Official Cert Guide

Study Planner

Review Exercises

CCNP Enterprise Advanced Routing

ENARSI 300-410

2nd Edition

RAYMOND LACOSTE
BRAD EDGEWORTH, CCIE® NO. 31574

ciscopress.com

FREE SAMPLE CHAPTER

CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide

Companion Website and Pearson Test Prep Access Code

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

To access the companion website, simply follow these steps:

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

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

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

This page intentionally left blank

CCNP Enterprise Advanced Routing

ENARSI 300-410

Official Cert Guide, Second Edition

RAYMOND LACOSTE

BRAD EDGEWORTH, CCIE No. 31574

Cisco Press

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

Raymond Lacoste, Brad Edgeworth

Published by:

Cisco Press

$PrintCode

Library of Congress Control Number: 2023911481

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

ISBN-10: 0-13-821752-1

Warning and Disclaimer

This book is designed to provide information about Implementing Cisco Enterprise Advanced Routing and Services (ENARSI 300-410). Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Trademark Acknowledgments

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

Figure credit: Figure 7-1 Wireshark

Special Sales

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

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

For questions about sales outside the U.S., please contact international@pearsoned.com.

Feedback Information

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

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

We greatly appreciate your assistance.

Vice President, IT Professional: Mark Taub

Alliances Manager, Cisco Press: Jaci Featherly; James Risler

Director, ITP Product Management: Brett Bartow

Managing Editor: Sandra Schroeder

Development Editor: Ellie C. Bru

Senior Project Editor: Mandie Frank

Copy Editor: Kitty Wilson

Technical Editor: Hector Mendoza, Jr

Editorial Assistant: Cindy Teeters

Designer: Chuti Prasertsith

Composition: Codemantra

Indexer: Erika Millen

Proofreader: Barbara Mack

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Pearson's Commitment to Diversity, Equity, and Inclusion

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

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

Our ambition is to purposefully contribute to a world where

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

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

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

About the Authors

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

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

About the Technical Reviewer

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

Dedications

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

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

Acknowledgments

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

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

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

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

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

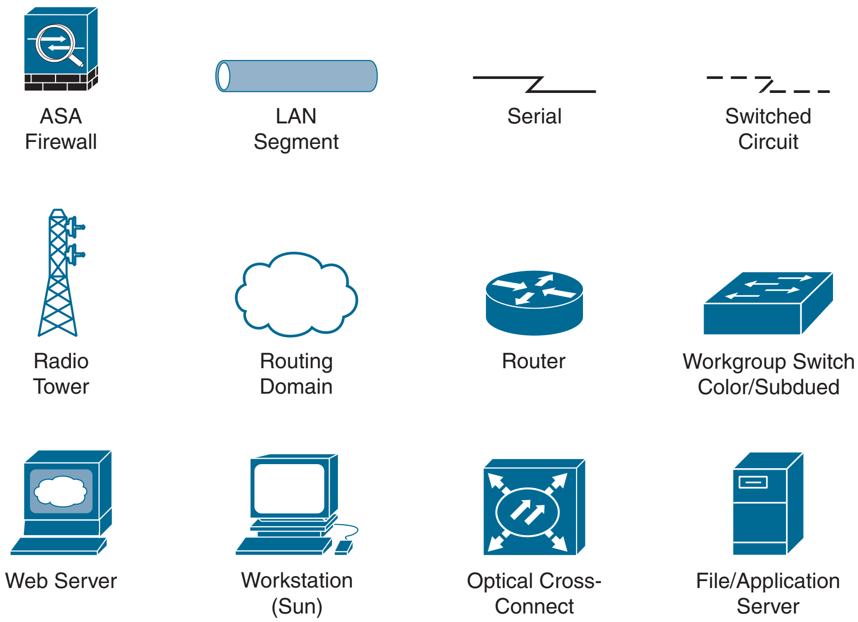
Many people within Cisco have shared their knowledge with me and taken a chance on me with various projects over the years. For that I'm forever indebted.

Contents at a Glance

Online Elements

Contents

Icons Used in This Book



Command Syntax Conventions

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

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

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

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

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

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

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

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

Goals and Methods

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

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

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

Who Should Read This Book?

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

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

Strategies for Exam Preparation

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

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

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

The Companion Website for Online Content Review

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

How to Access the Companion Website

To access the companion website, which gives you access to the electronic content with this book, start by establishing a login at www.ciscopress.com and registering your book. To do so, simply go to ciscopress.com/register and enter the ISBN of the print book: 9780138217525. After you have registered your book, go to your account page and click the Registered Products tab. From there, click the Access Bonus Content link to get access to the book's companion website.

