

CCIE Routing and Switching v5.1 Foundations

Bridging the Gap Between
CCNP and CCIE

Narbik Kocharians, CCIE No. 12410 (R&S, Security, SP)

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

CCIE Routing and Switching v5.1 Foundations

Narbik Kocharians

Copyright © 2017 Pearson Education, Inc

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

First Printing May 2017

Library of Congress Control Number: 2017935919

ISBN-13: 978-1-58714-472-1

ISBN-10: 1-58714-472-7

Warning and Disclaimer

This book is designed to provide information about the skills necessary to bridge the skills gap between the CCNP Routing and Switching Exams and the CCIE Routing and Switching Exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Trademark Acknowledgments

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

Special Sales

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

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

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

Feedback Information

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

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

We greatly appreciate your assistance.

Editor-in-Chief: Mark Taub

Product Line Manager: Brett Bartow

Business Operation Manager,
Cisco Press: Ronald Fligge

Managing Editor: Sandra Schroeder

Development Editor: Eleanor Bru

Project Editor: Mandie Frank

Copy Editor: Bart Reed

Technical Editors: Terry Vinson, Jeff Denton

Editorial Assistant: Vanessa Evans

Cover Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Erika Millen

Proofreader: Larry Sulky



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1110R)

About the Author

Narbik Kocharians, CCIE No. 12410 (Routing and Switching, Service Provider, and Security) is a triple CCIE with more than 40 years of experience in this industry. He has designed, implemented, and supported numerous 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-RS, CCIE-Security, and CCDE classes.

About the Technical Reviewers

Terry Vinson, CCIE No. 35347 (Routing and Switching, Data Center), is a seasoned instructor with nearly 25 years of experience teaching and writing technical courses and training materials. Terry has taught and developed training content as well as provided technical consulting for high-end firms in the Northern Virginia/Washington, D.C. area. His technical expertise lies in the Cisco arena, with a focus on all routing and switching technologies as well as the latest data center technologies, including Nexus switching, unified computing, and storage-area networking (SAN) technologies. Terry currently teaches CCIE R&S and Data Center Bootcamps for Micronics Training, Inc., and enjoys sailing and game design in his “free time.”

Jeffrey A. Denton is a network engineer leading the protection of secure enterprise network systems. Offering more than 12 years of experience designing, deploying, and supporting comprehensive networks for classified, defense-related systems integral to national security, he is an expert at leading complex projects and managing all phases of network installation, administration, and monitoring. Jeff is currently the network team lead for General Dynamics in Kabul, Afghanistan.

Dedication

I like to dedicate this book to my wife Janet, my children (Christopher, Patrick, Alexandra, and Daniel), and my students, colleagues, and friends.

Acknowledgments

I am thankful to God for giving me the opportunity to teach and write labs, which I truly love. I'd like to thank Janet, my wife of 31 years, for her encouragement and hard work in dealing with the day-to-day management of our training and consulting company. I'd like to thank both Terry Vinson and Jeff Denton for tech-editing this book in such a meticulous manner—thank you for an excellent job. Finally, I'd like to thank Brett Bartow and Eleanor Bru for their patience and constant changing of the deadline.

Contents at a Glance

	Introduction	xxvii
Chapter 1	Physical Topology	1
Chapter 2	Physical and Logical Topologies	7
Chapter 3	Spanning Tree Protocol	35
Chapter 4	Point-to-Point Protocol	169
Chapter 5	DMVPN	219
Chapter 6	IP Prefix-List	267
Chapter 7	EIGRP	287
Chapter 8	OSPF	381
Chapter 9	Redistribution	567
Chapter 10	Border Gateway Protocol	635
Chapter 11	IPv6	737
Chapter 12	Quality of Service	839
Chapter 13	IPSec VPN	911
Chapter 14	Multicast	959
Chapter 15	MPLS and L3VPNs	1025
	Index	1155
Online element: Appendix A Configuration Files		

Contents

	Introduction	xxvii
Chapter 1	Physical Topology	1
	Physical Layout of Switching Devices	1
	Serial Interconnections Between Routers	3
	Lab Options	5
	Summary	5
Chapter 2	Physical and Logical Topologies	7
	Topology Types	7
	Lab 2-1: Introductory Lab	8
	Lab 2-2: Physical-to-Logical Topology	18
	Task 1	20
	Task 2	20
	Task 3	20
	Summary	33
Chapter 3	Spanning Tree Protocol	35
	Lab 3-1: Basic Spanning Tree Protocol (802.1D)	35
	Task 1	36
	Task 2	41
	Task 3	43
	Task 4	46
	Task 5	48
	Lab 3-2: Advanced Spanning Tree Protocol (802.1D)	50
	Task 1	51
	Task 2	52
	Task 3	53
	Task 4	54
	Task 5	55
	Task 6	56
	Task 7	59
	Task 8	65
	Task 9	67
	Task 10	70

Lab 3-3: Rapid Spanning Tree Protocol (802.1w)	73
802.1w Port States	74
802.1w Port Roles	74
Operational Enhancements of 802.1w	74
802.1w Rapid Convergence Mechanisms	75
Lab Setup	75
Task 1	76
Task 2	78
Task 3	80
Task 4	83
Task 5	85
Task 6	89
Lab 3-4: Multiple Spanning Tree Protocol (802.1s)	93
MST Regions	94
MST Region Components	94
MST Spanning Tree Instances	95
<i>Internal Spanning Tree (IST)</i>	95
<i>IST Master</i>	95
<i>Hop Count</i>	95
Multiple-Instance Spanning Tree Protocol (MSTP)	96
Task 1	96
Task 2	96
Task 3	97
Task 4	97
Task 5	99
Lab 3-5: Spanning Tree PortFast	106
Task 1	106
Task 2	108
Task 3	110
Task 4	112
Task 5	114
Lab 3-6: UplinkFast	115
Task 1	115
Task 2	118
Lab 3-7: BPDU Guard	128
Task 1	129
Task 2	129

Task 3	132
Task 4	133
Lab 3-8: BPDU Filter	135
Task 1	136
Task 2	139
Task 3	142
Task 4	146
Lab 3-9: Spanning Tree Backbone Fast	148
Task 1	148
Task 2	151
Lab 3-10: Spanning Tree Root Guard	154
Task 1	155
Task 2	155
Lab 3-11: Spanning Tree Loop Guard	162
Task 1	163
Task 2	164
Chapter 4	Point-to-Point Protocol 169
Introduction to PPP	169
PPP Frame Format	170
PPP Control Plane	171
<i>Link Control Protocol and Basic PPP Session Establishment</i>	171
<i>Authentication Phase and Authentication Mechanisms</i>	175
<i>Network Control Protocols and Network Layer Protocol Phase</i>	177
Advanced PPP Features	179
<i>Compression</i>	179
<i>Multilink PPP</i>	180
<i>PPP over Ethernet</i>	180
Lab 4-1: PPP	182
Task 1	182
Task 2	185
Task 3	186
Task 4	187
Task 5	191
Task 6	195
Task 7	199
Task 8	200
Task 9	203

Task 10	209
Task 11	211
Task 12	214
Task 13	216
Summary	218

Chapter 5 DMVPN 219

Lab 5-1: DMVPN Phase 1 Using Static Mapping	219
Task 1	220
Task 2	223
Lab 5-2: DMVPN Phase 1 Using Dynamic Mapping	229
Task 1	229
Task 2	232
Lab 5-3: DMVPN Phase 2 Using Static Mapping	236
Task 1	237
Task 2	240
Lab 5-4: DMVPN Phase 2 Using Dynamic Mapping	244
Task 1	245
Task 2	247
Lab 5-5: DMVPN Phase 3	251
Task 1	253
Task 2	255

Chapter 6 IP Prefix-List 267

Lab 6-1: Configuring Prefix Lists	267
Task 1	267
Task 2	269
Task 3	272
Task 4	275
Task 5	277
Task 6	278
Task 7	281
Task 8	282
Task 9	283
Task 10	285
Task 11	286

Chapter 7 EIGRP 287

Lab 7-1: EIGRP 287

Task 1 287

Task 2 289

Task 3 293

Task 4 298

Task 5 301

Task 6 304

Lab 7-2: EIGRP Named Mode 311

Task 1 311

Task 2 316

Task 3 317

Task 4 318

Task 5 319

Task 6 320

Task 7 323

Task 8 324

Task 9 325

Task 10 327

Task 11 329

Task 12 331

Lab 7-3: EIGRP Metrics (Classic and Wide) 333

Task 1 334

Task 2 335

Task 3 337

Task 4 338

Task 5 339

Task 6 341

Task 7 342

Lab 7-4: EIGRP Summarization 349

Task 1 349

Task 2 350

Task 3 351

Task 4 351

Task 5 353

Task 6 355

Task 7	356
Task 8	357
Task 9	358
Lab 7-5: EIGRP Authentication	359
Task 1	359
Task 2	360
Task 3	361
Task 4	362
Lab 7-6: Default Route Injection	363
Task 1	363
Task 2	364
<i>Option #1</i>	<i>364</i>
<i>Option #2</i>	<i>365</i>
<i>Option #3</i>	<i>366</i>
<i>Option #4</i>	<i>367</i>
Lab 7-7: EIGRP Stub	368
Task 1	368
Task 2	370
Task 3	370
Task 4	372
Task 5	373
Task 6	375
Task 7	375
Task 8	376
Task 9	377
Task 10	378
Chapter 8	OSPF 381
Lab 8-1: Advertising Networks	381
Task 1	381
Task 2	385
Task 3	387
Task 4	388
Task 5	389
Task 6	391
Lab 8-2: OSPF Broadcast Networks	397
Task 1	397
Task 2	400

Lab 8-3: Non-Broadcast Networks	411
Task 1	411
Lab 8-4: OSPF Point-to-Point Networks	421
Task 1	421
Lab 8-5: OSPF Point-to-Multipoint and Point-to-Multipoint Non-Broadcast Networks	425
Task 1	425
Task 2	429
Lab 8-6: OSPF Authentication	431
Task 1	431
Task 2	433
Task 3	438
Task 4	440
Task 5	443
Task 6	444
Task 7	448
Task 8	450
Task 9	451
Task 10	455
Lab 8-7: OSPF Summarization	462
Task 1	463
Task 2	463
Task 3	464
Task 4	465
Task 5	467
Task 6	468
Task 7	470
Task 8	471
Task 9	472
Lab 8-8: OSPF Filtering	476
Task 1	476
Task 2	478
Task 3	480
Task 4	481
Task 5	482
Task 6	484
Task 7	486

Task 8	488
Task 9	490
Task 10	493
Task 11	494
Task 12	495
Task 13	496
Task 14	497
Task 15	501
Task 16	502
Lab 8-9: Virtual Links and GRE Tunnels	504
Task 1	506
Task 2	509
Task 3	513
Lab 8-10: OSPF Stub, Totally Stubby, and NSSA Areas	517
Task 1	518
Task 2	518
Task 3	519
Task 4	521
Task 5	523
Task 6	523
Task 7	526
Task 8	528
Task 9	532
Task 10	533
Task 11	534
Task 12	535
Lab 8-11: How Is This Possible?	536
Task 1	537
Lab 8-12: LSA Type 4 and Suppress FA	539
Task 1	539
Lab 8-13: Can OSPF Take a Suboptimal Path?	549
Task 1	549
Task 2	550
Lab 8-14: RFC 3101 and RFC 1587	556
Task 1	556
Task 2	560

Chapter 9 Redistribution 567

Lab 9-1: Basic Redistribution 1 567

Task 1 567

Task 2 569

Option #1 570*Option #2* 570

Task 3 571

Task 4 575

Task 5 578

Task 6 580

Task 7 583

Lab 9-2: Basic Redistribution 2 586

Task 1 587

Task 2 589

Task 3 591

Task 4 592

Task 5 593

Task 6 595

Task 7 595

Task 8 596

Task 9 597

Task 10 599

Task 11 602

Lab 9-3: Redistribute RIPv2 and EIGRP 604

Task 1 605

Task 2 606

Task 3 607

Task 4 607

Task 5 608

Solution #1 615*Solution #2* 617*Solution #3* 619*Solution #4* 622

Lab 9-4: Redistribute RIPv2 and OSPF 625

Task 1 626

Task 2 626

Task 3	628
Task 4	629
<i>Step #1:</i>	632
<i>Step #2:</i>	632
<i>Step #3:</i>	632
<i>Step #4:</i>	633

Chapter 10 Border Gateway Protocol 635

Lab 10-1: Establishing Neighbor Adjacencies	635
Task 1	635
Task 2	638
Lab 10-2: Router Reflectors	642
Task 1	643
Task 2	646
Lab 10-3: Conditional Advertisement and BGP Backdoor	650
Task 1	650
Task 2	651
Task 3	651
Task 4	653
Task 5	654
Task 6	658
Task 7	659
Task 8	662
Task 9	663
Lab 10-4: Community Attribute	667
Task 1	668
Task 2	672
Task 3	674
Task 4	675
Task 5	677
Lab 10-5: The AS-path Attribute	679
Task 1	680
Task 2	682
Task 3	685
Lab 10-6: The Weight Attribute	686
Task 1	687
Task 2	689

Task 3	691
Task 4	692
Lab 10-7: Multi-Exit Discriminator Attribute	695
Task 1	696
Task 2	699
Task 3	700
Task 4	701
Lab 10-8: Filtering Using Access Lists and Prefix Lists	704
Task 1	704
Task 2	708
Task 3	709
Task 4	711
Task 5	712
Task 6	713
Lab 10-9: Regular Expressions	714
Task 1	715
Task 2	717
Task 3	719
Task 4	719
Task 5	720
Task 6	721
Task 7	722
Task 8	723
Task 9	724
Task 10	725
Task 11	726
Task 12	727
Task 13	728
Task 14	728
Lab 10-10: BGP Confederation	731
Task 1	733
Chapter 11 IPv6	737
Lab 11-1: Acquiring an IPv6 Address	737
Modified EUI-64 Addressing	737
Using EUI-64 Addressing	738
Implement IPv6 Neighbor Discovery	739

Task 1 743

Task 2 746

Task 3 751

Task 4 754

Task 5 755

Lab 11-2: Configuring OSPFv3 763

Task 1 763

Lab 11-3: Summarization of Internal and External Networks 771

Task 1 771

Task 2 778

Task 3 782

Task 4 783

Task 5 786

Lab 11-4: LSAs in OSPFv3 790

Task 1 790

Task 2 800

Task 3 809

Task 4 813

Lab 11-5: EIGRPv6 817

Task 1 818

Task 2 819

Task 3 821

Task 4 824

Task 5 825

Task 6 826

Task 7 830

Task 8 830

Task 9 831

Task 10 833

Task 11 834

Task 12 835

Chapter 12 Quality of Service 839

Lab 12-1: MLS QOS 840

Task 1 840

Task 2 842

Task 3 844

Lab 12-2: Differential Service Code Point-Mutation	851
Task 1	851
Task 2	853
Step 1	853
Step 2	854
Step 3	855
Step 4	857
Lab 12-3: DSCP-COS Mapping	860
Task 1	861
Task 2	862
Task 3	862
Lab 12-4: COS-DSCP Mapping	865
Task 1	866
Task 2	866
Task 3	866
Lab 12-5: IP-Precedence-DSCP Mapping	870
Task 1	870
Lab 12-6: Match Input-Interface and Match NOT	873
Task 1	873
Task 2	877
Lab 12-7: Match Destination and Source Address MAC	881
Task 1	881
Task 2	882
Task 3	884
Lab 12-8: Match IP DSCP/Precedence vs. Match DSCP	885
Task 1	885
Task 2	890
Task 3	890
Lab 12-9: Match Protocol HTTP URL, MIME, and Host	893
Task 1	893
Task 2	894
Task 3	895
Task 4	896
Task 5	897
Lab 12-10: Class-Based Policing	898
Task 1	899
Task 2	903

Task 3 904

Task 4 906

Lab 12-11: Class-Based Shaping 907

Task 1 907

Chapter 13 IPsec VPN 911

Lab 13-1: Basic Site-to-Site IPsec VPN 911

Task 1 912

IKE Phase 1 (Main Mode) Message 1 917

IKE Phase 1 (Main Mode) Message 2 918

IKE Phase 1 (Main Mode) Message 3 919

IKE Phase 1 (Main Mode) Message 4 919

IKE Phase 1 (Main Mode) Message 5 920

IKE Phase 1 (Main Mode) Message 6 920

IKE Phase 2 (Quick Mode) Message 1 921

Task 2 925

Lab 13-2: Basic Site-to-Site IPsec VPN and NAT 925

Task 1 925

Task 2 926

Task 3 927

Lab 13-3: Configuring GRE/IPsec Tunnel Mode, Transport Mode, and S-VTI 930

Task 1 930

Task 2 937

Task 3 940

Task 4 942

Lab 13-4: Protecting DMVPN Tunnels 946

Task 1 946

Task 2 947

Task 3 949

Task 4 952

Chapter 14 Multicast 959

Lab 14-1: IGMP 959

Task 1 959

Task 2 963

Task 3 964

Task 4 965

Task 5	965
Task 6	967
Task 7	969
Task 8	971
Task 9	974
Task 10	976
Lab 14-2: Static RP	977
Task 1	977
Task 2	981
Task 3	983
Task 4	986
Task 5	991
Lab 14-3: Dynamic Rendezvous Point Learning and Auto-RP	993
Task 1	994
Task 2	994
Task 3	997
Task 4	1004
Task 5	1005
Task 6	1006
Task 7	1008
Task 8	1010
Lab 14-4: Bootstrap Router (BSR)	1013
Task 1	1013
Task 2	1014
Task 3	1017
Task 4	1022
Chapter 15 MPLS and L3VPNs	1025
Lab 15-1: Label Distribution Protocol	1026
Task 1	1026
Task 2	1029
Task 3	1033
Task 4	1042
Task 5	1044
Task 6	1044
Task 7	1048
Task 8	1051

Task 9	1055
Task 10	1058
Task 11	1064
Task 12	1065
Task 13	1067
Task 14	1068
Task 15	1072
Task 16	1073
Lab 15-2: RIPv2 Routing in a VPN	1078
Task 1	1079
Task 2	1081
Task 3	1084
Task 4	1088
Task 5	1091
Task 6	1096
Lab 15-3: EIGRP Routing in a VPN	1107
Task 6	1108
Lab 15-4: OSPF Routing in a VPN	1113
Task 6	1113
Lab 15-5: Backdoor Links and OSPF	1123
Task 1	1123
Task 2	1126
Task 3	1128
Task 4	1132
Task 5	1134
Task 6	1136
Task 7	1141
Lab 15-6: BGP Routing in a VPN	1148
Task 6	1148
Index	1155

Online element: Appendix A Configuration Files

Reader Services

Register your copy at www.ciscopress.com/title/9781587144721 for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account*. Enter the product ISBN 9781587144721 and click Submit. Once the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Icons Used in This Book



Router



Switch



Cloud



File/
Application Server

Command Syntax Conventions

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

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

Introduction

This book is designed to bridge the knowledge gap for those who are functional and well prepared in CCNP-level technologies. One of the biggest issues in preparing for the CCIE Routing and Switching exam is the significant gap between being a functional, well-trained network professional and the level of knowledge and experience needed to be a well-prepared CCIE candidate. This book is intended to provide significant hands-on exercises in all the critical domains of knowledge needed to prepare for the extensive demands of the CCIE examination. Industry leaders were consulted for technical accuracy throughout this book.

Who Should Read This Book?

This book is designed for those Routing and Switching Engineers and technologists who want to prepare for the CCIE Routing and Switching exam, or those looking for the equivalent knowledge. The reader is expected to have a network professional-level certification or the equivalent field experience.

How to Access the Lab Configuration Files

This book comes complete with the lab configuration files, which we have made available to you online. To access these files, simply register this book (ISBN: 9781587144721) at www.ciscopress.com/register. You will be asked to answer a security question based on the content of the book to verify your purchase. Once you have registered your book, you can access the lab files by going to your account page, clicking on the Registered Products tab, and then clicking the Access Bonus Content link under your registered book.

How This Book Is Organized

Chapter 1, “Physical Topology”: In this chapter, we explore the topology that will be used in subsequent chapters. The hope is to provide a clear and detailed explanation of the physical interconnection between devices that will be used to explore the technologies and features contained in this book.

Chapter 2, “Physical and Logical Topologies”: After decades of working with CCIE Candidates I have learned that there are some fundamental levels of knowledge that most students are missing. Among them is the ability to differentiate between physical and logical topologies. A well-prepared candidate should have an absolute mastery of the syntax and processes needed to discover the physical topology for any network deployment. Chapter 2 of this book focuses on that specific skill set.

Chapter 3, “Spanning Tree Protocol”: We explore all things Layer 2 in this chapter. In the Routing and Switching exam, the key focus seems to be on the Layer 3 components of routing; however, without a seamless Layer 2 infrastructure, routing

protocols will not work. In fact, not even the most basic of IP communications can take place. We will focus on this very critical network element that prevents the formation of bridging loops.

Chapter 4, “Point-to-Point Protocol”: PPP in all its various flavors has been a long-time “go-to” technology to support wide area networking (WAN) infrastructures. However, in recent years, with the advent of Ethernet-based WAN deployments, we have found ourselves needing the traditional serial-based functionality in the context of Ethernet interconnectivity. This makes understanding how to deploy Point-to-Point Protocol over Ethernet a very important skill. This chapter explores its deployment, optimization, and capabilities.

Chapter 5, “DMVPN”: Dynamic Multipoint Virtual Private Networks are the replacement for Frame Relay technologies in the context of the CCIE Routing and Switching exam. I personally feel that knowledge of DMVPN is a critical skill for anyone working in a modern network enterprise, but I have also observed that it is one of least understood domains in the CCIE exam. As a direct result of this observation, I first deal with the fundamental technologies that enable DMVPN and its operation. Once these have been highlighted, I provide very clear delineations between the DMVPN operational phases and behaviors, recognizing that there absolutely has to be a concrete understanding of these elements before you can even hope to understand how a routing protocol behaves when running on top of a DMVPN.

Chapter 6, “IP Prefix-List”: IP Prefix-List has applications in almost every aspect of prefix filtering and packet filtering. IP prefix lists offer capabilities to match traffic based on variable ranges of networks and mask lengths. This tool, unlike other pattern-matching tools such as access lists, allows us to match multiple aspects of a network simultaneously. This chapter explores all aspects of prefix lists as independent tools.

Chapter 7, “EIGRP”: Enhanced Interior Gateway Protocol figures significantly into the makeup of the CCIE RS Lab exam. This demands a concrete understanding of both classical and named operations. This book looks at the operation of both these modes from a command-line perspective as well as covers how the two modes can and do interoperate between enabled devices. But whether you are running named or classic mode, as a candidate you need to master how to manipulate the protocol. This chapter covers both basic and advanced EIGRP operations. EIGRP is the first protocol that provides granular traffic engineering and prefix filtering, as well as various methods for injecting default routes. All these capabilities are covered in the hands-on labs in this chapter.

Chapter 8, “OSPF”: Single handedly, OSPF is responsible for more failed CCIE attempts than any other protocol (including BGP). I have observed that most candidates do not have a firm understanding of what actually takes place behind the scenes with OSPF. OSPF has many varying modes and enhancements that make it difficult to master. Route filtering, LSA operation, various stub configurations, and update filtering are just a handful of the protocol’s operational aspects that need to be managed. The labs in this chapter illustrate the function and configuration of each of these topics. We focus on how OSPF operates in single- and multi-area configurations as well as on how to manipulate its behavior in every way possible.

Chapter 9, “Redistribution”: When you talk to students that are preparing for the CCIE Lab Exam, most will tell you that they are terrified of redistribution. This is a direct result of Grey Market Trainers flooding the Internet with horrendously complex and error-fraught redistribution labs. The average student sees this and is immediately intimidated by what should be a straightforward routing mechanism. What are missing are the foundational basics associated with how to perform redistribution, and what happens when you do. My approach to the topic is to discuss the methodology and situations where redistribution can be problematic. Again this will be illustrated in labs that focus on the types of loops that can be generated, how to mitigate loops that have occurred, and procedures that will insure they never occur.

Chapter 10, “Border Gateway Protocol”: Border Gateway Protocol introduces complexity based on its overall scope and capability to “tune” or engineer control plane exchange based on attributes. These attributes far exceed the capabilities of protocols such as RIPv2, EIGRP, and even OSPF. This brings with it an ordered approach to how to conduct configuration and some interesting configuration syntax based on the desired manner of deployment. First, this chapter focuses on a concrete understanding of BGP’s complex Adjacency State Machine capabilities. After the introduction of both the internal and external peering mechanisms employed by the protocol, we explore how and what next-hop information is exchanged, plus we explore how to manipulate these basic operations. From there, we explore how to manipulate attributes or decisions based on attributes via ACLs, prefix lists, route maps, and regular expressions. Lastly, we focus on mechanisms designed to simplify BGP configuration by providing reduced command sets, behavior optimizations, and streamlined configuration syntax.

Chapter 11, “IPv6”: Gone are the days of being able to focus just on IPv4 addressing and routing protocols. IPv6 figures significantly into the CCIE Routing and Switching exam in that the exam requires a full understanding of the variants of protocols that support IPv6. Additionally, this chapter explores the operation of IPv6 in non-broadcast multi-access (NBMA) topologies such as DMVPN.

Chapter 12, “Quality of Service”: Given that the majority of QOS mechanisms that involve hardware-optimized operation have been removed from the exam, it is important to focus intently on what remains. This chapter explores the key fundamentals of QOS in the IOS-driven enterprise. This includes all aspects of marking and classification of traffic via enhanced and traditional mechanisms. Lastly, the chapter deals with the manipulations of such traffic after it has been marked. Emphasis is given to both policing and shaping of traffic. This focuses on both classical serial WAN connections and high-speed Ethernet WAN connections.

Chapter 13, “IPSec VPN”: The focus of the CCIE Routing and Switching Lab has expanded significantly in its last iterations. This expansion has included the incorporation of site-to-site solutions such as GRE/IPSec Tunnel mode as well as multisite VPN technologies and their protection/encryption. This chapter covers the application of encryption on these tunnels and VPNs from a command-line level. At this point, you should be able to apply encryption to DMVPNs. By waiting until this point in the lab exploration, you are able to better separate the DMVPN configuration task requirements from the necessary encryption and security configurations.

Chapter 14, “Multicast”: This chapter explores solutions that require end-to-end IPv4 and IPv6 transport between all devices. This includes protocol-independent routing optimizations such as policy-based routing, First Hop Redundancy Protocols and network address translation.

Chapter 15, “MPLS and L3VPNs”: MPLS and L3VPNs are tested heavily in the CCIE Routing and Switching Lab exam. This chapter takes a step-by-step approach to demonstrating the operational capabilities and deployment concerns involved in VPNv4 tunnels. Specific focus is given to the protocols running between the customer edge and premises edge equipment.

IPSec VPN

VPN tunnels are used to connect physically isolated networks that are more often than not separated by nonsecure internetworks. To protect these connections, we employ the IP Security (IPSec) protocol to make secure the transmission of data, voice, and video between sites. These secure tunnels over the Internet public network are encrypted using a number of advanced algorithms to provide confidentiality of data that is transmitted between multiple sites. This chapter explores how to configure routers to create a permanent secure site-to-site VPN tunnel.

Encryption will be provided by IPSec in concert with VPN tunnels. The Internet Security Association and Key Management Protocol (ISAKMP) and IPSec are essential to building and encrypting VPN tunnels. ISAKMP, also called IKE (Internet Key Exchange), is the negotiation protocol that allows hosts to agree on how to build an IPSec security association.

ISAKMP negotiation consists of two phases:

- Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages.
- Phase 2 creates the tunnel that protects data.

IPSec then encrypts exchanged data by employing encryption algorithms that result in authentication, encryption, and critical anti-replay services.

