing table contents verification with show ip route vrf RED command, 730

redistribute command modification, 709

redistribute command modification in IPv4 address family configuration mode, 714

redistribute command verification on R1, 699

redistributed route verification
in ASBR routing table, 690
in BGP table, 695
in branch routing table, 700–701
in EIGRP topology table, 699
in OSPFv2 LSDB, 690
in R1 topology table, 700
in routing table, 699

reference BGP table, 487

reference BGP table before applying AS_Path access list, 496

RIB failure verification, 571

route administrative distance verification in routing table, 40–41

route confirmation from R1 to 10.1.5.5, 594

route existence to neighbor and successful ping verification, 551

route filter on R1 determination, 183

route filter verification
on branch, 698

in IPv6 routing table, 413

in OSPF database, 357–358

on R1, 702

in R1 routing table, 843

on R2, 702

on R5, 600–601

in routing table on R1, 355

in routing table on R2, 355

router interface verification with show cdp neighbors, 352

route redistribution verification into EIGRP for IPv4 (topology table), 685

route reflector originator ID and cluster list attributes, 454

route summarization verification with show ip protocols, 166

route to 2001:db8:f::f verification in IPv6 routing table on R1, 210

route to 2001:db8:f::f verification in IPv6 routing table on branch, 212

route verification, 654

on branch, 706

in IPv6 routing table, 413

in OSPF database, 357–358

on R1, 702

in R1 routing table, 843

on R2, 702

on R5, 600–601

in routing table on R1, 355

in routing table on R2, 355

RAs

suppression verification on R1, 55, 58–59

unsuppressed verification, 25

received route verification on R5, 573

recursive lookup on R1 for next-hop address, 42

recursive routing syslog messages on R11 for GRE tunnels, 789

RED VRF routing table contents verification with show ip route vrf RED command, 730

redistribute command modification, 709

redistribute command modification in IPv4 address family configuration mode, 714

redistribute command verification on R1, 699

redistributed route verification
in ASBR routing table, 690
in BGP table, 695
in branch routing table, 700–701
in EIGRP topology table, 699
in OSPFv2 LSDB, 690
in R1 topology table, 700
in routing table, 699

reference BGP table, 487

reference BGP table before applying AS_Path access list, 496

RIB failure verification, 571

route administrative distance verification in routing table, 40–41

route confirmation from R1 to 10.1.5.5, 594

route existence to neighbor and successful ping verification, 551

route filter on R1 determination, 183

route filter verification
on branch, 698

on R1, 212, 698, 843

with show ip protocols, 157–158, 332–333

route in R2's routing table determination, 182

route in R3's routing table determination, 178

route maps

application verification, 636
configuration modification, 631, 633
configuration verification, 631, 633, 635
configuration with continue keyword, 622–623
sample, 619

route redistribution verification into EIGRP for IPv4 (topology table), 685

route reflector originator ID and cluster list attributes, 454

route summarization verification with show ip protocols, 166

route to 2001:db8:f::f verification in IPv6 routing table on R1, 210

route to 2001:db8:f::f verification in IPv6 routing table on branch, 212

route verification, 654

on branch, 706

in IPv6 routing table, 413

in OSPF database, 357–358

on R1, 702

in R1 routing table, 843

on R2, 702

on R5, 600–601

in routing table on R1, 355

in routing table on R2, 355

router interface verification with show cdp neighbors, 352
routes

filtered by BGP distribute list, viewing, 488
learned by branch, verifying, 710
learned from R1, verifying, 592
learned verification from WAN interface, 124
received from R2 and R3, examining, 589–590
redistributed after changes, verifying, 709
sent from R3 to R5, examining, 590

routing tables

after area 23 is converted to totally stubby area, 286
after external summarization, 301–302
after OSPF interarea route summarization, 300
after stub area configuration, 283–284
in area 1 and area 2 without stub, 282–283
entries verification, 629–630
entry verification, 61
before external summarization, 301
before OSPF interarea route summarization, 299
of R3 and R4 before totally stubby areas, 285
with summarization, 785–786
with summarization and spoke-to-spoke traffic, 786–787
verification on branch, 697

SCP configuration on Cisco router, 877–878
SCP copy command on Cisco router, 878

selective connected network redistribution, 649
self-originating LSAs, viewing in OSPFv3 database, 380
sent route verification on R5, 574
show adjacency detail command output, 38
show cdp neighbors output on R1, 172
show eigrp protocols output, 205
show frame-relay map command output, 37
show ip arp command output, 36
show ip cef ip_address command output, 36
show ip cef ip_address subnet_mask command output, 36
show ip dhcp binding command output, 17
show ip eigrp interfaces on R3, 175
show ip eigrp interfaces output on R1, 171
show ip eigrp interfaces output on R2, 172
show ip eigrp neighbors on R2, 174
show ip eigrp topology command output, 154–155, 163
show ip eigrp topology comparison, 164
show ip nhrp brief command sample output, 771–772
show ip nhrp command output, 37
show ip ospf database output on R1, 330–331
show ip ospf database output on R2 confirming routes are missing, 351–352
show ip ospf database router 10.1.12.1 output on R1, 331
show ip ospf neighbor output on R1, 350
show ip protocols and show ipv6 protocols, 404
show ip protocols command output on R2, 160
show ip protocols output on R1, 170–171, 350
show ip route 10.1.1.0 255.255.255.0 command output, 330
show ip route 172.16.33.16 255.255.255.252 command output, 156
show ip route 192.168.1.0 255.255.255.0 output on R3, 358
show ip route eigrp command output, 155–156
show ip route ip_address command output, 34
show ip route ip_address subnet_mask command output, 35
show ip route ip_address subnet_mask longer-prefixes command output, 35
show ip route ospf command output, 329
show ip route ospf output on R3, 358
show ip route output after neighbor relationship with R2 is established, 174
show ip route output on R1, 170, 176, 349–350
show ip route output on R2, 174, 175–176, 351
show ip sla application output, 886–887
show ip sla configuration output, 887–888
show ip sla responder output, 890
show ip sla statistics output, 889
show policy-map control-plane command output, 862–863
show run | include ip route output, 359
show run | section router eigrp output on R2 and interface IP address verification, 172
SIA timers
  configuration, 113
  output, 113
simulated EIGRP topology for 10.1.1.0/24 network, 110
SLAAC enabling on router interface, 23
SNMP
  group verification, 884
  host verification, 884
  user verification, 884
  view verification, 884–885
SNMPv2 configuration example, 882
SNMPv3 configuration example, 883
solved issue confirmation, 603–604
solved problem verification, 599
specific route verification, 62
split horizon enabled for EIGRP on interface verification, 162
split horizon enabled on interface verification, 161
SSH connection verification, 875
SSH version verification, 874
standard numbered ACL sample, 828
stateless DHCPv6 verification, 28
static route verification on R1, 42
static route with exit interface specified, 43
statically configured OSPFv3 network type, viewing, 375
subinterfaces on R1, creating and assigning to correct VRF instances, 723
subnets keyword, adding to redistribute command, 704
suboptimal routing verification, 660–661
successful pings, 705