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

How to Access the Pearson Test Prep (PTP) App

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

- You can get your access code by registering the print ISBN (9780138217525) on ciscopress.com/register. Make sure to use the print book ISBN regardless of whether you purchased an eBook or the print book. Once you register the book, your access code will be populated on your account page under the Registered Products tab. Instructions for how to redeem the code are available on the book's companion website by clicking the Access Bonus Content link.
- Premium Edition: If you purchase the Premium Edition eBook and Practice Test directly from the Cisco Press website, the code will be populated on your account page after purchase. Just log in at ciscopress.com click Account to see details of your account, and click the digital purchases tab.

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

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

Step 1. Open this book's companion website, as shown earlier in this Introduction under the heading "How to Access the Companion Website."

Step 2. Click the Practice Exams button.

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

Note that if you want to use the web app only at this point, just navigate to pearsontestprep.com, log in using the same credentials used to register your book or purchase the Premium Edition, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

How This Book Is Organized

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

The chapters cover the following topics:

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

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

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

Certification Exam Topics and This Book

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

Table I-1 Enterprise Core Topics and Chapter References

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

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

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

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

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

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

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

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

Learning in a Lab Environment

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

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

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

This page intentionally left blank

CHAPTER 2

EIGRP

This chapter covers the following topics:

- **EIGRP Fundamentals:** This section explains how EIGRP establishes a 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 used to troubleshoot common problems.

"Do I Know This Already?" Quiz

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

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

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

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

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

5. What attributes does the EIGRP topology table contain? (Choose all that apply.)
  a. Destination network prefix
  b. Hop count
  c. Total path delay
  d. Maximum path bandwidth
  e. List of EIGRP neighbors

6. What destination addresses does EIGRP use when feasible? (Choose two.)
  a. IP address 224.0.0.9
  b. IP address 224.0.0.10
  c. IP address 224.0.0.8
  d. MAC address 01:00:5E:00:00:0A
  e. MAC address 0C:15:C0:00:00:01

7. Which of the following techniques can be used to initialize the EIGRP process? (Choose two.)
  a. Use the interface command **ip eigrp** *as-number* **ipv4 unicast**.
  b. Use the global configuration command **router eigrp** *as-number*.
  c. Use the global configuration command **router eigrp** *process-name*.
  d. Use the interface command **router eigrp** *as-number*.

8. True or false: The EIGRP router ID (RID) must be configured for EIGRP to be able to establish neighborship.
  a. True
  b. False

9. True or false: When using MD5 authentication between EIGRP routers, the keychain sequence numbers used on the routers can be different, as long as the password is the same.
  a. True
  b. False

10. Which value can be modified on a router to manipulate the path taken by EIGRP but does not have an impact on other routing protocols, like OSPF?
  a. Interface bandwidth
  b. Interface MTU
  c. Interface delay
  d. Interface priority

Foundation Topics

EIGRP Fundamentals

EIGRP overcomes the deficiencies of other distance vector routing protocols, such as Routing Information Protocol (RIP), with features such as unequal-cost load balancing, support for networks 255 hops away, and rapid convergence features. EIGRP uses a *diffusing update* *algorithm* (*DUAL*) to identify network paths and provides for fast convergence using precalculated loop-free backup paths. Most distance vector routing protocols use hop count as the metric for routing decisions. However, a route-selection algorithm that uses only hop count for path selection does not take into account link speed and total delay. EIGRP adds logic to the route-selection algorithm to use factors other than hop count alone.