Lab 13-1: Basic Site-to-Site IPSec VPN

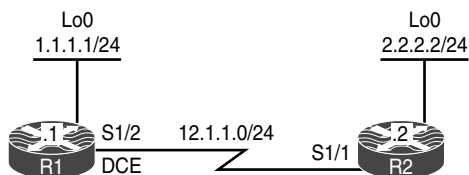


Figure 13-1 *Configuring Basic Site-to-Site IPSec VPN (Main Mode)*

Figure 13-1 illustrates the topology that will be used in the following lab.

Task 1

Configure a basic site-to-site IPsec VPN to protect traffic between IP addresses 1.1.1.1 and 2.2.2.2 using the policy shown in Table 13-1.

Table 13-1 Policy Guidelines for Configuring Task 1

ISAKMP Policy	IPsec Policy
Authentication: Pre-shared	Encryption: ESP-3DES
Hash: MD5	Hash: ESP-MD5-HMAC
DH Group: 2	Proxy-ID/Crypto ACL: 1.1.1.1 ↔ 2.2.2.2
Encryption: 3DES	
PSK: cisco	

Reachability to the loopback0 interfaces is provided in the initial configuration.

ISAKMP, originally defined in RFC 7296, covers the following:

- Procedures to authenticate a communicating peer
- How to create and manage security associations (SAs)
- Key-generation techniques
- Threat mitigation, such as denial-of-service (DoS) and replay attacks

IKE does not specify any details of key management or key exchange, and it's not bound to any key-generation techniques. Inside IKE, Cisco uses OAKLEY for the key exchange protocol.

OAKLEY enables you to choose between different well-known Diffie-Hellman (DH) groups. RFC 2412 describes the OAKLEY protocol and covers DH groups 1 through 5. Of these groups, Cisco supports DH groups 1, 2, and 5. RFC 3526 describes DH group 5 and groups 14 through 18. Cisco supports DH groups 5, 14, 15, and 16. RFC 5114 covers DH groups 19 through 26. Of these DH groups, Cisco supports 19, 20, 21, and 24. The following is a list of the DH groups supported by Cisco:

- 1: Diffie-Hellman group 1 (768 bit)
- 2: Diffie-Hellman group 2 (1024 bit)
- 5: Diffie-Hellman group 5 (1536 bit)
- 14: Diffie-Hellman group 14 (2048 bit)
- 15: Diffie-Hellman group 15 (3072 bit)
- 16: Diffie-Hellman group 16 (4096 bit)

- **19:** Diffie-Hellman group 19 (256-bit ECP)
- **20:** Diffie-Hellman group 20 (384-bit ECP)
- **21:** Diffie-Hellman group 21 (521-bit ECP)
- **24:** Diffie-Hellman group 24 (2048 bit, 256-bit subgroup)

ISAKMP and OAKLEY create an authenticated, secure tunnel between two entities, and then negotiate the SA for IPSec. Both peers must authenticate each other and establish a shared key.

Three authentication methods are available: RSA signatures (PKI), RSA encrypted pseudorandom numbers (nonces), and preshared keys (PSK). The DH protocol is used to agree on a common session key.

IPSec uses a different shared key from ISAKMP and OAKLEY. The IPSec shared key can be derived by using DH again to ensure Perfect Forward Secrecy (PFS) or by refreshing the shared secret derived from the original DH exchange.

IKE is a hybrid protocol that establishes a shared security policy and authenticated keys for services that require keys, such as IPSec. Before an IPSec tunnel is established, each device must be able to identify its peer. ISAKMP and IKE are both used interchangeably; however, these two items are somewhat different. IKE was originally defined by RFC 2409. IKE version 2 is currently described by RFC 7296.

IKE Phase 1: The two ISAKMP peers establish a secure and an authenticated channel. This channel is known as the ISAKMP SA. There are two modes defined by ISAKMP: Main Mode and Aggressive Mode.

IKE Phase 2: SAs are negotiated on behalf of services such as IPSec that need keying material. This phase is called Quick Mode.

To configure IKE Phase 1, you need to configure ISAKMP policies. It is possible to configure multiple policies with different configuration statements and then let the two hosts negotiate the policies. The first matched policy on the responder will be used.

Let's start configuring Phase 1 on both routers:

```
On R1:

R1(config)# crypto isakmp policy 10
R1(config-isakmp)# hash md5
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# encryption 3des
R1(config-isakmp)# exit
```

The IP address of a loopback interface can be used when there are multiple paths to reach the peer's IP address:

```
R1(config)# crypto isakmp key cisco address 12.1.1.2

On R2:

R2(config)# crypto isakmp policy 10
R2(config-isakmp)# hash md5
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)# encryption 3des
R2(config-isakmp)# exit

R2(config)# crypto isakmp key cisco address 12.1.1.1
```

To configure the Phase 2, we need to define the **transform-set**, which specifies the hashing, the security protocol, and the encryption used for Phase 2:

```
On Both Routers:

Rx(config)# crypto ipsec transform-set TSET esp-3des esp-md5-hmac
Rx(cfg-config-trans)# exit
```

Next, we need to define the crypto ACL/proxy ID, which defines the interesting traffic:

```
On R1:

R1(config)# access-list 100 permit ip host 1.1.1.1 host 2.2.2.2

On R2:

R2(config)# access-list 100 permit ip host 2.2.2.2 host 1.1.1.1
```

In the last step, a crypto map is configured to specify the peer, crypto ACL, and the transform set. There are three choices when configuring the following crypto map:

- **IPsec-ISAKMP:** This is the best option. It states that we are using ISAKMP to encrypt and decrypt the key.
- **IPsec-manual:** This is the worst choice. It means that the key needs to be entered manually. (Can you imagine entering a 512-bit key manually?)
- **GDOI:** This choice is used for GETVPN configuration. It stands for *group domain of interpretation*.

```
On R1:

R1(config)# crypto map TST 10 ipsec-isakmp
```

You should see the following console message:

```
% NOTE: This new crypto map will remain disabled until a peer
      and a valid access list have been configured.

R1(config-crypto-map)# set peer 12.1.1.2
R1(config-crypto-map)# match address 100
R1(config-crypto-map)# set transform-set TSET
R1(config-crypto-map)# exit

On R2:

R2(config)# crypto map TST 10 ipsec-isakmp
R2(config-crypto-map)# set peer 12.1.1.1
R2(config-crypto-map)# match address 100
R2(config-crypto-map)# set transform-set TSET
R2(config-crypto-map)# exit
```

The final step applies the crypto map to the interface facing the other peer:

```
On R1:

R1(config)# interface Serial 1/2
R1(config-if)# crypto map TST
```

You should see the following console message:

```
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

On R2:

R2(config)# interface Serial 1/1
R2(config-if)# crypto map TST
```

Let's verify the configuration before testing:

```
On R1:

R1# show crypto isakmp policy

Global IKE policy

Protection suite of priority 10
  encryption algorithm:  Three key triple DES
  hash algorithm:         Message Digest 5
  authentication method:  Pre-Shared Key
```

```

Diffie-Hellman group:  # 2 (1024 bit)
lifetime:              86400 seconds, no volume limit

R1# show crypto isakmp key

Keyring      Hostname/Address      Preshared Key
default     12.1.1.2              cisco

```

Now we can test the configuration:

```

On R1:

R1# debug crypto isakmp
Crypto ISAKMP debugging is on

R1# debug crypto ipsec
Crypto IPSEC debugging is on

R1# ping 2.2.2.2 source loopback0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1

```

The first ICMP packet triggers the ISAKMP process, as this is our interesting traffic matching the configured crypto ACL.

Before we actually start sending IKE packets to the peer, the router first checks whether there is a local SA (security association) matching that traffic. This check is against the IPsec SA and not an IKE SA.

We can see the outbound and remote IP addresses, port number, local proxy, and remote proxy. The protocol used is ESP, and the **transform-set** is the default mode of tunnel.

```

IPSEC(sa_request): ,
(key eng. msg.) OUTBOUND local= 12.1.1.1:500, remote= 12.1.1.2:500,
  local_proxy= 1.1.1.1/255.255.255.255/0/0 (type=1),
  remote_proxy= 2.2.2.2/255.255.255.255/0/0 (type=1),
  protocol= ESP, transform= esp-3des esp-md5-hmac (Tunnel),
  lifedur= 3600s and 4608000kb,
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0

```

The following highlighted line specifies that no SA was found. The router first tried to find an IPsec SA matching the outgoing connection, but it failed to find one.

```

ISAKMP:(0): SA request profile is (NULL)
ISAKMP: Created a peer struct for 12.1.1.2, peer port 500
ISAKMP: New peer created peer = 0x4B24E100 peer_handle = 0x80000003
ISAKMP: Locking peer struct 0x4B24E100, refcount 1 for isakmp_initiator
ISAKMP: local port 500, remote port 500
ISAKMP: set new node 0 to QM_IDLE
ISAKMP: Find a dup sa in the avl tree during calling isadb_insert sa = 4B331BEC

```

IKE Phase 1 (Main Mode) Message 1

By default, IKE Main Mode is used, so we should expect six packets for Phase 1. The following highlighted message states that the Aggressive Mode cannot start. However, this does not mean that we are experiencing errors; it just means that Aggressive Mode is not configured on the local router.

```

ISAKMP:(0): Can not start Aggressive mode, trying Main mode.

```

The router checks for the configured ISAKMP policy and sees that pre-shared key (PSK) authentication is configured. It has to check whether there is a key for the configured peer as well. After that, the first IKE packet is sent out to the peer's IP address on port UDP 500.

The packet contains locally configured ISAKMP policies to be negotiated by the peer. The pre-shared key for the remote peer is found, which means that ISAKMP is going to use it to authenticate the peer. This will happen in the last stage of IKE Phase 1.

```

ISAKMP:(0): found peer pre-shared key matching 12.1.1.2
ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID
ISAKMP:(0): constructed NAT-T vendor-07 ID
ISAKMP:(0): constructed NAT-T vendor-03 ID
ISAKMP:(0): constructed NAT-T vendor-02 ID
ISAKMP:(0): Input = IKE_MSG_FROM_IPSEC, IKE_SA_REQ_MM
ISAKMP:(0): Old State = IKE_READY New State = IKE_I_MM1

ISAKMP:(0): beginning Main Mode exchange
ISAKMP:(0): sending packet to 12.1.1.2 my_port 500 peer_port 500 (I) MM_NO_STATE

```

The router initiating the IKE exchange is called *the initiator*, and the router responding to IKE request is called *the responder*. The initiator (R1) has sent the ISAKMP policy along with vendor-specific IDs that are part of the IKE packet payload. **MM_NO_STATE** indicates that ISAKMP SA has been created, but nothing else has happened yet.

IKE Phase 1 (Main Mode) Message 2

It looks like everything is going smoothly. We received a response packet from the peer. However, this is one area where things can typically go wrong.

The received packet contains the SA chosen by the peer and some other useful information, such as vendor IDs. Those vendor-specific payloads are used to discover network address translation (NAT) along the path and to maintain keepalives. The router matches the ISAKMP policy from the packet to one that's locally configured. If there is a match, the tunnel-establishment process continues. If the policy configured on both routers is not the same, the crosscheck process fails and the tunnel is down.

```
ISAKMP:(0):Sending an IKE IPv4 Packet.
ISAKMP (0): received packet from 12.1.1.2 dport 500 sport 500 Global (I) MM_NO_STATE
ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Old State = IKE_I_MM1 New State = IKE_I_MM2

ISAKMP:(0): processing SA payload. message ID = 0
ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0):found peer pre-shared key matching 12.1.1.2
ISAKMP:(0): local preshared key found
ISAKMP : Scanning profiles for xauth ...
IS.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 44/45/48 ms
```

The router is processing ISAKMP parameters that have been sent as the reply. The vendor IDs are processed to determine whether the peer supports the NAT-Traversal, Dead Peer Detection feature. ISAKMP policy is checked against policies defined locally. The **atts are acceptable** message indicates that the ISAKMP policy matches with remote peer:

```
R1# AKMP:(0):Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP:(0):atts are acceptable. Next payload is 0
```

The lifetime timer has been started. Note that default value is used (86,400 seconds). This is the lifetime for ISAKMP SA. Note that IPsec SAs have their own **lifetime** parameters, which may be defined as number of seconds or kilobytes of transmitted traffic.

```

ISAKMP:(0):Acceptable atts:actual life: 0
ISAKMP:(0):Acceptable atts:life: 0
ISAKMP:(0):Fill atts in sa vpi_length:4
ISAKMP:(0):Fill atts in sa life_in_seconds:86400
ISAKMP:(0):Returning Actual lifetime: 86400
ISAKMP:(0)::Started lifetime timer: 86400.

ISAKMP:(0): processing vendor id payload
ISAKMP:(0): vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP (0): vendor ID is NAT-T RFC 3947
ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM2

```

IKE Phase 1 (Main Mode) Message 3

The third message is sent out containing key-exchange (KE) information for the Diffie-Hellman (DH) secure key-exchange process:

```

ISAKMP:(0): sending packet to 12.1.1.2 my_port 500 peer_port 500 (I) MM_SA_SETUP
ISAKMP:(0):Sending an IKE IPv4 Packet.
ISAKMP:(0):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(0):Old State = IKE_I_MM2 New State = IKE_I_MM3

```

IKE Phase 1 (Main Mode) Message 4

The fourth message has been received from the peer. This message contains the KE payload, and based on that information, both peers can generate a common session key to be used in securing further communication. The pre-shared key configured locally for the peer is used in this calculation.

After receiving this message, peers can determine whether there is NAT along the path.

```

ISAKMP (0): received packet from 12.1.1.2 dport 500 sport 500 Global (I) MM_SA_SETUP
ISAKMP:(0):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(0):Old State = IKE_I_MM3 New State = IKE_I_MM4

ISAKMP:(0): processing KE payload. message ID = 0
ISAKMP:(0): processing NONCE payload. message ID = 0
ISAKMP:(0):found peer pre-shared key matching 12.1.1.2
ISAKMP:(1002): processing vendor id payload
ISAKMP:(1002): vendor ID is Unity
ISAKMP:(1002): processing vendor id payload
ISAKMP:(1002): vendor ID is DPD
ISAKMP:(1002): processing vendor id payload

```

```

ISAKMP:(1002): speaking to another IOS box!
ISAKMP:received payload type 20
ISAKMP (1002): His hash no match - this node outside NAT
ISAKMP:received payload type 20
ISAKMP (1002): No NAT Found for self or peer
ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):Old State = IKE_I_MM4 New State = IKE_I_MM4

```

IKE Phase 1 (Main Mode) Message 5

The fifth message is used for sending out authentication information to the peer. This information is transmitted under the protection of the common shared secret.

```

ISAKMP:(1002):Send initial contact
ISAKMP:(1002):SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
ISAKMP (1002): ID payload
    next-payload : 8
    type         : 1
    address      : 12.1.1.1
    protocol     : 17
    port        : 500
    length      : 12
ISAKMP:(1002):Total payload length: 12
ISAKMP:(1002): sending packet to 12.1.1.2 my_port 500 peer_port 500 (I) MM_KEY_EXCH

```

MM_KEY_EXCH indicates that the peers have exchanged Diffie-Hellman public keys and have generated a shared secret. The ISAKMP SA remains unauthenticated. Note that the process of authentication has just been started.

```

ISAKMP:(1002):Sending an IKE IPv4 Packet.
ISAKMP:(1002):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1002):Old State = IKE_I_MM4 New State = IKE_I_MM5

```

IKE Phase 1 (Main Mode) Message 6

The peer identity is verified by the local router and the SA is established. This message finishes ISAKMP Main Mode (Phase I), and the status is changed to **IKE_P1_COMPLETE**.

```

ISAKMP (1002): received packet from 12.1.1.2 dport 500 sport 500 Global (I)
MM_KEY_EXCH
ISAKMP:(1002): processing ID payload. message ID = 0
ISAKMP (1002): ID payload
    next-payload : 8
    type         : 1

```



```

        address      : 12.1.1.2
        protocol     : 17
        port         : 500
        length       : 12
ISAKMP:(0):: peer matches *none* of the profiles
ISAKMP:(1002): processing HASH payload. message ID = 0
ISAKMP:(1002):SA authentication status:
    authenticated
ISAKMP:(1002):SA has been authenticated with 12.1.1.2
ISAKMP: Trying to insert a peer 12.1.1.1/12.1.1.2/500/, and inserted successfully
    4B24E100.
ISAKMP:(1002):Input = IKE_MSG_FROM_PEER, IKE_MM_EXCH
ISAKMP:(1002):Old State = IKE_I_MM5 New State = IKE_I_MM6

ISAKMP:(1002):Input = IKE_MSG_INTERNAL, IKE_PROCESS_MAIN_MODE
ISAKMP:(1002):Old State = IKE_I_MM6 New State = IKE_I_MM6

ISAKMP:(1002):Input = IKE_MSG_INTERNAL, IKE_PROCESS_COMPLETE
ISAKMP:(1002):Old State = IKE_I_MM6 New State = IKE_P1_COMPLETE

```

IKE Phase 2 (Quick Mode) Message 1

Now it's time for Phase 2, which is Quick Mode (QM). The router sends out the packet containing local proxy IDs (network/host addresses to be protected by the IPSec tunnel) and the security policy defined by the transform set.

The state of IKE is **QM_IDLE**. This indicates that the ISAKMP SA is idle. It remains authenticated with its peer and may be used for subsequent Quick Mode exchanges. It is in a quiescent state.

```

ISAKMP:(1002):beginning Quick Mode exchange, M-ID of 623921701
ISAKMP:(1002):QM Initiator gets spi
ISAKMP:(1002): sending packet to 12.1.1.2 my_port 500 peer_port 500 (I) QM_IDLE
ISAKMP:(1002):Sending an IKE IPv4 Packet.
ISAKMP:(1002):Node 623921701, Input = IKE_MSG_INTERNAL, IKE_INIT_QM
ISAKMP:(1002):Old State = IKE_QM_READY New State = IKE_QM_I_QM1
ISAKMP:(1002):Input = IKE_MSG_INTERNAL, IKE_PHASE1_COMPLETE
ISAKMP:(1002):Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE

ISAKMP (1002): received packet from 12.1.1.2 dport 500 sport 500 Global (I) QM_IDLE

```

The routers are negotiating the parameters for the IPSec tunnel that will be used for traffic transmission. These parameters are defined by the **crypto ipsec transform-set** command.

Note that lifetime values of the IPSec SA are visible at this moment. You are able to set this both globally and in the crypto map entry. The **attr are acceptable** message indicates that the IPSec parameters defined as the IPSec transform-set match on both sides.

```

ISAKMP:(1002): processing HASH payload. message ID = 623921701
ISAKMP:(1002): processing SA payload. message ID = 623921701
ISAKMP:(1002):Checking IPsec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP:  attributes in transform:
ISAKMP:  encaps is 1 (Tunnel)
ISAKMP:  SA life type in seconds
ISAKMP:  SA life duration (basic) of 3600
ISAKMP:  SA life type in kilobytes
ISAKMP:  SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:  authenticator is HMAC-MD5
ISAKMP:(1002):atts are acceptable.
IPSEC(validate_proposal_request): proposal part # 1
IPSEC(validate_proposal_request): proposal part # 1,

(key eng. msg.) INBOUND local= 12.1.1.1:0, remote= 12.1.1.2:0,
  local_proxy= 1.1.1.1/255.255.255.255/0/0 (type=1),

  remote_proxy= 2.2.2.2/255.255.255.255/0/0 (type=1),
  protocol= ESP, transform= NONE (Tunnel),
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0
Crypto mapdb : proxy_match
  src addr      : 1.1.1.1
  dst addr      : 2.2.2.2
  protocol      : 0
  src port      : 0
  dst port      : 0
ISAKMP:(1002): processing NONCE payload. message ID = 623921701
ISAKMP:(1002): processing ID payload. message ID = 623921701
ISAKMP:(1002): processing ID payload. message ID = 623921701

```

The local and remote proxies are defined. This indicates the sources and destinations set in crypto ACL, which defines the interesting traffic for the IPsec tunnel. Remember that it is enough when only one entry is mirrored. If not, you may get the following entry in the debug output: **PSEC(initialize_sas): invalid proxy IDs.**

```

ISAKMP:(1002): Creating IPsec SAs
  inbound SA from 12.1.1.2 to 12.1.1.1 (f/i)  0/ 0
  (proxy 2.2.2.2 to 1.1.1.1)
  has spi 0x2E5593AE and conn_id 0
  lifetime of 3600 seconds
  lifetime of 4608000 kilobytes

```

```

outbound SA from 12.1.1.1 to 12.1.1.2 (f/i) 0/0
(proxy 1.1.1.1 to 2.2.2.2)
has spi 0x5AEFD96D and conn_id 0
lifetime of 3600 seconds
lifetime of 4608000 kilobytes

```

The IPSec SAs have been created and inserted into the router's security associations database (SADB). SAs are distinguished by Security Parameter Index (SPI) values, which are also used to differentiate many tunnels terminated on the same router. Note that two SPI values are generated for one tunnel: one SPI for the inbound SA and one SPI for the outbound SA.

The SPI value is inserted in the ESP header of the packet leaving the router. At the other side of the tunnel, the SPI value inserted into the ESP header enables the router to reach parameters and keys that have been dynamically agreed upon during IKE negotiations, or session key refreshment in case of lifetime timeout.

```

ISAKMP:(1002): sending packet to 12.1.1.2 my_port 500 peer_port 500 (I) QM_IDLE
ISAKMP:(1002):Sending an IKE IPv4 Packet.
ISAKMP:(1002):deleting node 623921701 error FALSE reason "No Error"
ISAKMP:(1002):Node 623921701, Input = IKE_MSG_FROM_PEER, IKE_QM_EXCH
ISAKMP:(1002):Old State = IKE_QM_I_QM1 New State = IKE_QM_PHASE2_COMPLETE
IPSEC(key_engine): got a queue event with 1 KMI message(s)
Crypto mapdb : proxy_match

      src addr      : 1.1.1.1
      dst addr      : 2.2.2.2
      protocol      : 0
      src port      : 0
      dst port      : 0

IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same proxies and peer
12.1.1.2
IPSEC(policy_db_add_ident): src 1.1.1.1, dest 2.2.2.2, dest_port 0

IPSEC(create_sa): sa created,
(sa) sa_dest= 12.1.1.1, sa_proto= 50,
    sa_spi= 0x2E5593AE(777360302),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2003
    sa_lifetime(k/sec)= (4571378/3600)
IPSEC(create_sa): sa created,
(sa) sa_dest= 12.1.1.2, sa_proto= 50,
    sa_spi= 0x5AEFD96D(1525668205),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2004
    sa_lifetime(k/sec)= (4571378/3600)

```

```

IPSEC(update_current_outbound_sa): get enable SA peer 12.1.1.2 current outbound sa
to SPI 5AEFD96D
IPSEC(update_current_outbound_sa): updated peer 12.1.1.2 current outbound sa to SPI
5AEFD96D

ISAKMP:(1001):purging SA., sa=4B23D6D0, delme=4B23D6D0

R1# show crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
12.1.1.2     12.1.1.1     QM_IDLE        1002 ACTIVE

IPv6 Crypto ISAKMP SA

R1# show crypto ipsec sa

interface: Serial1/2
  Crypto map tag: TST, local addr 12.1.1.1

protected vrf: (none)
local ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (2.2.2.2/255.255.255.255/0/0)
current_peer 12.1.1.2 port 500
  PERMIT, flags={origin_is_acl,}
# pkts encaps: 4, # pkts encrypt: 4, # pkts digest: 4
# pkts decaps: 4, # pkts decrypt: 4, # pkts verify: 4
# pkts compressed: 0, # pkts decompressed: 0
# pkts not compressed: 0, # pkts compr. failed: 0
# pkts not decompressed: 0, # pkts decompress failed: 0
# send errors 1, # rcv errors 0

local crypto endpt.: 12.1.1.1, remote crypto endpt.: 12.1.1.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/2
current outbound spi: 0xE53B1D2(240366034)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xBDAF9A28(3182402088)
transform: esp-3des esp-md5-hmac ,
in use settings = {Tunnel, }
conn id: 2005, flow_id: NETGX:5, sibling_flags 80000046, crypto map: TST
sa timing: remaining key lifetime (k/sec): (4405715/2686)
IV size: 8 bytes

```

```

replay detection support: Y
Status: ACTIVE

inbound ah sas:
inbound pcp sas:

outbound esp sas:
spi: 0xE53B1D2 (240366034)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2006, flow_id: NETGX:6, sibling_flags 80000046, crypto map: TST
sa timing: remaining key lifetime (k/sec): (4405715/2686)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:
outbound pcp sas:

```

Task 2

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

Lab 13-2: Basic Site-to-Site IPsec VPN and NAT

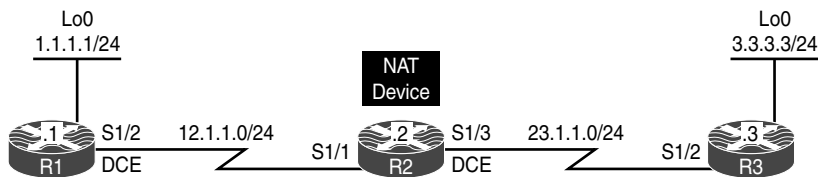


Figure 13-2 Configuring Basic Site-to-Site IPsec VPN and NAT

Figure 13-2 illustrates the topology that will be used in the following lab.

Task 1

Reachability to the loopback interfaces of R1 and R3 should be provided using static routes based on the following policy:

- R1 and R3 should be configured with a static default route pointing to R2.
- R2 should be configured with two static routes: one for network 1.1.1.0/24 through R1, and the second for 3.3.3.0/24 through R3.

```

On R1:

R1(config)# ip route 0.0.0.0 0.0.0.0 12.1.1.2

On R3:

R3(config)# ip route 0.0.0.0 0.0.0.0 23.1.1.2

On R2:

R2(config)# ip route 1.1.1.0 255.255.255.0 12.1.1.1
R2(config)# ip route 3.3.3.0 255.255.255.0 23.1.1.3

```

Let's test the configuration:

```

On R1:

R1# ping 3.3.3.3 source loopback0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms

```

Task 2

Configure static network address translation (NAT) on R2 so that R1's S1/2 IP address is seen on R3 as 23.1.1.1:

```

On R2:

R2(config)# interface Serial1/1
R2(config-if)# ip nat inside

R2(config)# interface Serial1/3
R2(config-if)# ip nat outside
R2(config-if)# exit

R2(config)# ip nat inside source static 12.1.1.1 23.1.1.1

```

Let's verify the configuration:

```
On R2:

R2# show ip nat translations

Pro Inside global      Inside local      Outside local      Outside global
--- 23.1.1.1           12.1.1.1         ---                ---
```

Task 3

Configure a basic site-to-site IPSec VPN to protect traffic between 1.1.1.1 and 3.3.3.3 networks using the policy shown in Table 13-2.