from 10.1.1.0/24 network to 10.1.3.0/24 network, 176, 180, 184
from 10.1.1.0/24 network to 192.168.1.0/24 network, 356
to 192.168.1.0/24 network, 359
from branch to various network IP addresses, 218
to IPv6 Internet resources, 415–416
no route to neighbor, 552
from PC1 to 10.1.3.10, 63
from PC1 to 192.0.2.1, 49, 52
from PC1 to default gateway, 48
from PC1 to web server at 2001:db8:d::1, 56, 60
from PC2 to 192.0.2.1, 48–49
successful telnet

from PC1 to 192.0.2.1, 838
from PC2 to 2001:db8:a:b::7, 842
from R1 to 2001:db8:a:b::7, 840
syslog configuration verification, 879–880
tagging routes during redistribution, 678–679
TCP session state verification, 554
time, viewing on Cisco router, 830
time range sample configured on R1, 830
time-based ACL sample, 830
topology table for 192.168.4.4/32, 654–655
totally NSSA configuration, 291
totally stubby area configurations, 286
trace from PC1 to R3's Gig0/0 interface, 63, 65
trace issuing to identify where issue might be, 701
traceroute for normal traffic flow, 625
traceroute showing R2 and R3 are bouncing packet back and forth, 357
traffic not set out of interface on which it was received, 627
transport protocol verification for line, 873
TTL expired in transit result from ping command on PC, 356
TTLs of eBGP and iBGP packet verification, 557
two default routes and path selection, 790
unequal-cost load balancing verification, 101–102
unique NHRP registration, 776
updated prefix list on R1, reviewing, 844
updated route verification in R1 routing table, 844
updated static route verification in routing table on R1, 62
variance and maximum paths verification, 168–169
virtual link displayed as OSPF neighbor, 306
virtual link verification, 347
VRF

connectivity verification between PCs, 733–734
connectivity verification from R1 to R3, 733
instance configuration on R1 with ip vrf command, 721
instance configuration verification on R1, 722
routing table verification, 724–725
vty line configuration verification, 874
vty login command verification, 873
weight manipulation configuration, 520
exit interfaces, 43–44
extended ACLs, 612, 613–614
extended numbered ACLs, 828
external BGP (eBGP), 423, 441
iBGP versus, 446–447
path selection, 540
topologies, 447–449
external routes (OSPF), 239–240, 294–295
route summarization, 300–302

F
failed exam, tips for, 915–916, 919–920
failure detection
DMVPN, 792
EIGRP, 108–109
OSPF, 252–253
feasibility conditions, 74
feasible distance (FD), 74
feasible successors, 74, 162–165
filtering. See also packet filtering
BGP routes, 486–487
   AS_Path, 489–497
distribute lists, 487–488
prefix lists, 488–489
troubleshooting, 572–577
EIGRP routes, 129–131, 157–158
EIGRPv6 routes, 196–197, 201–202
OSPFv2 routes, 332–334
Flexible NetFlow, troubleshooting, 892–900
flooding scopes (OSPFv3 LSAs), 378–384
forwarding address (OSPF), 659–662
FVRF (front door virtual routing and forwarding), 790
configuring, 790–791
static routes, 792
G
gateway command, 129
GRE (Generic Routing Encapsulation)
tunnels, 750–751
configuring, 751–756
encapsulation overhead, 753
H
hello packets (OSPF), 229–230
hello timers (OSPF), 252
hello-interval command, 108, 136
hierarchical tree spoke-to-spoke (DMVPN phase 3), 759
configuring, 773–775
high availability (DMVPN), 792
hold-time command, 136
HTTP, troubleshooting, 876–877
hub redundancy (DMVPN), 793
hub routers (DMVPN), 762–764
hyphen (-) regular expression, 493
I
iBGP (internal BGP), 423, 441–446
full mesh requirement, 443
loopback addresses, 444–446
path selection, 540
scalability, 450–458
   confederations, 454–458
   route reflectors, 450–454
topologies, 447–449
identity local address command, 822
Idle state (BGP), 427
IGP (interior gateway protocol)
  network selection, 613–614
  path selection, 540
IKEv2 keyring, 809–810
IKEv2 profile, 810–811
IKEv2 protection, 819–820
inherit peer-policy command, 510
inherit peer-session command, 510
instances (VRF), creating and verifying, 721–734
interarea routes (OSPF), 293–294
  route summarization, 297–300
interface interface-id command, 220
interfaces
  BGP, status of, 551
EIGRP
  ACLs, 150–151
  delay settings, 98–99
  enabling authentication, 91–93
  passive, 87–90, 146–147
  status of, 142, 160
  subnets, 148
  verifying, 83–84
EIGRPv6
  passive, 198–199
  status of, 198, 201
  verifying, 200
OSPF
  passive, 233
  verifying, 235–237
OSPFv2
  ACLs, 323
  disabled, 315–316, 328–329
  MTU mismatch, 323–325
  passive, 320–321
  status of, 315, 336
  subnets, 320
OSPFv3, passive, 372–373
    interface-specific configuration (OSPF), 233
    interface-specific route summarization, 114–116
interior gateway protocol (IGP)
  network selection, 613–614
  path selection, 540
internal BGP. See iBGP (internal BGP)
inter-router communication
  BGP, 424–428
  EIGRP, 76–77
  EIGRPv6, 191
  OSPF, 228–229
intra-area routes (OSPF), 292–293
IOS peer groups, 509–510, 560–561
IOS peer templates, 510–511
ip address dhcp command, 14
ip as-path access-list command, 496, 513
ip authentication key-chain eigrp
  as-number key-chain-name command, 104
ip authentication mode eigrp
  as-number md5 command, 104
ip bandwidth-percent eigrp command, 125
ip bgp-community new-format command, 500, 513
ip community-list command, 505, 513
ip dhcp excluded-address 10.8.8.1
  10.8.8.10 command, 15
ip dhcp pool POOL-A command, 15
ip flow egress command, 892–893
ip flow ingress command, 892–893
ip flow monitor command, 899
ip flow-cache entries command, 895–896
ip flow-cache timeout active command, 895–896
ip flow-cache timeout inactive command, 895–896
ip flow-export destination command, 892–893
ip flow-export source lo 0 command, 892–893
ip hello-interval eigrp as-number command, 136
ip hello-interval eigrp ip hold-time eigrp command, 108
ip helper-address command, 12, 13
ip hold-time eigrp as-number command, 136
ip local policy command, 626
ip mtu command, 793
ip nhrp authentication command, 775, 793, 800
ip nhrp holdtime command, 792, 793
ip nhrp map command, 765
ip nhrp map multicast command, 765
ip nhrp network-id command, 793, 800
ip nhrp nhs command, 765, 793
ip nhrp redirect command, 773, 793, 800
ip nhrp registration no-unique command, 776, 793, 800
ip nhrp registration timeout command, 792, 793
ip nhrp shortcut command, 773, 793, 800
ip ospf area command, 257, 312, 315, 316
ip ospf authentication-key command, 257
ip ospf command, 233
ip ospf cost command, 292, 308
ip ospf dead-interval command, 252
ip ospf hello-interval command, 252
ip ospf message-digest-key command, 257
ip ospf mtu-ignore command, 325
ip ospf network broadcast command, 245, 257
ip ospf network non-broadcast command, 246
ip ospf network point-to-multipoint command, 248, 257
ip ospf network point-to-point command, 248, 257
ip ospf priority command, 244, 257
ip radius source-interface Loopback1 command, 849–850
ip route command, 41
ip route vrf command, 792, 793
IP SLA, troubleshooting, 885–891
ip summary-address command, 115
ip summary-address eigrp as-number command, 136
ip tacacs source-interface Loopback1 command, 850
ip tcp adjust-mss command, 793
ip verify unicast source reachable-via command, 853, 866
ip vrf command, 721, 746
ip vrf forwarding command, 722, 746
ipconfig /all command, 67
IPv6 addressing, 20–21
SLAAC verification, 22–23
ipconfig command, 67
IPv4 addressing, 9–10, 11
IPv6 addressing, 19–20
SLAAC, 23–24
IPsec, 805–806
ESP modes, 807–808
IKEv2 protection, 819–820
IPv6 addressing