Autonomous Systems

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

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

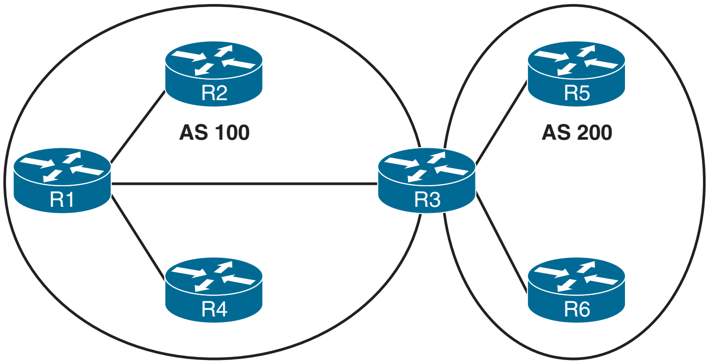


Figure 2-1 *EIGRP Autonomous Systems*

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

EIGRP Terminology

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

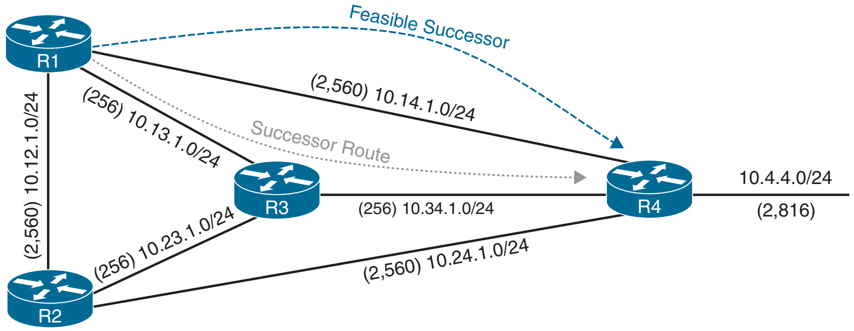


Figure 2-2 *EIGRP Reference Topology*

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

Key Topic

Table 2-2 EIGRP Terminology

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

Key Topic

Topology Table

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

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

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

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

```
R1#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS (100)/ID(192.168.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.12.1.0/24, 1 successors, FD is 2816
       via Connected, GigabitEthernet0/3
P 10.13.1.0/24, 1 successors, FD is 2816
       via Connected, GigabitEthernet0/1
P 10.14.1.0/24, 1 successors, FD is 5120
       via Connected, GigabitEthernet0/2
P 10.23.1.0/24, 1 successors, FD is 3072
       via 10.13.1.3 (3072/2816), GigabitEthernet0/1
       via 10.12.1.2 (5376/2816), GigabitEthernet0/3
P 10.34.1.0/24, 1 successors, FD is 3072
       via 10.13.1.3 (3072/2816), GigabitEthernet0/1
       via 10.14.1.4 (5376/2816), GigabitEthernet0/2
P 10.24.1.0/24, 1 successors, FD is 5376
       via 10.12.1.2 (5376/5120), GigabitEthernet0/3
       via 10.14.1.4 (7680/5120), GigabitEthernet0/2
P 10.4.4.0/24, 1 successors, FD is 3328            Feasible Distance
       via 10.13.1.3 (3328/3072), GigabitEthernet0/1  Successor Route
       via 10.14.1.4 (5376/2816), GigabitEthernet0/2

          Path Metric   Reported Distance   Feasible Successor

                                            Passes Feasibility Condition
                                            2816<3328
```

Figure 2-3 *EIGRP Topology Output*

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

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

EIGRP Neighbors

Unlike a number of routing protocols—such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Intermediate System-to-Intermediate System (IS-IS)—EIGRP does not rely on periodic advertisement of all the network prefixes in an autonomous system. EIGRP neighbors exchange the entire routing table when forming an adjacency, and they advertise incremental updates only as topology changes occur within a network. The neighbor adjacency table is vital for tracking neighbor status and the updates sent to each neighbor.

