



CCIE Enterprise Infrastructure Foundation

ciscopress.com

Narbik Kocharians, CCIE® No. 12410

FREE SAMPLE CHAPTER |



CCIE Enterprise Infrastructure Foundation

Narbik Kocharians

Cisco Press

CCIE Enterprise Infrastructure Foundation

Narbik Kocharians

Copyright© 2023 Pearson Education, Inc.

Published by: Cisco Press

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

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

ScoutAutomatedPrintCode

Library of Congress Control Number: 2022902108

ISBN-13: 978-0-13-737424-3

ISBN-10: 0-13-737424-0

Warning and Disclaimer

This book is designed to provide information about the CCIE Enterprise Infrastructure certification. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Trademark Acknowledgments

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

Special Sales

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

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

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

Feedback Information

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

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

We greatly appreciate your assistance.

Editor-in-Chief: Mark Taub

Alliances Manager, Cisco Press: Arezou Gol

Director, ITP Product Management: Brett Bartow

Executive Editor: James Manly

Managing Editor: Sandra Schroeder

Development Editor: Ellie Bru

Project Editor: Mandie Frank

Copy Editor: Kitty Wilson

Technical Editors: Sarah Anand; Dante McNeil

Editorial Assistant: Cindy Teeters

Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Timothy Wright

Proofreader: Donna E. Mulder



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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



CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks. Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks, and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCFP, CCNA, CCNP, CCSP, CCOVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Credits

Unnumbered figures on pages 860-861 PuTTY

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 Author

Narbik Kocharians, CCIE No. 12410 (Routing and Switching, Service Provider, and Security) is a triple CCIE with more than 46 years of experience in this industry. He has designed, implemented, and supported numerous small, mid-size, and large enterprise networks.

Narbik is the president of Micronics Networking and Training, Inc. (www.MicronicsTraining.com), where almost all Cisco-authorized and custom courses are conducted, including CCIE-DC, CCIE-SP, CCIE-Enterprise Infrastructure, CCDE, ACI, and many more.

About the Technical Reviewers

Sarah Anand has been affiliated with different networking technologies, including Cisco-specific implementations, for 7 years, with a focus on routing/switching and service provider technologies. Currently she works as a technical writer and editor, training network engineers in vendor-specific and industry-standard technologies. She has a degree in computer science and enjoys spending free time exploring passions in web design and search engine optimization.

Dante McNeil has 10 years of IT networking experience in the nonprofit, enterprise, K–12, and higher education spaces, with a focus on advanced networking implementations and Cisco technologies. He also spends time writing and creating network training content for networking engineers. He holds a bachelor of science degree in computing information sciences from Jacksonville University. In his spare time, he enjoys roller coasters, video games, and road trips.

Dedications

I would like to dedicate this book to my beautiful wife, Janet, my children and their spouses, Chris and Nona (aka Siroon Achik), Patrick and Diana (aka Bestelik Jan), Alexandra (aka Achiko) and Sevak, and Daniel (aka Chompolik), as well as our first grandson, Matthew (aka Jigar), whom I LOVE so much, he brightens my day every morning!

I would like to acknowledge with gratitude the support, sacrifice, and love of my family for making this book possible. I thank God for the health and wisdom that He has instilled in me, my lovely family, my first grandson Mathew, and my father, who was my best friend.

Acknowledgments

A very special thanks to James and Eleanor. I remember brainstorming with James for hours about this book, and eventually he came up with the ultimate solution. I would like to thank Eleanor for having a tremendous amount of patience and professionalism.

I would also like to thank my tech editors, Sarah Anand and Dante McNeil, two gifted network engineers with a tremendous amount of knowledge. God willing, I will be working with these two champions for a long time to come. They are not CCIEs yet, but their knowledge is on par with the best CCIEs out there.

Contents at a Glance

	Introduction	xxxiii
Chapter 1	Switching	1
Chapter 2	IP Prefix Lists	35
Chapter 3	RIPv2	39
Chapter 4	EIGRP	51
Chapter 5	OSPF	65
Chapter 6	BGP	95
Chapter 7	DMVPN	269
Chapter 8	MPLS and L3VPNs	585
Chapter 9	IPv6	609
Chapter 10	SD-WAN	637
Chapter 11	SD-Access	825
	Index	881

Contents

Introduction xxxiii

Chapter 1 Switching 1

Lab 1: Configuring Trunks 1

Task 1 2

Task 2 2

Task 3 2

Task 4 2

Task 5 3

Task 6 3

Task 7 3

Task 8 3

Task 9 3

Task 10 3

Task 11 4

Task 12 4

Task 13 4

Task 14 4

Task 15 5

Task 16 5

Task 17 5

Task 18 5

Task 19 5

VTP Pruning 5

Task 20 12

Task 21 12

Task 22 12

Task 23 12

Task 24 12

Task 25 12

Task 26 12

Task 27 12

Task 28 12

Lab 2: Configuring EtherChannels	13
Task 1	13
Task 2	13
Task 3	13
Task 4	13
Task 5	14
Task 6	14
Lab 3: Introducing Spanning Tree Protocol	14
802.1D Per-VLAN Spanning Tree Protocol	14
Task 1	15
Task 2	15
Task 3	16
Task 4	16
Configuration Tasks: 802.1D	16
Task 1	18
Task 2	18
Task 3	18
Task 4	18
Task 5	18
Task 6	18
Task 7	19
Task 8	19
Task 9	19
Task 10	19
Task 11	19
Task 12	19
Task 13	19
802.1w Per-VLAN Rapid Spanning Tree Protocol	20
Task 1	25
Task 2	25
Task 3	26
Task 4	26
802.1w Configuration Tasks	26
Task 1	26
Task 2	26
Task 3	26

	<i>Task 4</i>	26
	<i>Task 5</i>	26
	<i>Task 6</i>	26
	<i>Task 7</i>	26
	<i>Task 8</i>	27
	<i>Task 9</i>	27
	<i>Task 10</i>	27
	802.1s Multiple Spanning Tree Protocol	28
	<i>Task 1</i>	28
	<i>Task 2</i>	29
	<i>Task 3</i>	29
	<i>Task 4</i>	30
	Let's Explore 802.1s	30
	<i>Task 1</i>	32
	<i>Task 2</i>	32
	<i>Task 3</i>	33
	<i>Task 4</i>	33
Chapter 2	IP Prefix Lists	35
	Lab 1: Prefix Lists	35
	<i>Task 1</i>	36
	<i>Task 2</i>	36
	<i>Task 3</i>	36
	<i>Task 4</i>	36
	<i>Task 5</i>	36
	<i>Task 6</i>	36
	<i>Task 7</i>	36
	<i>Task 8</i>	36
	<i>Task 9</i>	36
	<i>Task 10</i>	37
	<i>Task 11</i>	37
Chapter 3	RIPv2	39
	Lab 1: Configuring RIPv2	39
	<i>Task 1</i>	40
	<i>Task 2</i>	40
	<i>Task 3</i>	40

Task 4	41
Task 5	41
Task 6	44
Task 7	44
Task 8	44
Task 9	45
Task 10	45
Task 11	45
Task 12	45
Task 13	45
Task 14	45
Task 15	45
Task 16	45
Task 17	46
Task 18	46
Task 19	46
Task 20	46

Lab 2: Helper Map 46

Task 1	47
Task 2	47
Task 3	47
Task 4	47

Lab 3: RIPv2 Challenge Lab 48

Ticket 1	48
Ticket 2	48
Ticket 3	49
Ticket 4	49
Ticket 5	49
Ticket 6	49
Ticket 7	49
Ticket 8	49
Ticket 9	49

Chapter 4 EIGRP 51

Lab 1: EIGRP Named Mode 51

Task 1	52
Task 2	52

Task 3	52
Task 4	53
Task 5	53
Task 6	53
Task 7	53
Task 8	53
Task 9	53
Task 10	53
Task 11	53
Task 12	54
Lab 2: EIGRP and Bidirectional Forwarding Detection (BFD)	54
Task 1	54
Task 2	54
Task 3	54
Task 4	54
Lab 3: EIGRP Stub	55
Task 1	55
Task 2	55
Task 3	55
Task 4	56
Task 5	56
Task 6	56
Task 7	56
Task 8	56
Task 9	56
Task 10	57
Task 11	57
Lab 4: EIGRP Filtering	57
Task 1	58
Task 2	58
Task 3	58
Task 4	58
Task 5	58
Task 6	58
Task 7	58

Lab 5: Advanced EIGRP Lab 59

- Task 1 60
- Task 2 60
- Task 3 60
- Task 4 60
- Task 5 61
- Task 6 61
- Task 7 61
- Task 8 61
- Task 9 61
- Task 10 61
- Task 11 61

Lab 6: EIGRP Authentication 62

- Task 1 62
- Task 2 62
- Task 3 62

Lab 7: EIGRP Challenge Lab 63

- Ticket 1 63
- Ticket 2 63
- Ticket 3 64
- Ticket 4 64
- Ticket 5 64
- Ticket 6 64
- Ticket 7 64
- Ticket 8 64

Chapter 5 OSPF 65

Lab 1: Running OSPF on the Interfaces 65

- Task 1 66
- Task 2 66
- Task 3 66
- Task 4 66
- Task 5 66
- Task 6 66
- Task 7 67
- Task 8 67

Lab 2: OSPF Broadcast Networks	67
Task 1	67
Task 2	68
Task 3	69
Lab 3: OSPF Non-broadcast Networks	69
Task 1	69
Task 2	70
Lab 4: OSPF Point-to-Point Networks	70
Task 1	70
Task 2	71
Lab 5: OSPF Point-to-Multipoint and Point-to-Multipoint Non-broadcast Networks	71
Task 1	71
Task 2	72
Task 3	72
Lab 6: OSPF Area Types	72
Task 1	73
Task 2	73
Task 3	73
Task 4	74
Task 5	74
Task 6	74
Task 7	75
Task 8	75
Task 9	75
Task 10	75
Task 11	76
Task 12	76
Task 13	76
Task 14	76
Task 15	76
Lab 7: OSPF Filtering	77
Task 1	77
Task 2	78
Task 3	78
Task 4	78

Task 5	78
Task 6	78
Task 7	78
Task 8	78
Task 9	78
Task 10	79
Task 11	79
Task 12	79
Task 13	79
Task 14	79
Task 15	79
Task 16	79
Task 17	80
Task 18	80
Task 19	80
Task 20	80
Lab 8: OSPF Summarization	80
Task 1	81
Task 2	81
Task 3	81
Task 4	82
Task 5	82
Task 6	82
Task 7	82
Task 8	82
Lab 9: Virtual Links and GRE Tunnels	83
Task 1	84
Task 2	84
Task 3	84
Task 4	85
Lab 10: Default Route Injection	85
Task 1	85
Task 2	85
Task 3	85
Task 4	85
Task 5	85

