Practice Tests

Flash Cards

Study Planner

Glossary

Official Cert Guide

Advance your IT career with hands-on learning

CCNP Security Virtual Private Networks

SVPN 300-730

Joseph Muniz
Steven Chimes, CCIE® NO. 35525
James Risler, CCIE® NO. 15412

ciscopress.com

CCNP Security Virtual Private Networks

SVPN 300-730

Official Cert Guide

JOSEPH MUNIZ,
STEVEN CHIMES, CCIE No. 35525
JAMES RISLER, CCIE No. 15412

Cisco Press

CCNP Security Virtual Private Networks SVPN 300-730 Official Cert Guide

Joseph Muniz, Steven Chimes, James Risler

Published by:
Cisco Press

ScoutAutomatedPrintCode

Library of Congress Control Number: 2021946078

ISBN-13: 978-0-13-666060-6

ISBN-10: 0-13-666060-6

Warning and Disclaimer

This book is designed to provide information about the CCNP Security VPN (SVPN) Implementation 300-730 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

Alliances Manager, Cisco Press: Arezou Gol

Director, ITP Product Management: Brett Bartow

Executive Editor: James Manly

Managing Editor: Sandra Schroeder

Development Editor: Ellie Bru

Senior Project Editor: Tonya Simpson

Copy Editor: Kitty Wilson

Technical Editor(s): Viktor Bobrov, Joseph Mlodzianowksi

Editorial Assistant: Cindy Teeters

Cover Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Ken Johnson

Proofreader: Gill Editorial Services

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.**

Pearson's Commitment to Diversity, Equity, and Inclusion

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

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

Our ambition is to purposefully contribute to a world where:

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

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

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

About the Author(s)

Joseph Muniz is an architect and security researcher in the Cisco Security Sales and Engineering organization. He is driven by making the world a safer place through education and adversary research. Joseph has extensive experience in designing security solutions and architectures as a trusted advisor for top Fortune 500 corporations and the U.S. government.

Joseph is a researcher and industry thought leader. He speaks regularly at international conferences, writes for technical magazines, and is involved with developing training for various industry certifications. He invented the fictitious character Emily Williams to create awareness around social engineering. Joseph runs The Security Blogger website, a popular resource for security and product implementation. He is the author of and contributor to several publications, including titles ranging from security best practices to exploitation tactics.

When Joseph is not using technology, you can find him on the futbal (soccer) field or raising the next generation of hackers, also known as his children. Follow Joseph at https://www.thesecurityblogger.com and @SecureBlogger.

Steven Chimes, CCIE No. 35525, is a security architect in the Security Sales Engineering organization at Cisco, focused on building cybersecurity solutions for Cisco's largest global customers. He has more than 15 years of experience in the networking and cybersecurity fields, specializing in cross-domain solutions and emerging technologies. He has led the technical design for projects across the IT spectrum, including networking, security, analytics, identity, collaboration, compute, data center, and cloud.

When not building solutions, Steven is either teaching or learning. He is a distinguished speaker at Cisco Live and has spoken at Cisco Live events all over the world. He is also a serial collector of certifications, including CCIE Security, CCNP Enterprise, DevNet Associate, CISSP-ISSAP, GMON, and GCIH, among many others. What Steven finds most fulfilling, though, is mentoring the next generation of inspired cybersecurity professionals through programs such as Cisco High. Follow Steven @StevenChimes on Twitter.

James Risler, CCIE No. 15412, is a security training development manager in the Cisco Customer Experience organization. As senior manager of security content engineering at Cisco, he's constantly discovering and exploring the latest trends and issues in security, IT, and business. In his current role, he oversees teams responsible for both security and collaboration course development.

James is passionate about helping organizations understand the impact that security events can have on business and how to mitigate that risk. That's why he works to educate individuals and organizations in a variety of cybersecurity topics, including threat defense, virtual private networks, and firewall configuration, among others. Besides his work at Cisco, James works to help create the next generation of security defenders by holding training sessions and presentations for the University of Tampa Cybersecurity Club.

James is a distinguished speaker at Cisco Live; he holds Certified Information Systems Security Professional (CISSP) and Cisco Certified Internetwork Expert (CCIE) certifications; and he has earned a master's of business administration (MBA) from the University of Tampa. When he is not at work, he is either homebrewing or cooking up a complex meal. Follow James @JimRisler on Twitter.

About the Technical Reviewers

Viktor Bobrov, CCIE No 31489, is a security technical leader on the Customer Experience team at Cisco. He joined Cisco nine years ago and has worked on many large-scale security projects across many industries.

Viktor focuses on Cisco ISE, network segmentation, Cisco ASA, and Cisco AnyConnect technologies. He is also well versed in other security technologies, including Cisco Security Manager (CSM), DMVPN, and GETVPN.