key management, 806
pre-shared key authentication, 808–817
  configuring, 816–817
  dead peer detection, 815
IKEv2 keyring, 809–810
IKEv2 profile, 810–811
NAT keepalives, 815
packet replay protection, 814–815
profile, 813–814
transform set, 812–813
tunnel interface encryption, 814
security associations, 806–807
security protocols, 806
verifying encryption, 817–819
IPv4 ACLs, troubleshooting, 827–830, 836–838
  packet filtering with ACLs, 829
  reading ACLs, 827–828
time-based ACLs, 829–830
IPv4 addressing, 7
  addresses within subnet, determining, 10–11
DHCP, 11
  clients, 14–15
  message types, 14
  operational overview, 11–16
  relay agent configuration, 12–13
  servers, 15
  troubleshooting, 16–18
  verifying, 16
IPv6 over IPv4, 466–470
MPLS Layer 3 VPNs, 741–742
  operational overview, 7–10
  static routes, 41–45
  troubleshooting, 47–52
  verifying, 10, 11
IPv6 ACLs, troubleshooting, 830–833, 839–842
  packet filtering with ACLs, 832–833
  reading ACLs, 831–832
ipv6 address autoconfig command, 23
ipv6 address command, 21
IPv6 addressing, 18–19
DHCPv6
  message types, 29
  operational overview, 29
  relay agents, 29–30
DMVPN
  configuring, 793–797
  verifying, 797–798
EUI-64 standard, 20–22
MP-BGP, 458–459
  configuring, 459–464
  IPv6 over IPv4, 466–470
  route summarization, 464–466
  troubleshooting, 583–587, 604–606
  operational overview, 19–22
OSPFv3, route summarization, 373–374
  prefix lists, 617–618
  redistribution troubleshooting, 705–710
SLAAC, 22–26
  default gateways, 26
  enabling, 23
  interface enabled, 25
  RA process, 23
  RA suppression, 25
  verifying, 22–23, 24
  stateful DHCPv6, 26–27
  stateless DHCPv6, 28
static routes, 45–47
troubleshooting, 53–60
verifying, 19–21
ipv6 dhcp relay destination command, 30
ipv6 dhcp server command, 26
ipv6 eigrp command, 200, 220
IPv6 First-Hop Security, 863–864
ipv6 flow monitor command, 899
ipv6 mtu command, 793
ipv6 nd other-config-flag command, 28
IPv6 neighbor discovery inspection/snooping, 864
ipv6 nhrp authentication command, 793
ipv6 nhrp holdtime command, 793
ipv6 nhrp network-id command, 793
ipv6 nhrp nhs command, 793
ipv6 nhrp redirect command, 793
ipv6 nhrp registration no-unique command, 793
ipv6 nhrp registration timeout command, 793
ipv6 nhrp shortcut command, 793
ipv6 route command, 45
ipv6 route vrf command, 793
ipv6 router eigrp as-number command, 220
IPv6 Source Guard, 864
ipv6 summary-address eigrp command, 195
ipv6 tcp adjust-miss command, 793
is ospf network non-broadcast command, 257
KEEPALIVE messages (BGP), 425–426
key chain command, 103
key command, 103
key management, 806
keychains, configuring, 91
keyring local command, 822
key-string command, 103
label stacks, 743–745
label switching routers (LSRs), 735
labels
format, 736–737
switching, 738–739
label-switched path (LSP), 736
Layer 3 connectivity, verifying, 551
LDP (Label Distribution Protocol), 737–738
LFIB (Label Forwarding Information Base), 734–735
LIB (Label Information Base), 734–735
link costs, 292
link-local forwarding (OSPFv3), 377–378
link-state advertisements. See LSAs (link-state advertisements)
link-state database (LSDB), fields, 264
load balancing
EIGRP, 99–102, 168–169
OSPFv2, 347–348
local origination attribute (BGP), 528
local PBR, 626–628
local preference attribute (BGP), 522–528
local routes (BGP), 553
Local-AS BGP community, 503–504
logging buffered command, 879
K values
EIGRP, 99, 145–146
EIGRPv6, 198
login authentication command, 866
login authentication CONSOLE_ACCESS command, 850
login authentication VTY_ACCESS command, 850
loop prevention
  BGP, 423
  route reflectors, 454
loopback addresses (iBGP), 444–446
loopback networks (OSPF), 251–252
lowest IGP metric attribute (BGP), 540
lowest neighbor address attribute (BGP), 541–542
LSAs (link-state advertisements), 261–262
  age, 262
  flooding, 262
  OSPFv3, 366–367
    additional types, 393
    flooding scopes, 378–384
  sequences, 262
  tracking, 341–343
  Type 1 (router link), 263–268
  Type 2 (network link), 269–271
  Type 3 (summary link), 271–274
  Type 4 (ASBR summary), 276–278
  Type 5 (external routes), 274–276
  Type 7 (NSSA external summary), 278–280
  type summary, 280–281, 342–343
LSDB (link-state database), fields, 264
LSP (label-switched path), 736
LSRs (label switching routers), 735