Task 6	86
Task 7	86
Task 8	86
Task 9	86
Lab 11: OSPF Authentication	87
Task 1	87
Task 2	87
Task 3	87
Task 4	88
Task 5	88
Task 6	88
Task 7	88
Task 8	88
Task 9	88
Task 10	89
Task 11	89
Task 12	89
Lab 12: OSPF Best-Path Determination	90
Task 1	91
Task 2	91
Task 3	91
Lab 13: OSPF Challenge Lab	92
Ticket 1	92
Ticket 2	92
Ticket 3	93
Ticket 4	93
Ticket 5	93
Ticket 6	93
Ticket 7	93
Ticket 8	93

Chapter 6 BGP 95

Lab 1: Establishing a BGP Session Using the Correct TTL Value	95
BGP Peering Session Overview	95
Task 1	97
Task 2	97
Task 3	97

Task 4	97
Task 5	97
Task 6	97
Task 7	98
Task 8	98
Task 9	98
Lab 2: Establishing Neighbor Adjacency Using Different Methods	98
Task 1	99
Task 2	99
Task 3	99
Task 4	99
Task 5	100
Task 6	100
Task 7	101
Task 8	101
Lab 3: Route Reflectors	101
Task 1	102
Task 2	102
Task 3	102
Task 4	103
Task 5	103
Task 6	103
Lab 4: BGP Confederation	104
Task 1	105
Task 2	105
Task 3	105
Task 4	105
Lab 5: BGP Backdoor and Conditional Advertisement	106
Task 1	106
Task 2	106
Task 3	107
Task 4	107
Task 5	107
Task 6	107
Task 7	107
Task 8	108

Task 9	109
Task 10	109
Task 11	109
Lab 6: BGP Aggregation	109
Task 1	110
Task 2	110
Task 3	110
Task 4	110
Task 5	110
Task 6	110
Task 7	110
Lab 7: BGP Filtering	111
Task 1	112
Task 2	112
Task 3	112
Task 4	112
Task 5	112
Task 6	113
Task 7	113
Task 8	113
Task 9	113
Task 10	113
Task 11	113
Task 12	113
Task 13	113
Task 14	113
Task 15	113
Task 16	114
Task 17	114
Lab 8: BGP Load Balancing	114
Task 1	115
Task 2	115
Task 3	115
Task 4	115
Task 5	115

Lab 9: Remove-Private-AS: A Walkthrough	116
Lab 10: AS Migration	133
Task 1	133
Task 2	133
Task 3	134
Task 4	134
Task 5	134
Task 6	134
Lab 11: BGP Best-Path Algorithm: A Walkthrough	134
Introduction	135
Building Blocks of BGP	135
Path Vector	135
Controlling Routing to Paths	136
Path Attributes	137
Modifying Path Attributes	137
The Best-Path Algorithm	138
<i>Step 1: WEIGHT</i>	140
<i>Step 2: Local Preference</i>	147
5.1.5. LOCAL_PREF	147
<i>Step 3: Locally Originated</i>	164
<i>Step 4: AS_PATH</i>	167
AS_PATH Inbound	179
5.3. AS_PATH and Path Selection	190
<i>Step 5: Origin Code</i>	194
<i>Step 6: MED</i>	198
<i>Step 7: eBGP over iBGP</i>	220
Confederations	223
<i>Step 8: Lowest IGP Metric to the Next Hop</i>	226
<i>Step 9: Determine if Multiple Paths Exist</i>	233
<i>Step 10: Oldest Route</i>	246
<i>Step 11: Lowest Router ID</i>	252
<i>Step 12: Minimum Cluster List Length</i>	260
<i>Step 13: Lowest Neighbor Address</i>	263

Chapter 7 DMVPN 269

Introduction to DMVPN	269
DMVPN Mechanics	283
DMVPN Designs	294

Phase 1: Hub-and-Spoke	294
<i>Dynamic Spoke-to-Spoke Tunnels</i>	296
<i>The Need for Spoke-to-Spoke Tunnels</i>	296
<i>Enabling Multipoint GRE on Spokes</i>	298
<i>Forming Spoke-to-Spoke Tunnels</i>	306
<i>Triggering NHRP Resolutions</i>	309
Phase 2: Spoke-Initiated Spoke-to-Spoke Tunnels	310
<i>Phase 2 Spoke-to-Spoke Tunnel Caveats</i>	315
Phase 3: Hub-Initiated Spoke-to-Spoke Tunnels	322
<i>Shortcut or Override</i>	327
Conclusion	329
Lab 1: Single Hub, Single Cloud	330
Implement Phase 1	331
<i>Design Goal</i>	331
DMVPN Tunnel Configuration	331
<i>Implement OSPF</i>	335
<i>Summarization with OSPF</i>	344
<i>Implement EIGRP</i>	347
<i>Implement iBGP</i>	352
<i>Implement eBGP</i>	359
Implement Phase 2	367
<i>Design Goal</i>	337
DMVPN Tunnel Configuration	368
<i>Implement OSPF</i>	372
<i>Implement EIGRP</i>	375
<i>Implement iBGP</i>	379
<i>Implement eBGP</i>	382
Implement Phase 3	387
<i>Design Goal</i>	387
DMVPN Tunnel Configuration	388
<i>Implement OSPF</i>	389
<i>Implement EIGRP</i>	390
<i>Implement iBGP</i>	395
<i>Implement eBGP</i>	399
Lab 2: Single Hub, Dual Cloud	406
Implement Phase 1	407
<i>Design Goal</i>	407

<i>DMVPN Tunnel Configuration</i>	407
<i>Implement OSPF</i>	411
<i>Broadcast Network Type</i>	411
<i>Implement EIGRP</i>	424
<i>Implement iBGP</i>	428
<i>Implement eBGP</i>	436
Implement Phase 2	445
<i>Design Goal</i>	445
<i>DMVPN Tunnel Configuration</i>	446
<i>Implement OSPF</i>	450
<i>Implement EIGRP</i>	461
<i>Implement iBGP</i>	470
<i>Implement eBGP</i>	477
<i>Potential Solution to Above Problems</i>	488
Implement Phase 3	492
<i>Design Goal</i>	492
<i>DMVPN Tunnel Configuration</i>	492
<i>Implement EIGRP</i>	495
<i>Implement iBGP</i>	500
<i>Implement eBGP</i>	504
Lab 3: Dual Hub, Single Cloud	511
Implement Phase 3	513
<i>Design Goal</i>	513
<i>DMVPN Tunnel Configuration</i>	513
<i>Implement EIGRP</i>	518
<i>Implement iBGP</i>	524
<i>Implement eBGP</i>	529
Lab 4: Dual Hub, Dual Cloud	537
Implement Phase 3	539
<i>Design Goal</i>	539
<i>DMVPN Tunnel Configuration</i>	539
<i>Implement EIGRP</i>	541
<i>Implement iBGP</i>	546
<i>Implement eBGP</i>	552
Lab 5: DMVPN NHS Clustering	559
Task 1	560
Task 2	562

Task 3	566
Task 4	572
Lab 6: DMVPN and DHCP	573
Task 1	574
Task 2	578
Task 3	584

Chapter 8 MPLS and L3VPNs 585

Lab 1: Configuring Label Distribution Protocol	585
Task 1	586
Task 2	586
Task 3	586
Task 4	586
Task 5	586
Task 6	587
Task 7	587
Task 8	587
Task 9	587
Task 10	587
Task 11	588
Task 12	588
Task 13	588
Task 14	588
Task 15	588
Task 16	588
Lab 2: Static and RIPv2 Routing in a VPN	589
Task 1	589
Task 2	589
Task 3	590
Task 4	590
Task 5	590
Task 6	590
Task 7	590
Lab 3: EIGRP Routing in a VPN	591
Task 1	591
Task 2	592
Task 3	592

Task 4	592
Task 5	592
Task 6	592
Task 7	593
Lab 4: EIGRP Site-of-Origin	593
Task 1	593
Task 2	594
Task 3	594
Task 4	594
Task 5	594
Lab 5: OSPF Routing in a VPN	595
Task 1	595
Task 2	596
Task 3	596
Task 4	596
Task 5	596
Task 6	597
Lab 6: Backdoor Links and OSPF	597
Task 1	598
Task 2	598
Task 3	598
Task 4	598
Task 5	598
Task 6	598
Task 7	598
Task 8	599
Task 9	599
Lab 7: BGP Routing in a VPN	599
Task 1	600
Task 2	600
Task 3	600
Task 4	600
Task 5	600
Task 6	600
Lab 8: MPLS and NAT	601
Task 1	601
Task 2	601

Task 3	602
Task 4	602
Task 5	602
Task 6	602
Lab 9: Route Targets, Import Maps, and Export Maps	603
Task 1	603
Task 2	604
Task 3	604
Task 4	604
Task 5	604
Task 6	605
Task 7	605
Task 8	605
Task 9	605
Task 10	605
Task 11	605
Task 12	605
Lab 10: Internet Access Methods: Partial Internet Routes	606
Task 1	606
Task 2	607
Task 3	607
Task 4	607
Chapter 9 IPv6	609
Lab 1: Acquiring an IPv6 Address	609
Task 1	610
Task 2	610
Task 3	610
Task 4	610
Task 5	611
Task 6	611
Task 7	611
Task 8	611
Lab 2: DMVPN and IPv6	612
Task 1	612
Task 2	612
Task 3	612

Task 4	613
Task 5	613
Task 6	613
Lab 3: Configuring OSPFv3	614
Task 1	614
Task 2	614
Task 3	615
Lab 4: Summarization of Internal and External Networks	615
Task 1	615
Task 2	615
Task 3	616
Task 4	616
Task 5	616
Task 6	616
Task 7	616
Lab 5: OSPFv3 Broadcast Networks	617
Task 1	617
Task 2	617
Task 3	617
Task 4	618
Lab 6: OSPFv3 Non-Broadcast Networks	618
Task 1	619
Task 2	619
Lab 7: OSPFv3 Point-to-Point Networks	620
Task 1	620
Task 2	620
Lab 8: OSPFv3 Point-to-Multipoint Networks	621
Task 1	621
Task 2	622
Task 3	622
Lab 9: OSPFv3 Cost and Auto-Cost	622
Task 1	623
Task 2	623
Task 3	623
Lab 10: LSAs in OSPFv3	624
Task 1	624
Task 2	625

Task 3	625
Task 4	625
Task 5	625
Lab 11: OSPFv3 Area Types	626
Task 1	627
Task 2	627
Task 3	627
Task 4	627
Task 5	627
Task 6	627
Task 7	627
Task 8	628
Task 9	628
Task 10	628
Task 11	628
Task 12	628
Task 13	629
Task 14	629
Lab 12: OSPFv3 Authentication	629
Task 1	630
Task 2	630
Task 3	630
Task 4	630
Task 5	630
Task 6	631
Task 7	631
Lab 13: EIGRPv6	632
Task 1	632
Task 2	633
Task 3	633
Task 4	633
Task 5	633
Task 6	633
Task 7	633
Task 8	633
Task 9	633