Table 13-2 Policy Guidelines for Configuring Task 3

ISAKMP Policy	IPSec Policy
Authentication: Pre-shared	Encryption: ESP-3DES
Hash: MD5	Hash: ESP-MD5-HMAC
DH Group: 2	Proxy-ID/Crypto ACL: 1.1.1.1 ↔ 3.3.3.3
Encryption: 3DES	
PSK: cisco	

By now we have a step-by-step process for IPSec configuration that we can use:

Step 1. Configure ISAKMP using pre-shared authentication, MD5 hashing, DH group 2, and a PSK of “cisco” on both R1 and R3:

```
On R1:

R1(config)# crypto isakmp policy 10
R1(config-isakmp)# hash md5
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# encryption 3des
R1(config-isakmp)# exit

On R3:

R3(config)# crypto isakmp policy 10
R3(config-isakmp)# hash md5
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# encryption 3des
R3(config-isakmp)# exit
```

Step 2. Configure the ISAKMP key and identify the peer:

```
On R1:

R1(config)# crypto isakmp key cisco address 23.1.1.3
```

Note R3 has to use the translated IP address because, from its perspective, it's establishing an IPsec tunnel with 23.1.1.1:

```
On R3:

R3(config)# crypto isakmp key cisco address 23.1.1.1
```

Step 3. Configure the IPsec transform set to use DES for encryption and MD5 for hashing:

```
On R1 and R3:

Rx(config)# crypto ipsec transform-set TSET esp-des esp-md5-hmac
Rx(cfg-config-trans)# exit
```

Step 4. Define interesting traffic:

```
On R1:

R1(config)# access-list 100 permit ip host 1.1.1.1 host 3.3.3.3

On R3:

R1(config)# access-list 100 permit ip host 3.3.3.3 host 1.1.1.1
```

Step 5. Configure a crypto map and reference the peer, the crypto ACL, and the transform set configured in the previous steps:

```
On R1:

R1(config)# crypto map TST 10 ipsec-isakmp
R1(config-crypto-map)# set peer 23.1.1.3
R1(config-crypto-map)# match address 100
R1(config-crypto-map)# set transform-set TSET
R1(config-crypto-map)# exit

On R3:

R3(config)# crypto map TST 10 ipsec-isakmp
```


The peer IP address should be the translated IP address:

```
R3(config-crypto-map)# set peer 23.1.1.1
R3(config-crypto-map)# match address 100
R3(config-crypto-map)# set transform-set TSET
R3(config-crypto-map)# exit
```

Step 6. Apply the crypto map to the outside interface:

```
On R1:

R1(config)# interface Serial1/2
R1(config-if)# crypto map TST

On R3:

R3(config)# interface Serial1/2
R3(config-if)# crypto map TST
```

Now let's test the configuration:

```
On R1:

R1# ping 3.3.3.3 source 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 88/91/92 ms

R1# show crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst          src          state        conn-id status
23.1.1.3     12.1.1.1    QM_IDLE     1001 ACTIVE

IPv6 Crypto ISAKMP SA

R1# show crypto ipsec sa | include #pkts

# pkts encaps: 4, # pkts encrypt: 4, # pkts digest: 4
# pkts decaps: 4, # pkts decrypt: 4, # pkts verify: 4
# pkts compressed: 0, # pkts decompressed: 0
```

```

# pkts not compressed: 0, # pkts compr. failed: 0
# pkts not decompressed: 0, # pkts decompress failed: 0

R1# show crypto engine connections active
Crypto Engine Connections

  ID  Type      Algorithm      Encrypt  Decrypt  LastSeqN  IP-Address
----  ---      -
1001  IKE       MD5+3DES      0        0        0          12.1.1.1
2001  IPsec     DES+MD5       0        4        4          12.1.1.1
2002  IPsec     DES+MD5       4        0        0          12.1.1.1

```

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

Lab 13-3: Configuring GRE/IPsec Tunnel Mode, Transport Mode, and S-VTI

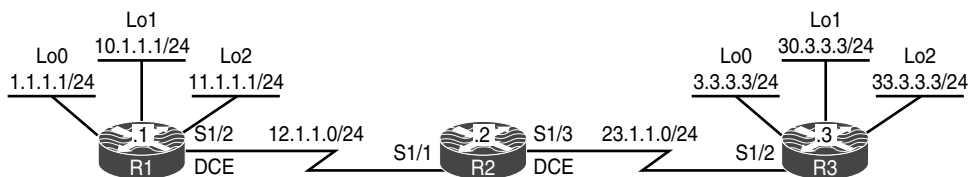


Figure 13-3 Configuring GRE/IPsec Tunnel Mode, Transport Mode, and S-VTI

Figure 13-3 illustrates the topology that will be used in the following lab.

Task 1

Configure a basic site-to-site IPsec VPN to protect traffic between the 1.1.1.0/24, 11.1.1.0/24, 2.2.2.0/24, and 22.2.2.0/24 networks using the policies shown in Table 13-3.

Table 13-3 Policy Guidelines for Configuring Task 1

ISAKMP Policy	IPsec Policy
Authentication: Pre-shared	Encryption: ESP-3DES
Hash: MD5	Hash: ESP-MD5-HMAC
DH Group: 2	Proxy-ID/Crypto ACL: 1.1.1.1 ↔ 2.2.2.2
Encryption: 3DES	
PSK: cisco	

Reachability is provided in the initial configuration.

- Step 1.** Configure ISAKMP using pre-shared authentication, MD5 hashing, DH group 2, and a PSK of “cisco” on both R1 and R3:

```

On R1:

R1(config)# crypto isakmp policy 10
R1(config-isakmp)# hash md5
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# encryption 3des
R1(config-isakmp)# exit

On R3:

R3(config)# crypto isakmp policy 10
R3(config-isakmp)# hash md5
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# encryption 3des
R3(config-isakmp)# exit

```

Step 2. Configure the ISAKMP key and identify the peer:

```

On R1:

R1(config)# crypto isakmp key cisco address 23.1.1.3

On R3:

R3(config)# crypto isakmp key cisco address 12.1.1.1

```

Step 3. Configure the IPSec transform set to use DES for encryption and MD5 for hashing:

```

On R1 and R3:

Rx(config)# crypto ipsec transform-set TSET esp-des esp-md5-hmac
Rx(cfg-config-trans)# exit

```

Step 4. Define interesting traffic. You can see how the crypto ACL can grow and grow. Can you imagine having 500 subnets trying to communicate with another 500 or more networks in a secure manner? The crypto ACL must be configured in a full mesh manner.

```

On R1:

R1(config)# access-list 100 permit ip host 1.1.1.1 host 3.3.3.3
R1(config)# access-list 100 permit ip host 1.1.1.1 host 30.3.3.3
R1(config)# access-list 100 permit ip host 1.1.1.1 host 33.3.3.3

```

```

R1(config)# access-list 100 permit ip host 10.1.1.1 host 3.3.3.3
R1(config)# access-list 100 permit ip host 10.1.1.1 host 30.3.3.3
R1(config)# access-list 100 permit ip host 10.1.1.1 host 33.3.3.3

R1(config)# access-list 100 permit ip host 11.1.1.1 host 3.3.3.3
R1(config)# access-list 100 permit ip host 11.1.1.1 host 30.3.3.3
R1(config)# access-list 100 permit ip host 11.1.1.1 host 33.3.3.3

On R3:

R3(config)# access-list 100 permit ip host 3.3.3.3 host 1.1.1.1
R3(config)# access-list 100 permit ip host 30.3.3.3 host 1.1.1.1
R3(config)# access-list 100 permit ip host 33.3.3.3 host 1.1.1.1

R3(config)# access-list 100 permit ip host 3.3.3.3 host 10.1.1.1
R3(config)# access-list 100 permit ip host 30.3.3.3 host 10.1.1.1
R3(config)# access-list 100 permit ip host 33.3.3.3 host 10.1.1.1

R3(config)# access-list 100 permit ip host 3.3.3.3 host 11.1.1.1
R3(config)# access-list 100 permit ip host 30.3.3.3 host 11.1.1.1
R3(config)# access-list 100 permit ip host 33.3.3.3 host 11.1.1.1

```

Step 5. Configure the crypto map and reference the peer, the crypto ACL, and the transform set configured in the previous steps:

```

On R1:

R1(config)# crypto map TST 10 ipsec-isakmp
R1(config-crypto-map)# set peer 23.1.1.3
R1(config-crypto-map)# match address 100
R1(config-crypto-map)# set transform-set TSET

On R3:

R3(config)# crypto map TST 10 ipsec-isakmp
R3(config-crypto-map)# set peer 12.1.1.1
R3(config-crypto-map)# match address 100
R3(config-crypto-map)# set transform-set TSET

```

Step 6. Apply the crypto map to the outside interface:

```

On R1:

R1(config)# interface Serial1/2
R1(config-if)# crypto map TST

```

```
On R3:
```

```
R3(config)# interface Serial1/2
R3(config-if)# crypto map TST
```

Let's test the configuration:

```
On R1:
```

```
R1# ping 3.3.3.3 source loopback0
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
```

```
Packet sent with a source address of 1.1.1.1
```

```
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 84/87/88 ms
```

```
R1# ping 3.3.3.3 source loopback1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
```

```
Packet sent with a source address of 10.1.1.1
```

```
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 84/87/88 ms
```

```
R1# ping 3.3.3.3 source loopback2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
```

```
Packet sent with a source address of 11.1.1.1
```

```
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 84/87/88 ms
```

```
R1# ping 30.3.3.3 source loopback0
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 30.3.3.3, timeout is 2 seconds:
```

```
Packet sent with a source address of 1.1.1.1
```

```
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 84/87/88 ms
```

```
R1# ping 30.3.3.3 source loopback1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 30.3.3.3, timeout is 2 seconds:
```

```
Packet sent with a source address of 10.1.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 84/87/88 ms

R1# ping 30.3.3.3 source loopback2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 11.1.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 84/87/88 ms

R1# ping 33.3.3.3 source loopback0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 33.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 84/87/88 ms

R1# ping 33.3.3.3 source loopback1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 33.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 84/87/88 ms

R1# ping 33.3.3.3 source loopback2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 33.3.3.3, timeout is 2 seconds:
Packet sent with a source address of 11.1.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 84/87/88 ms

R1# show crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst          src          state        conn-id status
23.1.1.3     12.1.1.1     QM_IDLE     1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

```

R1# show crypto ipsec sa | include local|remote|#pkts

      Crypto map tag: TST, local addr 12.1.1.1
local  ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (3.3.3.3/255.255.255.255/0/0)
# pkts encaps: 4, # pkts encrypt: 4, # pkts digest: 4
# pkts decaps: 4, # pkts decrypt: 4, # pkts verify: 4
# pkts compressed: 0, # pkts decompressed: 0
# pkts not compressed: 0, # pkts compr. failed: 0
# pkts not decompressed: 0, # pkts decompress failed: 0
      local crypto endpt.: 12.1.1.1, remote crypto endpt.: 23.1.1.3
local  ident (addr/mask/prot/port): (10.1.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (3.3.3.3/255.255.255.255/0/0)
# pkts encaps: 4, # pkts encrypt: 4, # pkts digest: 4
# pkts decaps: 4, # pkts decrypt: 4, # pkts verify: 4
# pkts compressed: 0, # pkts decompressed: 0
# pkts not compressed: 0, # pkts compr. failed: 0
# pkts not decompressed: 0, # pkts decompress failed: 0
      local crypto endpt.: 12.1.1.1, remote crypto endpt.: 23.1.1.3
local  ident (addr/mask/prot/port): (11.1.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (3.3.3.3/255.255.255.255/0/0)
# pkts encaps: 4, # pkts encrypt: 4, # pkts digest: 4
# pkts decaps: 4, # pkts decrypt: 4, # pkts verify: 4
# pkts compressed: 0, # pkts decompressed: 0
# pkts not compressed: 0, # pkts compr. failed: 0
# pkts not decompressed: 0, # pkts decompress failed: 0
      local crypto endpt.: 12.1.1.1, remote crypto endpt.: 23.1.1.3
local  ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (30.3.3.3/255.255.255.255/0/0)
# pkts encaps: 4, # pkts encrypt: 4, # pkts digest: 4
# pkts decaps: 4, # pkts decrypt: 4, # pkts verify: 4
# pkts compressed: 0, # pkts decompressed: 0
# pkts not compressed: 0, # pkts compr. failed: 0
# pkts not decompressed: 0, # pkts decompress failed: 0
      local crypto endpt.: 12.1.1.1, remote crypto endpt.: 23.1.1.3
local  ident (addr/mask/prot/port): (1.1.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (33.3.3.3/255.255.255.255/0/0)
# pkts encaps: 4, # pkts encrypt: 4, # pkts digest: 4
# pkts decaps: 4, # pkts decrypt: 4, # pkts verify: 4
# pkts compressed: 0, # pkts decompressed: 0
# pkts not compressed: 0, # pkts compr. failed: 0
# pkts not decompressed: 0, # pkts decompress failed: 0
      local crypto endpt.: 12.1.1.1, remote crypto endpt.: 23.1.1.3

```

```

local ident (addr/mask/prot/port): (10.1.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (30.3.3.3/255.255.255.255/0/0)
# pkts encaps: 4, # pkts encrypt: 4, # pkts digest: 4
# pkts decaps: 4, # pkts decrypt: 4, # pkts verify: 4
# pkts compressed: 0, # pkts decompressed: 0
# pkts not compressed: 0, # pkts compr. failed: 0
# pkts not decompressed: 0, # pkts decompress failed: 0
local crypto endpt.: 12.1.1.1, remote crypto endpt.: 23.1.1.3
local ident (addr/mask/prot/port): (11.1.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (30.3.3.3/255.255.255.255/0/0)
# pkts encaps: 4, # pkts encrypt: 4, # pkts digest: 4
# pkts decaps: 4, # pkts decrypt: 4, # pkts verify: 4
# pkts compressed: 0, # pkts decompressed: 0
# pkts not compressed: 0, # pkts compr. failed: 0
# pkts not decompressed: 0, # pkts decompress failed: 0
local crypto endpt.: 12.1.1.1, remote crypto endpt.: 23.1.1.3
local ident (addr/mask/prot/port): (10.1.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (33.3.3.3/255.255.255.255/0/0)
# pkts encaps: 4, # pkts encrypt: 4, # pkts digest: 4
# pkts decaps: 4, # pkts decrypt: 4, # pkts verify: 4
# pkts compressed: 0, # pkts decompressed: 0
# pkts not compressed: 0, # pkts compr. failed: 0
# pkts not decompressed: 0, # pkts decompress failed: 0
local crypto endpt.: 12.1.1.1, remote crypto endpt.: 23.1.1.3
local ident (addr/mask/prot/port): (11.1.1.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (33.3.3.3/255.255.255.255/0/0)
# pkts encaps: 4, # pkts encrypt: 4, # pkts digest: 4
# pkts decaps: 4, # pkts decrypt: 4, # pkts verify: 4
# pkts compressed: 0, # pkts decompressed: 0
# pkts not compressed: 0, # pkts compr. failed: 0
# pkts not decompressed: 0, # pkts decompress failed: 0
local crypto endpt.: 12.1.1.1, remote crypto endpt.: 23.1.1.3

```

This is definitely *not* scalable.

```
R1# show crypto engine connections active
```

```
Crypto Engine Connections
```

ID	Type	Algorithm	Encrypt	Decrypt	LastSeqN	IP-Address
1001	IKE	MD5+3DES	0	0	0	12.1.1.1
2001	IPsec	DES+MD5	0	4	4	12.1.1.1
2002	IPsec	DES+MD5	4	0	0	12.1.1.1
2003	IPsec	DES+MD5	0	4	4	12.1.1.1
2004	IPsec	DES+MD5	4	0	0	12.1.1.1
2005	IPsec	DES+MD5	0	4	4	12.1.1.1

2006	IPsec	DES+MD5	4	0	0	12.1.1.1
2007	IPsec	DES+MD5	0	4	4	12.1.1.1
2008	IPsec	DES+MD5	4	0	0	12.1.1.1
2009	IPsec	DES+MD5	0	4	4	12.1.1.1
2010	IPsec	DES+MD5	4	0	0	12.1.1.1
2011	IPsec	DES+MD5	0	4	4	12.1.1.1
2012	IPsec	DES+MD5	4	0	0	12.1.1.1
2013	IPsec	DES+MD5	0	4	4	12.1.1.1
2014	IPsec	DES+MD5	4	0	0	12.1.1.1
2015	IPsec	DES+MD5	0	4	4	12.1.1.1
2016	IPsec	DES+MD5	4	0	0	12.1.1.1
2017	IPsec	DES+MD5	0	4	4	12.1.1.1
2018	IPsec	DES+MD5	4	0	0	12.1.1.1

You can see the number of SPIs in the output of the preceding **show** command. You can also see that the legacy site-to-site IPSec VPNs are not scalable when the number networks that need to communicate increases.

Task 2

You are getting ready to add 500 more subnets to R1 and 500 more subnets to R3. Therefore, you need to configure a scalable solution that does not require the need for crypto ACLs. You will use GRE/IPSEC with Tunnel Mode to accomplish this task.

Because you need to totally cross-eliminate crypto ACLs, you can configure a GRE tunnel and encrypt all traffic that traverses the tunnel. Let's configure it:

Step 1. Configure the GRE tunnels.

When you're configuring the GRE tunnels, the **tunnel source** must reference the outside interface of the local router, and the **tunnel destination** must be the outside interface of the peer router. Also, the tunnel IP address should be a private IP address.

```
On R1:

R1(config)# interface tunnel13
R1(config-if)# ip address 10.1.13.1 255.255.255.0
R1(config-if)# tunnel source 12.1.1.1
R1(config-if)# tunnel destination 23.1.1.3

On R3:

R3(config)# interface tunnel31
R3(config-if)# ip address 10.1.13.3 255.255.255.0
R3(config-if)# tunnel source 23.1.1.3
R3(config-if)# tunnel destination 12.1.1.1
```

Step 2. Use an Interior Gateway Protocol (IGP) to advertise the networks in through the tunnel.

In this case, EIGRP AS 100 is used, but you can use any IGP to accomplish this step.

```
On R1:

R1(config)# router eigrp 100
R1(config-router)# netw 10.1.13.1 0.0.0.0

On R3:

R3(config)# router eigrp 100
R3(config-router)# netw 10.1.13.3 0.0.0.0
```

You should see the following console message:

```
%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.13.1 (Tunnel131) is up:
new adjacency
```

Let's verify the configuration:

```
On R3:

R3# show ip route eigrp | begin Gate
Gateway of last resort is 23.1.1.2 to network 0.0.0.0

    1.0.0.0/24 is subnetted, 1 subnets
D       1.1.1.0 [90/27008000] via 10.1.13.1, 00:02:15, Tunnel131
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D       10.1.1.0/24 [90/27008000] via 10.1.13.1, 00:02:15, Tunnel131
    11.0.0.0/24 is subnetted, 1 subnets
D       11.1.1.0 [90/27008000] via 10.1.13.1, 00:02:15, Tunnel131
```

Step 3. We need to delete the crypto ACLs and crypto maps. To remove the crypto map we previously applied to the interfaces:

```
On R1 and R3:

Rx(config)# no access-list 100

Rx(config)# interface Serial1/2
Rx(config-if)# no crypto map TST
Rx(config-if)# exit

Rx(config)# no crypto map TST
```

Step 4. Configure a crypto IPSec profile and reference the transform set:

```
On R1 and R3:

Rx(config)# crypto ipsec profile ABC
Rx(ipsec-profile)# set transform-set TSET
```

Step 5. Apply the crypto IPSec profile to the tunnel interface:

```
On R1:

R1(config)# interface tunnel13
R1(config-if)# tunnel protection ipsec profile ABC
```

Note EIGRP adjacency will go down because you are encrypting on one end and not the other. You should also see ISAKMP being enabled in the following console message:

```
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.13.3 (Tunnel13) is down:
holding time expired
```

```
On R3:

R3(config)# interface tunnel31
R3(config-if)# tunnel protection ipsec profile ABC
```

You should see the following console messages:

```
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.13.1 (Tunnel31) is up:
new adjacency
```

The **tunnel protection ipsec profile** command states that any traffic that traverses the tunnel should be encrypted with the IPSec profile called **ABC**.

Note In the legacy configuration, the crypto map had the following commands:

- **Set Transform-set:** In the legacy configuration, this is done in the **crypto ipsec profile**.
- **Set address:** This references the interesting traffic, and we saw in the previous task that this configuration is not scalable at all. In this configuration, the crypto ACLs are no

longer required because any traffic that traverses the tunnel will be encrypted, and as long as the configured routing protocol is pointing to the tunnel interface, all traffic from all subnets will be affected.

- **Set peer:** In the legacy configuration, this is achieved through the tunnel destination command when the actual GRE tunnel is configured.

Step 6. Now we need to verify that GRE/IPsec are running on the tunnels and that we are using Tunnel Mode:

```
R3# show crypto ipsec sa | section spi

current outbound spi: 0xFA948BE8(4204039144)
spi: 0xD090B49D(3499144349)
  transform: esp-des esp-md5-hmac ,
  in use settings ={Tunnel, }
  conn id: 2019, flow_id: NETGX:19, sibling_flags 80000046, crypto map:
    Tunnel31-head-0
  sa timing: remaining key lifetime (k/sec): (4598347/3082)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

spi: 0xFA948BE8(4204039144)
  transform: esp-des esp-md5-hmac ,
  in use settings ={Tunnel, }
  conn id: 2020, flow_id: NETGX:20, sibling_flags 80000046, crypto map:
    Tunnel31-head-0
  sa timing: remaining key lifetime (k/sec): (4598347/3082)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

R3# show interface tunnel31 | include Tunnel protocol
Tunnel protocol/transport GRE/IP
```

Task 3

After implementing the previous solution, you realize that every packet has duplicate IP addresses in the header. You need to keep the GRE tunnel but eliminate the duplicate IP addresses in the header of every packet.

To resolve this task, you must change the mode to Transport. Let's do that now:

On R1 and R3:

```
Rx(config)# crypto ipsec transform-set TSET esp-des esp-md5-hmac
Rx(cfg-crypto-trans)# mode transport
```

To verify this, you must clear `crypto ipsec sas`:

On Both Routers:

```
Rx# clear crypto sa
```

```
R1# show crypto ipsec sa
```

```
interface: Tunnel13
```

```
  Crypto map tag: Tunnel13-head-0, local addr 12.1.1.1
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (12.1.1.1/255.255.255.255/47/0)
```

```
remote ident (addr/mask/prot/port): (23.1.1.3/255.255.255.255/47/0)
```

```
current_peer 23.1.1.3 port 500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
  # pkts encaps: 9, # pkts encrypt: 9, # pkts digest: 9
```

```
  # pkts decaps: 7, # pkts decrypt: 7, # pkts verify: 7
```

```
  # pkts compressed: 0, # pkts decompressed: 0
```

```
  # pkts not compressed: 0, # pkts compr. failed: 0
```

```
  # pkts not decompressed: 0, # pkts decompress failed: 0
```

```
  # send errors 0, # rcv errors 0
```

```
local crypto endpt.: 12.1.1.1, remote crypto endpt.: 23.1.1.3
```

```
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/2
```

```
current outbound spi: 0x58BF5B22(1488935714)
```

```
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
```

```
  spi: 0x31C3E03A(834920506)
```

```
  transform: esp-des esp-md5-hmac ,
```

```
  in use settings ={Transport, }
```

```
  conn id: 2025, flow_id: NETGX:25, sibling_flags 80000006, crypto map:
  Tunnel13-head-0
```

```
  sa timing: remaining key lifetime (k/sec): (4430829/3568)
```

```

    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x58BF5B22(1488935714)
transform: esp-des esp-md5-hmac ,
in use settings ={Transport, }
conn id: 2026, flow_id: NETGX:26, sibling_flags 80000006, crypto map:
Tunnel13-head-0
sa timing: remaining key lifetime (k/sec): (4430829/3568)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

```

The transport protocol is still GRE. Let's verify this:

```

On R1:

R1# show interface tunnel13 | include Tunnel protocol

Tunnel protocol/transport GRE/IP

```

Task 4

Reconfigure R1 and R3 so that the tunnel protocol is IPsec; this way, the extra GRE overhead is no longer there.

In order to eliminate GRE altogether, you can change the tunnel mode to IPsec. Let's configure this and verify:

```

On R1:

R1(config)# interface tunnel13
R1(config-if)# tunnel mode ipsec ipv4

```

You should see the following console message:

```
%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.13.3 (Tunnel13) is down: holding
time expired

On R3:

R3(config)# interface tunnel31
R3(config-if)# tunnel mode ipsec ipv4
```

You should see EIGRP coming up again. This means that packets are being encrypted.

```
%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.13.1 (Tunnel31) is up: new
adjacency
```

Let's verify the configuration:

```
On R1:

R1# show crypto ipsec sa

interface: Tunnel13
  Crypto map tag: Tunnel13-head-0, local addr 12.1.1.1

  protected vrf: (none)
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 23.1.1.3 port 500
    PERMIT, flags={origin_is_acl,}
    # pkts encaps: 26, # pkts encrypt: 26, # pkts digest: 26
    # pkts decaps: 27, # pkts decrypt: 27, # pkts verify: 27
    # pkts compressed: 0, # pkts decompressed: 0
    # pkts not compressed: 0, # pkts compr. failed: 0
    # pkts not decompressed: 0, # pkts decompress failed: 0
    # send errors 8, # recv errors 0

  local crypto endpt.: 12.1.1.1, remote crypto endpt.: 23.1.1.3
  path mtu 1500, ip mtu 1500, ip mtu idb Serial1/2
  current outbound spi: 0x653D25F9(1698506233)
  PFS (Y/N): N, DH group: none

  inbound esp sas:
    spi: 0xF08E7802(4035868674)
      transform: esp-des esp-md5-hmac ,
      in use settings = {Tunnel1, }
```

```

conn id: 2029, flow_id: NETGX:29, sibling_flags 80000046, crypto map:
  Tunnel13-head-0
sa timing: remaining key lifetime (k/sec): (4571849/3511)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x653D25F9(1698506233)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
conn id: 2030, flow_id: NETGX:30, sibling_flags 80000046, crypto map:
  Tunnel13-head-0
sa timing: remaining key lifetime (k/sec): (4571849/3511)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

R1# show interface tunnel13 | include Tunnel protocol

Tunnel protocol/transport IPSEC/IP

```

Do not forget to make the following configuration on both routers in the topology.