M
MAC address lookups, 43
match address prefix-list command, 620
match as-path command, 513, 619, 638
match community command, 505
match community community-list command, 619
match fvrf command, 822
match identity remote address command, 822
match interface command, 648
match interface interface-id command, 619
match ip address command, 513, 620, 638
match ip address prefix-list command, 513, 638
match local-preference command, 513, 620, 638
match metric external command, 620
match route-type command, 648
match source-protocol command, 620
match tag command, 620
maximum prefix (BGP), 507–508
maximum-paths command, 104, 168, 295, 542–543, 544
maximum-paths ibgp command, 542–543, 544
MED (multi-exit discriminator), 534–539
metric weights command, 104
metrics
  EIGRP
    backward compatibility, 98
    classic formula, 93–96
    custom K values, 99, 145–146
    interface delay settings, 98–99
    load balancing, 99–102, 168–169
    route summarization, 116–117
    wide metrics, 96–98
  EIGRPv6, custom K values, 198
minimum cluster list length attribute (BGP), 541
mode command, 822
MP-BGP (Multiprotocol BGP), 458–459
configuring, 459–464
IPv6 over IPv4, 466–467
route summarization, 464–466
troubleshooting, 583–587, 604–606
MPLS (Multiprotocol Label Switching), 734
labels
  format, 736–737
  switching, 738–739
LDP, 737–738
LIB and LFIB, 734–735
LSP, 736
LSRs, 735
PHP, 739
MPLS Layer 3 VPNs, 739–741
label stacks, 743–745
VPNv4 addresses, 741–742
MTU mismatch (OSPFv2), 323–325
multi-exit discriminator (MED), 534–539
multiple match conditions, 620–621
Multiprotocol BGP. See MP-BGP (Multiprotocol BGP)
Multiprotocol Label Switching. See MPLS (Multiprotocol Label Switching)

N
	named configuration mode
    EIGRP, 79
    EIGRPv6, 192, 204–208, 213–218
    NAT keepalives, 815
    neighbor activate command, 583, 586
    neighbor address attribute (BGP), 541–542
    neighbor aigp command, 529, 544
    neighbor distribute-list command, 487, 513
    neighbor ebgp-multihop command, 559
    neighbor filter-list command, 496, 513
    neighbor ip-address activate command, 472
    neighbor ip-address remote-as command, 472
    neighbor ip-address timers keepalive holdtime command, 472
    neighbor ip-address update-source interface-id command, 472
    neighbor local-preference command, 522, 544
    neighbor maximum-prefix command, 507, 513
    neighbor next-hop-self command, 449, 472, 567–568
    neighbor peer-group command, 509, 513
    neighbor prefix-list command, 488, 513
    neighbor remote-as command, 553–555, 586
    neighbor remove-private-as command, 581
    neighbor route-map command, 497, 513
    neighbor route-reflector-client command, 452, 472
    neighbor send-community command, 500
    neighbor transport connection-mode command, 556
    neighbor update-source command, 445, 555
    neighbor weight command, 519, 544
neighbors
BGP
  status of, 426–428
  troubleshooting, 549–562, 587–604
EIGRP, 76–78
  forming, 77–78
  inter-router communication, 76–77
  troubleshooting, 141–151
  verifying, 84–85
EIGRPv6, troubleshooting, 197–201
OSPF, 230
  adjacency requirements, 230–232
  status of, 230
  verifying, 237
OSPFv2
  adjacency states, 314
  troubleshooting, 312–327
NetFlow, troubleshooting, 892–900
network area command, 312, 316
network command, 103, 141, 152–154, 233, 257
network mask command, 434, 472, 564–566
network statement (EIGRP), 80–81, 144–145, 152–154
network statement (OSPF), 232–233
next-hop addresses
  recursive lookups, 42
  unreachable in BGP, 566–568
next-hop manipulation (BGP), 449–450
NHRP (Next Hop Resolution Protocol), 756–758
  authentication, 775
  cache, viewing, 769–773
  mapping entries, 769–770
message extensions, 757–758
message flags, 770
message types, 757
routing table manipulation, 782–784
  with route summarization, 784–788
unique IP registration, 775–777
no auto-summary command, 118, 165
no bgp default ip4-unicast command, 472
no ip split-horizon command, 162
no ip split-horizon eigrp command, 128, 136, 162
no passive command, 233
no passive interface command, 87
no passive-interface command, 372–373
no service timestamps command, 880
no shutdown command, 737
no split-horizon command, 128, 136
No_Advertise BGP community, 501
No_Export BGP community, 502–503
No_Export_SubConfed BGP community, 503–504
nonbroadcast networks (OSPF), 246
NOTIFICATION messages (BGP), 426
NSSAs (not-so-stubby areas), 286–289

Object Tracking, troubleshooting, 891–892
offset lists, 132–134
offset-list command, 132, 137
oldest established attribute (BGP), 541
OPEN messages (BGP), 425
OpenConfirm state (BGP), 428
OpenSent state (BGP), 427–428
origin type attribute (BGP), 532–534
OSPF (Open Shortest Path First)

administrative distance, modifying, 676–677
areas, 226–228
authentication, 253–255
configuring, 232
examples, 233–235
interface-specific, 233
network statement, 232–233
distribute lists, 677
DR and BDR
elections, 243–244
operational overview, 242–243
placement, 244
failure detection and timers, 252–253
forwarding address, 659–662
hello packets, 229–230
interfaces
passive, 233
verifying, 235–237
inter-router communication, 228–229
LSAs, 261–262
age, 262
flooding, 262
sequences, 262
Type 1 (router link), 263–268
Type 2 (network link), 269–271
Type 3 (summary link), 271–274
Type 4 (ASBR summary), 276–278
Type 5 (external routes), 274–276
Type 7 (NSSA external summary), 278–280
type summary, 280–281, 342–343
neighbors, 230
adjacency requirements, 230–232
status of, 230
verifying, 237
network types
broadcast, 245
list of, 245
loopback, 251–252
nonbroadcast, 246
point-to-multipoint networks, 248–251
point-to-point, 247–248
operational overview, 225–226
packet types, 229
path selection, 292
equal-cost multipathing, 295
external routes, 294–295
interarea routes, 293–294
intra-area routes, 292–293
link costs, 292
route redistribution, 655–662, 688–693, 701–705
route summarization, 295–297
external routes, 300–302
interarea routes, 297–300
router ID (RID), 229
routes
default route advertising, 241–242
discontiguous networks, 302–303
external, 239–240
viewing, 238–239
virtual links, 303–306
Stubby areas, 281–282
not-so-stubby areas, 286–289
stub areas, 282–284
totally NSSAs, 289–291
totally stubby areas, 284–286
OSPF-to-OSPF redistribution, 658–659

OSPFv2
  areas
   mismatched numbers, 317–318
   mismatched type, 319–320
authentication, mismatched, 321–322
discontiguous networks, 345–347
DR and BDR elections, 336–339
interfaces
   ACLs, 323
   disabled, 315–316, 328–329
   MTU mismatch, 323–325
   passive, 320–321
   status of, 315, 336
   subnets, 320
load balancing, 347–348
LSAs, tracking, 341–343
neighbors
   adjacency states, 314
troubleshooting, 312–327
network types, mismatched, 326–327
OSPFv3 versus, 365–366
route summarization, 343–345
routes
   administrative distance, 329–332
default route advertising, 348
duplicate RIDs, 325, 340–341
filtering, 332–334
troubleshooting, 327–341
stub areas, configuring, 335
timers, mismatched, 316–317
troubleshooting
   discontiguous networks, 345–347
   load balancing, 347–348
   neighbor adjacencies, 312–327
   route summarization, 343–345
   routes, 327–341
trouble ticket examples, 348–361