Task 10 634

Task 11 634

Task 12 634

Task 13 634

Task 14 634

Lab 14: BGP Configuration 634

Task 1 634

Task 2 635

Task 3 635

Task 4 635

Chapter 10 SD-WAN 637

Lab 1: Onboarding WAN Edge Devices 638

Site 2: CSR 1000v Onboarding 655

Lab 2: Exploring Unicast Routing 664

Lab 3: Configuring Segmentation in All Sites Using VRF 100 and VRF 200 682

Branch-1 686

Branch-2 693

Lab 4: Configuring vEdge Using a Feature Template 703

Lab 5: Configuring vEdge Using a vManage Feature Template 729

Lab 6: Configuring cEdge Using a BR-2-Specific vManage Feature Template 753

Lab 7: Configuring vEdge Using a vManage Feature Template and ZTP 782
Creating a DHCP Server on ISP-1 805

Lab 8: Configuring an Application-Aware Routing Policy 816

Chapter 11 SD-Access 825

Lab 1: Configuring the SDA Policy Engine 826

Task 1: ISE Integration with DNA Center 826

Task 2: Finalize the Integration on DNA Center 831

Lab 2: SDA Design 835

Task 1: Design the Network Hierarchy 835

Task 2: Configure Common Network Settings 842

Task 3: Configure Device Credentials	845
Task 4: Create and Reserve IP Address Pools	847
Lab 3: Building the SDA Campus Fabric	855
Task 1: Discover Devices	855
Task 2: Provisioning the Devices	859
Lab 4: LAN Automation	869
Index	881

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

Enterprise networking has undergone many small changes over the years, building from simple shared bus LANs to intricate routing and switching architectures and wireless communications. Behind all of this is a need to ensure high reliability, agility, and speed. Through the decades, many different networking technologies, from physical connections to software protocols, have been created to assist enterprise networks in reaching those goals. For seasoned networking veterans, working with the various protocols and architectures is second nature. However, those who are just starting to build their careers and trying to study more advanced areas of network engineering may be overwhelmed by the multitude of routing protocols, Layer 2 features, and new buzzwords like “software-defined.”

This book is written as a foundation guide for the most common enterprise networking concepts that are required for a network engineer looking to move forward to more advanced aspects of networking. It combines aspects of theory instruction with practical application. Topics such as LAN switching, IP routing, and overlay networking technologies such as DMVPN are explained as foundational topics, including examples. Each chapter also functions as a lab manual with a task-oriented structure. Lab scenarios are presented as either configuration objectives, troubleshooting scenarios, or design scenarios. Each lab scenario includes full solutions and explanations. For beginner to intermediate readers, the solutions can be read while solving the tasks. Advanced readers can challenge their knowledge and skills by solving tasks first and then comparing their solutions to the ones provided in this book.

This book is not meant to be an exhaustive study of all the included technologies. It is meant to provide enough information on all topics to allow you to speak intelligently about each technology and even implement some of the configurations, if necessary, in your own environment. It takes topics from Cisco’s CCIE Enterprise Infrastructure certification blueprint but includes some legacy topics, where necessary, to facilitate understanding.

Who This Book Is For

Although the title of this book is *CCIE Enterprise Infrastructure Foundation*, the target audience is not limited to just those seeking expert-level certification. Any person looking to learn a little bit more about these foundational technologies will find this book very accessible.

This book breaks down complicated topics and provides examples to maximize understanding. It does, however, assume some basic networking knowledge. The following types of readers will get the most out of this book:

- Those who have completed CCNA certification and are part of the way through their preparation for CCNP Enterprise certification
- Those who have completed CCNP Enterprise certification and are pursuing CCIE Enterprise Infrastructure certification

- Those who are currently working in an environment that is implementing specific technologies covered in this book
- Those who are migrating from another vendor to a Cisco environment and need to understand Cisco configurations for common networking protocols

How This Book Is Organized

This book is divided into the 11 chapters described here. Every chapter can stand alone and can be used as a reference for the technologies it covers.

Chapter 1: Switching

Chapter 1 introduces Layer 2 concepts such as preventing loops with Spanning Tree Protocol, segmenting with VLANs, extending VLANs between switches through trunking, and bonding multiple Ethernet links together to increase bandwidth between network nodes. It covers topics such as Spanning Tree Protocol, RSTP, MSTP, VTP and VTP pruning, 802.1Q and ISL trunking, and LACP and PAgP.

Chapter 2: IP Prefix Lists

Chapter 2 introduces a common route filtering mechanism known as a prefix list. It explains why prefix lists were invented and why they are used over access lists for route filtering. This chapter shows how to write prefix lists and apply them in various routing protocols for filtering routes.

Chapter 3: RIPv2

Chapter 3 introduces Routing Information Protocol (RIP). RIP may not be included on the exam, but it is a perfect example of a simple distance vector routing protocol that follows all the standard distance vector designs. It focuses on the simplicity of RIP configuration, advanced RIP filtering scenarios, and RIP configuration challenges.

Chapter 4: EIGRP

Chapter 4 focuses on Cisco's improvement on its own version of Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP). It introduces EIGRP as a distance vector protocol that forms neighbor relationships and keeps a topology table like some other protocols. EIGRP is considered an advanced distance vector protocol that uses more than simple hop counts to learn loop-free paths through a network. This chapter covers EIGRP configuration topics such as EIGRP classic and address family configuration, EIGRP stub routing, and EIGRP with BFD.

Chapter 5: OSPF

Chapter 5 introduces the Open Shortest Path First (OSPF) routing protocol. It begins with an analysis of how OSPF builds its link-state database (LSDB) with various link-state advertisements (LSA) and uses that information to calculate loop-free routed paths through a network. This chapter also details multiarea OSPF design, filtering, and virtual links. It includes a detailed walkthrough on OSPF's best-path determination to help you understand OSPF's path selection process.

Chapter 6: BGP

Chapter 6 introduces Border Gateway Protocol (BGP), the protocol that routes the Internet. It explains BGP operation between autonomous systems (external BGP, or eBGP) and within a single autonomous system (internal BGP, or iBGP). Topics covered include BGP session establishment, route reflectors and confederations, aggregation, and filtering. This chapter includes a detailed walkthrough of the BGP best-path determination process.

Chapter 7: DMVPN

Chapter 7 focuses on Cisco's original SD-WAN technology, known as Dynamic Multipoint VPN (DMVPN). It explains DMVPN from the ground up, introducing concepts such as overlay and underlay networking, the link between DMVPN and NHRP, DMVPN routing using common routing protocols, and different DMVPN designs. It covers DMVPN Phase 1 through Phase 3 configurations, NHRP shortcut switching enhancements, hub-and-spoke networking designs, and (m)GRE tunnels.

Chapter 8: MPLS and L3VPNs

Chapter 8 introduces Multiprotocol Label Switching (MPLS) and the suite of services MPLS can provide. This chapter begins with an introduction to MPLS labels and Label Distribution Protocol (LDP). It also introduces the most common MPLS service, MPLS Layer 3 VPN (L3VPN). Topics covered include CE and PE routers, MPLS core configuration, LDP session establishment, BGP route targets and route distinguishers, and exchange of IGP routes between two sites connected by an MPLS L3VPN.

Chapter 9: IPv6

Chapter 9 introduces Internet Protocol Version 6 (IPv6), which is the successor to IPv4 due to its massive address space. It also details IPv6 address types, assignment, and configuration. Topics covered include IPv6 NDP, IPv6 SLAAC, DMVPN for IPv6, OSPF for IPv6 (OSPFv3), EIGRP for IPv6, and BGP for IPv6.

Chapter 10: SD-WAN

Chapter 10 introduces Cisco's new SD-WAN platform, which is based on its acquisition of Viptela. This chapter details basic SD-WAN components, such as vSmart, vManage, and vBond, as well as the setup and configuration required to join vEdge routers to an SD-WAN solution. Topics covered include onboarding WAN edge devices, unicast routing, segmentation, vManage device templates, ZTP, and application-aware policies.

Chapter 11: SD-Access

Chapter 11 introduces Cisco's SD-Access solution for creating scalable, automated, and resilient enterprise fabric. This chapter covers configuration of the SD-Access policy engine as well as SDA design and implementation. Topics covered include Cisco ISE, pxGrid, XMPP, SDA hierarchy global IP pools, DNAC, and LAN automation.

Before Starting the First Chapter

Bookmark the Companion Website

The companion website contains the config files, topology diagrams, CLI output, and explanations for the labs in this book. These elements are essential and a fundamental part of your learning experience. To use this book effectively, you need to have them. Use the config files, reference the topology diagrams, and work through the labs while checking your work against the CLI output on the companion website. At the end of each lab, read through the explanations for further insight.

To access the book's companion website, simply follow these steps:

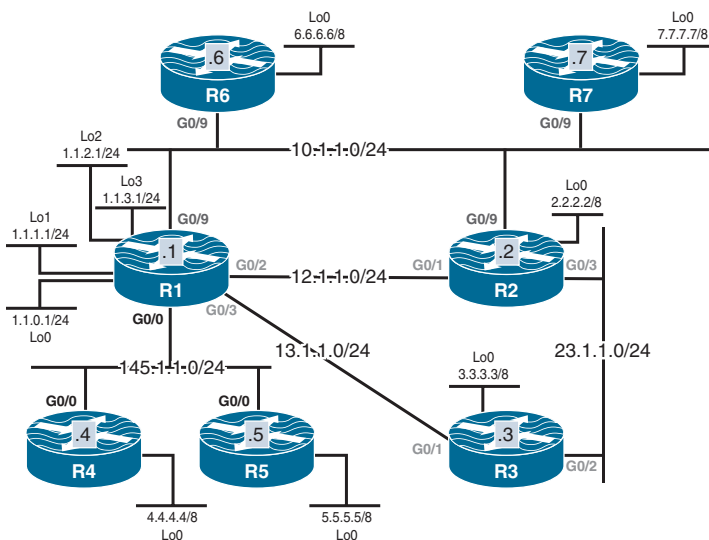
1. Go to www.ciscopress.com/register.
2. Enter the print book **ISBN: 9780137374243**.
3. Answer the security question to validate you purchase.
4. Go to your account page.
5. Click on the **Registered Product** tab.
6. Under the book listings, click on **Access Bonus Content** link.

If you have any issues accessing the companion website, you can contact our support team by going to <http://pearsonitp.echelp.org>.