```

Rx(config)# crypto ipsec transform-set TSET esp-des esp-md5-hmac
Rx(cfg-crypto-trans)# mode tunnel

Rx# clear crypto sa

```

You should wait for the tunnel to come up:

```

R1# show crypto ipsec sa

interface: Tunnel13
  Crypto map tag: Tunnel13-head-0, local addr 12.1.1.1

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

```



```

remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 23.1.1.3 port 500
  PERMIT, flags={origin_is_acl,}
# pkts encaps: 14, # pkts encrypt: 14, # pkts digest: 14
# pkts decaps: 13, # pkts decrypt: 13, # pkts verify: 13
# pkts compressed: 0, # pkts decompressed: 0
# pkts not compressed: 0, # pkts compr. failed: 0
# pkts not decompressed: 0, # pkts decompress failed: 0
# send errors 0, # recv errors 0

local crypto endpt.: 12.1.1.1, remote crypto endpt.: 23.1.1.3
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/2
current outbound spi: 0x8CD7122B(2362905131)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0xD5DFBB05(3588209413)
  transform: esp-des esp-md5-hmac ,
  in use settings ={Tunnel, }
  conn id: 2031, flow_id: NETGX:31, sibling_flags 80000046, crypto map:
    Tunnel13-head-0
  sa timing: remaining key lifetime (k/sec): (4580543/3568)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x8CD7122B(2362905131)
  transform: esp-des esp-md5-hmac ,
  in use settings ={Tunnel, }
  conn id: 2032, flow_id: NETGX:32, sibling_flags 80000046, crypto map:
    Tunnel13-head-0
  sa timing: remaining key lifetime (k/sec): (4580543/3568)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

outbound ah sas:

outbound pcp sas:

```

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

Lab 13-4: Protecting DMVPN Tunnels

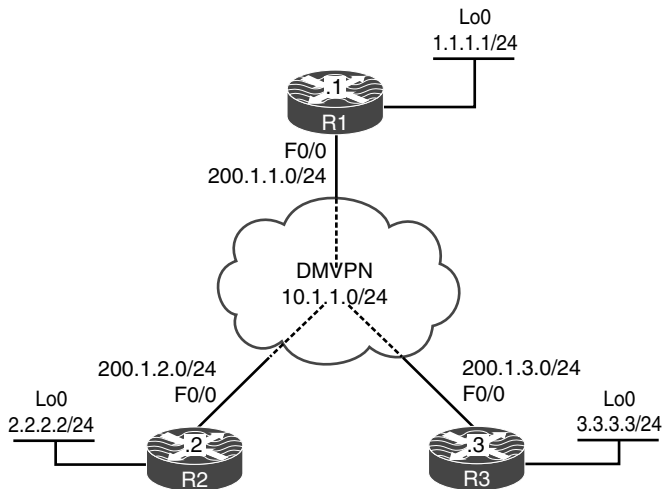


Figure 13-4 *Configuring Protecting DMVPN Tunnels*

Figure 13-4 illustrates the topology that will be used in the following lab.

Task 1

SW1 represents the Internet; configure the ports on the switch based on the following and then enable IP routing:

- F0/1: 200.1.1.10/24
- F0/2: 200.1.2.10/24
- F0/3: 200.1.3.10/24

```
On SW1:

SW1(config)# interface FastEthernet 0/1
SW1(config-if)# no switchport
SW1(config-if)# ip address 200.1.1.10 255.255.255.0
SW1(config-if)# no shutdown

SW1(config)# interface FastEthernet 0/2
SW1(config-if)# no switchport
SW1(config-if)# ip address 200.1.2.10 255.255.255.0
SW1(config-if)# no shutdown
```

```

SW1(config)# interface FastEthernet 0/3
SW1(config-if)# no switchport
SW1(config-if)# ip address 200.1.3.10 255.255.255.0
SW1(config-if)# no shutdown

SW1(config)# ip routing

```

Task 2

Configure the F0/0 and loopback0 interfaces of R1, R2, and R3 based on the configurations shown in Table 13-4.

Table 13-4 Configurations for Task 2

Router	Interfaces
R1	loopback0: 1.1.1.1/24 F0/0: 200.1.1.1/24
R2	loopback0: 2.2.2.2/24 F0/0: 200.1.2.2/24
R3	loopback0: 3.3.3.3/24 F0/0: 200.1.3.3/24

Ensure that these routers have full reachability to each other using static routes:

```

On R1:

R1(config)# interface loopback0
R1(config-if)# ip address 1.1.1.1 255.255.255.0

R1(config)# interface FastEthernet 0/0
R1(config-if)# ip address 200.1.1.1 255.255.255.0
R1(config-if)# no shutdown

R1(config)# ip route 200.1.2.0 255.255.255.0 200.1.1.10
R1(config)# ip route 200.1.3.0 255.255.255.0 200.1.1.10

On R2:

R2(config)# interface loopback0
R2(config-if)# ip address 2.2.2.2 255.255.255.0

R2(config)# interface FastEthernet 0/0
R2(config-if)# ip address 200.1.2.2 255.255.255.0
R2(config-if)# no shutdown

```

```

R2(config)# ip route 200.1.1.0 255.255.255.0 200.1.2.10
R2(config)# ip route 200.1.3.0 255.255.255.0 200.1.2.10

On R3:

R3(config)# interface loopback 0
R3(config-if)# ip address 3.3.3.3 255.255.255.0

R3(config)# interface FastEthernet 0/0
R3(config-if)# ip address 200.1.3.3 255.255.255.0
R3(config-if)# no shutdown

R3(config)# ip route 200.1.1.0 255.255.255.0 200.1.3.10
R3(config)# ip route 200.1.2.0 255.255.255.0 200.1.3.10

```

Let's verify the configuration:

```

On R1:

R1# ping 200.1.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1# ping 200.1.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.3.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

On R2:

R2# ping 200.1.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.3.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```

Task 3

Configure DMVPN Phase 2 such that R1 is the hub. R2 and R3 should be configured as the spokes. You should use 10.1.1.x/24, where *x* is the router number. If this configuration is performed correctly, these routers should have full reachability to all loopback interfaces and tunnel endpoints. You should *not* configure static mappings on the hub router to accomplish this task. Use EIGRP to provide reachability.

```

On R1:

R1(config)# interface tunnel123
R1(config-if)# ip address 10.1.1.1 255.255.255.0
R1(config-if)# tunnel source FastEthernet 0/0
R1(config-if)# tunnel mode gre multipoint
R1(config-if)# ip nhrp network-id 111
R1(config-if)# ip nhrp map multicast dynamic

On R2:

R2(config)# interface tunnel123
R2(config-if)# ip address 10.1.1.2 255.255.255.0
R2(config-if)# tunnel source FastEthernet 0/0
R2(config-if)# tunnel mode gre multipoint
R2(config-if)# ip nhrp network-id 222
R2(config-if)# ip nhrp nhs 10.1.1.1
R2(config-if)# ip nhrp map 10.1.1.1 200.1.1.1

On R3:

R3(config)# interface tunnel123
R3(config-if)# ip address 10.1.1.3 255.255.255.0
R3(config-if)# tunnel source FastEthernet 0/0
R3(config-if)# tunnel mode gre multipoint
R3(config-if)# ip nhrp network-id 333
R3(config-if)# ip nhrp nhs 10.1.1.1
R3(config-if)# ip nhrp map 10.1.1.1 200.1.1.1

```

Let's verify the configuration:

```

On R1:

R1# show ip nhrp

10.1.1.2/32 via 10.1.1.2
  Tunnel123 created 00:03:43, expire 01:56:16
  Type: dynamic, Flags: unique registered
  NBMA address: 200.1.2.2

```

```

10.1.1.3/32 via 10.1.1.3
  Tunnel123 created 00:02:18, expire 01:57:41
  Type: dynamic, Flags: unique registered
  NBMA address: 200.1.3.3

R1# show dmvpn detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
       N - NATed, L - Local, X - No Socket
       # Ent --> Number of NHRP entries with same NBMA peer
       NHS Status: E --> Expecting Replies, R --> Responding, W --> Waiting
       UpDn Time --> Up or Down Time for a Tunnel
=====

Interface Tunnel123 is up/up, Addr. is 10.1.1.1, VRF ""
  Tunnel Src./Dest. addr: 200.1.1.1/MGRE, Tunnel VRF ""
  Protocol/Transport: "multi-GRE/IP", Protect ""
  Interface State Control: Disabled
Type:Hub, Total NBMA Peers (v4/v6): 2

# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb  Target Network
-----
   1    200.1.2.2      10.1.1.2  UP 00:04:47  D    10.1.1.2/32
   1    200.1.3.3      10.1.1.3  UP 00:03:22  D    10.1.1.3/32

Crypto Session Details:
-----

Pending DMVPN Sessions:

R1# ping 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms

R1# ping 10.1.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```

Now we can run EIGRP:

```
R1(config)# router eigrp 100
R1(config-router)# network 1.1.1.1 0.0.0.0
R1(config-router)# network 10.1.1.1 0.0.0.0

R1(config)# interface tunnel123
R1(config-if)# no ip split-horizon eigrp 100
R1(config-if)# no ip next-hop-self eigrp 100

On R2:

R2(config)# router eigrp 100
R2(config-router)# network 2.2.2.2 0.0.0.0
R2(config-router)# network 10.1.1.2 0.0.0.0
```

You should see the following console message:

```
%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.1 (Tunnel123) is up:
new adjacency

R2(config)# interface tunnel123
R2(config-if)# ip nhrp map multicast 200.1.1.1

On R3:

R3(config)# router eigrp 100
R3(config-router)# network 3.3.3.3 0.0.0.0
R3(config-router)# network 10.1.1.3 0.0.0.0
```

You should also see this console message:

```
%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.1 (Tunnel123) is up:
new adjacency

R3(config)# interface tunnel123
R3(config-if)# ip nhrp map multicast 200.1.1.1
```

Let's verify the configuration:

```
On R2:

R2# show ip route eigrp | begin Gate
Gateway of last resort is not set

      1.0.0.0/24 is subnetted, 1 subnets
D       1.1.1.0 [90/27008000] via 10.1.1.1, 00:02:19, Tunnel123
```

```

    3.0.0.0/24 is subnetted, 1 subnets
D       3.3.3.0 [90/28288000] via 10.1.1.3, 00:01:31, Tunnel123

R2# ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R2# ping 3.3.3.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

```

Task 4

Protect the traffic between 1.1.1.0/24, 2.2.2.0/24, and 3.3.3.0/24 using an IPsec VPN based on the policy shown in Table 13-5.

Table 13-5 Policy Guidelines for Configuring Task 4

ISAKMP Policy	IPsec Policy
Authentication: Pre-shared	Encryption: ESP-3DES
Hash: MD5	Hash: ESP-MD5-HMAC
DH Group: 2	Proxy-ID/Crypto ACL: 1.1.1.1 ↔ 2.2.2.2
Encryption: 3DES	
PSK: cisco	

Let's go through the steps.

First, we begin by configuring IKE Phase 1:

```

On R1:

R1(config)# crypto isakmp policy 10
R1(config-isakmp)# hash md5
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# encryption 3des

```


Note The address is set to 0.0.0.0 because the edge devices may acquire different IP addresses, and/or spoke-to-spoke communication may occur between any spokes. Therefore, the IP address *must* be set to 0.0.0.0:

```
R1(config)# crypto isakmp key cisco address 0.0.0.0
```

Now with that done, we can create a transform set based on the requirement in the task:

```
R1(config)# crypto ipsec transform-set TSET esp-des esp-md5-hmac
R1(cfg-crypto-trans)# mode transport
```

Next, we configure **crypto ipsec profile** to reference the transform set:

```
R1(config)# crypto ipsec profile TST
R1(ipsec-profile)# set transform-set TSET
```

The **crypto ipsec profile** is configured in the tunnel to protect all traffic traversing the tunnel interface:

```
R1(config)# interface tunnel123
R1(config-if)# tunnel protection ipsec profile TST
```

Once this is configured on R1, you will see that ISAKMP is enabled. Because this is the only site configured, EIGRP neighbor adjacency will be lost to R2 and R3:

```
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.2 (Tunnel123) is down:
holding time expired

%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.3 (Tunnel123) is down:
holding time expired
```

You will also see the following console messages stating that you are receiving packets that are not encrypted:

```
%CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet. (ip)
vrf/dest_addr= /200.1.1.1, src_addr= 200.1.2.2, prot= 47

On R2:

R2(config)# crypto isakmp policy 10
R2(config-isakmp)# hash md5
```

```

R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)# encryption 3des

R2(config)# crypto isakmp key cisco address 0.0.0.0

R2(config)# crypto ipsec transform-set TSET esp-des esp-md5-hmac
R2(cfg-crypto-trans)# mode transport

R2(config)# crypto ipsec profile TST
R2(ipsec-profile)# set transform-set TSET

R2(config)# interface tunnel 123
R2(config-if)# tunnel protection ipsec profile TST

```

You should see the following console message:

```

%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.1 (Tunnel123) is up:
new adjacency

On R3:

R3(config)# crypto isakmp policy 10
R3(config-isakmp)# hash md5
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# encryption 3des

R3(config)# crypto isakmp key cisco address 0.0.0.0

R3(config)# crypto ipsec transform-set TSET esp-des esp-md5-hmac
R3(cfg-crypto-trans)# mode transport

R3(config)# crypto ipsec profile TST
R3(ipsec-profile)# set transform-set TSET

R3(config)# interface tunnel 123
R3(config-if)# tunnel protection ipsec profile TST

%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

%DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.1 (Tunnel123) is up:
new adjacency

```

Let's verify the configuration:

```

On R2:

R2# show crypto ipsec sa

interface: Tunnel123
  Crypto map tag: Tunnel123-head-0, local addr 200.1.2.2

protected vrf: (none)
local ident (addr/mask/prot/port): (200.1.2.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (200.1.1.1/255.255.255.255/47/0)
current_peer 200.1.1.1 port 500
  PERMIT, flags={origin_is_acl,}
  # pkts encaps: 176, # pkts encrypt: 176, # pkts digest: 176
  # pkts decaps: 178, # pkts decrypt: 178, # pkts verify: 178
  # pkts compressed: 0, # pkts decompressed: 0
  # pkts not compressed: 0, # pkts compr. failed: 0

  # pkts not decompressed: 0, # pkts decompress failed: 0
  # send errors 0, # rcv errors 0

local crypto endpt.: 200.1.2.2, remote crypto endpt.: 200.1.1.1
path mtu 1500, ip mtu 1500, ip mtu idb (none)
current outbound spi: 0x97BEF376(2545873782)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x7AC150C4(2059489476)
  transform: esp-des esp-md5-hmac ,
  in use settings ={Transport, }
  conn id: 2003, flow_id: NETGX:3, sibling_flags 80000006, crypto map:
    Tunnel123-head-0
  sa timing: remaining key lifetime (k/sec): (4428305/2843)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x97BEF376(2545873782)
  transform: esp-des esp-md5-hmac ,

```

```

in use settings ={Transport, }
conn id: 2004, flow_id: NETGX:4, sibling_flags 80000006, crypto map:
  Tunnel123-head-0
sa timing: remaining key lifetime (k/sec): (4428305/2843)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (200.1.2.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (200.1.3.3/255.255.255.255/47/0)
current_peer 200.1.3.3 port 500
  PERMIT, flags={origin_is_acl,}
# pkts encaps: 0, # pkts encrypt: 0, # pkts digest: 0
# pkts decaps: 0, # pkts decrypt: 0, # pkts verify: 0

# pkts compressed: 0, # pkts decompressed: 0
# pkts not compressed: 0, # pkts compr. failed: 0
# pkts not decompressed: 0, # pkts decompress failed: 0
# send errors 0, # rcv errors 0

local crypto endpt.: 200.1.2.2, remote crypto endpt.: 200.1.3.3
path mtu 1500, ip mtu 1500, ip mtu idb (none)
current outbound spi: 0x539AB1EC(1402647020)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xCC3D2892(3426560146)
transform: esp-des esp-md5-hmac ,
in use settings ={Transport, }
conn id: 2007, flow_id: NETGX:7, sibling_flags 80000006, crypto map:
  Tunnel123-head-0
sa timing: remaining key lifetime (k/sec): (4529448/2854)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

```

```

outbound esp sas:
  spi: 0x539AB1EC(1402647020)
  transform: esp-des esp-md5-hmac ,
  in use settings ={Transport, }
  conn id: 2008, flow_id: NETGX:8, sibling_flags 80000006, crypto map: Tunnel123-head-0
  sa timing: remaining key lifetime (k/sec): (4529448/2854)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

```

```
outbound ah sas:
```

```
outbound pcg sas:
```

```
R2# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
```

dst	src	state	conn-id	status
200.1.2.2	200.1.3.3	QM_IDLE	1003	ACTIVE
200.1.2.2	200.1.1.1	QM_IDLE	1002	ACTIVE
200.1.1.1	200.1.2.2	QM_IDLE	1001	ACTIVE
200.1.3.3	200.1.2.2	QM_IDLE	1004	ACTIVE

```
IPv6 Crypto ISAKMP SA
```

```
R2# ping 3.3.3.3 source loopback0
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
```

```
Packet sent with a source address of 2.2.2.2
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

```
R2# show crypto ipsec sa | include local|remote|#pkts
```

```

Crypto map tag: Tunnel123-head-0, local addr 200.1.2.2
local ident (addr/mask/prot/port): (200.1.2.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (200.1.1.1/255.255.255.255/47/0)
# pkts encaps: 304, # pkts encrypt: 304, # pkts digest: 304
# pkts decaps: 306, # pkts decrypt: 306, # pkts verify: 306
# pkts compressed: 0, # pkts decompressed: 0
# pkts not compressed: 0, # pkts compr. failed: 0
# pkts not decompressed: 0, # pkts decompress failed: 0
local crypto endpt.: 200.1.2.2, remote crypto endpt.: 200.1.1.1

```

```
local ident (addr/mask/prot/port): (200.1.2.2/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (200.1.3.3/255.255.255.255/47/0)
# pkts encaps: 5, # pkts encrypt: 5, # pkts digest: 5
# pkts decaps: 5, # pkts decrypt: 5, # pkts verify: 5
# pkts compressed: 0, # pkts decompressed: 0
# pkts not compressed: 0, # pkts compr. failed: 0
# pkts not decompressed: 0, # pkts decompress failed: 0
local crypto endpt.: 200.1.2.2, remote crypto endpt.: 200.1.3.3
```

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

Index

Numbers

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

A

AAA servers, 176

ABR (Area Border Router), 467

access control lists

MAC address access lists, 904–906
verifying, 9

access lists, filtering with, 704–714

access list configuration, 712–713

BGP peering, 704–708

outbound prefixes, filtering, 713–714

prefix-list and distribute-list
configuration, 709–710

R2 configuration, 708–709

R3 configuration, 711–712

ACFC (Address and Control Field
Compression), 179

ACLs. *See* access control lists

acquiring IPv6 addresses

DHCP client/server configuration,
746–751

DHCP prefix delegation, 755–763
modified EUI-64 addressing,
737–739

neighbor discovery, 739–743

overview of, 737

R2 configuration, 751–754

R5 configuration, 754–755

SLAAC (stateless address
auto-configuration), 743–746

Address and Control Field

Compression (ACFC), 179

Address field (PPP), 170–171

addresses (IP), 36

acquiring

*DHCP client/server
configuration, 746–751*

*DHCP prefix delegation,
755–763*

*modified EUI-64 addressing,
737–739*

neighbor discovery, 739–743

overview of, 737

R2 configuration, 751–754

- R5 configuration, 754–755*
- SLAAC (stateless address auto-configuration), 743–746*
- assigning, 187–190
- configuration, 387–388
- addresses (MAC), 36, 904–906**
 - MAC address access lists, 904–906
 - match destination and source address
 - MAC
 - overview of, 885*
 - R2 configuration to classify and mark IP routed traffic, 882–885*
 - RIPv2 configuration, 881*
- address-family command, 312**
- adjacency**
 - neighbor adjacencies, 635–641
 - OSPF (Open Shortest Path First), 391–397
- advertising**
 - conditional label advertising, 1058–1064
 - loopback interfaces, 501–502
 - networks, 381
 - DMVPN configuration, 389–391*
 - IP addressing, 387–388*
 - OSPF adjacency, 391–397*
 - OSPF summarization and, 468–469, 472–475*
 - R1 and R4 connections and loopback interfaces, 385–387*
 - R4, R5, and R6 connections, 381–385*
 - static default routes, 388–389*
 - of prefixes originating in own AS, preventing, 721–723
- af-interface default command, 324**
- always keyword, 824**
- announcements (RP), filtering, 1004–1005**
- application-specific integrated circuits (ASICs), 839**
- area 2 nssa command, 534**
- Area Border Router (ABR), 467**
- area range command, 473, 783**
- ARP table, showing, 9**
- AS-path attribute (BGP), 679–686**
- ASBR (Autonomous System Boundary Router), 467**
- ASICs (application-specific integrated circuits), 839**
- attributes**
 - Cluster-ID, 642
 - community, 667–679
 - BGP peering, 668–671*
 - R1 configuration, 672–673*
 - R2 configuration, 677–679*
 - R3 configuration, 675–677*
 - R5 configuration, 674–675*
 - multi-exit discriminator, 695–703
 - Originator-ID, 642
 - AS-path, 679–686
 - weight, 686–695
- AUTH-ACK message, 190, 194**
- Authenticate-Request message, 177**
- authentication**
 - CHAP (Challenge-Handshake Authentication Protocol)
 - messages, 198–200*
 - one-way authentication, 198–201*
 - overview of, 175–179*
 - R4, configuring to authenticate R3, 202–207*

two-way authentication,
 201–202

EAP (Extensible Authentication Protocol), 175–176, 216–218

EIGRP (Enhanced Interior Gateway Routing Protocol)

- EIGRP AS 100 configuration*, 360–361
- HMAC-SHA-256*, 362–363, 833–834
- MD5*, 361, 831–833
- router configuration*, 359–360
- topology*, 359

MS-CHAP (Microsoft CHAP), 175–176, 215–218

OSPF (Open Shortest Path First), 431

- demand circuits*, 456–457
- MD5 authentication*, 440–462
- plaintext authentication*, 433–439
- router interfaces in Area 0*, 431–433

PAP (Password Authentication Protocol)

- one-way authentication*, 190–192
- overview of*, 175–179
- two-way authentication*, 192–194

PPP (Point-to-Point Protocol), 175–177

Authentication Phase (PPP), 175–177

AUTH-REQ message, 190, 194

autoconfiguration (LDP), enabling, 1068–1071

Autonomous System Boundary Router (ASBR), 467

autonomous-system command, 1108

Auto-RP, 993

Lo0 interface of R1, 1006–1010

OSPF Area 0 configuration, 994

PIM sparse-dense-mode configuration, 994–997

primary and backup RP configuration, 997–1003

R3 configuration, 1005–1006

RP announcements, filtering on R6, 1004–1005

B

backdoor (BGP), 650–667

- configuration, 654–658
- IP address, removing from F0/0 interfaces, 658
- loopback1 interfaces, advertising, 653
- peer session configuration, 650–651
- policies for R1 configuration, 659–667
- R1, R2, and R3 configuration, 651
- RIPv2 and EIGRP 100 configuration, 651–652

backdoor links and OSPF, 1123

- CE (customer edge) router configuration, 1136–1141
- F0/1 interface of R1 and the G0/1 interface of R7, 1141–1147
- LDP configuration between core routers, 1128–1132
- MP-BGP AS 100 configuration between R2 and R6, 1132–1133
- OSPF configuration on core MPLS routers, 1123–1128
- RDs (route distinguishers), 1134–1136
- RTs (route targets), 1134–1136
- topology, 1123–1125

- VRF (Virtual Routing and Forwarding), 1134–1136
- backup RP (rendezvous point) configuration**, 997–1003, 1017–1022
- bandwidth usage, configuring (EIGRP)**, 324–325, 830
- bandwidth-percent command**, 324
- bba-group**, 207
- BGP (Border Gateway Protocol)**, 635
 - community attribute, 667–679
 - BGP peering*, 668–671
 - R1 configuration*, 672–673
 - R2 configuration*, 677–679
 - R3 configuration*, 675–677
 - R5 configuration*, 674–675
 - conditional advertisement and BGP backdoor, 650–667
 - backdoor configuration*, 654–658
 - IP address, removing from F0/0 interfaces*, 658
 - loopback1 interfaces, advertising*, 653
 - peer session configuration*, 650–651
 - policies for R1 configuration*, 659–667
 - R1, R2, and R3 configuration*, 651
 - RIPv2 and EIGRP 100 configuration*, 651–652
 - confederation, 731–736
 - filtering with access lists and prefix lists, 704–714
 - access list configuration*, 712–713
 - BGP peering*, 704–708
 - outbound prefixes, filtering*, 713–714
 - prefix-list and distribute-list configuration*, 709–710
 - R2 configuration*, 708–709
 - R3 configuration*, 711–712
 - multi-exit discriminator attribute, 695–703
 - neighbor adjacencies, establishing, 635–641
 - AS-path attribute, 679–686
 - regular expressions, 714–731
 - advertising of prefixes originating in own AS, preventing*, 721–723
 - BGP peering*, 715–717
 - prefixes from directly connected neighbors, blocking*, 725–726
 - prefixes originating in AS 200, blocking*, 723–725
 - prefixes originating in AS 300, blocking*, 727–728
 - prefixes originating in AS 300, filtering*, 717–719
 - prefixes with AS 300 in path list, filtering*, 719–721
 - prefixes with prepended AS numbers, blocking*, 728–731
 - router reflectors, 642–649
 - in VPN, 1148–1154
 - weight attribute, 686–695
- binary conversion**, 279
- Bootstrap Router. See BSR (Bootstrap Router)**
- boundary ports (MST)**, 94
- BPDU (bridge protocol data unit)**
 - BPDU Guard, 128–134
 - filtering

F0/21 interface configuration, 139–142
forwarding loops, 142–146
overview of, 135–136
policies, 146–148
router and switch configuration, 136–139

bridge-group 1 command, 132

Broad Band Aggregation, 207

broadcast keyword, 225

broadcast networks (OSPF), 397–410

BSR (Bootstrap Router), 1013

Lo0 interface of R1, 1022–1023

OSPF Area 0 configuration, 1013–1014

PIM sparse mode configuration, 1014–1017

ping command, 1022–1023

primary and backup RP configuration, 1017–1022

C

candidate RPs (rendezvous points), 997–998

Candidate-BSRs, 1019

CCP (Compression Control Protocol), 180

CDP (Cisco Discovery Protocol), 11

CE (customer edge) routers

BGP routing in VPN, 1148–1154

OSPF (Open Shortest Path First), 1136–1141

CEF (Cisco Express Forwarding), 899

Challenge packet (CHAP), 199

Challenge-Handshake Authentication Protocol. *See* CHAP (Challenge-Handshake Authentication Protocol)

CHAP (Challenge-Handshake Authentication Protocol), 198–200

one-way authentication, 198–201

overview of, 175–179

R4, configuring to authenticate R3, 202–207

two-way authentication, 201–202

Cisco Discovery Protocol. *See* CDP (Cisco Discovery Protocol)

Cisco Lab Builder, 5

Class A networks

filtering through IP prefix lists, 269–272

identifying, 271

Class B networks

filtering through IP prefix lists, 272–275

identifying, 274

Class C networks

filtering through IP prefix lists, 275–278

identifying, 276

class of service. *See* COS (class of service)

class-based policing, 898

F0/0 interface on R2, configuring, 903–904

HTTP, FTP, and ICMP traffic, 906–907

MAC address access lists, 904–906

S1/2 interface on R1, configuring, 899–902

class-based shaping, 907–910

classic mode (EIGRP), 337–338

clear ip route command, 608, 616

clients, DHCP, 746–751

Cluster-ID attribute, 642

Code-Reject message, 175

commands

- address-family, 312
- af-interface default, 324
- area 2 nssa, 534
- area range, 473, 783
- autonomous-system, 1108
- bandwidth-percent, 324
- bridge-group 1, 132
- clear ip route, 608, 616
- crypto ipsec transform-set, 921
- debug ip igmp, 968, 973–974
- debug ip ospf lsa-generation, 631
- debug ip pim auto-rp, 999
- debug ip rip, 631
- debug ip route, 574–575
- debug ip routing, 578, 631
- debug ipv6 dhcp, 748, 754
- debug nhrp cache, 248
- debug nhrp packet, 248
- debug ppp authentication, 190, 194, 200, 202
- debug ppp negotiation, 183
- default-metric, 604, 626
- discard-route external 255, 585
- distance, 581
- distribute-list OUT, 494
- distribute-list prefix-list, 836
- eigrp stub, 378–379
- eigrp stub connected, 373–374
- eigrp stub receive-only, 377–378
- eigrp stub redistributed, 376–377
- eigrp stub static, 375–376
- eigrp stub summary, 375
- frame-relay map, 225
- igmp immediate-leave group-list 1, 969
- igmp join-group, 969
- import, 1092
- interface-configuration, 568
- ip address negotiated, 187
- ip helper-address, 212, 752
- ip igmp join-group, 963, 968
- ip igmp limit, 973
- ip igmp querier-timeout, 962
- ip igmp query-interval, 962, 974
- ip igmp query-max-response-time, 962, 976
- ip igmp static-group, 963
- ip local pool, 212
- ip multicast boundary, 1004
- ip nhrp map, 248
- ip nhrp network-id, 265
- ip nhrp nhs, 248, 249
- ip nhrp redirect, 255, 266
- ip nhrp shortcut, 255, 266, 310
- ip ospf demand-circuit, 816
- ip ospf network point-to-point, 770
- ip pim send-rp-announce, 999
- ip routing, 221, 230, 238, 245, 253
- ip summary-address, 257, 262
- ip summary-address eigrp 100 0.0.0.0 0.0.0.0, 304
- IP vrf, 1091
- ipv6 address, 759
- ipv6 address autoconfig default, 748, 750
- ipv6 address dhcp, 750
- ipv6 bandwidth-percent eigrp, 830
- ipv6 dhcp client pd, 758
- ipv6 enable, 748
- ipv6 nd managed-config-flag, 747
- ipv6 nd other-config-flag, 747
- ipv6 nd prefix default no-advertise, 751

ipv6 router ospf, 765
 leak-map, 355
 match ip route-source, 598
 match source-address mac, 904
 metric rib-scale, 340
 mls qos, 853
 mls qos cos 2, 846, 849
 mls qos cos override, 846, 847
 mls qos trust cos, 846, 849
 mls qos trust dscp, 854
 mpls ip, 1033
 mpls label protocol, 1033
 mpls label protocol ldp, 1033
 mpls label range 16 1048575, 1048
 mpls ldp advertise-labels, 1058
 mpls ldp router-id, 1033
 no auto-summary, 312
 no discard-route internal, 585
 no mpls ip propagate-ttl local, 1066
 no peer neighbor-route, 185
 peer default ip address 23.1.1.3
 interface, 187
 peer default ip address pool, 212
 ping, 1022–1023
 ppp authentication chap, 198, 203
 ppp authentication pap, 190
 ppp chap hostname, 199, 203
 ppp chap password, 177
 ppp pap sent-username, 191
 redistribute, 572–573
 redistribute connected, 570, 579
 route-map tst permit 90, 570
 router ospf, 765
 router ospfv3, 765
 Rx(config)#ip multicast-routing, 959
 sh interface, 41, 48
 sh mac address-table dynamic vlan
 21, 48
 sh mac-address-table, 41
 sh spanning-tree, 37
 sh spanning-tree vlan 12 interface
 f0/19 detail, 44
 sh version | inc Base, 37
 show cdp neighbors, 20
 show ip bgp peer-group TST, 641
 show ip eigrp topology 8.8.8.0/24,
 341
 show ip route | include 3.3.3.0, 629
 show ipv6 ospf database, 795
 show ipv6 route, 750
 show ppp all, 193
 show ppp interface, 195
 spanning-tree portfast, 75
 summary-address, 783
 summary-prefix, 783
 traceroute, 613–614
 traceroute 3.3.3.3, 263
 username R4 password Cisco, 203
 VRF definition, 1091
community attribute (BGP), 667–679
 BGP peering, 668–671
 R1 configuration, 672–673
 R2 configuration, 677–679
 R3 configuration, 675–677
 R5 configuration, 674–675
composite metrics, filtering, 602–604
compression (PPP), 179–180
Compression Control Protocol
 (CCP), 180
conditional advertisement, 650–667
 backdoor configuration, 654–658
 IP address, removing from F0/0
 interfaces, 658