OSPFv3
address families, troubleshooting, 402–416
authentication, 375–377
configuring, 368–371
interfaces, passive, 372–373
link-local forwarding, 377–378
LSAs, 366–367
   additional types, 393
   flooding scopes, 378–384
network types, 374–375
OSPFv2 versus, 365–366
packet types, 367–368
route summarization, 373–374
troubleshooting
   address families, 402–416
   commands, 388–394
trouble ticket examples, 395–402
verifying, 371–372
ospfv3 authentication command, 375
ospfv3 command, 402–403
ospfv3 encryption command, 375, 376
ospfv3 network command, 374, 385
overlay networks, troubleshooting
   outbound interface selection, 789–790
P

packet filtering
with IPv4 ACLs, 829
with IPv6 ACLs, 832–833
packet forwarding, 30. See also MPLS (Multiprotocol Label Switching)
operational overview, 30–34

PBR
  configuring, 624–626
  local, 626–628
  operational overview, 623–624
  troubleshooting, 628–636
 troubleshooting, 34–38
packet replay protection, 814–815
parentheses () regular expression, 494
passive command, 233, 257
passive interface default command, 233, 257

passive interfaces
  EIGRP, 87–90, 146–147
  EIGRPv6, 198–199
  OSPF, 233
  OSPFv2, 320–321
  OSPFv3, 372–373
  passive-interface command, 87, 103, 372–373, 385
  passive-interface default command, 87, 372–373, 385

password encryption levels, verifying, 875
path attributes (BGP), 423, 439, 517–518

path selection (BGP), 516–517
  best path, 517–518, 577–581
    AIGP, 528–529
    eBGP over iBGP, 540
    local origination, 528
    local preference, 522–528
    lowest IGP metric, 540
    lowest neighbor address, 541–542
    MED, 534–539
    minimum cluster list length, 541
    oldest established, 541
    origin type, 532–534
    RID (router ID), 541
    shortest AS_Path, 530–532
    weight, 519–522
equal-cost multipathing, 542–543
 troubleshooting, 577–583, 587–604
path selection (OSPF), 292
equal-cost multipathing, 295
 external routes, 294–295
 interarea routes, 293–294
 intra-area routes, 292–293
 link costs, 292
PBR (policy-based routing)
  configuring, 624–626
  local, 626–628
  operational overview, 623–624
  troubleshooting, 628–636
peer command, 822
peer groups. See IOS peer groups
period (.) regular expression, 494
phases (DMVPN), 759
  comparison, 760–761
    hierarchical tree spoke-to-spoke (phase
      3), 759
    configuring, 773–775
    spoke-to-hub (phase 1), 759
      spoke configuration, 764–766
    spoke-to-spoke (phase 2), 759
      configuring, 777–782
PHP (penultimate hop popping), 739
ping vrf command, 733, 747
pipe (|) regular expression, 494
plus sign (+) regular expression, 494
point-to-multipoint networks (OSPF), 248–251
point-to-point networks (OSPF), 247–248
policy maps, creating, 859–860
policy-based routing. See PBR (policy-based routing)
practice exams, tips for, 916–918
prefix advertisement (BGP), 433–436
prefix lists
BGP, 488–489
conditional matching with, 614–618
troubleshooting, 833–836, 842–844
processing prefix lists, 835–836
reading prefix lists, 833–835
prefix-list command, 512, 638
pre-shared key authentication, 808–817
configuring, 816–817
dead peer detection, 815
IKEv2 keyring, 809–810
IKEv2 profile, 810–811
NAT keepalives, 815
packet replay protection, 814–815
profile, 813–814
transform set, 812–813
tunnel interface encryption, 814
pre-shared-key command, 822
private ASNs (autonomous system numbers), 581
private BGP communities, 506–507
profile (IPsec), 813–814
proxy ARP disabled, 45
proxy ARP enabled, 44–45

Q
question mark (?) regular expression, 495

R
RA Guard, 863–864
RA process, 23
RA suppression, verifying, 25
radius server RADSRV1 command, 849
reading
IPv4 ACLs, 827–828
IPv6 ACLs, 831–832
prefix lists, 833–835
recursive lookups, next-hop addresses, 42
recursive routing, 788–789
redistribute command, 648, 666
redistribute static command, 348
redistribute-internal command, 650
redistribution
destination protocols
BGP, 662–664, 693–695
EIGRP, 650–655, 683–688
OSPF, 655–662, 688–693
as nontransitive, 643–644
operational overview, 641–643, 680–683
protocol-specific configuration, 648–649
RIB and, 645–647
seed metrics, 647–648, 682
sequential protocol redistribution, 645
source protocols, 643
BGP, 649–650
connected networks, 649
troubleshooting
in BGP, 693–695, 711–715
in EIGRP, 683–688, 697–701
IPv6 routes, 705–710
in OSPF, 688–693, 701–705
with route maps, 696
routing loops, 673–680
suboptimal routing, 671–673
targets for, 683
trouble ticket examples, 696–715

regular expressions, 489–495
relay agents
DHCP, 12–13
DHCPv6, 29–30
Reliable Transport Protocol (RTP), 77
remote transfer, troubleshooting, 875–878
reported distance (RD), 74
RIB (Routing Information Base)
in NHRP, 782
OSPF installed routes, 238–239
redistribution and, 645–647
RID (router ID), 86, 229, 325, 340–341, 541
route maps, 618–619
BGP, 497–499
complex matching, 621
continue keyword, 622–623
multiple match conditions, 620–621
optional actions, 621–622
route redistribution commands, 648–649
troubleshooting, 628–636, 696
route redistribution. See redistribution
route reflectors (iBGP), 450–454
route summarization
BGP, 476
with AS_SET, 483–485
aggregate addresses, 476–481
atomic aggregate attribute, 481–483
EIGRP, 113–114
automatic, 117–118
discard routes, 116
interface-specific, 114–116
metrics, 116–117
EIGRPv6, 195–196
MP-BGP, 464–466
NHRP routing table manipulation with, 784–788
OSPF, 295–297
external routes, 300–302
interarea routes, 297–300
OSPFv2, 343–345
OSPFv3, 373–374
troubleshooting, 167
route tags, 678–680
route-map command, 512, 638
router bgp command, 472
router eigrp as-number command, 103
router eigrp command, 142, 220, 730
router eigrp process-name command, 103
router ID (RID), 86, 229, 325, 340–341, 541
router ospf command, 232–233, 257, 308
router ospfv3 command, 385
router-id command, 229, 325
routes
BGP
administrative distance, 569–571
default, 552
filtering, 486–497, 572–577
local, 553
maximum prefix, 507–508
next-hop addresses, 566–568
processing, 436–441
sources, 554–555
split horizon, 568–569
troubleshooting, 562–577, 587–604

EIGRP
displaying, 85–86
filtering, 129–131, 157–158
traffic steering with offset lists, 132–134
troubleshooting, 151–162