This page intentionally left blank

EIGRP

Lab 1: EIGRP Named Mode



[This lab should be conducted on the Enterprise POD.](#)

Lab Setup:

[If you are using EVE-NG, and you have imported the EVE-NG topology from the EVE-NG-Topology folder, ignore the following tasks and use Lab 1-EIGRP Named Mode in the EIGRP folder in EVE-NG.](#)

[To copy and paste the initial configurations, go to the Initial-config folder → EIGRP folder → Lab-1.](#)

Task 1

Configure EIGRP on R1, R2, and R3 based on the following policy:

Router	Interface	AS Number
R1	G0/9	200
	G0/0	100
	G0/2	100
	G0/3	100
	Loopback0–Loopback3	100
R2	G0/9	200
	G0/1	100
	G0/3	100
	Loopback0	100
R3	G0/1	100
	G0/2	100
	Loopback0	100

- R1 should be configured to use unicast to establish an EIGRP neighbor adjacency with R2.
- R1 should use multicast to establish an EIGRP neighbor adjacency with R3.
- R1, R2, and R3 should use an EIGRP named mode configuration to accomplish this task.

Task 2

Configure R4 and R5 in EIGRP AS 100. You must use named mode to accomplish this task.

Task 3

Configure R1, R4, and R5 to use unicast to establish their EIGRP neighbor adjacency.

Task 4

Configure R6 in EIGRP AS 200. This router should run EIGRP AS 200 on its G0/9 and Loopback0 interfaces. You should use an EIGRP named mode configuration to accomplish this task.

Task 5

Configure OSPF Area 0 on R6's G0/9 and R7's G0/9 and Loopback0 interfaces. The router ID of these routers should be configured as 0.0.0.x, where x is the router number.

Task 6

Configure R6 to redistribute OSPF into EIGRP such that R1 and R2 go directly to R7 to reach the 7.0.0.0/8 network.

Task 7

Configure the hello interval of all routers in AS 200 to be twice the default hello interval.

Task 8

Configure R4 such that in the worst-case scenario, it uses 10% of the bandwidth for its EIGRP updates. This policy should apply to the existing and future interfaces.

Task 9

Configure R1 to summarize its loopback interfaces and advertise a single summary in the EIGRP AS 100 routing domain.

Task 10

Configure R1 to limit the number of received prefixes from R5 to 10. R1 should be configured to receive a warning message once 50% of this threshold is reached and a warning message for every additional route that exceeds the threshold. You should configure Lo1–Lo10 on R5 by copying and pasting the initial configuration, called **EIGRP-Lab-1-Task10**.

Task 11

Configure R1 to limit the number of prefixes received from R4 to five. R1 should be configured to tear down the adjacency if R4 exceeds the specified threshold. Copy and paste the **EIGRP-Lab-1-Task11** initial configuration on R4.

Task 12

Erase the startup configuration and reload the routers before proceeding to the next lab.

Lab 2: EIGRP and Bidirectional Forwarding Detection (BFD)



Task 1

Configure the routers based on the previous diagram. *Do not* configure any routing protocol.

Task 2

Configure EIGRP AS 100 on all directly connected interfaces of these two routers and ensure reachability. R5 should be configured using EIGRP classical mode, and R6 should use the EIGRP named mode configuration style.

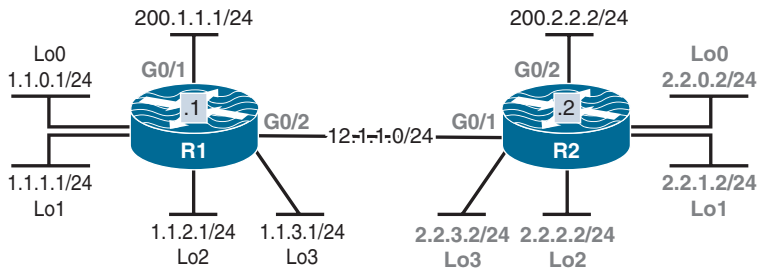
Task 3

Configure and test BFD on these two routers.

Task 4

Erase the startup configuration of these two routers and reload the devices before proceeding to the next lab.

Lab 3: EIGRP Stub



Lab Setup:

If you are using EVE-NG, and you have imported the EVE-NG topology from the EVE-NG-Topology folder, ignore the following tasks and use Lab 3-EIGRP Stub in the EIGRP folder in EVE-NG.

To copy and paste the initial configurations, go to the Initial-config folder → EIGRP folder → Lab-3.

Task 1

Configure EIGRP AS 100 on the G0/2 and G0/1 interfaces of R1 and R2, respectively, as well as on all loopback interfaces of these two routers. On R1 configure EIGRP using the classic mode, and on R2 configure EIGRP in named mode to accomplish this task. **Do not** run EIGRP on the G0/1 interface of R1 or the G0/2 interface of R2.

Task 2

Configure R1 and R2 to summarize their loopback interfaces in EIGRP.

Task 3

Configure the following static routes on R1 and R2 and redistribute them into EIGRP:

- On R1: 11.0.0.0/8 via G0/1
- On R2: 22.0.0.0/8 via G0/2

Task 4

Advertise the G0/1 interface of R1 and the G0/2 interface of R2 into RIPv2 and disable auto-summarization. You should redistribute RIPv2 into EIGRP and use any metric for the redistributed routes.

Task 5

Configure EIGRP stub routing on R1 by using the command **eigrp stub connected**. Test this option and verify the routes in the routing tables of both routers.

Task 6

Remove the **eigrp stub connected** option configured in the previous task and reconfigure EIGRP stub routing on R1 by using the **eigrp stub summary** command. Test this option and verify the routes in the routing tables of both routers.

Task 7

Remove the **eigrp stub summary** option configured in the previous task and reconfigure EIGRP stub routing on R1 by using the command **eigrp stub static**. Test this option and verify the routes in the routing tables of both routers.

Task 8

Remove the **eigrp stub static** option configured in the previous task and reconfigure EIGRP stub routing on R1 by using the command **eigrp stub redistributed**. Test this option and verify the routes in the routing tables of both routers.

Task 9

Remove the **eigrp stub redistributed** option configured in the previous task and reconfigure EIGRP stub routing on R1 by using the command **eigrp stub receive-only**. Test this option and verify the routes in the routing tables of both routers.

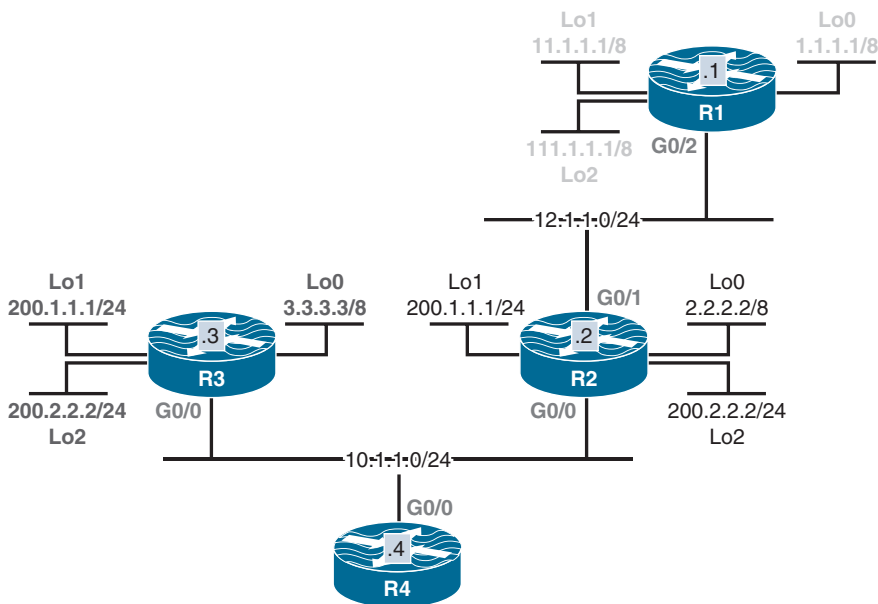
Task 10

Remove the `eigrp stub receive-only` option configured in the previous task and reconfigure EIGRP stub routing on R1 by using the command `eigrp stub`. Test this option and verify the routes in the routing tables of both routers.

Task 11

Erase the startup configuration and reload the routers before proceeding to the next lab.

Lab 4: EIGRP Filtering



Lab Setup:

If you are using EVE-NG, and you have imported the EVE-NG topology from the EVE-NG-Topology folder, ignore the following tasks and use Lab 4-EIGRP Filtering in the EIGRP folder in EVE-NG.

To copy and paste the initial configurations, go to the Initial-config folder → EIGRP folder → Lab-4.

Task 1

Configure EIGRP 100 on all routers and advertise their directly connected links into EIGRP.

Task 2

Configure R4 such that it filters existing (1.0.0.0/8, 11.0.0.0/8, and 111.0.0.0/8) and future networks behind R1. Do not use **distribute-list**, **access-list**, **prefix-list**, or **route-map** to accomplish this task.

Task 3

Configure R4 such that it uses R2 as its only connection to network 200.1.1.0 /24. You should use an access list to accomplish this task.

Task 4

Configure R4 such that it takes R3 to reach network 200.2.2.0 /24. R4 should only use R2 as the next hop to reach network 200.2.2.0/24 when R3 is down. You should use a standard access list to accomplish this task.

Task 5

Filter network 2.0.0.0/8 on R4. Do not use **distribute-list** or **route-map** to accomplish this task.

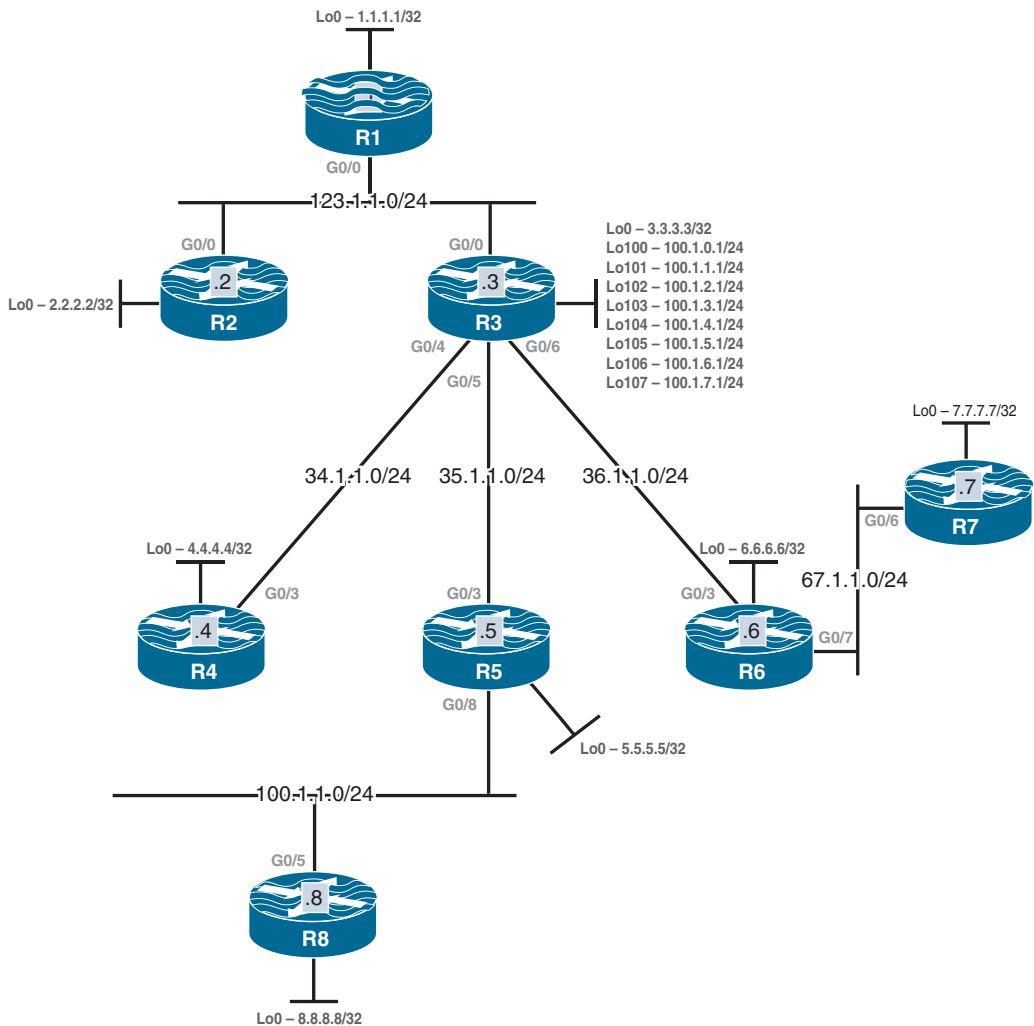
Task 6

Configure R4 to filter network 3.0.0.0/8.