- loopback1 interfaces, advertising, 653
- peer session configuration, 650–651
- policies for R1 configuration, 659–667
- R1, R2, and R3 configuration, 651
- RIPv2 and EIGRP 100 configuration, 651–652
- conditional label advertising, 1058–1064
- CONFACK (Configure-Ack) message, 172–175
- confederation (BGP), 731–736
- configuration
 - advertising networks, 381
 - DMVPN, 389–391
 - IP addressing, 387–388
 - OSPF adjacency, 391–397
 - R1 and R4 connections and loopback interfaces, 385–387
 - R4, R5, and R6 connections, 381–385
 - static default routes, 388–389
 - authentication
 - EIGRP AS 100, 360–361
 - HMAC-SHA-256, 362–363
 - MD5, 361
 - router configuration, 359–360
 - topology, 359
 - backdoor links and OSPF, 1123
 - CE (customer edge) router, 1136–1141
 - F0/1 interface of R1 and the G0/1 interface of R7, 1141–1147
 - LDP configuration between core routers, 1128–1132
 - MP-BGP AS 100 configuration between R2 and R6, 1132–1133
 - OSPF configuration on core MPLS routers, 1123–1128
 - RDs (route distinguishers), 1134–1136
 - RTs (route targets), 1134–1136
 - topology, 1123–1125
 - VRF (Virtual Routing and Forwarding), 1134–1136
- BGP
 - BGP routing in VPN, 1148–1154
 - community attribute, 667–679
 - conditional advertisement and BGP backdoor, 650–667
 - confederation, 731–736
 - filtering with access lists and prefix lists, 704–714
 - multi-exit discriminator attribute, 695–703
 - neighbor adjacencies, 635–641
 - AS-path attribute, 679–686
 - regular expressions, 714–731
 - router reflectors, 642–649
 - weight attribute, 686–695
- BPDU filtering
 - F0/21 interface, 139–142
 - forwarding loops, 142–146
 - overview of, 135–136
 - policies, 146–148
 - router and switch configuration, 136–139
- BPDU Guard, 128–134
- BSR, 1013
 - Lo0 interface of R1, 1022–1023
 - OSPF Area 0, 1013–1014

- PIM sparse mode*, 1014–1017
- ping command*, 1022–1023
- primary and backup RPs*, 1017–1022
- class-based policing
 - F0/0 interface on R2*, 903–904
 - HTTP, FTP, and ICMP traffic*, 906–907
 - MAC address access lists*, 904–906
 - overview of*, 898
 - S1/2 interface on R1*, 899–902
- class-based shaping, 907–910
- COS-DSCP mapping
 - F0/1 interface on R2*, 866
 - F0/1 interface on SW1*, 866
 - F0/19 interface SW2*, 866–869
- default route injection, 363–368
- DMVPN Phase 1
 - dynamic mapping*, 229–236
 - static mapping*, 219–229
- DMVPN Phase 2
 - dynamic mapping*, 244–251
 - static mapping*, 236–244
- DMVPN Phase 3
 - hub and spoke configuration*, 255–266
 - interface and router configuration*, 253–255
 - overview of*, 251–252
- DMVPN tunnel protection, 946
 - F0/0 and loopback0 interfaces of R1, R2, and R3*, 947–948
 - hub and spoke configuration*, 948–952
 - IP routing, enabling*, 946–947
 - traffic protection*, 952–958
- DSCP-COS mapping
 - overview of*, 860
 - R1 configuration*, 862
 - R2 configuration*, 861
 - SW2 configuration*, 862–865
- DSCP-Mutation
 - DSCP rewrites, enabling*, 857–860
 - DSCP-mutation map*, 855–857
 - mls qos, enabling on SW2*, 853–854
 - mls qos trust dscp*, 854–855
 - MQC on R1, configuring to mark egress traffic with DSCP value of 1*, 851–852
 - overview of*, 851
- dynamic RP learning and Auto-RP, 993
 - Lo0 interface of R1*, 1006–1010
 - OSPF Area 0*, 994
 - PIM sparse-dense-mode*, 994–997
 - primary and backup RPs*, 997–1003
 - R3 configuration*, 1005–1006
 - RP announcements, filtering on R6*, 1004–1005
- EIGRP basic configuration
 - configuring for future DMVPN spokes*, 304–311
 - DMVPN Phase 1*, 289–292
 - DMVPN Phase 2*, 298–301
 - EIGRP AS 100*, 293–297
 - loopback interfaces*, 301–304
 - static default routes*, 287–289
- EIGRP metrics
 - classic mode*, 337–338
 - EIGRP AS 100*, 334–335

- FD set to Infinity, resolving, 343–348*
- mutual redistribution between RIPv2 and EIGRP, 335–337*
- named mode, 338–341*
- topology, 333*
- Wide Metric support, 341–342*
- EIGRP named mode, 311
 - bandwidth usage, configuring, 324–325*
 - EIGRP 200, 318–319*
 - EIGRP AS 100, 316–317*
 - fixed metric for the EIGRP summary route, 327–328*
 - hello intervals, 323–324*
 - number of received prefixes, limiting, 329–333*
 - OSPF, 319–323*
 - policy for configuring, 311–315*
 - summarization, 325–327*
 - unicast, 317–318*
- EIGRP routing in VPN, 1107–1113
- EIGRP stub
 - EIGRP AS 100, 368–370*
 - eigrp stub connected option, 373–374*
 - eigrp stub option, 378–379*
 - eigrp stub receive-only option, 377–378*
 - eigrp stub redistributed option, 376–377*
 - eigrp stub static option, 375–376*
 - eigrp stub summary option, 375 redistribution, 372–373*
 - static routes, 370–372*
 - summarization, 370*
 - topology, 368*
- EIGRP summarization
 - loopback interfaces for R1, 349–350*
 - loopback interfaces for R2, 350*
 - loopback interfaces for R3, 351*
 - loopback interfaces for R4, 351–353*
 - R1 configuration, 358–359*
 - R2 configuration, 353–356*
 - R3 configuration, 357–358*
 - R4 configuration, 356–357*
 - topology, 349*
- EIGRPv6
 - bandwidth usage, 830*
 - EIGRPv6 AS 100, 819–820*
 - external routes, filtering, 834–837*
 - Hello interval and Hold timer, 825–826*
 - HMAC-SHA-256 authentication, 833–834*
 - loopback1 interface on R1, 830–831*
 - loopback1 interface on R2, 826–829*
 - MD5 authentication, 831–833*
 - OSPFv3 Area 0, 818–819*
 - overview of, 817–818*
 - on R1, R2, R3, and R4, 821–824*
 - redistributing OSPFv3 into, 824–825*
- hostnames, 20
- IGMP, 959
 - F0/0 and F0/1 interface configuration on R1 and R2, 959–962*
 - F0/0 interface configuration on R3 and R4, 963*

- F0/1 interface configuration on R5 and R6, 964*
- G0/1 interface on R7, 965*
- hosts connected to F0/1 on R1, restricting, 965–967*
- hosts connected to F0/1 on R2, stopping multicast traffic with, 967–969*
- mroute states, limiting, 971–974*
- query max response time, 976–977*
- query messages, sending, 969–971*
- querying router and the query interval, 974–976*
- input-interface and match NOT
 - f0/0 interface on R4, configuring, 873–876*
 - overview of, 873*
 - s1/1 interface on R2, configuring, 877–881*
- interfaces, verifying, 9–10
- IP prefix lists, 267
 - allowing only unsubnetted Class B networks, 272–275*
 - allowing only unsubnetted Class C networks, 275–278*
 - allowing unsubnetted Class A networks, plus Class B and C networks, 269–272*
 - basic configuration, 267–269*
 - configuring loopback interfaces, 277–278, 285*
 - denying certain prefixes, 278–281*
 - filtering existing and future host routes, 286*
 - filtering networks with certain prefix lengths, 283–285*
 - injecting default route in EIGRP routing domain, 281–283*
- IP-precedence-DSCP mapping, 870–873
- IPv6 addresses
 - DHCP server configuration, 746–751*
 - SLAAC (stateless address auto-configuration), 743–746*
- LDP, 1026
 - conditional label advertising, 1058–1064*
 - control plane for the 7.7.70/24 prefix, 1051–1057*
 - hello intervals, 1042–1044*
 - hold timer, 1042–1044*
 - labels, 1048–1051*
 - LDP autoconfiguration, enabling, 1068–1071*
 - LDP router ID (RID), 1033*
 - Loopback1 interface of R1, 1044–1048*
 - LSRs (label switch routers), 1033–1037*
 - MLPS structure, biding, 1065–1067*
 - MPLS forwarding, 1034*
 - neighbor discovery, 1037–1042*
 - OSPF Area 0, 1029–1032*
 - serial connection between R3 and R5, 1072–1073*
 - session keepalives, 1044*
 - session protection, 1073–1077*
 - topology, 1026–1029*
 - TTL propagation, testing, 1064–1065*
- LSA Type 4 and FA suppression, 539–548

- LSAs in OSPFv3, 790
 - Intra-Area Prefix LSAs*, 799–800
 - Link LSAs*, 795–799
 - Network LSAs*, 795
 - OSPF Area 0 on DMVPN network*, 813–816
 - OSPF Area 0 on F0/1 and loopback0 interfaces of R1, R2, and R4*, 790–793
 - OSPF Area 13 on S1/3 and loopback13 interfaces of R3*, 800–809
 - OSPF Area 37 on F0/0*, 809–813
 - Router LSAs*, 793–795
- match destination and source address
 - MAC
 - overview of*, 881
 - R2 configuration to classify and mark IP routed traffic*, 882–885
 - RIPv2 configuration*, 881
 - match IP DSCP/Precedence vs. match DSCP, 885–893
 - match protocol HTTP URL, MIME, and Host, 893–898
- MLS QoS
 - f0/1 interface on SW1, configuring to mark ingress traffic with COS marking of 2*, 844–850
 - mls qos, enabling on SW1*, 842–844
 - overview of*, 840
 - R1, configuring to send all traffic with COS marking of 1*, 840–842
- MST, 93–94
 - boundary ports*, 94
 - configuring with policies*, 99–106
 - edge ports*, 94
 - IST (Internal Spanning Tree)*, 95
 - MSTP (Multiple Instance Spanning Tree Protocol)*, 96
 - port configuration*, 96
 - regions*, 94
 - switch hostname configuration*, 96
 - trunking mode*, 97
 - VLAN configuration*, 97–99
- OSPF authentication, 431
 - demand circuits*, 456–457
 - MD5 authentication*, 440–462
 - plaintext authentication*, 433–439
 - router interfaces in Area 0*, 431–433
- OSPF broadcast networks, 397–410
- OSPF filtering, 476
 - loopback interface advertisement*, 501–502
 - loopback interface redistribution*, 493
 - loopback interfaces of R1 and R2*, 481–482
 - LSA flooding, preventing*, 502–504
 - network filtering in Area 0*, 486–488
 - network filtering in Area 0 and Area 2*, 488–490
 - network filtering in Area 2*, 484–486
 - network filtering on all routers except R1*, 490–493

- network filtering on all routers except R5, 494–495*
- network filtering on R1's routing table, 496*
- network filtering on R2, 482–483*
- R1 and R2's directly connected interfaces, 476–478*
- removing, 497–501*
- serial connection between R3 and R4, 478–479*
- serial connection between R4 and R5, 480–481*
- OSPF non-broadcast networks, 411–421
- OSPF point-to-multipoint networks, 425–430
- OSPF point-to-point networks, 421–424
- OSPF routing in VPN, 1113–1122
- OSPF stub, totally stubby, and NSSA areas, 517
 - default route injection, 533–536*
 - loopback interfaces on R5, 532–533*
 - loopback30 interface on R3, 522–523*
 - NSSA configuration, 528–532*
 - R1's directly connected interfaces, 518*
 - R2's directly connected interfaces, 518–519*
 - R3's directly connected interfaces, 519–520*
 - R4's directly connected interfaces, 521–523*
 - stub area configuration, 523–526*
 - totally stubby area configuration, 526–528*
- OSPF suboptimal paths, 549–555
- OSPF summarization
 - advertising networks, 468–469, 472–475*
 - discard routes, 471–472*
 - external route summarization, 467–468*
 - network summarization, 470*
 - R1 configuration, 465–466*
 - R2 configuration, 464–465*
 - R3 configuration, 463–464*
 - R4 configuration, 463*
- OSPFv3, 763–771
- physical-to-logical topology
 - desired topology, 18–19*
 - hostname configuration, 20*
 - port shutdown, 20*
 - VLAN 12, 23–24*
 - VLAN 13, 20–22*
 - VLAN 28, 24–25*
 - VLAN 34, 27–29*
 - VLAN 45, 29–30*
 - VLAN 56, 30–33*
 - VLAN 789, 26–27*
- PPP
 - DHCP server, 212–215*
 - EAP authentication, 216–218*
 - interfaces, 182–186*
 - IP address assignment, 187–190*
 - loopback0 interface, pinging, 186–187*
 - MLPPP (Multilink PPP), 216–218*
 - MPPE protocol and MS-CHAP authentication, 215–218*
 - one-way CHAP authentication, 198–201*

- one-way PAP authentication,*
 - 190–192
- PPPoE (PPP over Ethernet),*
 - 207–212
- R1 and R2 serial interfaces,*
 - 215–218
- R4, configuring to authenticate*
 - R3, 202–207
- two-way CHAP authentication,*
 - 201–202
- two-way PAP authentication,*
 - 192–194
- Rapid STP
 - lab setup,* 75–77
 - link type,* 83–85
 - operational enhancements of,*
 - 74
 - overview of,* 73
 - port roles,* 74
 - port states,* 74
 - rapid convergence mechanisms,*
 - 75, 78–80
 - rapid convergence process,*
 - demonstrating,* 80–83
 - SW2, enabling for RSTP mode,*
 - 89–92
 - switch operation,* 85–89
- redistribution (basic)
 - composite metrics, filtering,*
 - 602–604
 - eigrp 100 redistribution into*
 - ospf 1,* 592–593
 - EIGRP AS 100,* 578–580,
 - 589–590
 - link between R1 and R3,*
 - 567–569
 - loopback interfaces on R2,* 583
 - loopback interfaces on R2/R3,*
 - 575–578
 - loopback interfaces on R3,* 569
 - network 4.4.4.0 /24, filtering on*
 - R2,* 596–597
 - ospf 1 and eigrp 100*
 - redistribution into ospf 36,*
 - 599–602
 - ospf 1 redistribution into eigrp*
 - 100,* 595–596
 - OSPF area 0,* 587–589, 591
 - overview of,* 567
 - R1/R2,* 571–575
 - RIP redistribution into EIGRP,*
 - 580–583
 - RIPv2 redistribution into*
 - OSPF,* 584–586
 - route maps,* 570–571
 - routes originated by R4,*
 - filtering with R5,* 597–599
 - routes tag of 111, configuring*
 - R4 to filter,* 593–594, 595
- RFC 3101 and RFC 1587, 556–566
- RIPv2 and EIGRP redistribution
 - allowing only required routes*
 - to be redistributed,* 617–619
 - control plane mechanism,*
 - 614–615
 - EIGRP AS 100 configuration,*
 - 607–608
 - filtering RIP routes from being*
 - advertised out of F0/1*
 - interface,* 615–617
 - filtering tagged routes,*
 - 619–622
 - loopback0 interface,* 607
 - mutual redistribution between*
 - RIPv2 and EIGRP,* 608–614
 - overview of,* 604–605
 - RIPv2 configuration on R2, R3,*
 - and R4,* 605–606
 - summarization,* 622–625

- RIPv2 and OSPF redistribution
 - mutual redistribution on R1, 629–634*
 - OSPF area 0 configuration on f0/0 interface, 626*
 - overview of, 625–626*
 - RIPv2 configuration on R1, R2, and R3, 626–627*
 - update, invalidation, and flush timer values, 628–629*
- RIPv2 routing in VPN, 1078
 - configuration between R1 and PE-2, 1096–1107*
 - configuration between R7 and PE-6, 1096–1107*
 - LDP configuration on core MPLS routers, 1084–1088*
 - MP-BGP AS 100 configuration on R2 to R6, 1088–1090*
 - OSPF configuration on core MPLS routers, 1081–1083*
 - RDs (route distinguishers), 1091–1095*
 - RTs (route targets), 1091–1095*
 - topology, 1079–1081*
 - VRF (Virtual Routing and Forwarding), 1091–1095*
- site-to-site IPsec VPN, 911
 - GRE/IP with Transport mode, 940–942*
 - GRE/IPsec with Tunnel mode, 937–940*
 - IKE configuration, 913–917*
 - IKE Phase 1 message 1, 917*
 - IKE Phase 1 message 2, 918–919*
 - IKE Phase 1 message 3, 919*
 - IKE Phase 1 message 4, 919–920*
 - IKE Phase 1 message 5, 920*
 - IKE Phase 1 message 6, 920–921*
 - IKE Phase 2 message 1, 921–925*
 - ISAKMP, 912*
 - and NAT, 925–930*
 - non-scalable configuration, 930–937*
 - OAKLEY, 912–913*
 - policy guidelines, 912*
 - S-VTI, 942–946*
- Spanning Tree Backbone Fast, 148–154
- Spanning Tree Loop Guard, 162–167
- Spanning Tree Portfast, 106–115
- Spanning Tree Root Guard, 154–162
- static RP, 977
 - PIM sparse mode, 983–985*
 - R2 and R3 configuration, 986–991*
 - S1/4 interface on R5, 991–993*
 - topology, 981–983*
- STP
 - designated ports, moving, 43–45*
 - initial configuration, 36–41*
 - overview of, 50*
 - policy, 59–64*
 - root bridge, 56–59, 65–67*
 - root primary macro, 46–48*
 - spanning-tree cost on port in VLAN 12, raising, 41–42*
 - spanning-tree port ID, raising, 48–49*
 - switch hostnames, 51–52*
 - switches, 54–55*
 - trunk port, 52–54*

- VLAN 100, 200, 300, and 400
creation, 55–56
 - VLAN 500 creation, 67–70
 - VLAN 600 creation, 70–73
 - summarization of internal/external
networks
 - discard routes, 786–789
 - external route summarization,
782–786
 - loopback interface
summarization, 778–782
 - OSPFv3 configuration,
771–778
 - overview of, 771
 - UplinkFast, 115–128
 - virtual links and GRE tunnels
 - GRE tunnel configuration,
513–516
 - OSPF configuration, 506–509
 - overview of, 504–506
 - virtual link configuration,
509–513
 - VLANs, 12
 - Configure-Ack (CONFACK) message,
172–175
 - Configure-Nak (CONFNAK) message,
173–175
 - Configure-Reject (CONFREJ)
message, 174–175
 - Configure-Request (CONFREQ)
message, 172–175
 - CONFNAK (Configure-Nak) message,
173–175
 - CONFREJ (Configure-Reject)
message, 174–175
 - CONFREQ (Configure-Request)
message, 172–175
 - contiguous identical bits, 279–280
 - Control field (PPP), 170–171
 - control plane, 171
 - authentication, 175–177
 - examining, 1051–1057
 - LCP (Link Control Protocol),
171–175
 - NCPs (Network Control Protocols),
177–179
 - COS (class of service)
 - COS-DSCP mapping
 - R2 F0/1 interface, configuring,
866
 - SW1 F0/1 interface,
configuring, 866
 - SW2 F0/19 interface,
configuring, 866–869
 - DSCP-COS mapping
 - overview of, 860
 - R1 configuration, 862
 - R2 configuration, 861
 - SW2 configuration, 862–865
 - CRC (cyclic redundancy check), 171
 - crypto ipsec transform-set command,
921
 - customer edge (CE) routers
 - BGP routing in VPN, 1148–1154
 - OSPF (Open Shortest Path First),
1136–1141
 - cyclic redundancy check (CRC), 171
- ## D
-
- DAD (Duplicate Address Protection),
748
 - databases
 - filtering. *See* filtering
 - verifying, 11–12
 - debug ip igmp command, 968,
973–974

- debug ip ospf lsa-generation command, 631
- debug ip pim auto-rp command, 999
- debug ip rip command, 631
- debug ip route command, 574–575
- debug ip routing command, 578, 631
- debug ipv6 dhcp command, 748, 754
- debug nhrp cache command, 248
- debug nhrp packet command, 248
- debug output (RSTP)
 - link type, 83–85
 - rapid convergence mechanisms, 78–80
 - rapid convergence process, demonstrating, 80–83
 - switch operation, 85–89
- debug ppp authentication command, 190, 194, 200, 202
- debug ppp negotiation command, 183
- DEFAULT distribute list, 284–285
- default route injection
 - configuration, 364–368
 - DMVPN Phase 1 using static mapping, 220–239
 - EIGRP AS 100, 363–364
 - EIGRP routing domain, 281–283
 - OSPF (Open Shortest Path First), 533–536
 - overview of, 363
- default-metric command, 604, 626
- delay (DLY), 338
- demand circuits, 456–457
- dense mode (PIM), 959–962, 994–997
- denying. *See* filtering
- designated ports, moving, 43–45
- destination keyword, 752
- DH (Diffie-Hellman) groups, 912
- DHCP (Dynamic Host Configuration Protocol)
 - client configuration, 746–751
 - prefix delegation, 755–763
 - server configuration, 212–215, 746–751
- Dialer interface, 208–209
- Differential Service Code Point. *See* DSCP (Differential Service Code Point)
- Diffie-Hellman (DH) groups, 912
- disabling
 - debug command, 575
 - Spanning Tree Portfast, 114–115
- discard routes, 471–472, 786–789
- discard-route external 255 command, 585
- discovery, neighbor, 739–743, 1037–1042
- Discovery stage (PPPoE), 181–182
- distance command, 581
- distribute-list OUT command, 494
- distribute-list prefix-list command, 836
- DLY (delay), 338
- DMVPNs (dynamic multipoint virtual private networks)
 - configuration, 389–391
 - configuring for EIGRP
 - DMVPN Phase 1*, 289–292
 - DMVPN Phase 2*, 298–301
 - DMVPN Phase 1 using dynamic mapping
 - hub and spoke configuration*, 232–236
 - interface and router configuration*, 229–232
 - overview of*, 229

DMVPN Phase 1 using static mapping

hub and spoke configuration, 223–229

interface and router configuration, 220–239

NHRP (Next-Hop Resolution Protocol), 223

overview of, 219

DMVPN Phase 2 using dynamic mapping

hub and spoke configuration, 247–251

interface and router configuration, 245–247

overview of, 244

DMVPN Phase 2 using static mapping

hub and spoke configuration, 240–244

interface and router configuration, 237–240

overview of, 236–237

DMVPN Phase 3

hub and spoke configuration, 255–266

interface and router configuration, 253–255

overview of, 251–252

overview of, 219

tunnels, protecting, 946

F0/0 and loopback0 interfaces of R1, R2, and R3, 947–948

hub and spoke configuration, 948–952

IP routing, enabling, 946–947

traffic protection, 952–958

DSCP (Differential Service Code Point)

class-based policing

F0/0 interface on R2, configuring, 903–904

HTTP, FTP, and ICMP traffic, 906–907

MAC address access lists, 904–906

overview of, 898

S1/2 interface on R1, configuring, 899–902

class-based shaping, 907–910

COS-DSCP mapping

F0/1 interface on R2, configuring, 866

F0/1 interface on SW1, configuring, 866

F0/19 interface SW2, configuring, 866–869

DSCP-COS mapping

overview of, 860

R1 configuration, 862

R2 configuration, 861

SW2 configuration, 862–865

DSCP-Mutation

DSCP rewrites, enabling, 857–860

DSCP-mutation map configuration, 855–857

mls qos, enabling on SW2, 853–854

mls qos trust dscp configuration, 854–855

MQC on R1, configuring to mark egress traffic with DSCP value of 1, 851–852

overview of, 851

- IP-precedence-DSCP mapping, 870–873
- match IP DSCP/Precedence vs. match DSCP, 885–893
- rewrites, enabling, 857–860
- duplicate address protection, 740–741, 744**
- Duplicate Address Protection (DAD), 748**
- Dynamic Host Configuration Protocol. *See* DHCP (Dynamic Host Configuration Protocol)**
- dynamic mapping, DMVPN Phase 1 using**
 - hub and spoke configuration, 232–236
 - interface and router configuration, 229–232
 - overview of, 229
- dynamic multipoint virtual private networks. *See* DMVPNs (dynamic multipoint virtual private networks)**
- dynamic RP learning and Auto-RP, 993**
 - Lo0 interface of R1, 1006–1010
 - OSPF Area 0 configuration, 994
 - PIM sparse-dense-mode configuration, 994–997
 - primary and backup RP configuration, 997–1003
 - R3 configuration, 1005–1006
 - RP announcements, filtering on R6, 1004–1005

E

- EAP (Extensible Authentication Protocol)**
 - configuration, 216–218
 - overview of, 175–176

- Echo-Reply message, 175**
- Echo-Request message, 175**
- edge ports, 75, 94**
- EIGRP (Enhanced Interior Gateway Routing Protocol)**
 - authentication
 - EIGRP AS 100 configuration, 360–361*
 - HMAC-SHA-256, 362–363*
 - MD5, 361*
 - router configuration, 359–360*
 - topology, 359*
 - basic configuration
 - configuring for future DMVPN spokes, 304–311*
 - DMVPN Phase 1, 289–292*
 - DMVPN Phase 2, 298–301*
 - EIGRP AS 100, 293–297*
 - loopback interfaces, 301–304*
 - static default routes, 287–289*
 - default route injection
 - configuration, 364–368*
 - EIGRP AS 100, 363–364*
 - overview of, 363*
 - EIGRP AS 100 configuration, 578–580, 589–590*
 - EIGRPv6**
 - bandwidth usage, configuring, 830*
 - configuration on R1, R2, R3, and R4, 821–824*
 - EIGRPv6 AS 100 configuration, 819–820*
 - external routes, filtering, 834–837*
 - Hello interval and Hold timer, 825–826*