EIGRPv6
default route advertising, 196
filtering, 196–197, 201–202
troubleshooting, 201–203

OSPF
default route advertising, 241–242
discontiguous networks, 302–303
external, 239–240, 294–295
interarea, 293–294
intra-area, 292–293
viewing, 238–239
virtual links, 303–306

OSPFv2
administrative distance, 329–332
default route advertising, 348
duplicate RIDs, 325, 340–341
filtering, 332–334
troubleshooting, 327–341

Routing Information Base. See RIB (Routing Information Base)
routing information sources, 38
administrative distance, 39–41
data structures and routing table, 38–39
static routes, 41
IPv4, 41–45
IPv6, 45–47

routing loops, troubleshooting, 673–680

routing tables
data structures and, 38–39
NHRP routing table manipulation, 782–784
with route summarization, 784–788

RTP (Reliable Transport Protocol), 77

scalability (BGP), 509
IOS peer groups, 509–510, 560–561
IOS peer templates, 510–511
SCP (Secure Copy Protocol), troubleshooting, 877–878
Secure Shell (SSH), troubleshooting, 874–875
security
elements of, 803–805
IPsec, 805–806
ESP modes, 807–808
IKEv2 protection, 819–820
key management, 806
pre-shared key authentication, 808–817
security associations, 806–807
security protocols, 806
verifying encryption, 817–819
IPv6 First-Hop Security, 863–864
security associations, 806–807
seed metrics, 647–648, 682
sequential protocol redistribution, 645
server name RADSRV1 command, 849–850
server name TACSRV1 command, 850
servers (DHCP), 15
service dhcp command, 13
service password-encryption command, 875
service policies applying, 861–863
defining, 859–860
service timestamps command, 880
sessions (BGP)
clearing connections, 499
eBGP, 446–447
iBGP, 441–446, 450–458
topologies, 447–449
types of, 423, 441
set aigp-metric command, 529, 544
set as-path prepend command, 530, 544, 622, 638, 648
set community additive command, 506
set community command, 513
set community local-as command, 503
set community no-advertise command, 501
set community no-export command, 502
set ikev2-profile command, 822
set ip next-hop command, 622, 638, 648
set local-preference command, 522, 544, 622, 638, 648
set metric command, 535, 544, 622, 649, 651
set origin command, 532, 544, 622, 649
set tag command, 622, 638
set transform-set command, 822
set weight command, 519, 544, 622, 649
shortest AS Path attribute (BGP), 530–532
show access-list command, 333, 856
show access-lists 10 command, 158
show access-lists 100 command, 150, 323
show access-lists command, 845, 866
show adjacency detail command, 38
show bgp afi safi command, 472
show bgp afi safi neighbor ip-address advertised routes command, 472
show bgp afi safi neighbors ip-address command, 472
show bgp afi safi summary command, 472
show bgp all command, 717
show bgp command, 436, 438
show bgp community command, 504, 513
show bgp community local-as command, 504
show bgp community no-advertise command, 501
show bgp community no-export command, 503
show bgp detail command, 504
show bgp ipv4 unicast command, 447, 521, 566, 570, 572
show bgp ipv4 unicast neighbors advertised-routes command, 572
show bgp ipv4 unicast neighbors command, 549, 576–577, 717
show bgp ipv4 unicast neighbors routes command, 572
show bgp ipv4 unicast regex _300_ command, 491
show bgp ipv4 unicast regex 100 command, 490
show bgp ipv4 unicast rib-failure command, 571
show bgp ipv4 unicast summary command, 440, 549, 551, 552, 558, 569, 717
show bgp ipv6 unicast command, 463, 584, 585, 586
show bgp ipv6 unicast neighbors command, 461
show bgp ipv6 unicast summary command, 461, 467, 583, 586
show bgp neighbor advertised routes command, 440
show bgp neighbors command, 431
show bgp regexp command, 489, 513
show bgp summary command, 431
show bgp unicast command, 608
show bgp unicast neighbors command, 608
show bgp unicast summary command, 608
show cdp neighbors command, 142, 315
show cef interface command, 854
show class-map command, 858, 866
show clock command, 830, 845
show crypto ikev2 profile command, 811, 822
show crypto ikev2 stats command, 819
show crypto ipsec profile command, 813, 822
show crypto ipsec sa command, 375–376, 818
show debug condition command, 911
show dmvpn command, 766–768, 794, 797
show dmvpn detail command, 768–769, 817
show eigrp address-family ipv4 interfaces command, 206, 221
show eigrp address-family ipv4 interfaces detail command, 206–207, 221
show eigrp address-family ipv4 neighbors command, 207, 221
show eigrp address-family ipv4 topology command, 207–208, 221
show eigrp address-family ipv6 interfaces command, 206, 221
show eigrp address-family ipv6 interfaces detail command, 206–207, 221
show eigrp address-family ipv6 neighbors command, 207, 221
show eigrp address-family ipv6 topology command, 221
show eigrp address-family ipv6 topology command, 207–208
show eigrp protocols command, 205, 221
show flow exporter command, 899, 911
show flow interface command, 899, 911
show flow monitor command, 896, 897, 899, 911
show flow record command, 896, 911
show frame-relay map command, 37
show interface command, 98, 148
show interface tunnel command, 754
show ip access-lists command, 575, 845
show ip arp command, 36, 68
show ip cache flow command, 893, 896, 911
show ip cef command, 68
show ip cef exact-route command, 36, 68
show ip cef ip_address command, 36
show ip cef ip_address subnet_mask command, 36
show ip dhcp binding command, 17, 67
show ip dhcp conflict command, 17, 67
show ip eigrp interface command, 83–84, 104, 137
show ip eigrp interface detail command, 148–149
show ip eigrp interfaces command, 88–89, 144, 154, 186
show ip eigrp interfaces detail command, 109, 151, 162, 186
show ip eigrp neighbor command, 84–85
show ip eigrp neighbors command, 141, 186
show ip eigrp neighbors detail command, 160, 186
show ip eigrp topology active command, 112–113
show ip eigrp topology command, 75, 95–96, 104, 112, 137, 154–155, 162–165, 187, 685, 717
show ip eigrp vrf interfaces command, 730
show ip eigrp vrf neighbors command, 731
show ip flow export command, 911
show ip flow interface command, 911
show ip interface brief command, 142, 315, 551
show ip interface command, 9–10, 67, 148, 150, 153, 161, 186, 323, 829, 845
show ip nhrp brief command, 771–772
show ip nhrp command, 37, 769, 770–771, 794
show ip nhrp nhs command, 794
show ip nhrp traffic command, 794
show ip ospf command, 319, 321–322, 335, 343, 362
show ip ospf database asbr-summary command, 278
show ip ospf database command, 263, 308, 330, 363, 689–690, 717
show ip ospf database external command, 275–276
show ip ospf database network command, 269
show ip ospf database nssa-external command, 280
show ip ospf database router command, 264–266
show ip ospf database summary command, 272–273