Task 7

Erase the startup configuration and reload the routers before proceeding to the next task.

Lab 5: Advanced EIGRP Lab



Lab Setup:

If you are using EVE-NG, and you have imported the EVE-NG topology from the EVE-NG-Topology folder, ignore the following tasks and use Lab 5-Advanced EIGRP Lab in the EIGRP folder in EVE-NG.

To copy and paste the initial configurations, go to the Initial-config folder → EIGRP folder → Lab-5.

Task 1

Configure the G0/0 interfaces of R1, R2, and R3 in EIGRP AS 100. These routers should be configured to advertise their Lo0 interfaces in this AS, using the following policy:

- These routers should be configured to reach each other's loopback interface/s by going through R1.
- *Do not* use Policy-based Routing (PBR) or configure another AS to accomplish this task.

Task 2

Configure R3's G0/4, G0/5, and G0/6 in AS 300. Configure R4's, R5's, and R6's G0/3 and loopback 0 interfaces in this AS.

Configure R3 to summarize its Lo100–Lo107.

The summary route should be advertised to R4, R5, and R6 based on the following policy:

- R4 should receive the summary *only*.
- R5 should receive the summary plus network 100.1.3.0 /24.
- R6 should receive the summary plus all the specific routes.
- Configure the minimum number of **ip summary-address** commands possible to accomplish this task.

Task 3

Configure EIGRP 300 on R4's Lo134 and Lo135 and advertise a single summary in AS 300.

Task 4

Configure the G0/7 and Lo0 interfaces of R6 and the G0/6 and loopback 0 interfaces on R7 for EIGRP in AS 67.

R7 should be configured to advertise its Lo130, such that the command **show ip route eigrp 67** on R6 produces the following output:

```
D EX 130.3.0.0/16 [170/130816] via 67.1.1.7, 00:00:16,
GigabitEthernet0/7
```

R7 should use **redistribute static** to accomplish this task. *Do not* configure a static route to accomplish this task.

Task 5

Configure the routers in AS 67 such that they log neighbor warning messages and repeat the warning messages every 10 minutes. You should disable logging of neighbor changes for this AS.

Task 6

Configure the routers in AS 67 such that a dead neighbor is detected within 3 seconds.

Task 7

Routers in AS 100 should be configured to use **Bandwidth** and *not* **Bandwidth + DLY** when calculating their composite metric.

Task 8

Configure R2 such that EIGRP *never* uses more than 25% of its G0/0 link's bandwidth.

Task 9

Configure the G0/8 interface of R5 and the G0/5 and the Lo0 interfaces of R8 in AS 500.

Task 10

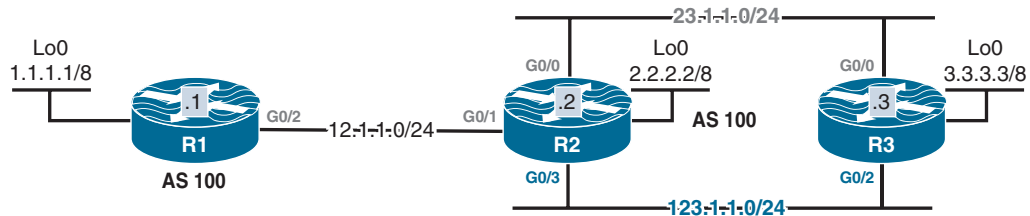
Configure R5 to inject a default route in AS 500 based on the following policy:

- R5 should be configured to inject a default route plus networks 4.0.0/8 and 6.0.0/8 from AS 300.

Task 11

Erase the startup configuration and reload the routers before proceeding to the next task.

Lab 6: EIGRP Authentication



Lab Setup:

If you are using EVE-NG, and you have imported the EVE-NG topology from the EVE-NG-Topology folder, ignore the following tasks and use Lab 6-EIGRP Authentication in the EIGRP folder in EVE-NG.

To copy and paste the initial configurations, go to the Initial-config folder → EIGRP folder → Lab-6.

Task 1

Configure EIGRP based on the previous diagram. If this configuration is successful, these routers should be able to see and have reachability to all routes. You should use named mode configuration style when configuring R2 and R3 and classic EIGRP configuration style when configuring R1 to accomplish this task.

Task 2

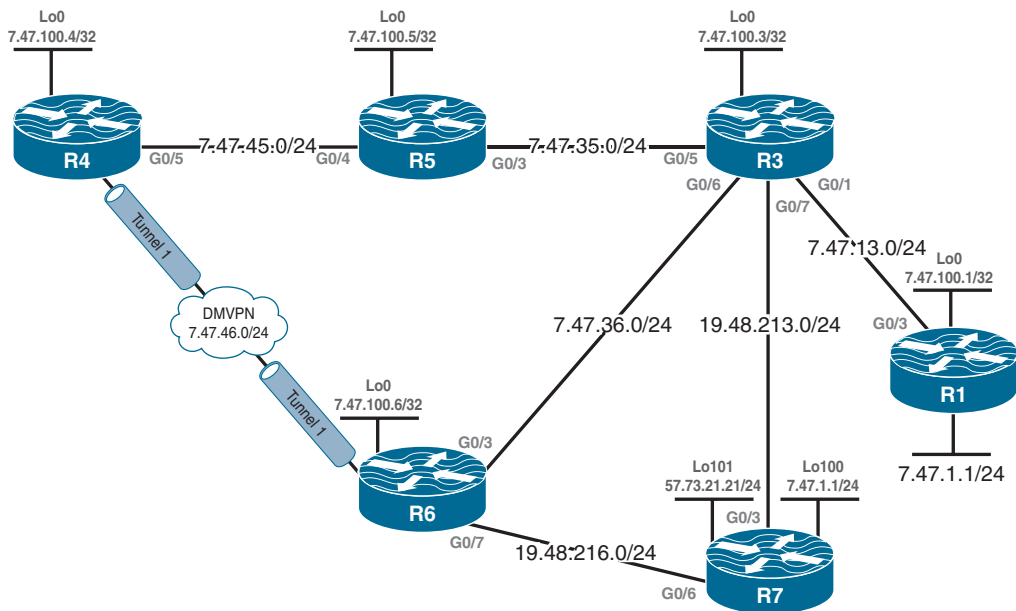
Configure R2 to authenticate all existing and future directly connected interfaces using the strongest authentication method available. Use the minimum number of commands and CCIE as the password to accomplish this task.

- R2 should authenticate R1 using MD5 and Cisco as the password.
- In the future, R3 may have other neighbors that won't need authentication.

Task 3

Erase the startup configuration and reload the routers before proceeding to the next lab.

Lab 7: EIGRP Challenge Lab



Lab Setup:

If you are using EVE-NG, and you have imported the EVE-NG topology from the EVE-NG-Topology folder, ignore the following tasks and use Lab 7-EIGRP Challenge Lab in the EIGRP folder in EVE-NG.

To copy and paste the initial configurations, go to the Initial-config folder → EIGRP folder → Lab-7.

NOTE Do not access R7 at all. You should only fix the problem identified in the ticket.

Ticket 1

R1 can't reach R3's Lo0. You must configure R1 to fix the problem.

Ticket 2

R6 does not have a stable EIGRP adjacency with R4. Do not use an EIGRP command to fix this ticket.

Ticket 3

When R3's G0/1, G0/7, and G0/6 are down, R3 can't reach R4's Lo0. Do not remove any commands to fix this ticket.

Ticket 4

R1's Lo0 should always have reachability to R4's Lo0 and G0/5 interfaces, but it does not. You should fix this problem without configuring R1 or R4. You should not remove any commands to resolve this ticket.

Ticket 5

R3 is configured to use multiple paths to R4's Lo0. However, it's using only one of the paths.

Ticket 6

R6 can't reach R7's Lo101.

Ticket 7

R3 should establish a EIGRP adjacency with R8 over its G0/8 interface. You should make configuration changes on R3 only.

Ticket 8

Erase the startup configuration and reload the devices before proceeding to the next lab.