Inter-Router Communication

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

Key Topic

Table 2-3 EIGRP Packet Types

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

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

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

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

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

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

2

Key Topic

Forming EIGRP Neighbors

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

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

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

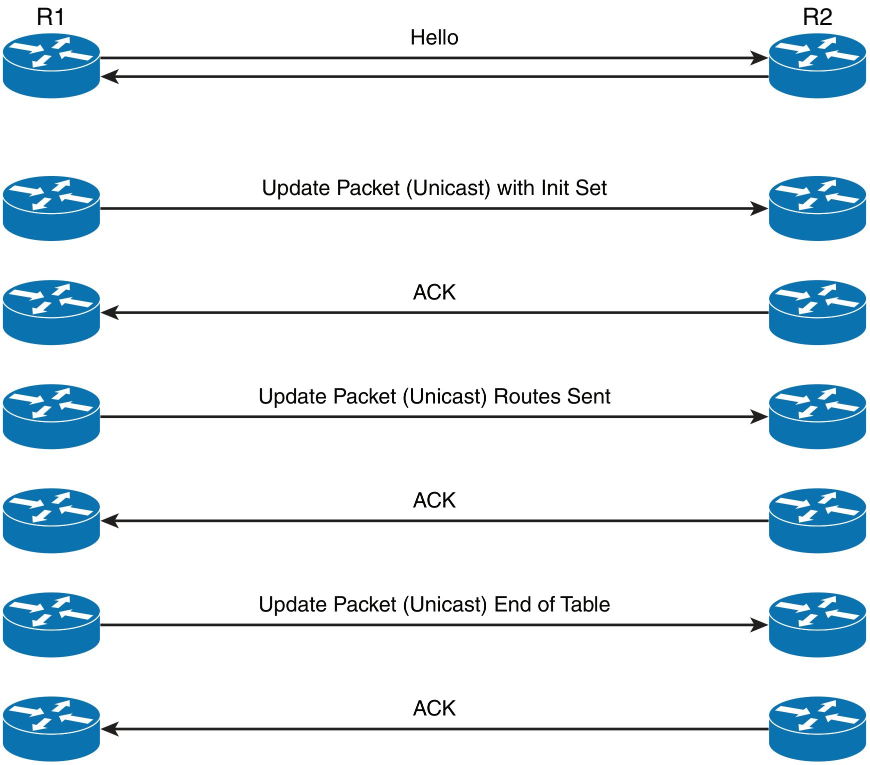


Figure 2-4 *EIGRP Neighbor Adjacency Process from R1's Perspective*

EIGRP Configuration Modes

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

Classic Configuration Mode

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

Key Topic

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

Key Topic

EIGRP Named Mode

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

EIGRP named configuration provides the following benefits:

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

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

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

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

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

Step 1. Initialize the EIGRP process by using the command **router eigrp** *process-name*. (If a number is used for *process-name*, the *number* does not correlate to the autonomous system number.)

Step 2. Initialize the EIGRP instance for the appropriate address family with the command **address-family {IPv4 | IPv6} {unicast | vrf** *vrf-name*} **autonomous-system** *as-number*.

Step 3. Enable EIGRP on interfaces by using the command **network** *network wildcard-mask*.

EIGRP Network Statement

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

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

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

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

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

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

Table 2-4 Table of Sample Interface and IP Addresses

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

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

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

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

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

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

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

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

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

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

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

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

Sample Topology and Configuration

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

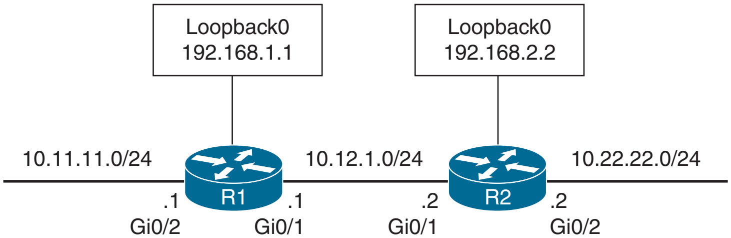


Figure 2-5 *EIGRP Sample Topology*

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

Example 2-3 *Sample EIGRP Configuration*

```
R1 (Classic Configuration)
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
!
interface GigabitEthernet0/1
    ip address 10.12.1.1 255.255.255.0
!
interface GigabitEthernet0/2
    ip address 10.11.11.1 255.255.255.0
!
router eigrp 100
 network 10.11.11.1 0.0.0.0
 network 10.12.1.1 0.0.0.0
 network 192.168.1.1 0.0.0.0
```

```
R2 (Named Mode Configuration)
interface Loopback0
 ip address 192.168.2.2 255.255.255.255
!
interface GigabitEthernet0/1
    ip address 10.12.1.2 255.255.255.0
!
interface GigabitEthernet0/2
    ip address 10.22.22.2 255.255.255.0
!
router eigrp EIGRP-NAMED
 address-family ipv4 unicast autonomous-system 100
  network 0.0.0.0 255.255.255.255
```

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

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

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

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

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

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

Confirming Interfaces

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

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

Example 2-5 *Verifying EIGRP Interfaces*

```
R1# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(100)
                 Xmit Queue   PeerQ        Mean   Pacing Time  Multicast  Pending
Interface Peers  Un/Reliable  Un/Reliable  SRTT   Un/Reliable  Flow Timer Routes
Gi0/2        0       0/0        0/0          0       0/0            0           0
```

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

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

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

Table 2-5 EIGRP Interface Fields

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

Verifying EIGRP Neighbor Adjacencies

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

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

Example 2-6 *EIGRP Neighbor Confirmation*

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

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

Table 2-6 EIGRP Neighbor Columns

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

Displaying Installed EIGRP Routes

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

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

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

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

```
Gateway of last resort is not set

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