show ip ospf interface brief command, 236, 244, 315, 317, 324, 363
show ip ospf neighbor command, 237, 257, 313, 323, 347, 363
show ip ospf virtual-links command, 304, 347, 363
show ip prefix-list command, 333, 833
show ip route 10.1.1.2 command, 42
show ip route bgp command, 440, 563
show ip route command, 40–41, 68, 101, 116, 156, 329, 563, 570–571, 685, 690, 746
show ip route eigrp command, 85–86, 155–156, 187
show ip route ip_address command, 34
show ip route ip_address subnet_mask command, 35
show ip route ip_address subnet_mask longer-prefixes command, 35
show ip route longer-prefixes command, 68
show ip route next-hop-override command, 783
show ip route ospf command, 238–239, 257, 363
show ip route ospfv3 command, 411
<table>
<thead>
<tr>
<th>Command</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip route static command</td>
<td>42, 68</td>
</tr>
<tr>
<td>show ip route vrf command</td>
<td>724, 726, 728, 747</td>
</tr>
<tr>
<td>show ip route vrf eigrp command</td>
<td>732</td>
</tr>
<tr>
<td>show ip sla application command</td>
<td>886, 911</td>
</tr>
<tr>
<td>show ip sla configuration command</td>
<td>887, 911</td>
</tr>
<tr>
<td>show ip sla responder command</td>
<td>890, 911</td>
</tr>
<tr>
<td>show ip sla statistics command</td>
<td>888, 911</td>
</tr>
<tr>
<td>show ip ssh command</td>
<td>910</td>
</tr>
<tr>
<td>show ip vrf command</td>
<td>721, 722, 746</td>
</tr>
<tr>
<td>show ip vrf interfaces command</td>
<td>724, 726, 728, 747</td>
</tr>
<tr>
<td>show ipv6 access-list command</td>
<td>845</td>
</tr>
<tr>
<td>show ipv6 dhcp binding command</td>
<td>27, 67</td>
</tr>
<tr>
<td>show ipv6 dhcp interface command</td>
<td>27, 68</td>
</tr>
<tr>
<td>show ipv6 dhcp pool command</td>
<td>27, 68</td>
</tr>
<tr>
<td>show ipv6 eigrp interface command</td>
<td>193, 220</td>
</tr>
<tr>
<td>show ipv6 eigrp interfaces command</td>
<td>200, 201, 220</td>
</tr>
<tr>
<td>show ipv6 eigrp interfaces detail command</td>
<td>199–200, 203, 220</td>
</tr>
<tr>
<td>show ipv6 eigrp neighbors command</td>
<td>193, 197, 220</td>
</tr>
<tr>
<td>show ipv6 eigrp neighbors detail command</td>
<td>202, 220</td>
</tr>
<tr>
<td>show ipv6 eigrp topology command</td>
<td>687, 717</td>
</tr>
<tr>
<td>show ipv6 interface brief command</td>
<td>198</td>
</tr>
<tr>
<td>show ipv6 interface command</td>
<td>21–22, 24, 67, 394, 832, 845</td>
</tr>
<tr>
<td>show ipv6 interface gigabitEthernet 0/0 command</td>
<td>28</td>
</tr>
<tr>
<td>show ipv6 neighbors command</td>
<td>68</td>
</tr>
<tr>
<td>show ipv6 nhrp command</td>
<td>794</td>
</tr>
<tr>
<td>show ipv6 nhrp nhs command</td>
<td>794</td>
</tr>
<tr>
<td>show ipv6 nhrp traffic command</td>
<td>794</td>
</tr>
<tr>
<td>show ipv6 ospf command</td>
<td>389–390, 417</td>
</tr>
<tr>
<td>show ipv6 ospf database command</td>
<td>391–393, 418, 691, 717</td>
</tr>
<tr>
<td>show ipv6 ospf interface brief command</td>
<td>390, 417</td>
</tr>
<tr>
<td>show ipv6 ospf interface command</td>
<td>390–391, 417</td>
</tr>
<tr>
<td>show ipv6 ospf neighbor command</td>
<td>391, 418</td>
</tr>
<tr>
<td>show ipv6 prefix-list command</td>
<td>833</td>
</tr>
<tr>
<td>show ipv6 protocols command</td>
<td>193, 198–199, 200, 201, 202, 220, 389, 403–404, 417, 686, 691, 694, 717</td>
</tr>
<tr>
<td>show ipv6 route command</td>
<td>418</td>
</tr>
<tr>
<td>show ipv6 route eigrp command</td>
<td>193, 220</td>
</tr>
<tr>
<td>show ipv6 route ospf command</td>
<td>372, 393–394, 411</td>
</tr>
<tr>
<td>show ipv6 route static command</td>
<td>68</td>
</tr>
<tr>
<td>show key chain command</td>
<td>92, 104, 148–149, 186, 199–200</td>
</tr>
<tr>
<td>show line vty include Allowed command</td>
<td>910</td>
</tr>
<tr>
<td>show line vty include Allowed input transports command</td>
<td>910</td>
</tr>
<tr>
<td>show logging command</td>
<td>879, 911</td>
</tr>
<tr>
<td>show ospfv3 command</td>
<td>404–406, 418</td>
</tr>
<tr>
<td>show ospfv3 database command</td>
<td>382, 408–411, 418</td>
</tr>
<tr>
<td>show ospfv3 database link command</td>
<td>382, 385</td>
</tr>
<tr>
<td>show ospfv3 database network command</td>
<td>381, 385</td>
</tr>
<tr>
<td>show ospfv3 database router command</td>
<td>379, 385</td>
</tr>
</tbody>
</table>
show ospfv3 interface brief command, 372, 406–407, 418
show ospfv3 interface command, 371, 373, 376, 385, 407–408, 418
show ospfv3 ipv6 neighbor command, 371, 385
show ospfv3 neighbor command, 408, 418
show policy-map command, 860, 866
show policy-map control-plane command, 861–863, 866
show route bgp command, 608
show route-map command, 158, 333
show run command, 186, 220, 866
show run interface command, 148–149, 186, 320, 321–322, 324
show run section ipv6 router eigrp command, 201
show run section line vty command, 910
show run section router eigrp command, 144
show run section router ospf command, 348
show running-config flow record command, 896
show snmp group command, 883, 911
show snmp host command, 884, 911
show snmp user command, 884, 911
show snmp view command, 884, 911
show ssh command, 875, 910
show tcp brief all command, 554
show tcp brief command, 427
show time-range command, 829, 845
show track command, 891, 911
show users command, 910
SIA (stuck in active), 112–113
SLAAC (stateless address autoconfiguration), 22–26
default gateways, 26
enabling, 23
interface enabled, 25
RA process, 23
RA suppression, 25
verifying, 22–23, 24
SNMP (Simple Network Management Protocol), troubleshooting, 881–885
Source Guard, 864
source protocols for redistribution, 643
BGP, 649–650
connected networks, 649
seed metrics, 648
split horizon
BGP, 568–569
EIGRP, 126–128, 160–162
EIGRPv6, 203
spoke routers (DMVPN), 764–766
spoke-to-hub (DMVPN phase 1), 759
spoke configuration, 764–766
spoke-to-spoke (DMVPN phase 2), 759
configuring, 777–782
SSH (Secure Shell), troubleshooting, 874–875
standard ACLs, 612–613
standard numbered ACLs, 828
stateful DHCPv6, 26–27
stateless DHCPv6, 28
static routes, 41
FVRF, 792
IPv4, 41–45
IPv6, 45–47
troubleshooting, 60–65
stub areas
OSPF, 282–284
OSPFV2, configuring, 335
stub routers 118–121, 158–160
EIGRP 108–109, 151
EIGRPv6, 200
stub sites, 121–125
stub areas, 282–284
totally NSSAs, 289–291
totally stubby areas, 284–286
stub-site wan-interface command, 123, 136
stuck in active (SIA), 112–113
study resources, 920–921
subnets determining addresses within, 10–11
EIGRP interfaces, 148
OSPFv2 interfaces, 320
suboptimal routing in EIGRP, 154–157
in EIGRPv6, 201
troubleshooting, 671–673
successor routes, 74
successors, 74
summarization. See route summarization
summary-address command, 115, 136, 301, 308, 344
summary-metric command, 117, 136
switching labels, 738–739
syslog, troubleshooting, 879–881