Index

Numerics

802.1D, 16–19

- blocking ports, 18
- bridges, 16
- broadcast frames, 17
- broadcast storm, 17
- CAM (Content Addressable Memory) table, 17
- root bridge, 17
- root port, 18
- single collision domain, 16
- switches, 17
- unknown unicast flooding, 17

802.1w. *See* RSTP (Rapid Spanning Tree Protocol)

A

AAR policy, creating, 816–824

active open attempt, 96

adjacency table, CEF (Cisco Express Forwarding), 310–312, 316–320

application-aware routing policy, 816–824

area range command, 345

area types, OSPF, 72–76, 626–629

ARP (Address Resolution Protocol), 275

ASN (autonomous system number), 118

AS_PATH attribute, 122–123, 167–173

in confederations, 181–188–190

inbound, 179–181

outbound, 173–179

path selection and, 190–194

authentication

EIGRP, 62

OSPF, 87–89, 629–631

auto-cost, 622–623

automation, LAN, 869–879

B

backdoor links, OSPF and, 597–599

backup port, 22

- best-path algorithm, 134–135, 138–140**
- AS_PATH attribute, 167–173
 - in confederations, 181–188–190*
 - inbound, 179–181*
 - outbound, 173–179*
 - path selection and, 190–194*
- confederation and, 223–225
- determine if multiple paths exist, 233–236
 - external and internal paths, 240–244*
 - external paths, 236–240*
 - internal paths, 244–246*
- eBGP over iBGP, 220–223
- LOCAL_PREF attribute, 147–164
- locally originated path, 164–167
- lowest neighbor address, 263–268
- lowest router ID, 252–260
- minimum cluster list length, 260–263
- oldest route, 246–252
- WEIGHT attribute, 140–147
- best-path determination, 90–91**
- BFD (Bidirectional Forwarding Detection), 54**
- BGP (Border Gateway Protocol), 120–122. *See also* iBGP; spoke-to-spoke tunnels**
- AS_PATH attribute, 122–123
- aggregation, 109–110
- ASN (autonomous system number), 118
- backdoor and conditional advertisement, 106–109
- best-path algorithm, 134–135, 138–140
- AS_PATH attribute, 167–173–179–181–188, 188–190
 - confederation and, 223–225*
 - determine if multiple paths exist, 233–246*
 - eBGP over iBGP, 220–223*
 - LOCAL_PREF attribute, 147–164*
 - locally originated path, 164–167*
 - lowest neighbor address, 263–268*
 - lowest router ID, 252–260*
 - MED attribute, 198–220*
 - minimum cluster list length, 260–263*
 - oldest route, 246–252*
 - ORIGIN attribute, 194–197*
 - path selection, 190–194*
 - WEIGHT attribute, 140–147*
- building blocks of, 135
- confederation, 104–105, 148
- configuring, 634–635
- controlling routing to paths, 136–137
- dynamic neighbor feature, 353
- dynamic peering, 379
- establishing a neighbor adjacency, 98–101
- establishing a session using the correct TTL value, 95–98
- filtering, 111–114
- internal routers, 148
- limited transit capability, 147
- load balancing, 114–115
- loop prevention, 363–365
- AS migration, 122–134
- path attributes, 136–138

- path vector, 135–136
- remove-private-as all command, 126–131, 132
- remove-private-as command, 119–120, 122, 123–125
- route reflectors, 101–103
- routing in a VPN, 599–600
- suboptimal routing, 158
- third-party next hop, 361
- transit AS, 136
- bgp always-compare-med command, 214–216**
- bgp bestpath as-path ignore command, 191–194, 250–252**
- bgp bestpath compare-routerid command, 258–260**
- bgp bestpath med missing-as-worst command, 209–211**
- bgp deterministic-med command, 217–218**
- bgp listen range command, 353–354**
- bgp redistribute-internal command, 527, 548**
- blocking ports, 18
- BPDU, 20–21, 23–24
- bridges, 16
- broadcast frames, 17
- broadcast network type, 67–69, 336–340, 411–418, 617–618
- broadcast storm, 17

C

- CAM (Content Addressable Memory) table, 17**
- CEF (Cisco Express Forwarding), adjacency table, 310–312, 316–320**

- clear ip bgp command, 122, 153**
- clear ip nhrp command, 503–504, 528**
- Cluster Length attribute, 260–263**
- commands**
 - area range, 345
 - bgp always-compare-med, 214–216
 - bgp bestpath as-path ignore, 191–194, 250–252
 - bgp bestpath compare-routerid, 258–260
 - bgp bestpath med missing-as-worst, 209–211
 - bgp deterministic-med, 217–218
 - bgp listen range, 353–354
 - bgp redistribute-internal, 527, 548
 - clear ip bgp, 122, 153
 - clear ip nhrp, 503–504, 528
 - debug ip bgp update, 159
 - debug ip nhrp packet, 300
 - debug nhrp detail, 287–288
 - debug nhrp packet, 287–288
 - default-originate, 500
 - distance, 465
 - interface, 673
 - interface tunnel 100, 331
 - ip dhcp support tunnel unicast, 581, 583
 - ip helper-address, 581
 - ip nhrp map multicast dynamic, 280, 291, 332, 333–334
 - ip nhrp network id 1, 276–277
 - ip nhrp network-id 100, 332
 - ip nhrp nhs, 286
 - ip nhrp nhs 100.1.1.1 nbma 15.1.1.1 multicast, 368
 - ip nhrp nhs fallback, 570

- ip nhrp nhs nbma multicast, 304–305
- ip nhrp shortcut, 388
- ip ospf hello-interval, 342, 418
- ip ospf network broadcast, 336–337, 372–373
- ip ospf network point-to-multipoint, 341–342
- ip ospf network point-to-point, 342
- ip ospf priority 0, 372–373
- ip split-horizon eigrp 100, 350–351
- ip summary-address eigrp, 392–393, 425, 495
- ip summary-address eigrp 1, 296
- listen range, 470–471
- maximum-paths, 234–235
- neighbor, 96
- neighbor default-originate, 356
- neighbor spokes next-hop-self, 404
- neighbor spokes remote-as, 359–360
- neighbor x.x.x.x weight, C02.119
- network, 347, 382, 384, 470–471
- network eigrp, 583
- no ip next-hop-self eigrp 100, 375
- no ip split-horizon eigrp, 282–283, 375, 461–462, 565
- no route bgp 100, 437–438
- passive-interface, 337–338, 390–391
- ping, 277, 285–286, 299, 306–307, 417, 422–423, 427–428, 435, 444–445, 456, 467, 476, 487–488, 497, 509, 569, 570–571, 675–676, 680–681, 728–729, 752–753, 809–810
- remove-private-as, 119–120, 122
- remove-private-as all, 126–131, 132
- remove-private-as command, 123–125
- set origin code, 196–197
- show adjacency, 312
- show dmvpn, 288, 290–291, 300, 301–302, 305, 369–370, 371–372, 515–516, 562
- show interface e0/1 pruning, 10–11
- show interfaces trunk, 8, 10
- show ip bgp, 120, 123, 125, 131–132, 133, 141, 145–146, 149, 160, 355, 357–359, 360, 365, 380–381, 383–384, 396–397, 401–402, 431–432, 438–439, 440–441, 444, 471–472, 479–480, 483–484, 486, 502–503, 526, 531, 554, 556
- show ip bgp neighbors, 155–156
- show ip bgp summary, 355, 363, 482
- show ip cef, 340
- show ip cef internal, 311, 321–322
- show ip dhcp pool TST, 581
- show ip eigrp 100 neighbor, 348, 391–392
- show ip eigrp neighbors, 292–293, 303–304, 305–306, 376–377, 463–465
- show ip nhrp, 277, 288, 307, 389, 561, 576–577
- show ip nhrp multicast, 280, 291–292, 302–303, 370
- show ip ospf, 345
- show ip ospf database network, 457–459
- show ip ospf database router, 459
- show ip ospf interface brief, 414–415
- show ip ospf neighbor, 343, 413, 452
- show ip ospf neighbor command, 373–374

- show ip ospf neighbor detail, 337
 - show ip protocols, 238
 - show ip route, 272, 277–278, 352, 460–461, 469
 - show ip route bgp, 356, 381
 - show ip route eigrp, 293, 295, 310, 315, 318, 320, 496–497, 554, 564–565–566–567, 568–570, 571, 698–700
 - show ip route eigrp 100, 377, 468, 490, 534, 543, 548–549, 582–583
 - show ip route next-hop-override, 329
 - show ip route nhrp, 325, 394, 398
 - show ip route nhrp nhs redundancy, 572
 - show ip route ospf, 339, 343–344, 374, 413–414, 416, 420–421, 423, 452–453, 454, 677–678, 688–690, 692–693, 701–703
 - show ip route vpn 100, 674–675
 - show ip route vrf 100, 669–671, 673–674, 676–677
 - show ip routes omp, 681–682
 - show omp routes, 664–667, 683–686, 690–692
 - show run interface tunnel1, 295
 - show running-config system, 808
 - show sdwan control local properties, 649–650
 - show sdwan omp peers, 650
 - show sdwan omp routes, 668–669
 - show sdwan running-config, 643–644, 678–679
 - switchport trunk pruning vlan, 10, 11
 - traceroute, 152, 273, 316, 318–319, 320–321, 323–324, 334–335, 351, 371, 374–375, 377–379, 382, 386–387, 393, 397–398, 416–417, 455, 457, 466, 467–468, 475, 481–482, 483, 487, 490, 499, 503, 507–509–510, 529, 534–535, 544–545, 550–552, 557, 558
 - tunnel destination, 274, 298, 300
 - tunnel mode gre multipoint, 298, 331
 - confederation, 104–105, 148, 223–225**
 - AS_PATH attribute and, 181–183, 188–190
 - advertising paths within, 183–188
 - convergence, 22–23, 435–436**
 - cost, 622–623**
- ## D
-
- debug ip bgp update command, 159**
 - debug ip nhrp packet command, 300**
 - debug nhrp detail command, 287–288**
 - debug nhrp packet command, 287–288**
 - default route injection, 85–86**
 - default-originate command, 500**
 - DHCP (Dynamic Host Configuration Protocol)**
 - creating a server, 805–816
 - DMVPN and, 572–573
 - relay agent, 580
 - distance command, 465**
 - distance vector protocols, 135**
 - DMVPN (Dynamic Multipoint VPN), 269, 283. *See also* dual hub, single cloud design; single hub, dual cloud design; single hub, single cloud design**
 - adding a spoke, 290–291
 - DHCP and, 572–573

- hub redundancy, 329
- hub routers, 285
- IPv6 and, 612–613
- NHRP
 - NHS clustering*, 567–572
 - registration*, 285–289
- Phase 1, 294–309
 - debug ip nhrp packet command*, 300
 - enabling multipoint GRE on spokes*, 298–306
 - forming spoke-to-spoke tunnels*, 306–309
 - implement eBGP*, 359–367
 - implement iBGP*, 352–359
 - implement OSPF*, 335–346
 - implementing EIGRP*, 347–351
 - ip nhrp nbs nbma multicast command*, 304–305
 - NHRP resolution*, 306–309
 - OSPF summarization*, 344–346
 - show dmvpn command*, 300, 301–302, 305
 - show ip eigrp neighbors command*, 303–304, 305–306
 - show ip nhrp command*, 307
 - show ip nhrp multicast command*, 302–303
 - show ip route eigrp command*, 294–295
 - show run interface tunnel1 command*, 295–296
 - spoke-to-spoke tunnels*, 296–298
 - triggering NHRP resolutions*, 309
 - tunnel configuration*, 331–335
 - tunnel destination command*, 300
- Phase 2, 309–322, 367
 - CEF adjacency table*, 310–312, 316–320
 - implement eBGP*, 382–387
 - implement EIGRP*, 375–379
 - implement iBGP*, 379–382
 - implement OSPF*, 372–375
 - NHRP resolution*, 313–315
 - show adjacency command*, 312
 - show ip cef internal command*, 311, 321–322
 - show ip route eigrp command*, 310, 315, 318, 320
 - spoke-to-spoke tunnel caveats*, 315–322
 - tunnel configuration*, 368–372
- Phase 3, 277–329
 - implement eBGP*, 399–405
 - implement EIGRP*, 390–394
 - implement iBGP*, 395–398
 - implement OSPF*, 389–390
 - NHRP resolution*, 381–390
 - overriding next hop information*, 325–329
 - show ip route eigrp command*, 328
 - show ip route next-hop-override command*, 329
 - show ip route nhrp command*, 325
 - tunnel configuration*, 388
 - verifying tunnel configuration*, 388–389

dual hub, dual cloud design, 537–538

DMVPN Phase 3

*implement eBGP, 552–558**implement EIGRP, 541–545**implement iBGP, 546–552**tunnel configuration, 539–541***dual hub, single cloud design,
511–513**