- HMAC-SHA-256 authentication*, 833–834
- loopback1 interface on R1*, 830–831
- loopback1 interface on R2*, 826–829
- MD5 authentication*, 831–833
- OSPFv3 Area 0*, 818–819
- overview of*, 817–818
- redistributing OSPFv3 into*, 824–825
- metrics, 604
 - classic mode configuration*, 337–338
 - EIGRP AS 100 configuration*, 334–335
 - FD set to Infinity, resolving*, 343–348
 - mutual redistribution between RIPv2 and EIGRP*, 335–337
 - named mode configuration*, 338–341
 - topology*, 333
 - Wide Metric support*, 341–342
- named mode
 - bandwidth usage, configuring*, 324–325
 - EIGRP 200 configuration*, 318–319
 - EIGRP AS 100 configuration*, 316–317
 - fixed metric for the EIGRP summary route*, 327–328
 - hello intervals*, 323–324
 - number of received prefixes, limiting*, 329–333
 - OSPF configuration*, 319–323
 - overview of*, 311
 - policy for configuring*, 311–315
 - summarization*, 325–327
 - unicast configuration*, 317–318
- redistribution
 - eigrp 100 redistribution into ospf 1*, 592–593
 - network 4.4.4.0 /24, filtering on R2*, 596–597
 - ospf 1 and eigrp 100 redistribution into ospf 36*, 599–602
 - ospf 1 redistribution into eigrp 100*, 595–596
 - overview of*, 604–605
 - RIP redistribution into EIGRP*, 580–583
 - routes originated by R4, filtering with R5*, 597–599
- RIPv2 and EIGRP redistribution
 - allowing only required routes to be redistributed*, 617–619
 - control plane mechanism*, 614–615
 - EIGRP AS 100 configuration*, 607–608
 - filtering RIP routes from being advertised out of F0/1 interface*, 615–617
 - filtering tagged routes*, 619–622
 - loopback0 interface*, 607
 - mutual redistribution between RIPv2 and EIGRP*, 608–614
 - summarization*, 622–625
- routing domain, injecting default route into, 281–283
- stub
 - EIGRP AS 100 configuration*, 368–370
 - eigrp stub connected option*, 373–374

- eigrp stub option*, 378–379
 - eigrp stub receive-only option*, 377–378
 - eigrp stub redistributed option*, 376–377
 - eigrp stub static option*, 375–376
 - eigrp stub summary option*, 375
 - redistribution*, 372–373
 - static routes*, 370–372
 - summarization*, 370
 - topology*, 368
 - summarization
 - loopback interfaces for R1*, 349–350
 - loopback interfaces for R2*, 350
 - loopback interfaces for R3*, 351
 - loopback interfaces for R4*, 351–353
 - R1 configuration*, 358–359
 - R2 configuration*, 353–356
 - R3 configuration*, 357–358
 - R4 configuration*, 356–357
 - topology*, 349
 - in VPN, 1107–1113
 - eigrp stub command**, 378–379
 - eigrp stub connected command**, 373–374
 - eigrp stub receive-only command**, 377–378
 - eigrp stub redistributed command**, 376–377
 - eigrp stub static command**, 375–376
 - eigrp stub summary command**, 375
 - enabling. *See* configuration
 - encryption, MPPE (Microsoft Point-to-Point Encryption), 215–218
 - Enhanced Interior Gateway Routing Protocol**. *See* EIGRP (Enhanced Interior Gateway Routing Protocol)
 - establishing PPP (Point-to-Point Protocol) sessions**
 - Authentication Phase, 175–177
 - Link Establishment Phase, 171–175
 - Network Layer Protocol Phase, 177–179
 - Ethernet, PPP over**. *See* PPPoE (PPP over Ethernet)
 - EUI-64 addressing**, 737–739
 - expressions, regular**. *See* regular expressions
 - Extensible Authentication Protocol**. *See* EAP (Extensible Authentication Protocol)
 - external network summarization**
 - discard routes, 786–789
 - external route summarization, 782–786
 - loopback interface summarization, 778–782
 - OSPFv3 configuration, 771–778
 - overview of, 771
 - external routes**
 - filtering, 834–837
 - summarization, 467–468, 782–786
- ## F
-
- FA (forward address), suppressing**, 539–548
 - FD set to Infinity, resolving**, 343–348
 - FEC (forwarding equivalence class)**, 1025
 - filtering**
 - with access lists and prefix lists, 704–714

BPDU filtering

F0/21 interface configuration, 139–142

forwarding loops, 142–146

overview of, 135–136

policies, 146–148

router and switch configuration, 136–139

composite metrics, 602–604

with IP prefix lists, 267

allowing only unsubnetted Class B networks, 272–275

allowing only unsubnetted Class C networks, 275–278

allowing unsubnetted Class A networks, plus Class B and C networks, 269–272

basic configuration, 267–269

denying certain prefixes, 278–281

filtering existing and future host routes, 286

filtering networks with certain prefix lengths, 283–285

injecting default route in EIGRP routing domain, 281–283

loopback interfaces, 277–278, 285

network 4.4.4.0 /24 on R2, 596–597

OSPF (Open Shortest Path First), 476

loopback interface advertisement, 501–502

loopback interface redistribution, 493

loopback interfaces of R1 and R2, 481–482

LSA flooding, preventing, 502–504

network filtering in Area 0, 486–488

network filtering in Area 0 and Area 2, 488–490

network filtering in Area 2, 484–486

network filtering on all routers except R1, 490–493

network filtering on all routers except R5, 494–495

network filtering on R1's routing table, 496

network filtering on R2, 482–483

R1 and R2's directly connected interfaces, 476–478

removing, 497–501

serial connection between R3 and R4, 478–479

serial connection between R4 and R5, 480–481

prefixes

advertising of prefixes originating in own AS, 721–723

prefixes from directly connected neighbors, 725–726

prefixes originating in AS 200, 723–725

prefixes originating in AS 300, 717–719, 727–728

prefixes with AS 300 in path list, 719–721

prefixes with prepended AS numbers, 728–731

routes, 593–595, 597–599

RP announcements, 1004–1005

tagged routes, 619–622

Flag field (PPP), 170–171

flooding (LSA), 502–504
 flush timer, 628–629
 forward address (FA), suppressing,
 539–548
 forwarding equivalence class (FEC),
 1025
 Forwarding Information Base, 306
 forwarding loops (BPDU),
 142–146
 frame format (PPP), 170–171
 frame-relay map command, 225
 FSC field (PPP), 171
 future host routes, denying, 286

G

GDOI (group domain of
 interpretation), 914
 Generic Routing Encapsulation
 (GRE), 223
 Global IGMP State Limiter, 971
 GRE (Generic Routing Encapsulation)
 GRE/IPSec
 Transport mode, 940–942
 Tunnel mode, 937–940
 overview of, 223
 tunnels
 configuration, 513–516
 overview of, 504–506
 group domain of interpretation
 (GDOI), 914

H

Hashed Message Authentication
 Code-Secure Hash Algorithm-256,
 362–363

hashing, 176
 HDLC (High-Level Data Link
 Control), 169–170
 header compression, 179–180
 Hello interval
 EIGRP (Enhanced Interior Gateway
 Routing Protocol), 323–324,
 825–826
 LDP (Label Distribution Protocol)
 configuration, 1042–1044
 hiding MPLS structure,
 1065–1067
 High-Level Data Link Control
 (HDLC), 169–170
 HMAC-SHA-256 authentication,
 362–363, 833–834
 Hold timer, 825–826,
 1042–1044
 hop count (SIT), 95
 host routes, denying, 286
 hostnames
 configuration, 20
 switch hostnames, 51–52, 96
 hosts
 auto-configuration, 740
 match protocol HTTP URL, MIME,
 and Host, 893–898
 HTTP URL, 893–898
 hubs (DMVPN)
 DMVPN Phase 1
 dynamic mapping, 232–236
 static mapping, 223–229
 DMVPN Phase 2
 dynamic mapping, 247–251
 static mapping, 240–244
 DMVPN Phase 3, 255–266

icmp rate-limit parameter, 616

IGMP (Internet Group Management Protocol), 959

F0/0 and F0/1 interface configuration on R1 and R2, 959–962

F0/0 interface configuration on R3 and R4, 963

F0/1 interface configuration on R5 and R6, 964

G0/1 interface on R7, 965

hosts connected to F0/1 on R1, restricting, 965–967

hosts connected to F0/1 on R2, stopping multicast traffic with, 967–969

mroute states, limiting, 971–974

query max response time, 976–977

query messages, sending, 969–971

querying router and the query interval, 974–976

igmp immediate-leave group-list 1 command, 969

igmp join-group command, 969

IKE (Internet Key Exchange), 911

Phase 1

configuration, 913–917

message 1, 917, 921–925

message 2, 918–919

message 3, 919

message 4, 919–920

message 5, 920

message 6, 920–921

Phase 2, 914–917

import command, 1092

include-connected keyword, 825

Infinity, FD set to, 343–348

Information field (PPP), 171

interface configuration, verifying, 9–10

interface-configuration command, 568

interfaces. *See also* loopback interfaces

Dialer, 208–209

DMVPNs (dynamic multipoint virtual private networks)

DMVPN Phase 1 using dynamic mapping, 229–232

DMVPN Phase 1 using static mapping, 220–239

DMVPN Phase 2 using dynamic mapping, 245–247

DMVPN Phase 2 using static mapping, 237–240

DMVPN Phase 3, 253–255

PPP (Point-to-Point Protocol)

configuration, 182–186

DHCP server configuration, 212–215

EAP authentication, 216–218

IP address assignment, 187–190

MLPPP (Multilink PPP), 216–218

MPPE protocol and MS-CHAP authentication, 215–218

one-way CHAP authentication, 198–201

one-way PAP authentication, 190–192

PPPoE (PPP over Ethernet), 207–212

R1 and R2 serial interface configuration, 215–218

R4, configuring to authenticate R3, 202–207

- two-way CHAP authentication*, 201–202
 - two-way PAP authentication*, 192–194
- trunk interfaces, verifying, 12–13
- Virtual-Template, 207
- internal network summarization**
 - discard routes, 786–789
 - external route summarization, 782–786
 - loopback interface summarization, 778–782
 - OSPFv3 configuration, 771–778
 - overview of, 771
- Internal Spanning Tree (IST)**, 95
- Internet Group Management.**
 - See* IGMP (Internet Group Management Protocol)
- Internet Key Exchange.** *See* IKE (Internet Key Exchange)
- Internet Security Association and Key Management Protocol (ISAKMP)**, 911, 912
- intervals**
 - Hello interval
 - EIGRP (Enhanced Interior Gateway Routing Protocol)*, 323–324, 825–826
 - LDP (Label Distribution Protocol) configuration*, 1042–1044
 - query interval (IGMP), 974–976
- Intra-Area Prefix LSAs**, 799–800
- ip address negotiated command**, 187
- IP CEF**, 899
- IP DSCP/Precedence**, 881
- ip helper-address command**, 212, 752
- ip igmp join-group command**, 963, 968
- ip igmp limit command**, 973
- ip igmp querier-timeout command**, 962
- ip igmp query-interval command**, 962, 974
- ip igmp query-max-response-time command**, 962, 976
- ip igmp static-group command**, 963
- ip local pool command**, 212
- ip multicast boundary command**, 1004
- ip nhrp map command**, 248
- ip nhrp network-id command**, 265
- ip nhrp nhs command**, 248, 249
- ip nhrp redirect command**, 255, 266
- ip nhrp shortcut command**, 255, 266, 310
- ip ospf demand-circuit command**, 816
- ip ospf network point-to-point command**, 770
- ip pim send-rp-announce command**, 999
- IP prefix list configuration**, 267
 - allowing only unsubnetted Class B networks, 272–275
 - allowing only unsubnetted Class C networks, 275–278
 - allowing unsubnetted Class A networks, plus Class B and C networks, 269–272
 - basic configuration, 267–269
 - configuring loopback interfaces, 277–278, 285
 - denying certain prefixes, 278–281
 - filtering existing and future host routes, 286
 - filtering networks with certain prefix lengths, 283–285
 - injecting default route in EIGRP routing domain, 281–283

- ip routing command, 221, 230, 238, 245, 253
- ip summary-address command, 257, 262
- ip summary-address eigrp 100 0.0.0.0 0.0.0.0 command, 304
- IP vrf command, 1091
- IP-precedence-DSCP mapping, 870–873
- IPSec VPN
 - basic site-to-site IPSec VPN, 911
 - GRE/IP with Transport mode*, 940–942
 - GRE/IPSec with Tunnel mode*, 937–940
 - IKE configuration*, 913–917
 - IKE Phase 1 message 1*, 917
 - IKE Phase 1 message 2*, 918–919
 - IKE Phase 1 message 3*, 919
 - IKE Phase 1 message 4*, 919–920
 - IKE Phase 1 message 5*, 920
 - IKE Phase 1 message 6*, 920–921
 - IKE Phase 2 message 1*, 921–925
 - ISAKMP, 912
 - and NAT*, 925–930
 - non-scalable configuration*, 930–937
 - OAKLEY, 912–913
 - policy guidelines*, 912
 - S-VTI, 942–946
- DMVPN tunnels, protecting, 946
 - F0/0 and loopback0 interfaces of R1, R2, and R3*, 947–948
 - hub and spoke configuration*, 948–952
 - IP routing, enabling*, 946–947
 - traffic protection*, 952–958
- overview of, 911
- IPv4 addresses, 36
 - assigning, 187–190
 - configuration, 387–388
- IPv6
 - addresses, acquiring
 - DHCP client/server configuration*, 746–751
 - DHCP prefix delegation*, 755–763
 - modified EUI-64 addressing*, 737–739
 - neighbor discovery*, 739–743
 - overview of*, 737
 - R2 configuration*, 751–754
 - R5 configuration*, 754–755
 - SLAAC (stateless address auto-configuration)*, 743–746
- EIGRPv6
 - bandwidth usage, configuring*, 830
 - configuration on R1, R2, R3, and R4*, 821–824
 - EIGRPv6 AS 100 configuration*, 819–820
 - external routes, filtering*, 834–837
 - Hello interval and Hold timer*, 825–826
 - HMAC-SHA-256 authentication*, 833–834
 - loopback1 interface on R1*, 830–831
 - loopback1 interface on R2*, 826–829
 - MD5 authentication*, 831–833

- OSPFv3 Area 0 configuration, 818–819
 - overview of, 817–818
 - redistributing OSPFv3 into, 824–825
 - LSAs in OSPFv3, 790
 - Intra-Area Prefix LSAs, 799–800
 - Link LSAs, 795–799
 - Network LSAs, 795
 - OSPF Area 0 on DMVPN network, 813–816
 - OSPF Area 0 on F0/1 and loopback0 interfaces of R1, R2, and R4, 790–793
 - OSPF Area 13 on S1/3 and loopback13 interfaces of R3, 800–809
 - OSPF Area 37 on F0/0, 809–813
 - Router LSAs, 793–795
 - OSPFv3 configuration, 763–771
 - summarization of internal/external networks
 - discard routes, 786–789
 - external route summarization, 782–786
 - loopback interface summarization, 778–782
 - OSPFv3 configuration, 771–778
 - overview of, 771
 - ipv6 address autoconfig default command, 748, 750
 - ipv6 address command, 759
 - ipv6 address dhcp command, 750
 - ipv6 bandwidth-percent eigrp command, 830
 - ipv6 dhcp client pd command, 758
 - ipv6 enable command, 748
 - ipv6 nd managed-config-flag command, 747
 - ipv6 nd other-config-flag command, 747
 - ipv6 nd prefix default no-advertise command, 751
 - ipv6 router ospf command, 765
 - ISAKMP (Internet Security Association and Key Management Protocol), 911, 912
 - IST (Internal Spanning Tree), 95
- ## J-K-L
- Lab Builder, 5
 - Label Forwarding Information Base (LFIB), 1073
 - Label Information Base (LIB), 1073
 - label switch routers. *See* LSRs (label switch routers)
 - labels
 - advertising, 1105
 - assignment, 1105
 - conditional label advertising, 1058–1064
 - configuration, 1048–1051
 - labs
 - advanced STP
 - overview of, 50
 - policy configuration, 59–64
 - root bridge configuration, 56–59, 65–67
 - switch configuration, 54–55
 - switch hostname configuration, 51–52
 - trunk port configuration, 52–54

- VLAN 100, 200, 300, and 400 creation, 55–56
- VLAN 500 creation, 67–70
- VLAN 600 creation, 70–73
- advertising networks, 381
 - DMVPN configuration, 389–391
 - IP addressing, 387–388
 - OSPF adjacency, 391–397
 - R1 and R4 connections and loopback interfaces, 385–387
 - R4, R5, and R6 connections, 381–385
 - static default routes, 388–389
- authentication
 - EIGRP AS 100 configuration, 360–361
 - HMAC-SHA-256, 362–363
 - MD5, 361
 - router configuration, 359–360
 - topology, 359
- backdoor links and OSPF, 1123
 - CE (customer edge) router configuration, 1136–1141
 - F0/1 interface of R1 and the G0/1 interface of R7, 1141–1147
 - LDP configuration between core routers, 1128–1132
 - MP-BGP AS 100 configuration between R2 and R6, 1132–1133
 - OSPF configuration on core MPLS routers, 1123–1128
 - RDs (route distinguishers), 1134–1136
 - RTs (route targets), 1134–1136
 - topology, 1123–1125
- VRF (Virtual Routing and Forwarding), 1134–1136
- basic redistribution 1
 - EIGRP AS 100, 578–580
 - link between R1 and R3, 567–569
 - loopback interfaces on R2, 583
 - loopback interfaces on R2/R3, 575–578
 - loopback interfaces on R3, 569
 - overview of, 567
 - R1/R2, 571–575
 - RIP redistribution into EIGRP, 580–583
 - RIPv2 redistribution into OSPF, 584–586
 - route maps, 570–571
- basic redistribution 2
 - composite metrics, filtering, 602–604
 - eigrp 100 redistribution into ospf 1, 592–593
 - EIGRP AS 100, 589–590
 - network 4.4.4.0 /24, filtering on R2, 596–597
 - ospf 1 and eigrp 100 redistribution into ospf 36, 599–602
 - ospf 1 redistribution into eigrp 100, 595–596
 - OSPF area 0, 587–589, 591
 - overview of, 586
 - routes originated by R4, filtering with R5, 597–599
 - routes tag of 111, configuring R4 to filter, 593–594, 595
- basic site-to-site IPsec VPN, 911
 - IKE configuration, 913–917
 - IKE Phase 1 message 1, 917

- IKE Phase 1 message 2, 918–919
- IKE Phase 1 message 3, 919
- IKE Phase 1 message 4, 919–920
- IKE Phase 1 message 5, 920
- IKE Phase 1 message 6, 920–921
- IKE Phase 2 message 1, 921–925
- ISAKMP, 912
- OAKLEY, 912–913
 - policy guidelines, 912
- basic site-to-site IPSec VPN and NAT, 925–930
- basic STP
 - designated ports, moving, 43–45
 - initial configuration, 36–41
 - root primary macro configuration, 46–48
 - spanning-tree cost on port in VLAN 12, raising, 41–42
 - spanning-tree port ID, raising, 48–49
- BGP (Border Gateway Protocol)
 - BGP confederation, 731–736
 - community attribute, 667–679
 - conditional advertisement and BGP backdoor, 650–667
 - filtering with access lists and prefix lists, 704–714
 - multi-exit discriminator attribute, 695–703
 - neighbor adjacencies, establishing, 635–641
 - AS-path attribute, 679–686
 - regular expressions, 714–731
 - router reflectors, 642–649
 - weight attribute, 686–695
- BGP routing in VPN, 1148–1154
- BPDU filtering
 - F0/21 interface configuration, 139–142
 - forwarding loops, 142–146
 - overview of, 135–136
 - policies, 146–148
 - router and switch configuration, 136–139
- BPDU Guard, 128–134
- BSR (Bootstrap Router), 1013
 - Lo0 interface of R1, 1022–1023
 - OSPF Area 0 configuration, 1013–1014
 - PIM sparse mode configuration, 1014–1017
 - ping command, 1022–1023
 - primary and backup RP configuration, 1017–1022
- class-based policing
 - F0/0 interface on R2, configuring, 903–904
 - HTTP, FTP, and ICMP traffic, 906–907
 - MAC address access lists, 904–906
 - overview of, 898
 - S1/2 interface on R1, configuring, 899–902
- class-based shaping, 907–910
- COS-DSCP mapping
 - F0/1 interface on R2, configuring, 866
 - F0/1 interface on SW1, configuring, 866
 - F0/19 interface SW2, configuring, 866–869
- default route injection
 - configuration, 364–368

- EIGRP AS 100*, 363–364
 - overview of*, 363
- DMVPN Phase 1 using dynamic mapping
 - hub and spoke configuration*, 232–236
 - interface and router configuration*, 229–232
 - overview of*, 229
- DMVPN Phase 1 using static mapping
 - hub and spoke configuration*, 223–229
 - interface and router configuration*, 220–239
 - NHRP (Next-Hop Resolution Protocol)*, 223–225
 - overview of*, 219
- DMVPN Phase 2 using dynamic mapping
 - hub and spoke configuration*, 247–251
 - interface and router configuration*, 245–247
 - overview of*, 244
- DMVPN Phase 2 using static mapping
 - hub and spoke configuration*, 240–244
 - interface and router configuration*, 237–240
 - overview of*, 236–237
- DMVPN Phase 3
 - hub and spoke configuration*, 255–266
 - interface and router configuration*, 253–255
 - overview of*, 251–252
- DMVPN tunnels, protecting, 946
- F0/0 and loopback0 interfaces of R1, R2, and R3*, 947–948
- hub and spoke configuration*, 948–952
- IP routing, enabling*, 946–947
- traffic protection*, 952–958
- DSCP-COS mapping
 - overview of*, 860
 - R1 configuration*, 862
 - R2 configuration*, 861
 - SW2 configuration*, 862–865
- DSCP-Mutation
 - DSCP rewrites, enabling*, 857–860
 - DSCP-mutation map configuration*, 855–857
 - mls qos, enabling on SW2*, 853–854
 - mls qos trust dscp configuration*, 854–855
 - MQC on R1, configuring to mark egress traffic with DSCP value of 1*, 851–852
 - overview of*, 851
- dynamic RP learning and Auto-RP, 993
 - Lo0 interface of R1*, 1006–1010
 - OSPF Area 0 configuration*, 994
 - PIM sparse-dense-mode configuration*, 994–997
 - primary and backup RP configuration*, 997–1003
 - R3 configuration*, 1005–1006
 - RP announcements, filtering on R6*, 1004–1005
- EIGRP basic configuration
 - configuring for future DMVPN spokes*, 304–311

- DMVPN Phase 1*, 289–292
- DMVPN Phase 2*, 298–301
- EIGRP AS 100*, 293–297
- loopback interfaces*, 301–304
- static default routes*, 287–289
- EIGRP metrics
 - classic mode configuration*, 337–338
 - EIGRP AS 100 configuration*, 334–335
 - FD set to Infinity, resolving*, 343–348
 - mutual redistribution between RIPv2 and EIGRP*, 335–337
 - named mode configuration*, 338–341
 - topology*, 333
 - Wide Metric support*, 341–342
- EIGRP named mode, 311
 - bandwidth usage, configuring*, 324–325
 - EIGRP 200 configuration*, 318–319
 - EIGRP AS 100 configuration*, 316–317
 - fixed metric for the EIGRP summary route*, 327–328
 - hello intervals*, 323–324
 - number of received prefixes, limiting*, 329–333
 - OSPF configuration*, 319–323
 - policy for configuring*, 311–315
 - summarization*, 325–327
 - unicast configuration*, 317–318
- EIGRP routing in VPN, 1107–1113
- EIGRP stub
 - EIGRP AS 100 configuration*, 368–370
 - eigrp stub connected option*, 373–374
 - eigrp stub option*, 378–379
 - eigrp stub receive-only option*, 377–378
 - eigrp stub redistributed option*, 376–377
 - eigrp stub static option*, 375–376
 - eigrp stub summary option*, 375
 - redistribution*, 372–373
 - static routes*, 370–372
 - summarization*, 370
 - topology*, 368
- EIGRP summarization
 - loopback interfaces for R1*, 349–350
 - loopback interfaces for R2*, 350
 - loopback interfaces for R3*, 351
 - loopback interfaces for R4*, 351–353
 - R1 configuration*, 358–359
 - R2 configuration*, 353–356
 - R3 configuration*, 357–358
 - R4 configuration*, 356–357
 - topology*, 349
- EIGRPv6
 - bandwidth usage, configuring*, 830
 - configuration on R1, R2, R3, and R4*, 821–824
 - EIGRPv6 AS 100 configuration*, 819–820
 - external routes, filtering*, 834–837
 - Hello interval and Hold timer*, 825–826

- HMAC-SHA-256 authentication*, 833–834
- loopback1 interface on R1*, 830–831
- loopback1 interface on R2*, 826–829
- MD5 authentication*, 831–833
- OSPFv3 Area 0 configuration*, 818–819
- overview of*, 817–818
- redistributing OSPFv3 into*, 824–825
- GRE/IPSec Tunnel mode, Transport mode, and S-VTI
 - GRE/IP with Transport mode*, 940–942
 - GRE/IPSec with Tunnel mode configuration*, 937–940
 - non-scalable configuration*, 930–937
 - S-VTI*, 942–946
- How Is This Possible? 536–538
- IGMP (Internet Group Management Protocol), 959
 - F0/0 and F0/1 interface configuration on R1 and R2*, 959–962
 - F0/0 interface configuration on R3 and R4*, 963
 - F0/1 interface configuration on R5 and R6*, 964
 - G0/1 interface on R7*, 965
 - hosts connected to F0/1 on R1, restricting*, 965–967
 - hosts connected to F0/1 on R2, stopping multicast traffic with*, 967–969
 - mroute states, limiting*, 971–974
 - query max response time*, 976–977
 - query messages, sending*, 969–971
 - querying router and the query interval*, 974–976
- input-interface and match NOT
 - f0/0 interface on R4, configuring*, 873–876
 - overview of*, 873
 - s1/1 interface on R2, configuring*, 877–881
- introductory lab, 8–17
- IP-precedence-DSCP mapping, 870–873
- IPv6 addresses, acquiring
 - DHCP client/server configuration*, 746–751
 - DHCP prefix delegation*, 755–763
 - modified EUI-64 addressing*, 737–739
 - neighbor discovery*, 739–743
 - overview of*, 737
 - R2 configuration*, 751–754
 - R5 configuration*, 754–755
 - SLAAC (stateless address auto-configuration)*, 743–746
- LDP (Label Distribution Protocol)
 - conditional label advertising*, 1058–1064
 - control plane for the 7.7.70/24 prefix*, 1051–1057
 - hello intervals*, 1042–1044
 - hold timer*, 1042–1044
 - labels*, 1048–1051
 - LDP autoconfiguration, enabling*, 1068–1071