```
R2# show ip route eigrp
! Output omitted for brevity
Gateway of last resort is not set

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

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

Router ID

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

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

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

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

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

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

Key Topic

Passive Interfaces

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Example 2-12 *show ip eigrp interfaces Output*

```
R1# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(100)
                 Xmit Queue   PeerQ        Mean   Pacing Time  Multicast  Pending
Interface Peers  Un/Reliable  Un/Reliable  SRTT   Un/Reliable  Flow Timer Routes
Gi0/1       1        0/0       0/0           9       0/0           50           0
```

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

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

Example 2-13 *show ip protocols Output*

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

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

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

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

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

Key Topic

Authentication

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

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

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

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

Keychain Configuration

Keychain creation is accomplished with the following steps:

Step 1. Create the keychain by using the command **key chain** *key-chain-name*.

Step 2. Identify the key sequence by using the command **key** *key-number*, where *key-number* can be anything from 0 to 2147483647.

Step 3. Specify the preshared password by using the command **key-string** *password*.

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

Enabling Authentication on the Interface

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

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

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

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

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

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

Example 2-14 *Configuring EIGRP Authentication*

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

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

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

Example 2-15 *Verifying Keychain Settings*

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

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

Example 2-16 *Verifying EIGRP Authentication*

```
R1# show ip eigrp interface detail
EIGRP-IPv4 Interfaces for AS(100)
                  Xmit Queue   PeerQ        Mean   Pacing Time   Multicast    Pending
Interface   Peers  Un/Reliable  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Gi0/1         0        0/0          0/0        0        0/0            50           0
  Hello-interval is 5, Hold-time is 15
  Split-horizon is enabled
  Next xmit serial <none>
  Packetized sent/expedited: 10/1
  Hello's sent/expedited: 673/12
```

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

Key Topic

Path Metric Calculation

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

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

Figure 2-6 *EIGRP Metric Formula*

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

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

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

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

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

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

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

Key Topic

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

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

Equals

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

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

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

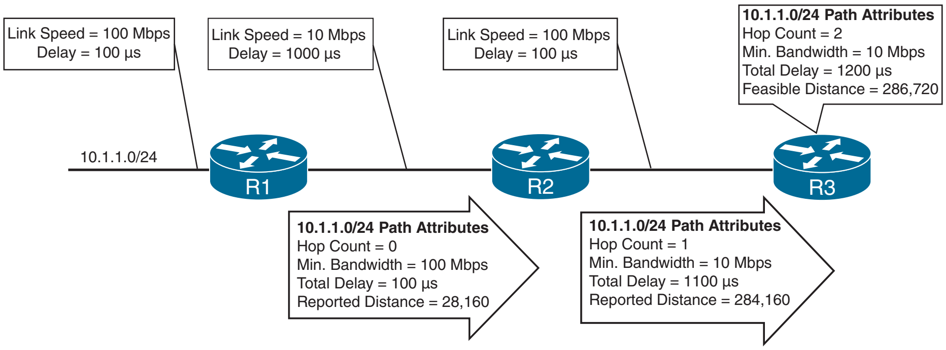


Figure 2-9 *EIGRP Attribute Propagation*

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

Table 2-7 Default EIGRP Interface Metrics for Classic Metrics

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

Using the topology from Figure 2-2, the metrics from R1 and R2 for the 10.4.4.0/24 network are calculated using the formula in Figure 2-10. The link speed for both routers is 1 Gbps, and the total delay is 30 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).

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

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

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

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

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

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

Wide Metrics

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

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

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

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

```
GigabitEthernet:
Scaled Bandwidth = 10,000,000 / 1,000,000
Scaled Delay = 10 / 10
Composite Metric = 10 + 1 * 256 = 2816

10 GigabitEthernet:
Scaled Bandwidth = 10,000,000 / 10,000,000
Scaled Delay = 10 / 10
Composite Metric = 1 + 1 * 256 = 512

11 GigabitEthernet:
Scaled Bandwidth = 10,000,000 / 11,000,000
Scaled Delay = 10 / 10
Composite Metric = 0 + 1 * 256 = 256

20 GigabitEthernet:
Scaled Bandwidth = 10,000,000 / 20,000,000
Scaled Delay = 10 / 10
Composite Metric = 0 + 1 * 256 = 256
```

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

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

Key Topic

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

Figure 2-11 *EIGRP Wide Metrics Formula*

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

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

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

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

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

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

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

Example 2-19 *Verifying EIGRP Metric Style*

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

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

Metric Backward Compatibility

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

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

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

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

2

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, you can query the values dynamically by using the command **show interface** *interface-id*. The output displays the EIGRP interface delay, in microseconds, after the DLY field. Example 2-20 provides sample output of the command on R1 and R2. The output shows that both interfaces have a delay of 10 µs.