DMVPN Phase 3

*implement eBGP, 529–536**implement EIGRP, 518–523**implement iBGP, 524–529**tunnel configuration, 513–518*

E**eBGP, 220–223**DMVPN Phase 1 configuration,
359–367*spokes in different autonomous
systems, 359–361, 436–441**spokes in the same autonomous
system, 362–367*DMVPN Phase 2 configuration,
382–387*spokes in different autonomous
systems, 477–485**spokes in the same autonomous
system, 485–488*

DMVPN Phase 3 configuration

spokes in different autonomous
systems, 402–405, 507–510,
532–536, 555–558*spokes in the same autonomous
system, 399–402, 504–507,
530–531, 552–554***edge ports, 23****EIGRP, 279, 285, 291, 632–634**

advanced lab, 59–61

authentication, 62

BFD (Bidirectional Forwarding
Detection) and, 54

challenge lab, 63–64

DMVPN Phase 1 configuration,
347–351, 424–428DMVPN Phase 2 configuration,
375–379, 461–470DMVPN Phase 3 configuration,
390–394, 495–500, 518–523,
541–545

filtering, 57–58

named mode, 51–54

routing in a VPN, 591–593

site-of-origin, 593–594

stub, C05.127–57

EtherChannel, configuring, 13–14**export maps, 603–605****external networks, summarization,
615–616**

F**feature template, 703–729–753–782****filtering**

BGP, 111–114

EIGRP, 57–58

OSPF, 77–80

full-mesh topology, 297

G-H-I**GRE (Generic Routing Encapsulation)
tunnels, 270–272–273**

virtual links and, 83–85

hub-and-spoke topology, 283–285.
 See also spoke-to-spoke tunnels
 iBGP, 220–223
 DMVPN Phase 1 configuration,
 352–359, 428–436
 DMVPN Phase 2 configuration,
 379–382, 470–477
 DMVPN Phase 3 configuration,
 395–398, 500–504, 524–529,
 546–552
 import maps, 603–605
 inter-area routes, 345
 interface command, 673
 interface tunnel 100 command, 331
 internal networks, summarization,
 615–616
 internal routers, 148
 Internet access, partial internet
 routes, 606–607
 ip dhcp support tunnel unicast
 command, 581, 583
 ip helper-address command, 581
 ip nhrp map multicast dynamic
 command, 280, 291, 332
 ip nhrp network id 1 command,
 276–277
 ip nhrp network-id 100 command,
 332, 333–334
 ip nhrp nhs 100.1.1.1 nbma 15.1.1.1
 multicast command, 368
 ip nhrp nhs command, 286
 ip nhrp nhs fallback command, 570
 ip nhrp nhs nbma multicast command,
 304–305, 567–568
 ip nhrp shortcut command, 388
 ip ospf hello-interval command, 342,
 418

ip ospf network broadcast command,
 336–337, 372–373
 ip ospf network point-to-multipoint
 command, 341–342
 ip ospf network point-to-point
 command, 342
 ip ospf priority 0 command,
 372–373
 ip split-horizon eigrp 100 command,
 350–351
 ip summary-address eigrp 1
 command, 296
 ip summary-address eigrp command,
 392–393, 425, 495
 IPv6
 acquiring an address, 609–611
 DMVPN and, 612–613

J-K-L

labs

Acquiring an IPv6 address, 609–611
 Advanced EIGRP lab, 59–61
 AS migration, 122–134
 Backdoor links and OSPF, 597–599
 BGP aggregation, 109–110
 BGP backdoor and conditional
 advertisement, 106–109
 BGP best-path algorithm, 134–135,
 138–140, 223–225
 AS_PATH attribute, 167–
 173–179–181–188, 188–190
 building blocks of BGP, 135
 controlling routing to paths,
 136–137
 determine if multiple paths
 exist, 233–246

- eBGP over iBGP*, 220–223
- LOCAL_PREF attribute*, 147–164
- locally originated path*, 164–167
- lowest IGP metric to the next hop*, 226–232
- lowest neighbor address*, 263–268
- lowest router ID*, 252–260
- MED attribute*, 198–220
- minimum cluster list length*, 260–263
- oldest route*, 246–252
- ORIGIN attribute*, 194–197
- path attributes*, 136–138
- path selection*, 190–194
- path vector*, 135–136
- WEIGHT attribute*, 140–147
- BGP confederation, 104–105
- BGP configuration, 634–635
- BGP filtering, 111–114
- BGP load balancing, 114–115
- BGP routing in a VPN, 599–600
- Building the SDA campus fabric, 855–868
- Configuring an application-aware routing policy, 816–824
- Configuring cEdge using a BR-2-specific vManage feature template, 753–782
- Configuring EtherChannels, 13–14
- Configuring Label Distribution Protocol, 585–588
- Configuring OSPFv3, 614–615
- Configuring segmentation in all sites using VRF 100 and VRF 200, 682–686
 - Branch-1*, 686–693
 - Branch-2*, 693–703
- Configuring the SDA policy engine, 826–834
- Configuring trunks, 1–2
 - show interfaces trunk command*, 8
 - VTP pruning*, 5–7, 8–12
- Configuring vEdge using a feature template, 703–729
- Configuring vEdge using a vManage feature template, 729–753
- Configuring vEdge using a vManage feature template and ZTP, 782–805–816
- Default route injection, 85–86
- DMVPN and DHCP, 572–573
- DMVPN and IPv6, 612–613
- DMVPN NHS clustering, 559–572
- Dual hub, single cloud design, 511–536
- EIGRP and Bidirectional Forwarding Detection (BFD), 54
- EIGRP authentication, 62
- EIGRP challenge lab, 63–64
- EIGRP filtering, 57–58
- EIGRP named mode, 51–54
- EIGRP routing in a VPN, 591–593
- EIGRP site-of-origin, 593–594
- EIGRP stub, C05.127–57
- EIGRPv6, 632–634
- Establishing a BGP session using the correct TTL value, 95–98

- Establishing neighbor adjacency using different methods, 98–101
- Exploring unicast routing, 664–682
- Helper map, 46–47
- Internet access methods: Partial internet routes, 606–607
- Introducing Spanning Tree Protocol, 14–16. *See also* Spanning Tree Protocol
 - 802.1D*, 16–19
 - RSTP (Rapid Spanning Tree Protocol)*, 20–28
- LAN automation, 869–879
- LSAs in OSPFv3, 624–625
- MPLS and NAT, 601–602
- Multiple Spanning Tree Protocol, 28–48
- Onboarding WAN edge devices
 - CSR 1000v onboarding*, 655–662
 - CSR1/CSR2 onboarding*, 638–655
 - vEdge cloud router onboarding*, 655–662
- OSPF area types, 72–76
- OSPF authentication, 87–89
- OSPF best-path determination, 90–91
- OSPF broadcast networks, 67–69
- OSPF challenge lab, 92–93
- OSPF filtering, 77–80
- OSPF non-broadcast networks, 69–70
- OSPF point-to-multipoint and point-to-multipoint non-broadcast networks, 71–72
- OSPF point-to-point networks, 70–71
- OSPF routing in a VPN, 595–597
- OSPF summarization, 80–82
- OSPFv3 area types, 626–629
- OSPFv3 authentication, 629–631
- OSPFv3 broadcast networks, 617–618
- OSPFv3 cost and auto-cost, 622–623
- OSPFv3 non-broadcast networks, 618–619
- OSPFv3 point-to-multipoint networks, 621–622
- OSPFv3 point-to-point networks, 620
- Prefix lists, 35–37
- Remove-private-AS: A walkthrough, 116–132
- RIPv2, 39–46
- RIPv2 challenge lab, 48–49
- Route reflectors, 101–103
- Route targets, import maps, and export maps, 603–605
- Running OSPF on the interfaces, 65–67
- SDA design, 835–854
- Single hub, dual cloud design
 - DMVPN Phase 1*, 407–445
 - DMVPN Phase 2*, 445–492
 - DMVPN Phase 3*, 492–510
- Single hub, single cloud design
 - DMVPN Phase 1*, 331–367
 - DMVPN Phase 2*, 367–387
 - DMVPN Phase 3*, 387–405
- Static and RIPv2 routing in a VPN, 589–590

Summarization of internal and external networks, 615–616
 Virtual links and GRE tunnels, 83–85
LAN automation, 869–879
LDP (Label Distribution Protocol), 585–588
limited transit capability, 147
link-state protocols, 135
listen range command, 470–471
load balancing, BGP, 114–115
LOCAL_PREF attribute, 147–164
loop prevention, BGP, 363–365
loopback interfaces, 40–41
LSAs (link-state advertisement), 344, 624–625

M

manual pruning, 8
maximum-paths command, 234–235
MED attribute, 198–199, 201–207, 209–211, 214–216, 218–220
 deterministic evaluation, 217–218
 evaluation, 207–208
 missing values, 208–209
 modifying the evaluation, 211–214
 setting, 199–201
mGRE (multipoint Generic Routing Encapsulation) tunnels, 274–283, 285
MPLS (Multiprotocol Label Switching), NAT and, 601–602
MST (Multiple Spanning Tree Protocol), 28–30
 instances, 31
 regions, 32
multicast IP addresses, 279
multicasting, 47
multipoint GRE, enabling on spokes, 298–306

N

NAT, MPLS and, 601–602
NBMA (non-broadcast multiple-access) networks, 275–276
neighbor command, 96
neighbor default-originate command, 356
neighbor spokes next-hop-self command, 404
neighbor spokes remote-as command, 359–360
neighbor x.x.x.x weight command, C02.119
network command, 347, 382, 384, 470–471
network eigrp command, 583
NHC (next hop client), 275
NHRP (Next Hop Resolution Protocol), 275–279
 domain, 276
 multicast mapping table, 291
 NHC (next hop client), 275
 NHS (next hop server), 275
 NHS clustering, 567–572
 pseudo-multicasting, 279
 registration, 285–289
 registration message, 275
 resolution, 306–309, 313–315, 381–390
 shortcut switching enhancements, 323

NHS (next hop server), 275
no ip next-hop-self eigrp 100
 command, 375
no ip split-horizon eigrp, 375
no ip split-horizon eigrp command,
 282–283, 461–462, 565
no route bgp 100 command,
 437–438
non-broadcast networks, 69–70,
 618–619