- LDP router ID (RID), 1033*
- loopback1 interface of R1, 1044–1048*
- LSRs (label switch routers), 1033–1037*
- MLPS structure, hiding, 1065–1067*
- MPLS forwarding, 1034*
- neighbor discovery, 1037–1042*
- OSPF Area 0, 1029–1032*
- serial connection between R3 and R5, 1072–1073*
- session keepalives, 1044*
- session protection, 1073–1077*
- topology, 1026–1029*
- TTL propagation, testing, 1064–1065*
- LDP (Label Distribution Protocol) configuration, 1026
- LSA Type 4 and Suppress FA, 539–548
- LSAs in OSPFv3, 790
 - Intra-Area Prefix LSAs, 799–800*
 - Link LSAs, 795–799*
 - Network LSAs, 795*
 - OSPF Area 0 on DMVPN network, 813–816*
 - OSPF Area 0 on F0/1 and loopback0 interfaces of R1, R2, and R4, 790–793*
 - OSPF Area 13 on S1/3 and loopback13 interfaces of R3, 800–809*
 - OSPF Area 37 on F0/0, 809–813*
 - Router LSAs, 793–795*
- match destination and source address
 - MAC
 - overview of, 881*
 - R2 configuration to classify and mark IP routed traffic, 882–885*
 - RIPv2 configuration, 881*
- match IP DSCP/Precedence vs. match DSCP, 885–893
- match protocol HTTP URL, MIME, and Host, 893–898
- MLS QoS
 - f0/1 interface on SW1, configuring to mark ingress traffic with COS marking of 2, 844–850*
 - mls qos, enabling on SW1, 842–844*
 - overview of, 840*
 - R1, configuring to send all traffic with COS marking of 1, 840–842*
- MST (Multiple Spanning Tree), 93–94
 - boundary ports, 94*
 - configuring with policies, 99–106*
 - edge ports, 94*
 - IST (Internal Spanning Tree), 95*
 - MSTP (Multiple Instance Spanning Tree Protocol), 96*
 - port configuration, 96*
 - regions, 94*
 - switch hostname configuration, 96*
 - trunking mode, 97*
 - VLAN configuration, 97–99*
- OSPF authentication, 431
 - demand circuits, 456–457*

- MD5 authentication*, 440–462
 - plaintext authentication*, 433–439
 - router interfaces in Area 0*, 431–433
- OSPF broadcast networks, 397–410
- OSPF filtering, 476
 - loopback interface advertisement*, 501–502
 - loopback interface redistribution*, 493
 - loopback interfaces of R1 and R2*, 481–482
 - LSA flooding, preventing*, 502–504
 - network filtering in Area 0*, 486–488
 - network filtering in Area 0 and Area 2*, 488–490
 - network filtering in Area 2*, 484–486
 - network filtering on all routers except R1*, 490–493
 - network filtering on all routers except R5*, 494–495
 - network filtering on R1's routing table*, 496
 - network filtering on R2*, 482–483
 - R1 and R2's directly connected interfaces*, 476–478
 - removing*, 497–501
 - serial connection between R3 and R4*, 478–479
 - serial connection between R4 and R5*, 480–481
- OSPF non-broadcast networks, 411–421
- OSPF point-to-multipoint networks, 425–430
- OSPF point-to-point networks, 421–424
- OSPF routing in VPN, 1113–1122
- OSPF stub, totally stubby, and NSSA areas, 517
 - default route injection*, 533–536
 - loopback interfaces on R5*, 532–533
 - loopback30 interface on R3*, 522–523
 - NSSA configuration*, 528–532
 - R1's directly connected interfaces*, 518
 - R2's directly connected interfaces*, 518–519
 - R3's directly connected interfaces*, 519–520
 - R4's directly connected interfaces*, 521–523
 - stub area configuration*, 523–526
 - totally stubby area configuration*, 526–528
- OSPF suboptimal paths, 549–555
- OSPF summarization
 - advertising networks*, 468–469, 472–475
 - discard routes*, 471–472
 - external route summarization*, 467–468
 - network summarization*, 470
 - R1 configuration*, 465–466
 - R2 configuration*, 464–465
 - R3 configuration*, 463–464
 - R4 configuration*, 463
- OSPFv3 configuration, 763–771
- physical-to-logical topology
 - desired topology*, 18–19
 - hostname configuration*, 20

- port shutdown*, 20
- VLAN 12, 23–24
- VLAN 13, 20–22
- VLAN 28, 24–25
- VLAN 34, 27–29
- VLAN 45, 29–30
- VLAN 56, 30–33
- VLAN 789, 26–27
- PPP (Point-to-Point Protocol)
 - DHCP server configuration, 212–215
 - EAP authentication, 216–218
 - interface configuration, 182–186
 - IP address assignment, 187–190
 - loopback0 interface, pinging, 186–187
 - MLPPP (Multilink PPP), 216–218
 - MPPE protocol and MS-CHAP authentication, 215–218
 - one-way CHAP authentication, 198–201
 - one-way PAP authentication, 190–192
 - PPPoE (PPP over Ethernet), 207–212
 - R1 and R2 serial interface configuration, 215–218
 - R4, configuring to authenticate R3, 202–207
 - two-way CHAP authentication, 201–202
 - two-way PAP authentication, 192–194
- prefix list configuration, 267
 - allowing only unsubnetted Class B networks, 272–275
 - allowing only unsubnetted Class C networks, 275–278
 - allowing unsubnetted Class A networks, plus Class B and C networks, 269–272
 - basic configuration, 267–269
 - configuring loopback interfaces, 277–278, 285
 - denying certain prefixes, 278–281
 - filtering existing and future host routes, 286
 - filtering networks with certain prefix lengths, 283–285
 - injecting default route in EIGRP routing domain, 281–283
- Rapid STP
 - lab setup, 75–77
 - link type, 83–85
 - operational enhancements of, 74
 - overview of, 73
 - port roles, 74
 - port states, 74
 - rapid convergence mechanisms, 75, 78–80
 - rapid convergence process, demonstrating, 80–83
 - SW2, enabling for RSTP mode, 89–92
 - switch operation, 85–89
- RFC 3101 and RFC 1587, 556–566
- RIPv2 and EIGRP redistribution
 - allowing only required routes to be redistributed, 617–619
 - control plane mechanism, 614–615
 - EIGRP AS 100 configuration, 607–608

- filtering RIP routes from being advertised out of F0/1 interface, 615–617*
- filtering tagged routes, 619–622*
- loopback0 interface, 607*
- mutual redistribution between RIPv2 and EIGRP, 608–614*
- overview of, 604–605*
- RIPv2 configuration on R2, R3, and R4, 605–606*
- summarization, 622–625*
- RIPv2 and OSPF redistribution
 - mutual redistribution on R1, 629–634*
 - OSPF area 0 configuration on f0/0 interface, 626*
 - overview of, 625–626*
 - RIPv2 configuration on R1, R2, and R3, 626–627*
 - update, invalidation, and flush timer values, 628–629*
- RIPv2 routing in VPN, 1078
 - configuration between R1 and PE-2, 1096–1107*
 - configuration between R7 and PE-6, 1096–1107*
 - LDP configuration on core MPLS routers, 1084–1088*
 - MP-BGP AS 100 configuration on R2 to R6, 1088–1090*
 - OSPF configuration on core MPLS routers, 1081–1083*
 - RDs (route distinguishers), 1091–1095*
 - RTs (route targets), 1091–1095*
 - topology, 1079–1081*
 - VRF (Virtual Routing and Forwarding), 1091–1095*
- Spanning Tree Backbone Fast, 148–154
- Spanning Tree Loop Guard, 162–167
- Spanning Tree Portfast, 106–115
- Spanning Tree Root Guard, 154–162
- static RP (rendezvous point), 977
 - PIM sparse mode, 983–985*
 - R2 and R3 configuration, 986–991*
 - S1/4 interface on R5, 991–993*
 - topology, 981–983*
- summarization of internal/external networks
 - discard routes, 786–789*
 - external route summarization, 782–786*
 - loopback interface summarization, 778–782*
 - OSPFv3 configuration, 771–778*
 - overview of, 771*
- UplinkFast, 115–128
- virtual links and GRE tunnels
 - GRE tunnel configuration, 513–516*
 - OSPF configuration, 506–509*
 - overview of, 504–506*
 - virtual link configuration, 509–513*
- LCP (Link Control Protocol), 171–175
- LDP (Label Distribution Protocol) configuration, 1026
 - backdoor links
 - CE (customer edge) router configuration, 1136–1141*
 - F0/1 interface of R1 and the G0/1 interface of R7, 1141–1147*

- LDP configuration between core routers, 1128–1132*
- MP-BGP AS 100 configuration between R2 and R6, 1132–1133*
- RDs (route distinguishers), 1134–1136*
- RTs (route targets), 1134–1136*
- VRF (Virtual Routing and Forwarding), 1134–1136*
- conditional label advertising, 1058–1064
- control plane for the 7.7.0/24 prefix, 1051–1057
- hello intervals, 1042–1044
- hold timer, 1042–1044
- labels, 1048–1051
- LDP autoconfiguration, enabling, 1068–1071
- LDP router ID (RID), 1033
- loopback1 interface of R1, 1044–1048
- LSRs (label switch routers), 1033–1037
- MLPS structure, hiding, 1065–1067
- MPLS forwarding, 1034
- neighbor discovery, 1037–1042
- OSPF Area 0, 1029–1032
- RIPv2 routing in VPN
 - LDP configuration on core MPLS routers, 1084–1088*
 - MP-BGP AS 100 configuration on R2 to R6, 1088–1090*
- serial connection between R3 and R5, 1072–1073
- session keepalives, 1044
- session protection, 1073–1077
- topology, 1026–1029
- TTL propagation, testing, 1064–1065
- leak-map command, 355
- LFI (Link Fragmentation and Interleaving), 180
- LFIB (Label Forwarding Information Base), 1073
- LIB (Label Information Base), 1073
- Link Control Protocol (LCP), 171–175
- Link Establishment Phase (PPP), 171–175
- Link Fragmentation and Interleaving (LFI), 180
- Link Layer, 7–8
- Link LSAs, 795–799
- links
 - backdoor links and OSPF, 1123
 - CE (customer edge) router configuration, 1136–1141*
 - F0/1 interface of R1 and the G0/1 interface of R7, 1141–1147*
 - LDP configuration between core routers, 1128–1132*
 - MP-BGP AS 100 configuration between R2 and R6, 1132–1133*
 - OSPF configuration on core MPLS routers, 1123–1128*
 - RDs (route distinguishers), 1134–1136*
 - RTs (route targets), 1134–1136*
 - topology, 1123–1125*
 - VRF (Virtual Routing and Forwarding), 1134–1136*
 - RSTP link types, 83–85
 - sham links, 1141–1147
- link-state advertisements. *See* LSAs (link-state advertisements)

link-state databases, filtering items in.*See filtering***lists, prefix. *See prefix lists*****logical topology**

definition of, 8

transitioning physical topology to,
18–33*desired topology, 18–19**hostname configuration, 20**port shutdown, 20**VLAN 12 configuration,
23–24**VLAN 13 configuration,
20–22**VLAN 28 configuration, 24–25**VLAN 34 configuration, 27–29**VLAN 45 configuration, 29–30**VLAN 56 configuration, 30–33**VLAN 789 configuration,
26–27*transitioning to physical topology,
8–17**loopback interfaces**

advertising networks

*R1 and R4 loopback interfaces,
385–387**R4, R5, and R6 loopback
interfaces, 381–385*BGP (Border Gateway Protocol), 653
configuration, 575–578, 583DMVPNs (dynamic multipoint
virtual private networks),
947–948

EIGRP redistribution, 607

EIGRP summarization

*loopback interfaces for R1,
349–350**loopback interfaces for R2, 350**loopback interfaces for R3, 351**loopback interfaces for R4,
351–353*

EIGRPv6, 826–829

LDP (Label Distribution Protocol),
1044–1048OSPF (Open Shortest Path First),
501–502*OSPF filtering, 481–482**OSPF stub, totally stubby,
and NSSA areas, 522–523,
532–533*

pinging, 186–187

redistribution, 493, 569

summarization, 325–327,
778–782**LSAs (link-state advertisements)**

flooding, 502–504

in OSPFv3, 790

*Intra-Area Prefix LSAs,
799–800**Link LSAs, 795–799**Network LSAs, 795**OSPF Area 0 on DMVPN
network, 813–816**OSPF Area 0 on F0/1 and
loopback0 interfaces of R1,
R2, and R4, 790–793**OSPF Area 13 on S1/3 and
loopback13 interfaces of R3,
800–809**OSPF Area 37 on F0/0,
809–813**Router LSAs, 793–795*

Type-4 LSAs, 539–548

LSRs (label switch routers)

configuration, 1033–1037

hello intervals, 1042–1044

M

MAC (media access control)

addresses, 36

MAC address access lists, 904–906

match destination and source address

MAC

overview of, 885

*R2 configuration to classify
and mark IP routed traffic,
882–885*

RIPv2 configuration, 881

mapping

COS-DSCP mapping

*F0/1 interface on R2,
configuring, 866*

*F0/1 interface on SW1,
configuring, 866*

*F0/19 interface SW2,
configuring, 866–869*

DSCP-COS mapping

overview of, 860

R1 configuration, 862

R2 configuration, 861

SW2 configuration, 862–865

DSCP-mutation maps, 855–857

dynamic mapping, DMVPN Phase 1

using

*hub and spoke configuration,
232–236*

*interface and router
configuration, 229–232*

overview of, 229

IP-precedence-DSCP mapping,
870–873

mapping agents, 998

route map configuration, 570–571

static mapping

DMVPN Phase 1, 219–229

DMVPN Phase 2, 236–244

match interface option, 569

match ip route-source command, 598

match source-address mac command,
904

matches, configuring

class-based policing

*F0/0 interface on R2,
configuring, 903–904*

*HTTP, FTP, and ICMP traffic,
906–907*

*MAC address access lists,
904–906*

overview of, 898

*S1/2 interface on R1,
configuring, 899–902*

class-based shaping, 907–910

input-interface and match NOT

*f0/0 interface on R4,
configuring, 873–876*

overview of, 873

*s1/1 interface on R2,
configuring, 877–881*

match destination and source address

MAC

overview of, 881

*R2 configuration to classify
and mark IP routed traffic,
882–885*

RIPv2 configuration, 881

match IP DSCP/Precedence vs. match
DSCP, 885–893

match protocol HTTP URL, MIME,
and Host, 893–898

MD5 authentication, 176

configuration, 361

*authentication password,
448–451*

- EIGRPv6, 831–833*
- between R1 and R2, 444–447, 455–462*
- on serial links, 440–443*
- removing, 443–444, 451–455
- media access control addresses. *See* MAC (media access control) addresses
- messages
 - CHAP (Challenge-Handshake Authentication Protocol), 198–200
 - IGMP (Internet Group Management Protocol), 969–971
 - IPv6, 739–742
 - LCP (Link Control Protocol), 172–175
 - NHRP (Next-Hop Resolution Protocol), 251–252
 - PAP (Password Authentication Protocol), 190
 - PPPoE (PPP over Ethernet), 181
- metric rib-scale command, 340
- metrics
 - composite metrics, filtering, 602–604
 - EIGRP (Enhanced Interior Gateway Routing Protocol), 604
 - classic mode configuration, 337–338*
 - EIGRP AS 100 configuration, 334–335*
 - FD set to Infinity, resolving, 343–348*
 - mutual redistribution between RIPv2 and EIGRP, 335–337*
 - named mode configuration, 338–341*
 - topology, 333*
 - Wide Metric support, 341–342*
 - mGRE (Multipoint Generic Routing Encapsulation), 219, 223
 - Microsoft CHAP. *See* MS-CHAP (Microsoft CHAP)
 - Microsoft Point-to-Point Encryption. *See* MPPE (Microsoft Point-to-Point Encryption)
 - MIME (Multipurpose Internet Mail Extensions), 893–898
 - MLPPP (Multilink PPP), 180, 216–218
 - MLS QoS
 - f0/1 interface, configuring to mark ingress traffic with COS marking of 2, 844–850
 - mls qos, enabling on SW1, 842–844
 - overview of, 840
 - R1, configuring to send all traffic with COS marking of 1, 840–842
 - mls qos command, 853
 - mls qos cos 2 command, 846, 849
 - mls qos cos override command, 846, 847
 - mls qos trust cos command, 846, 849
 - mls qos trust dscp command, 854
 - modified EUI-64 addressing, 737–739
 - Modular Quality of Service Command Line Interface (MQC), 844
 - moving designated ports, 43–45
 - MPLS (Multiprotocol Label Switching)
 - backdoor links and OSPF, 1123
 - CE (customer edge) router configuration, 1136–1141*
 - F0/1 interface of R1 and the G0/1 interface of R7, 1141–1147*

- LDP configuration between core routers, 1128–1132*
- MP-BGP AS 100 configuration between R2 and R6, 1132–1133*
- OSPF configuration on core MPLS routers, 1123–1128*
- RDs (route distinguishers), 1134–1136*
- RTs (route targets), 1134–1136*
- topology, 1123–1125*
- VRF (Virtual Routing and Forwarding), 1134–1136*
- BGP routing in VPN, 1148–1154
- EIGRP routing in VPN, 1107–1113
- LDP (Label Distribution Protocol), 1026
 - conditional label advertising, 1058–1064*
 - control plane for the 7.7.70/24 prefix, 1051–1057*
 - hello intervals, 1042–1044*
 - hold timer, 1042–1044*
 - labels, 1048–1051*
 - LDP autoconfiguration, 1068–1071*
 - LDP router ID (RID), 1033*
 - loopback1 interface of R1, 1044–1048*
 - LSRs (label switch routers), 1033–1037*
 - MLPS structure, hiding, 1065–1067*
 - MPLS forwarding, 1034*
 - neighbor discovery, 1037–1042*
 - OSPF Area 0, 1029–1032*
 - serial connection between R3 and R5, 1072–1073*
 - session keepalives, 1044*
 - session protection, 1073–1077*
 - topology, 1026–1029*
 - TTL propagation, testing, 1064–1065*
- OSPF routing in VPN, 1113–1122
- overview of, 1025
- RIPv2 routing in VPN, 1078
 - configuration between R1 and PE-2, 1096–1107*
 - configuration between R7 and PE-6, 1096–1107*
 - LDP configuration on core MPLS routers, 1084–1088*
 - MP-BGP AS 100 configuration on R2 to R6, 1088–1090*
 - OSPF configuration on core MPLS routers, 1081–1083*
 - RDs (route distinguishers), 1091–1095*
 - RTs (route targets), 1091–1095*
 - topology, 1079–1081*
 - VRF (Virtual Routing and Forwarding), 1091–1095*
- mpls ip command, 1033**
- mpls label protocol command, 1033**
- mpls label protocol ldp command, 1033**
- MPLS label range 16 1048575 command, 1048**
- mpls ldp advertise-labels command, 1058**
- mpls ldp router-id command, 1033**
- MPPE (Microsoft Point-to-Point Encryption), 215–218**
- MQC (Modular Quality of Service Command Line Interface), 844**
- mroute states (IGMP), 971–974**
- MS-CHAP (Microsoft CHAP), 175–176, 215–218**

MST (Multiple Spanning Tree), 93–94

- boundary ports, 94
- configuring with policies, 99–106
- edge ports, 94
- IST (Internal Spanning Tree), 95
- MSTP (Multiple Instance Spanning Tree Protocol), 96
- port configuration, 96
- regions, 94
- switch hostname configuration, 96
- trunking mode, 97
- VLAN configuration, 97–99

MSTP (Multiple Instance Spanning Tree Protocol), 96**multicast**

- BSR (Bootstrap Router), 1013
 - Lo0 interface of R1, 1022–1023*
 - OSPF Area 0 configuration, 1013–1014*
 - PIM sparse mode configuration, 1014–1017*
 - ping command, 1022–1023*
 - primary and backup RP configuration, 1017–1022*
- dynamic RP learning and Auto-RP, 993
 - Lo0 interface of R1, 1006–1010*
 - OSPF Area 0 configuration, 994*
 - PIM sparse-dense-mode configuration, 994–997*
 - primary and backup RP configuration, 997–1003*
 - R3 configuration, 1005–1006*
 - RP announcements, filtering on R6, 1004–1005*
- IGMP (Internet Group Management Protocol), 959

F0/0 and F0/1 interface configuration on R1 and R2, 959–962

F0/0 interface configuration on R3 and R4, 963

F0/1 interface configuration on R5 and R6, 964

G0/1 interface on R7, 965

hosts connected to F0/1 on R1, restricting, 965–967

hosts connected to F0/1 on R2, stopping multicast traffic with, 967–969

mroute states, limiting, 971–974

query max response time, 976–977

query messages, sending, 969–971

querying router and the query interval, 974–976

static RP (rendezvous point), 977

PIM sparse mode, 983–985

R2 and R3 configuration, 986–991

S1/4 interface on R5, 991–993 topology, 981–983

multi-exit discriminator attribute (BGP), 695–703

Multilink PPP (MLPPP), 180

Multiple Instance Spanning Tree (MSTP), 96

Multiple Spanning Tree. *See* MST (Multiple Spanning Tree)

Multipoint Generic Routing Encapsulation (mGRE), 219, 223

Multiprotocol Label Switching. *See* MPLS (Multiprotocol Label Switching)

Multipurpose Internet Mail Extensions (MIME), 893–898

mutation map (DSCP), 855–857

mutual redistribution between RIPv2 and EIGRP, 335–337, 608–614

- allowing only required routes to be redistributed, 617–619
- control plane mechanism, 614–615
- filtering RIP routes from being advertised out of F0/1 interface, 615–617
- filtering tagged routes, 619–622
- summarization, 622–625

N

Name field (CHAP), 199

named mode (EIGRP), 311

- bandwidth usage, configuring, 324–325
- EIGRP 200 configuration, 318–319
- EIGRP AS 100 configuration, 316–317
- fixed metric for the EIGRP summary route, 327–328
- hello intervals, 323–324
- metrics and, 338–341
- number of received prefixes, limiting, 329–333
- OSPF configuration, 319–323
- policy for configuring, 311–315
- summarization, 325–327
- unicast configuration, 317–318

NAT (network address translation), 224, 925–930

NBAR (Network Based Application Recognition), 899

NBMA (Non-Broadcast Multi-Access), 219, 294

NCPs (Network Control Protocols), 177–179

neighbor adjacencies, establishing, 635–641

neighbor advertisements, 740

neighbor discovery, 739–743, 1037–1042

neighbor routes, 182

NET prefix list, 268–269

network address translation (NAT), 224

Network Based Application Recognition (NBAR), 899

Network Control Protocols (NCPs), 177–179

Network Layer Protocol Phase (PPP), 177–179

network layer reachability information (NLRI), 509

Network LSAs, 795

Next Hop Server (NHS), 219

NHRP (Next-Hop Resolution Protocol)

- DMVPNs (dynamic multipoint virtual private networks)
 - DMVPN Phase 1 using dynamic mapping*, 232
 - DMVPN Phase 1 using static mapping*, 223–225
 - DMVPN Phase 2 using dynamic mapping*, 248–249
 - DMVPN Phase 3*, 255–259
- NHRP Redirect, 251–252
- NHRP Response, 252
- NHRP Shortcut, 252
- Resolution requests, 251, 301
- Traffic Indication message, 265

NHS (Next Hop Server), 219

NLRI (network layer reachability information), 509
no auto-summary command, 312
no discard-route internal command, 585
no mpls ip propagate-ttl local command, 1066
no peer neighbor-route command, 185
Non-Broadcast Multi-Access (NBMA), 294
Non-Broadcast Multi-Access (NBMA) address, 219
non-broadcast networks (OSPF)
 configuration, 411–421
 point-to-multipoint networks, 425–430
nonces, 913
NSSA (not-so-stubby area), 517
 configuration, 528–532
 default route injection, 533–536
 loopback interfaces on R5, 532–533
 loopback30 interface on R3, 522–523
 R1's directly connected interfaces, 518
 R2's directly connected interfaces, 518–519
 R3's directly connected interfaces, 519–520
 R4's directly connected interfaces, 521–523
number of received prefixes, limiting, 329–333

O

OAKLEY, 912–913
one-way PAP authentication, 190–192
Open Shortest Path First. See OSPF (Open Shortest Path First)

Originator-ID attribute, 642
OSPF (Open Shortest Path First), 536–538. *See also* EIGRP (Enhanced Interior Gateway Routing Protocol)
 advertising networks, 381
 DMVPN configuration, 389–391
 IP addressing, 387–388
 OSPF adjacency, 391–397
 R1 and R4 connections and loopback interfaces, 385–387
 R4, R5, and R6 connections, 381–385
 static default routes, 388–389
 authentication, 431
 demand circuits, 456–457
 MD5 authentication, 440–462
 plaintext authentication, 433–439
 router interfaces in Area 0, 431–433
 backdoor links, 1123
 OSPF configuration on core MPLS routers, 1123–1128
 topology, 1123–1125
 basic redistribution
 eigrp 100 redistribution into ospf 1, 592–593
 network 4.4.4.0 /24, filtering on R2, 596–597
 ospf 1 and eigrp 100 redistribution into ospf 36, 599–602
 ospf 1 redistribution into eigrp 100, 595–596
 OSPF area 0 configuration, 587–589, 591

- RIPv2 redistribution into OSPF, 584–586*
- routes originated by R4, filtering with R5, 597–599*
- broadcast networks, 397–410
- EIGRP (Enhanced Interior Gateway Routing Protocol) configuration, 319–323
- filtering, 476
 - loopback interface advertisement, 501–502*
 - loopback interface redistribution, 493*
 - loopback interfaces of R1 and R2, 481–482*
 - LSA flooding, preventing, 502–504*
 - network filtering in Area 0, 486–488*
 - network filtering in Area 0 and Area 2, 488–490*
 - network filtering in Area 2, 484–486*
 - network filtering on all routers except R1, 490–493*
 - network filtering on all routers except R5, 494–495*
 - network filtering on R1's routing table, 496*
 - network filtering on R2, 482–483*
 - R1 and R2's directly connected interfaces, 476–478*
 - removing, 497–501*
 - serial connection between R3 and R4, 478–479*
 - serial connection between R4 and R5, 480–481*
- LSA Type 4 and FA suppression, 539–548
- LSAs in OSPFv3, 790
 - Intra-Area Prefix LSAs, 799–800*
 - Link LSAs, 795–799*
 - Network LSAs, 795*
 - OSPF Area 0 on DMVPN network, 813–816*
 - OSPF Area 0 on F0/1 and loopback0 interfaces of R1, R2, and R4, 790–793*
 - OSPF Area 13 on S1/3 and loopback13 interfaces of R3, 800–809*
 - OSPF Area 37 on F0/0, 809–813*
 - Router LSAs, 793–795*
- non-broadcast networks, 411–421
- OSPFv3, 763–771
 - bandwidth usage, configuring, 830*
 - Hello interval and Hold timer, 825–826*
 - loopback1 interface on R2, 826–829*
 - redistributing into EIGRPv6, 824–825*
- point-to-multipoint networks, 425–430
- point-to-point networks, 421–424
- RFC 3101 and RFC 1587, 556–566
- RIPv2 and OSPF redistribution
 - mutual redistribution on R1, 629–634*
 - OSPF area 0 configuration on f0/0 interface, 626*
 - overview of, 625–626*
 - RIPv2 configuration on R1, R2, and R3, 626–627*

- update, invalidation, and flush timer values, 628–629*
- RIPv2 routing in VPN, 1081–1083
- stub, totally stubby, and NSSA areas, 517
 - default route injection, 533–536*
 - loopback interfaces on R5, 532–533*
 - loopback30 interface on R3, 522–523*
 - NSSA configuration, 528–532*
 - R1's directly connected interfaces, 518*
 - R2's directly connected interfaces, 518–519*
 - R3's directly connected interfaces, 519–520*
 - R4's directly connected interfaces, 521–523*
 - stub area configuration, 523–526*
 - totally stubby area configuration, 526–528*
- suboptimal paths, 549–555
- summarization
 - advertising networks, 468–469, 472–475*
 - discard routes, 471–472, 786–789*
 - external route summarization, 467–468, 782–786*
 - loopback interface summarization, 778–782*
 - network summarization, 470*
 - OSPFv3 configuration, 771–778*
 - overview of, 771*
 - R1 configuration, 465–466*
 - R2 configuration, 464–465*

- R3 configuration, 463–464*
- R4 configuration, 463*
- virtual links and GRE tunnels
 - GRE tunnel configuration, 513–516*
 - OSPF configuration, 506–509*
 - overview of, 504–506*
 - virtual link configuration, 509–513*
- in VPN, 1113–1122