Example 2-20 *Verifying EIGRP Interface Delay*

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

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

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

Example 2-21 demonstrates the modification of the delay on R1 to 100, increasing the delay to 1000 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 *Configuring Interface Delay*

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

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

Key Topic

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 K*1 *K*2 *K*3 *K*4 *K*5 [*K*6] under the EIGRP process. *TOS* always has a value of 0, and *K*6 is used for named mode configurations.

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

Load Balancing

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

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

Example 2-22 *Changing the EIGRP Maximum Paths*

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

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

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 variance value up to the maximum number of ECMP routes, as discussed earlier.

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

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

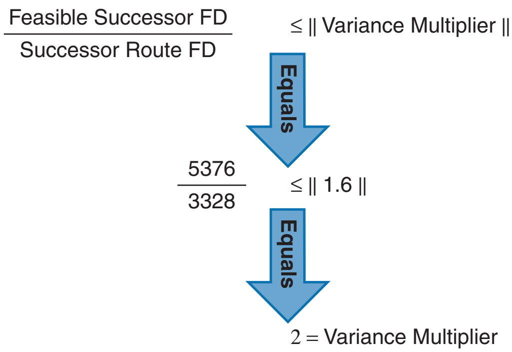


Figure 2-14 *EIGRP Variance Multiplier Formula*

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

Example 2-23 *Configuring EIGRP Variance*

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

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

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

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

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

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

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

References in This Chapter

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

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

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

Exam Preparation Tasks

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

Review All Key Topics

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

Table 2-8 Key Topics

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

Define Key Terms

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

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

Use the Command Reference to Check Your Memory

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

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

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

Table 2-9 Command Reference

Task	Command Syntax
Initialize EIGRP in a classic configuration.	**router eigrp** *as-number* **network** *network wildcard-mask*
Initialize EIGRP in a named mode configuration.	**router eigrp** *process-name* **address-family** {**ipv4** | **ipv6**} {**unicast** | **vrf** *vrf-name*} **autonomous-system** *as-number* **network** *network wildcard-mask*
Define the EIGRP router ID.	**eigrp router-id** *router-id*
Configure an EIGRP-enabled interface to prevent neighbor adjacencies.	Classic: **(EIGRP process)** **passive-interface** *interface-id* Named mode: **af-interface** {**default** | *interface-id*} **passive-interface**
Configure a keychain for EIGRP MD5 authentication.	**key chain** *key-chain-name* **key** *key-number* **key-string** *password*
Configure MD5 authentication for an EIGRP interface.	Classic: **(EIGRP process)** **ip authentication key-chain eigrp** *as-number key-chain-name* **ip authentication mode eigrp** *as-number* **md5** Named mode: **af-interface** {**default** | *interface-id*} **authentication key-chain eigrp** *key-chain-name* **authentication mode md5**
Configure SHA authentication for EIGRP named mode interfaces.	Named mode: **af-interface** {**default** | *interface-id*} **authentication mode hmac-sha-256** *password*
Modify the interface delay for an interface.	**delay** *tens-of-microseconds*
Modify the EIGRP K values.	**metric weights** *TOS* K_1 K_2 K_3 K_4 K_5 [K_6]
Modify the default number of EIGRP maximum paths that can be installed into the RIB.	**maximum-paths** *maximum-paths*
Modify the EIGRP variance multiplier for unequal-cost load balancing.	**variance** *multiplier*
Display the EIGRP-enabled interfaces.	**show ip eigrp interface** [{*interface-id* [**detail**] | **detail**}]
Display the EIGRP topology table.	**show ip eigrp topology** [**all-links**]
Display the configured EIGRP keychains and passwords.	**show key chain**
Display the IP routing protocol information configured on the router.	**show ip protocols**

This page intentionally left blank

Index

Symbols

A

B

C

D

E

F

G

H

I

J-K

M

N

O

Q

R

S

U

V

W

X-Y-Z