T

tacacs server TACSRV1 command, 849
tagging routes, 678–680
telnet access, troubleshooting, 872–873
terminal monitor command, 879
TFTP, troubleshooting, 875–876
time budget for exam, 912–914
time to live (TTL), 557–559
time-based ACLs, 829–830
timers
BGP, 561–562
EIGRP, 108–109, 151
EIGRPv6, 200
OSPF, 252–253
OSPFv2, mismatched, 316–317
timers active-time command, 113
topology base command, 118
topology tables (EIGRP), 75–76
totally NSSAs (not-so-stubby areas), 289–291
totally stubby areas (OSPF), 284–286
tracking LSAs, 341–343
traffic steering with offset lists, 132–134
transform set (IPsec), 812–813
transport mode, 807, 808
troubleshooting
BFD, 900–901
BGP neighbors, 549–562
path selection, 577–583
route filtering, 572–577
routes, 562–577
trouble ticket examples, 587–604
Cisco DNA Center Assurance, 901–908
Cisco IOS AAA, 849–852
Cisco IOS IP SLA, 885–891
console access, 871–872
CoPP, 854–863
ACL creation, 854–856
class map creation, 856–858
policy map creation, 859–860
service policy application, 861–863
DHCP, 16–18
  commands, 17–18
  issues, 16–17
EIGRP
  discontiguous networks, 165–166
  feasible successors, 162–165
  load balancing, 168–169
  neighbor adjacencies, 141–151
  route summarization, 167
  routes, 151–162
  trouble ticket examples, 169–184
EIGRPv6
  named configuration mode, 204–208, 213–218
  neighbors, 197–201
  routes, 201–203
  trouble ticket examples, 208–218
Flexible NetFlow, 892–900
HTTP, 876–877
IPv4 ACLs, 827–830, 836–838
  packet filtering with ACLs, 829
  reading ACLs, 827–828
  time-based ACLs, 829–830
IPv4 addressing, 47–52
IPv6 ACLs, 830–833, 839–842
  packet filtering with ACLs, 832–833
  reading ACLs, 831–832
IPv6 addressing, 53–60
MP-BGP, 583–587, 604–606
NetFlow, 892–900
Object Tracking, 891–892
OSPFv2
  discontiguous networks, 345–347
  load balancing, 347–348
  neighbor adjacencies, 312–327
  route summarization, 343–345
  routes, 327–341
  trouble ticket examples, 348–361
OSPFv3
  address families, 402–416
  commands, 388–394
  trouble ticket examples, 395–402
overlay networks
  outbound interface selection, 789–790
  recursive routing, 788–789
packet forwarding, 34–38
PBR, 628–636
prefix lists, 833–836, 842–844
  processing prefix lists, 835–836
  reading prefix lists, 833–835
redistribution
  in BGP, 693–695, 711–715
  in EIGRP, 683–688, 697–701
  IPv6 routes, 705–710
  in OSPF, 688–693, 701–705
  with route maps, 696
  routing loops, 673–680
  suboptimal routing, 671–673
  targets for, 683
  trouble ticket examples, 696–715
remote transfer, 875–878
route maps, 628–636, 696
SCP, 877–878
SNMP, 881–885
SSH, 874–875
static routes, 60–65
syslog, 879–881
Telnet access, 872–873
TFTP, 875–876
uRPF, 852–854
vty access, 872–875
TTL (time to live), 557–559
tunnel destination command, 800
tunnel interface encryption, 814
tunnel key command, 800
tunnel mode, 807, 808
tunnel mode gre multipoint command, 793, 800
tunnel mode gre multipoint ipv6 command, 793, 795
tunnel protection ipsec profile command, 814
tunnel protection ipsec profile profile-name command, 822
tunnel security. See IPsec
tunnel source command, 800
tunnel status, verifying, 766–769
tunnel vrf command, 800
Type 1 LSAs (router link), 263–268, 281, 342
Type 2 LSAs (network link), 269–271, 281, 342
Type 3 LSAs (summary link), 271–274, 281, 343
Type 4 LSAs (ASBR summary), 276–278, 281, 343
Type 5 LSAs (external routes), 274–276, 281, 343
Type 7 LSAs (NSSA external summary), 278–280, 281, 343

_.underline_ ( ) regular expression, 490–491
unique IP registration, 775–777
UPDATE messages (BGP), 426

uRPF (unicast Reverse Path Forwarding), troubleshooting, 852–854
username admin password 0 letmein command, 849
username password command, 866

V

variance multiplier command, 104
verifying
administrative distance, 40–41
in BGP, 569–571
in EIGRPv6, 201
in OSPFv2, 329–332
BGP, 431–433
default gateways, 26
DHCP-assigned IP addresses, 16
DHCPv6, 27
DMVPN IPv6, 797–798
DMVPN tunnel status, 766–769
EIGRP interfaces, 83–84
EIGRP neighbors, 84–85
EIGRPv6, 192–195
EIGRPv6 authentication, 199–200
EIGRPv6 interfaces, 200
EUI-64 standard, 21–22
interface enabled for IPv6, 25
IPsec DMVPN encryption, 817–819
IPv4 addressing, 10, 11
IPv6 addressing, 19–21
IPv6 static routes, 46
Layer 3 connectivity, 551
local PBR, 627
OSPF
interfaces, 235–237
neighbors, 237
timers, 253
Verifying instances, creating and verifying, 721–734
VRF-Lite, 721
vty access, troubleshooting, 872–875

W

WANs (wide-area networks)
with EIGRP
  bandwidth percentage, 125
  split horizon, 126–128
  stub routers, 118–121
  stub sites, 121–125
secure transport elements, 803–805
weight attribute (BGP), 519–522
well-known BGP communities, 500–504
wide metrics (EIGRP), 96–98