P

- Packet Description Language Modules (PDLM), 899
- packet label assignment, 1106
- Padding field (PPP), 171
- PADI (PPPoE Active Discovery Initiation) frame, 181
- PADO (PPPoE Active Discovery Offer) frame, 181
- PADR (PPPoE Active Discovery Request) frame, 181
- PADS (PPPoE Active Discovery Session) frame, 181
- PADT (PPPoE Active Discovery Termination) message, 181
- PAP (Password Authentication Protocol)
 - AUTH-ACK message, 190, 194
 - AUTH-REQ message, 190, 194
 - one-way CHAP authentication, 198–201
 - one-way PAP authentication, 190–192
 - overview of, 175–179
 - R4, configuring to authenticate R3, 202–207

- two-way CHAP authentication, 201–202
- two-way PAP authentication, 192–194
- passwords, authentication passwords, 448–451
- payload compression, 179–180
- PDLM (Packet Description Language Modules), 899
- peer default ip address 23.1.1.3 interface command, 187
- peer default ip address pool command, 212
- peer session configuration, 650–651
- peering (BGP), 704–708, 715–717
- Perfect Forward Secrecy (PFS), 913
- PFC (Protocol Field Compression), 179
- PFS (Perfect Forward Secrecy), 913
- Phase 1 DMVPN (dynamic multipoint virtual private network)
 - configuring for EIGRP, 289–292
 - NHRP (Next-Hop Resolution Protocol), 223
 - using dynamic mapping
 - hub and spoke configuration*, 232–236
 - interface and router configuration*, 229–232
 - overview of*, 229
 - using static mapping
 - hub and spoke configuration*, 223–229
 - interface and router configuration*, 220–239
 - overview of*, 219
- Phase 2 DMVPN (dynamic multipoint virtual private network)
 - configuring for EIGRP, 298–301
 - using dynamic mapping
 - hub and spoke configuration*, 247–251
 - interface and router configuration*, 245–247
 - overview of*, 244
 - using static mapping
 - hub and spoke configuration*, 240–244
 - interface and router configuration*, 237–240
 - overview of*, 236–237
- Phase 3 DMVPN (dynamic multipoint virtual private network)
 - hub and spoke configuration, 255–266
 - interface and router configuration, 253–255
 - overview of, 251–252
- physical topology
 - definition of, 7–8
 - serial connections between routers, 3–5
 - switching devices, 1–3
 - transitioning logical topology to, 8–17
 - transitioning to logical topology, 18–33
 - desired topology*, 18–19
 - hostname configuration*, 20
 - port shutdown*, 20
 - VLAN 12 configuration*, 23–24
 - VLAN 13 configuration*, 20–22
 - VLAN 28 configuration*, 24–25
 - VLAN 34 configuration*, 27–29
 - VLAN 45 configuration*, 29–30
 - VLAN 56 configuration*, 30–33
 - VLAN 789 configuration*, 26–27

PIM (Protocol-Independent Multicast)

dense mode, 959–962

sparse mode, 983–985, 994–997,
1014–1017**ping command, 1022–1023****plaintext authentication**

configuration, 433–438

removing, 438–439

**point-to-multipoint networks (OSPF),
425–430****point-to-point networks (OSPF),
421–424****Point-to-Point Protocol. *See* PPP
(Point-to-Point Protocol)****policing, class-based. *See* class-based
policing****Portfast, 106–115****ports**

edge ports, 75

shutting down, 20

STP (Spanning Tree Protocol)*boundary ports, 94**designated ports, moving,
43–45**edge ports, 94**MSTP (Multiple Instance
Spanning Tree Protocol), 96**port roles, 74**port states, 74**spanning-tree port ID, raising,
48–49**trunk port configuration,
52–54**trunking mode, 97***PPP (Point-to-Point Protocol)**

control plane, 171

*authentication, 175–177**LCP (Link Control Protocol),
171–175**NCPs (Network Control
Protocols), 177–179*

frame format, 170–171

header compression, 179–180

lab, 180–182

*DHCP server configuration,
212–215**EAP authentication,
216–218**interface configuration,
182–186**IP address assignment,
187–190**loopback0 interface, pinging,
186–187**MLPPP (Multilink PPP),
216–218**MPPE protocol and
MS-CHAP authentication,
215–218**one-way CHAP authentication,
198–201**one-way PAP authentication,
190–192**PPPoE (PPP over Ethernet),
207–212**R1 and R2 serial interface
configuration, 215–218**R4, configuring to authenticate
R3, 202–207**two-way CHAP authentication,
201–202**two-way PAP authentication,
192–194*

MLPPP (Multilink PPP), 180

overview of, 169–170

payload compression, 179–180

- PPPoE (PPP over Ethernet), 180–182
 - session establishment
 - Authentication Phase*, 175–177
 - Link Establishment Phase*, 171–175
 - Network Layer Protocol Phase*, 177–179
 - ppp authentication chap command, 198, 203
 - ppp authentication pap command, 190
 - ppp chap hostname command, 199, 203
 - ppp chap password command, 177
 - PPP over Ethernet. *See* PPPoE (PPP over Ethernet)
 - ppp pap sent-username command, 191
 - PPPoE (PPP over Ethernet), 180–182, 207–212
 - PPPoE Active Discovery Initiation (PADI) frame, 181
 - PPPoE Active Discovery Offer (PADO) frame, 181
 - PPPoE Active Discovery Request (PADR) frame, 181
 - PPPoE Active Discovery Session (PADS) frame, 181
 - PPPoE Active Discovery Termination (PADT) message, 181
 - precedence, IP-precedence-DSCP mapping, 870–873
 - prefix delegation (DHCP), 755–763
 - prefix lists
 - configuration, 267
 - allowing only unsubnetted Class B networks*, 272–275
 - allowing only unsubnetted Class C networks*, 275–278
 - allowing unsubnetted Class A networks, plus Class B and C networks*, 269–272
 - basic configuration*, 267–269
 - configuring loopback interfaces*, 277–278, 285
 - denying certain prefixes*, 278–281
 - filtering existing and future host routes*, 286
 - filtering networks with certain prefix lengths*, 283–285
 - injecting default route in EIGRP routing domain*, 281–283
 - filtering with, 704–714
 - access list configuration*, 712–713
 - BGP peering*, 704–708
 - outbound prefixes, filtering*, 713–714
 - prefix-list and distribute-list configuration*, 709–710
 - R2 configuration*, 708–709
 - R3 configuration*, 711–712
- prefixes, filtering
 - advertising of prefixes originating in own AS, 721–723
 - prefixes from directly connected neighbors, 725–726
 - prefixes originating in AS 200, 723–725
 - prefixes originating in AS 300, 717–719, 727–728
 - prefixes with AS 300 in path list, 719–721
 - prefixes with prepended AS numbers, 728–731
- preshared keys (PSK), 913

primary RP (rendezvous point)
 configuration, 997–1003,
 1017–1022
propagation (TTL), testing,
 1064–1065
Protocol field (CHAP), 198
Protocol Field Compression (PFC),
 179
Protocol field (PPP), 171
Protocol-Independent Multicast.
See PIM (Protocol-Independent
 Multicast)
Protocol-Reject (PROTREJ) message,
 178–179
Protocol-Reject message, 175
PROTREJ (Protocol-Reject) message,
 178–179
PSK (preshared keys), 913

Q

QoS (quality of service)

class-based policing
F0/0 interface on R2,
configuring, 903–904
HTTP, FTP, and ICMP traffic,
 906–907
MAC address access lists,
 904–906
overview of, 898
S1/2 interface on R1,
configuring, 899–902
 class-based shaping, 907–910
 COS-DSCP mapping
F0/1 interface on R2,
configuring, 866
F0/1 interface on SW1,
configuring, 866

F0/19 interface SW2,
configuring, 866–869
 DSCP-COS mapping
overview of, 860
R1 configuration, 862
R2 configuration, 861
SW2 configuration, 862–865
 DSCP-Mutation
DSCP rewrites, enabling,
 857–860
DSCP-mutation map
configuration, 855–857
mls qos, enabling on SW2,
 853–854
mls qos trust dscp
configuration, 854–855
MQC on R1, configuring to
mark egress traffic with
DSCP value of 1, 851–852
overview of, 851
 input-interface and match NOT
f0/0 interface on R4,
configuring, 873–876
overview of, 873
s1/1 interface on R2,
configuring, 877–881
 IP-precedence-DSCP mapping,
 870–873
 LFI (Link Fragmentation and
 Interleaving), 180
 match destination and source address
 MAC
overview of, 881
R2 configuration to classify
and mark IP routed traffic,
 882–885
RIPv2 configuration, 881
 match IP DSCP/Precedence vs. match
 DSCP, 885–893

match protocol HTTP URL, MIME,
and Host, 893–898

MLS QoS

*f0/1 interface on SW1,
configuring to mark ingress
traffic with COS marking of
2, 844–850*

*mls qos, enabling on SW1,
842–844*

overview of, 840

*R1, configuring to send all
traffic with COS marking of
1, 840–842*

overview of, 839–840

quality of service. *See* QoS (quality
of service)

queries (IGMP)

query interval, 974–976

query max response time, 976–977

query messages, 969–971

querying router, 974–976

querying router and the query
interval, 974–976

R

RA (router advertisement) messages,
739–740, 744

raising spanning-tree cost on port in
VLAN 12, 41–42

rapid convergence (RSTP), 75

link type, 83–85

rapid convergence mechanisms,
78–80

rapid convergence process,
demonstrating, 80–83

Rapid STP (Spanning Tree Protocol)

lab setup, 75–77

link type, 83–85

operational enhancements of, 74

overview of, 73

port roles, 74

port states, 74

rapid convergence mechanisms, 75,
78–80

rapid convergence process,
demonstrating, 80–83

SW2, enabling for RSTP mode,
89–92

switch operation, 85–89

rapid-commit option, 755

RDs (route distinguishers),
1091–1095, 1134–1136

Redirect message, 251–252, 740

redistribute command, 572–573

redistribute connected command,
570, 579

redistribution

basic configuration

*composite metrics, filtering,
602–604*

*eigrp 100 redistribution into
ospf 1, 592–593*

*EIGRP AS 100, 578–580,
589–590*

*link between R1 and R3,
567–569*

loopback interfaces on R2, 583

*loopback interfaces on R2/R3,
575–578*

loopback interfaces on R3, 569

*network 4.4.4.0 /24, filtering on
R2, 596–597*

*ospf 1 and eigrp 100
redistribution into ospf 36,
599–602*

*ospf 1 redistribution into eigrp
100, 595–596*

- OSPF area 0, 587–589, 591
- overview of, 567
- R1/R2, 571–575
- RIP redistribution into EIGRP, 580–583
- RIPv2 redistribution into OSPF, 584–586
- route maps, 569
- routes originated by R4, filtering with R5, 597–599
- routes tag of 111, configuring R4 to filter, 593–594
- routes tag of 222, configuring R4 to filter, 595
- RIPv2 and EIGRP redistribution
 - allowing only required routes to be redistributed, 617–619
 - control plane mechanism, 614–615
 - EIGRP AS 100 configuration, 607–608
 - filtering RIP routes from being advertised out of F0/1 interface, 615–617
 - filtering tagged routes, 619–622
 - loopback0 interface, 607
 - mutual redistribution between RIPv2 and EIGRP, 608–614
 - overview of, 604–605
 - RIPv2 configuration on R2, R3, and R4, 605–606
 - summarization, 622–625
- RIPv2 and OSPF redistribution
 - mutual redistribution on R1, 629–634
 - OSPF area 0 configuration on f0/0 interface, 626
 - overview of, 625–626
 - RIPv2 configuration on R1, R2, and R3, 626–627
 - update, invalidation, and flush timer values, 628–629
- reflectors, router, 642–649
- regions (MST), 94
- regular expressions, 714–731
 - advertising of prefixes originating in own AS, preventing, 721–723
 - BGP peering, 715–717
 - prefixes from directly connected neighbors, blocking, 725–726
 - prefixes originating in AS 200, blocking, 723–725
 - prefixes originating in AS 300, blocking, 727–728
 - prefixes originating in AS 300, filtering, 717–719
 - prefixes with AS 300 in path list, filtering, 719–721
 - prefixes with prepended AS numbers, blocking, 728–731
- Rendezvous Point Set (RP-SET), 1019
- rendezvous points. *See* RPs (rendezvous points)
- Resolution requests (NHRP), 251, 301
- Response message
 - CHAP (Challenge-Handshake Authentication Protocol), 199
 - NHRP (Next-Hop Resolution Protocol), 252
- rewrites (DSCP), enabling, 857–860
- RFC 1587, 556–566
- RFC 3101, 556–566
- RIB (Routing Information-Base), 306
- RID (router ID), 1033
- RIPv2 (Routing Information Protocol version 2), 295

- basic redistribution
 - overview of*, 604–605
 - redistribution into OSPF*, 584–586
 - RIPv2 configuration on R2, R3, and R4*, 605–606
- EIGRP redistribution
 - allowing only required routes to be redistributed*, 617–619
 - control plane mechanism*, 614–615
 - EIGRP AS 100 configuration*, 607–608
 - filtering RIP routes from being advertised out of F0/1 interface*, 615–617
 - filtering tagged routes*, 619–622
 - loopback0 interface*, 607
 - mutual redistribution*, 335–337
 - mutual redistribution between RIPv2 and EIGRP*, 608–614
 - summarization*, 622–625
- match destination and source address MAC, 881
- OSPF redistribution
 - mutual redistribution on R1*, 629–634
 - OSPF area 0 configuration on f0/0 interface*, 626
 - overview of*, 625–626
 - RIPv2 configuration on R1, R2, and R3*, 626–627
 - update, invalidation, and flush timer values*, 628–629
- redistribution into EIGRP, 580–583
- in VPN, 1078
 - configuration between R1 and PE-2*, 1096–1107
 - configuration between R7 and PE-6*, 1096–1107
 - LDP configuration on core MPLS routers*, 1084–1088
 - MP-BGP AS 100 configuration on R2 to R6*, 1088–1090
 - OSPF configuration on core MPLS routers*, 1081–1083
 - RDs (route distinguishers)*, 1091–1095
 - RTs (route targets)*, 1091–1095
 - topology*, 1079–1081
 - VRF (Virtual Routing and Forwarding)*, 1091–1095
- roles, port, 74
- root bridge configuration, 56–59, 65–67
- root primary macro configuration, 46–48
- route distinguishers (RDs), 1091–1095, 1134–1136
- route map configuration, 570–571
- route maps, 598–604
- route redistribution. *See* redistribution
- route targets (RTs), 1091–1095, 1134–1136
- route-map tst permit 90 command, 570
- router advertisement (RA) messages, 739–740, 744
- router configuration. *See* configuration
- router discovery, 741
- router ID (RID), 1033
- Router LSAs, 793–795
- router ospf command, 765

router ospfv3 command, 765
 router reflectors, 642–649
 router solicitation, 740
 Routing Information Protocol. *See*
 RIPv2 (Routing Information
 Protocol version 2)
 Routing Information-Base (RIB),
 306
 routing tables, filtering items in. *See*
 filtering
 RPs (rendezvous points)
 candidate RPs, 997–998
 dynamic RP learning and Auto-RP,
 993
 Lo0 interface of R1,
 1006–1010
 OSPF Area 0 configuration,
 994
 PIM sparse-dense-mode
 configuration, 994–997
 primary and backup RP
 configuration, 997–1003
 R3 configuration, 1005–1006
 RP announcements, filtering on
 R6, 1004–1005
 static RP (rendezvous point), 977
 PIM sparse mode, 983–985
 R2 and R3 configuration,
 986–991
 S1/4 interface on R5, 991–993
 topology, 981–983
 RP-SET (Rendezvous Point Set), 1019
 RSA encrypted pseudorandom
 numbers, 913
 RSA signatures, 913
 RTs (route targets), 1091–1095,
 1134–1136
 Rx(config)#ip multicast-routing
 command, 959

S

sending messages. *See* messages
 serial connections between routers,
 3–5
 servers
 AAA servers, 176
 DHCP server configuration, 746–751
 DHCP servers, 212–215
 session keepalives, 1044
 session protection (LDP), 1073–1077
 Session stage (PPPoE), 181–182
 sessions (PPP), establishing
 Authentication Phase, 175–177
 Link Establishment Phase, 171–175
 Network Layer Protocol Phase,
 177–179
 sh interface command, 41, 48
 sh mac address-table dynamic vlan 21
 command, 48
 sh mac-address-table command, 41
 sh spanning-tree command, 37
 sh spanning-tree vlan 12 interface
 f0/19 detail command, 44
 sh version | inc Base command, 37
 sham links, 1141–1147
 shaping, class-based, 907–910
 Shortcut message (NHRP), 252
 show cdp neighbors command, 20
 show ip bgp peer-group TST
 command, 641
 show ip eigrp topology 8.8.8.0/24
 command, 341
 show ip route | include 3.3.3.0
 command, 629
 show ipv6 ospf database command,
 795
 show ipv6 route command, 750

- show ppp all command, 193
- show ppp interface command, 195
- shutting down ports, 20
- site-to-site IPsec VPN
 - basic site-to-site IPsec VPN, 911
 - IKE configuration*, 913–917
 - IKE Phase 1 message 1*, 917
 - IKE Phase 1 message 2*, 918–919
 - IKE Phase 1 message 3*, 919
 - IKE Phase 1 message 4*, 919–920
 - IKE Phase 1 message 5*, 920
 - IKE Phase 1 message 6*, 920–921
 - IKE Phase 2 message 1*, 921–925
 - ISAKMP, 912
 - OAKLEY, 912–913
 - policy guidelines*, 912
 - basic site-to-site IPsec VPN and NAT, 925–930
 - DMVPN tunnels, protecting, 946
 - F0/0 and loopback0 interfaces of R1, R2, and R3*, 947–948
 - hub and spoke configuration*, 948–952
 - IP routing, enabling*, 946–947
 - traffic protection*, 952–958
 - GRE/IP with Transport mode, 940–942
 - GRE/IPsec with Tunnel mode, 937–940
 - non-scalable configuration, 930–937
 - S-VTI, 942–946
 - SLAAC (stateless address auto-configuration), 743–746
 - source-protocol option, 600
 - Spanning Tree Backbone Fast, 148–154
 - Spanning Tree Loop Guard, 162–167
 - Spanning Tree Portfast, 106–115
 - Spanning Tree Root Guard, 154–162
 - spanning-tree portfast command, 75
 - sparse mode (PIM), 983–985, 994–997
 - spokes (DMVPN)
 - configuring for future DMVPN spokes, 304–311
 - Phase 1
 - dynamic mapping*, 232–236
 - static mapping*, 223–229
 - Phase 2
 - dynamic mapping*, 247–251
 - static mapping*, 240–244
 - Phase 3, 255–266
 - stateless address auto-configuration (SLAAC), 743–746
 - states
 - mroute states (IGMP), 971–974
 - port states, 74
 - static default routes
 - EIGRP (Enhanced Interior Gateway Routing Protocol), 287–289
 - OSPF (Open Shortest Path First), 388–389
 - static mapping
 - DMVPN Phase 1
 - hub and spoke configuration*, 223–229
 - NHRP (Next-Hop Resolution Protocol)*, 223–225
 - overview of*, 219, 220–239
 - DMVPN Phase 2
 - hub and spoke configuration*, 240–244

- interface and router configuration*, 237–240
 - overview of*, 236–237
- static RP (rendezvous point)**, 977
 - PIM sparse mode, 983–985
 - R2 and R3 configuration, 986–991
 - S1/4 interface on R5, 991–993
 - topology, 981–983
- static virtual tunnel interfaces (S-VTI)**, 942–946
- STP (Spanning Tree Protocol)**
 - advanced STP (Spanning Tree Protocol)
 - overview of*, 50
 - policy configuration*, 59–64
 - root bridge configuration*, 56–59, 65–67
 - switch configuration*, 54–55
 - switch hostname configuration*, 51–52
 - trunk port configuration*, 52–54
 - VLAN 100, 200, 300, and 400 *creation*, 55–56
 - VLAN 500 *creation*, 67–70
 - VLAN 600 *creation*, 70–73
 - basic STP (Spanning Tree Protocol)
 - designated ports, moving*, 43–45
 - initial configuration*, 36–41
 - IP and MAC addressing*, 36
 - root primary macro configuration*, 46–48
 - spanning-tree cost on port in VLAN 12, raising*, 41–42
 - spanning-tree port ID, raising*, 48–49
- BPDU filtering
 - F0/21 interface configuration*, 139–142
 - forwarding loops*, 142–146
 - overview of*, 135–136
 - policies*, 146–148
 - router and switch configuration*, 136–139
- BPDU Guard, 128–134
- MST (Multiple Spanning Tree), 93–94
 - boundary ports*, 94
 - configuring with policies*, 99–106
 - edge ports*, 94
 - IST (Internal Spanning Tree), 95
 - MSTP (Multiple Instance Spanning Tree Protocol), 96
 - port configuration*, 96
 - regions*, 94
 - switch hostname configuration*, 96
 - trunking mode*, 97
 - VLAN *configuration*, 97–99
- Rapid STP
 - initial configuration*, 76–77
 - lab setup*, 75–76
 - link type*, 83–85
 - operational enhancements of*, 74
 - overview of*, 73
 - port roles*, 74
 - port states*, 74
 - rapid convergence mechanisms*, 75, 78–80
 - rapid convergence process, demonstrating*, 80–83

- SW2, enabling for RSTP mode, 89–92*
- switch operation, 85–89*
- Spanning Tree Backbone Fast, 148–154
- Spanning Tree Loop Guard, 162–167
- Spanning Tree Portfast, 106–115
- Spanning Tree Root Guard, 154–162
- UplinkFast, 115–128
- stubs**
 - EIGRP (Enhanced Interior Gateway Routing Protocol)
 - EIGRP AS 100 configuration, 368–370*
 - igrp stub connected option, 373–374*
 - igrp stub option, 378–379*
 - igrp stub receive-only option, 377–378*
 - igrp stub redistributed option, 376–377*
 - igrp stub static option, 375–376*
 - igrp stub summary option, 375*
 - redistribution, 372–373*
 - static routes, 370–372*
 - summarization, 370*
 - topology, 368*
 - OSPF (Open Shortest Path First), 517
 - configuration, 523–526*
 - default route injection, 533–536*
 - loopback interfaces on R5, 532–533*
 - loopback30 interface on R3, 522–523*
 - R1's directly connected interfaces, 518*
 - R2's directly connected interfaces, 518–519*
 - R3's directly connected interfaces, 519–520*
 - R4's directly connected interfaces, 521–523*
- subnets keyword, 570, 626**
- suboptimal paths (OSPF), 549–555**
- Success message (CHAP), 199**
- summarization**
 - EIGRP (Enhanced Interior Gateway Routing Protocol)
 - configuration, 325–327*
 - fixed metric for the EIGRP summary route, 327–328*
 - loopback interfaces for R1, 349–350*
 - loopback interfaces for R2, 350*
 - loopback interfaces for R3, 351*
 - loopback interfaces for R4, 351–353*
 - R1 configuration, 358–359*
 - R2 configuration, 353–356*
 - R3 configuration, 357–358*
 - R4 configuration, 356–357*
 - topology, 349*
 - of internal/external networks
 - discard routes, 786–789*
 - external route summarization, 782–786*
 - loopback interface summarization, 778–782*
 - OSPFv3 configuration, 771–778*
 - overview of, 771*
 - OSPF (Open Shortest Path First)
 - advertising networks, 468–469, 472–475*

- discard routes*, 471–472
- external route summarization*, 467–468
- network summarization*, 470
- R1 configuration*, 465–466
- R2 configuration*, 464–465
- R3 configuration*, 463–464
- R4 configuration*, 463
- summary-address command, 783
- summary-prefix command, 783
- suppressing FA (forward address), 539–548
- SVCs (switched virtual circuits), 456–457
- S-VTI (static virtual tunnel interfaces), 942–946
- switch hostnames, 51–52, 96
- switch topology, 1–3
- switched virtual circuits (SVCs), 456–457

T

- tables (ARP), 9. *See also* filtering
- tagged routes, filtering, 619–622
- TCP/IP architecture, 7–8
- Terminate-Ack message, 175
- Terminate-Request message, 175
- testing TTL propagation, 1064–1065
- timers. *See* Hold timer
- topologies. *See* logical topology; physical topology
- TOS Byte field, 839
- totally stubby areas (OSPF), 517
 - configuration, 526–528
 - default route injection, 533–536
 - loopback interfaces on R5, 532–533
 - loopback30 interface on R3, 522–523
 - R1's directly connected interfaces, 518
 - R2's directly connected interfaces, 518–519
 - R3's directly connected interfaces, 519–520
 - R4's directly connected interfaces, 521–523
- traceroute 3.3.3.3 command, 263
- traceroute command, 613–614
- Traffic Indication message (NHRP), 265
- Transport mode (GRE/IPSec), 940–942
- trunk interfaces, verifying, 12–13
- trunk port configuration, 52–54
- trunking mode, 97
- tst-pool, 207
- TTL propagation, testing, 1064–1065
- tunnels
 - DMVPNs (dynamic multipoint virtual private networks)
 - DMVPN Phase 1 using dynamic mapping*, 232
 - DMVPN Phase 1 using static mapping*, 225–226
 - DMVPN Phase 2 using dynamic mapping*, 248–249
 - DMVPN Phase 3*, 259
 - protecting*, 946–952
 - GRE (Generic Routing Encapsulation), 504–506, 513–516
 - GRE/IPSec Tunnel mode, 937–940
 - S-VTI (static virtual tunnel interfaces), 942–946

two-way PAP authentication,
192–194

Type of Services (TOS Byte) field,
839

Type-1 LSAs, 793–795

Type-2 LSAs, 795

Type-4 LSAs, 539–548

Type-8 LSAs, 795–799

Type-9 LSAs, 799–800

U

U/L (universal/local) bit, 738

unicast configuration, 317–318

universal/local (U/L) bit, 738

UP phase (PPP), 177–179

UplinkFast, 115–128

username R4 password Cisco
command, 203

V

Value field (CHAP), 199

VIRL (Virtual Internet Routing
Lab), 5

virtual links
configuration, 509–513
overview of, 504–506

virtual local area networks. *See*
VLANs (virtual LANs)

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

Virtual Routing and Forwarding
(VRF), 1091–1095, 1134–1136

Virtual-Template interface, 207

VLANs (virtual LANs)
databases, verifying, 11–12
global configuration mode, 12

physical-to-logical topology lab
VLAN 12, 23–24
VLAN 13, 20–22
VLAN 28, 24–25
VLAN 34, 27–29
VLAN 45, 29–30
VLAN 56, 30–33
VLAN 789, 26–27

STP (Spanning Tree Protocol)
MST (Multiple Spanning Tree),
97–99
policies, 59–64
root bridge configuration,
56–59, 65–67
VLAN 100, 200, 300, and 400,
55–56
VLAN 500 creation, 67–70
VLAN 600 creation, 70–73

VPNID, 1094

VPNs (virtual private networks). *See*
also DMVPNs (dynamic multipoint
virtual private networks); IPsec
VPN

BGP routing in, 1148–1154

EIGRP routing in, 1107–1113

OSPF routing in, 1113–1122

RIPv2 routing in, 1078
*configuration between R1 and
PE-2*, 1096–1107
*configuration between R7 and
PE-6*, 1096–1107
*LDP configuration on core
MPLS routers*, 1084–1088
*MP-BGP AS 100 configuration
on R2 to R6*, 1088–1090
*OSPF configuration on core
MPLS routers*, 1081–1083
RDs (route distinguishers),
1091–1095

RTs (route targets), 1091–1095
topology, 1079–1081

VRF (Virtual Routing and Forwarding), 1091–1095

VRF (Virtual Routing and Forwarding), 1091–1095, 1134–1136

vrf definition command, 1091

W-X-Y-Z

weight attribute (BGP), 686–695

Wide Metric support (EIGRP), 341–342

Wireshark, 190