O

onboarding WAN edge devices
 CSR 1000v onboarding, 655–662
 CSR1/CSR2 onboarding, 638–655
 vEdge cloud router onboarding,
 662–664
ORIGIN attribute, 194–197
OSPF (Open Shortest Path First), 47,
 335
 area types, 72–76, 626–629
 authentication, 87–89, 629–631
 auto-cost, 622–623
 backdoor links and, 597–599
 best-path determination, 90–91
 broadcast network type, 67–69,
 336–340, 411–418, 617–618
 challenge lab, 92–93
 configuring, 614–615
 cost, 622–623
 DMVPN Phase 1 configuration,
 411–423
 DMVPN Phase 2 configuration,
 372–375, 450–461
 DMVPN Phase 3 configuration,
 389–390

filtering, 77–80
 inter-area routes, 345
 LSAs (link-state advertisement), 344,
 624–625
 non-broadcast networks, 69–70,
 618–619
 point-to-multipoint network type,
 71–72, 341–344, 621–622
 point-to-point network type, 70–71,
 341–344, 418–423, 620
 routing in a VPN, 595–597
 running on interfaces, 65–67
 summarization, 80–82, 344–346

outer header, 270

overlay network, 270

P

partial internet routes, 606–607
partial-mesh topology, 297–298
passive-interface command, 337–338,
 390–391
path attributes, BGP, 136–138
ping command, 277, 285–286, 299,
 306–307, 417, 422–423, 427–428,
 435, 444–445, 456, 467, 476,
 487–488, 497, 509, 569, 570–571,
 675–676, 680–681, 728–729,
 752–753, 809–810
point-to-multipoint network type,
 71–72, 341–344, 621–622
point-to-point network type, 70–71,
 341–344, 418–423, 620
policy, AAR, 816–824
prefix lists, 35–37, 144
private IP addressing, 270

protocol analyzers, 270
 pruning ineligible, 9, 11
 pseudo-multicasting, 279
 public IP addressing, 270

Q-R

redundancy, hub and transport,
 329–330
 registration, NHRP (Next Hop
 Resolution Protocol), 285–289
 remove-private-as all command,
 126–131, 132
 remove-private-as command,
 119–120, 122, 123–125
 RFC 6793, 118
 RIPv2, 47, 272
 challenge lab, 48–49
 configuring, 39–46
 VPN (virtual private network) and,
 589–590
 root bridge, 17
 root port, 18
 route maps, prefix lists and, 144
 route reflectors, 101–103
 route targets, 603–605
 routing protocols, 135
 RSTP (Rapid Spanning Tree Protocol),
 20–28
 backup port, 22
 BPDUs, 20–21, 23–24
 convergence, 22–23
 edge ports, 23
 link type, 23
 port roles, 21
 states, 21

S

SD-Access
 building the campus fabric, 855–868
 configuring the policy engine,
 826–834
 designing, 835–854
 LAN automation, 869–879
 SD-WAN
 application-aware routing policy,
 816–824
 configuring vEdge
 using a feature template,
 703–729
 using a vManage template,
 729–753–782
 using a vManage template and
 ZTP, 782–816
 onboarding WAN edge devices
 CSR 1000v onboarding,
 655–662
 CSR1/CSR2 onboarding,
 638–655
 vEdge cloud router onboarding,
 655–662
 segmentation, 682–686–693–703
 unicast routing, 664–682
 segmentation, 682–686
 set origin code command, 196–197
 show adjacency command, 312
 show dmvpn command, 288,
 290–291, 300, 301–302, 305,
 369–370, 371–372, 515–516, 562
 show interface e0/1 pruning
 command, 10–11
 show interfaces trunk command, 8,
 10
 show ip bgp command, 120, 123,
 125, 131–132, 133, 141, 145–146,

- 149, 160, 355, 357–359, 360, 365, 380–381, 383–384, 396–397, 401–402, 431–432, 438–439, 440–441, 445, 471–472, 479–480, 483–484, 486, 502–503, 526, 531, 554, 556
- show ip bgp neighbors command, 155–156
- show ip bgp summary command, 355, 363, 482
- show ip bp command, 444
- show ip cef command, 340
- show ip cef internal command, 311, 321–322
- show ip dhcp pool TST command, 581
- show ip eigrp 100 neighbor command, 348, 391–392, 463–465
- show ip eigrp neighbors command, 292–293, 303–304, 305–306, 376–377
- show ip nhrp command, 277, 288, 307, 389, 561, 576–577
- show ip nhrp multicast command, 280, 291–292, 302–303, 370
- show ip ospf command, 345
- show ip ospf database network command, 457–459
- show ip ospf database router command, 459
- show ip ospf int brief command, 672–673
- show ip ospf interface brief command, 414–415, 453–454
- show ip ospf neighbor command, 343, 373–374, 413, 452
- show ip ospf neighbor detail command, 337
- show ip protocols command, 238
- show ip route bgp command, 356, 381
- show ip route command, 272, 277–278, 352, 460–461, 469
- show ip route eigrp 100 command, 377, 468, 490, 534, 543, 548–549, 582–583
- show ip route eigrp command, 293, 295, 310, 315, 318, 320, 496–497, 554, 564–565–566–567, 568–569–570, 571, 698–700
- show ip route next-hop-override command, 329
- show ip route nhrp command, 325, 394, 398
- show ip route nhrp nhs redundancy command, 572
- show ip route ospf command, 339, 343–344, 346, 374, 413–414, 416, 420–421, 423, 452–453, 454, 677–678, 688–690, 692–693, 701–703
- show ip route vpn 100 command, 674–675
- show ip route vrf 100 command, 668, 669–671, 673–674, 676–677
- show ip routes omp command, 681–682
- show omp routes command, 664–667, 683–686, 690–692
- show run interface tunnel1 command, 295
- show running-config system command, 808
- show sdwan control local properties command, 649–650
- show sdwan omp peers command, 650
- show sdwan omp routes command, 668–669

- show sdwan running-config
 - command, 643–644, 678–679
- single collision domain, 16
- single hub, dual cloud design, 404, 445
 - convergence, 435–436
 - DMVPN Phase 1
 - implement eBGP, 436–445
 - implement EIGRP, 424–428
 - implement iBGP, 428–436
 - implement OSPF, 411–423
 - tunnel configuration, 407–410
 - DMVPN Phase 2
 - implement eBGP, 477–488
 - implement EIGRP, 461–470
 - implement iBGP, 470–477
 - implement OSPF, 450–461
 - tunnel configuration, 446–449
 - DMVPN Phase 3
 - implement eBGP, 504–510
 - implement EIGRP, 495–500
 - implement iBGP, 500–504
 - tunnel configuration, 492–494
 - implement eBGP, spokes in the same autonomous system, 441–445
 - potential solutions to problems, 488–492
- single hub, single cloud design
 - DMVPN Phase 1
 - implement eBGP, 359–367
 - implement EIGRP, 347–351
 - implement iBGP, 352–359
 - implement OSPF, 335–344
 - summarization with OSPF, 344–346
 - tunnel configuration, 331–335
 - DMVPN Phase 2
 - implement eBGP, 382–387
 - implement EIGRP, 375–379
 - implement iBGP, 379–382
 - implement OSPF, 372–375
 - tunnel configuration, 368–372
 - DMVPN Phase 3
 - implement eBGP, 399–405
 - implement EIGRP, 390–394
 - implement iBGP, 395–398
 - implement OSPF, 389–390
 - tunnel configuration, 388–389
- Spanning Tree Protocol. *See also* MST (Multiple Spanning Tree Protocol)
 - 802.1D, 16–19
 - blocking ports, 18
 - bridges, 16
 - broadcast frames, 17
 - broadcast storm, 17
 - CAM (Content Addressable Memory) table, 17
 - convergence, 27
 - root bridge, 17
 - root port, 18
 - single collision domain, 16
 - switches, 17
 - unknown unicast flooding, 17
 - MST, 28–30
 - instances, 31
 - regions, 32
 - RSTP (Rapid Spanning Tree Protocol), 20–28
 - backup port, 22
 - BPDU, 20–21, 23–24
 - convergence, 22–23
 - edge ports, 23

link type, 23

port roles, 21

states, 21

split horizon, 282, 349

spokes

adding to DMVPN cloud, 290–291

enabling multipoint GRE on,
298–306

spoke-to-spoke tunnels, 296–298

caveats, 315–322

forming, 306–309

hub-initiated, 322–329

static routing, VPN (virtual private network) and, 589–590

summarization

of internal and external networks,
615–616

OSPF, 80–82, 344–346

switches, 16, 17, 23

**switchport trunk pruning vlan
command**, 10, 11

T

TCP

active open attempt, 96

sessions, 95

three-way handshake, 353

third-party next hop, 361

three-way handshake, 353

topologies

full-mesh, 297

partial-mesh, 297–298

traceroute command, 152, 273, 316,
318–319, 320–321, 323–324,
334–335, 340, 371, 374–375,
377–379, 382, 386–387, 393,
397–398, 416–417, 455, 457, 466,

467–468, 475, 481–482, 483,
487, 490, 499, 503, 507–509–510,
517–518, 529, 534–535, 544–545,
550–551–552, 557, 558

transparent bridge, 16

transport redundancy, 329–330

trunks

configuring, 1–20

VTP pruning, 5–7

pruning ineligible, 9, 11

*show interface e0/1 pruning
command*, 10–11

*show interfaces trunk
command*, 8, 10

*switchport trunk pruning vlan
command*, 10, 11

*VMA (VTP membership
advertisement)*, 8

tunnel destination command, 274,
298, 300

tunnel mode gre multipoint command,
298, 331

tunnels, 270

DMVPN Phase 1 configuration,
331–335

DMVPN Phase 2 configuration,
368–372, 446–449

DMVPN Phase 3 configuration,
388–389, 492–494, 513–518,
539–541

GRE (Generic Routing
Encapsulation), 270–272–273

mGRE (multipoint Generic Routing
Encapsulation), 274–283

overlay network, 270

spoke-to-spoke, 296–298, 306–309

underlay network, 270

U

underlay network, 270
unicast routing, 664–682
unknown unicast flooding, 17

V

verifying, DMVPN Phase 3 tunnel configuration, 388–389
virtual links, GRE tunnels and, 83–85
virtual network, 270
VMA (VTP membership advertisement), 8
vManage template, 729–753–782
VPN (virtual private network)
 BGP routing in a, 599–600

EIGRP routing in a, 591–593

OSPF routing in a, 595–597

static and RIPv2 routing in a,
 589–590

VTP pruning, 5–7

 pruning ineligible, 9, 11

 show interfaces trunk command, 8,
 10

 switchport trunk pruning vlan
 command, 10, 11

 VMA (VTP membership
 advertisement), 8

W-X-Y-Z

WEIGHT attribute, 140–147

ZTP server configuration, 809–816