Prior to joining Cisco, Viktor worked at a global advertising company as a global network architect, leading a team of network engineers to manage a network of 1000+ locations.

Aside from Cisco technologies, Viktor is also well versed in Microsoft Active Directory, public key infrastructure (PKI), mobile device management (MDM), and load balancers.

Viktor is a dual CCIE No. 31489 (Enterprise Infrastructure and Security).

Joseph Mlodzianowski is a highly respected member of the cybersecurity community, with more than 25 years in the industry. Joseph spent 8 years working for the Department of Defense and has multiple industry certifications, including CISSP, CCIE, CNE, ACMA, ITIL, and CERT, and he is a member of industry groups such as CyManII, M3aawg, and others.

Joseph is a hacker, instructor, author, and researcher, and he has worked with law enforcement on some of the largest botnet cases, including several industrial control system threats. Joseph is also a founding member of the DEFCON Red Team Village and has run events at some of the largest cybersecurity events in the world, including Black Hat, DEFCON, and RSA Conference. He is currently involved in organizing the Texas Cyber Summit in San Antonio, Texas, and the Grayhat Conference in Orlando, Florida.

Dedications

Joseph Muniz:

I would like to dedicate this book to two people. First, I want to dedicate it to Atticus Muniz, who can't read this book at one and half years old and will likely just use it as a seat or throwing object. Hopefully he will accomplish something great and, while doing so, make time to read this book. Second, I want to dedicate this book to Raylin Muniz, who is 11 going on 20. She continues to impress me with the number of books she consumes each week in between school and other things. Hopefully she also will add this book to her reading list and say she learned something from her dad. That probably won't happen, though.

Steven Chimes:

To my parents, for teaching me that anything is possible.

And to my wife, for making everything possible.

James Risler:

When you dedicate a book to someone, it must be for a compelling reason. Ann, this book is dedicated to you. Thank you for all you do for me. I cannot thank you enough for your love and support. Love, Jim

Acknowledgments

I'll start by apologizing to James Risler and Steven Chimes for sucking them into writing a book with me. Seriously, though, thanks, guys for putting up with me during the writing process. It's a lot of work but worth the impact we have in the security community.

I also want to thank the technical reviewers, Viktor Bobrov and Joseph Mlodzianowksi, who had to sort through our gibberish rough drafts and help us polish them into what ends up at the bookstore. Thank you, James Manly, Eleanor Bru, and the rest of the Pearson army that takes care of me every time we work on a project such as this one. You always are professional and make me feel like I'm part of the Pearson family. Thanks for that.

Finally, the most important thank-you goes to my friends and family. Anjelica Ruda, thank you for supporting me while I worked on this project during all of those late nights. Thank you, Gary McNiel, for mentoring me as well as giving me the ability to balance work, family, and writing. Finally, thank you to everybody who has supported me throughout my career. I truly feel lucky to have met the people in my life who have helped lead me to this moment: publishing this book.

—Joseph Muniz

First, to Joey Muniz and James Risler, thank you for unknowingly agreeing to write a book with me in the middle of a global pandemic; you both are nothing short of amazing. To Joey, a special thank-you, first for inviting me to write this book with you, but more importantly for helping guide it through to completion.

To Viktor Bobrov, thank you for always entertaining my challenging AnyConnect questions. I would spend a lot more time stumped in the lab if it were not for you. To both Viktor and Joseph Mlodzianowski, thank you for painstakingly wading through all the pages to find all of our mistakes; the final book would not be nearly as polished if it were not for your attention to detail. To James Manly, Eleanor Bru, and the rest of the Pearson team, thank you for everything you've done to make this book a success.

To my fellow Cisco colleagues, both past and present, thank you for all you have taught me throughout the years; there is not a day that goes by that I don't learn something new, and I can't imagine a better work family.

Last, but certainly not least, to my friends and family, thank you for all the love and support. To my mom and dad especially, thank you for nurturing the spark you saw so many years ago. And to my wife, Asra, and my daughter, Laila, words cannot express what your love and encouragement mean to me. I am a better person because of you.

—Steven Chimes

Thank you, Joey, for putting up with me as someone new to this process. You were a godsend. Also, Steven, thank you for all your help on VIRL. I really appreciated the time you took to help me get it up and running. You are both security professionals who set the standard for others to follow.

A special thank-you to my family for the support over the years. I am especially thankful to my security team at Cisco. Each of you has been instrumental in helping me over the years: Pat, Paul, Jagdeep, and Bill, know that I really appreciate it. I also want to thank Steven Sowell for his guidance and sticking with me through both the tough times and the good times.

Of course, last but not least, thank you to my friends and family, who have continued to provide love and support. Thank you, Ellie. I think you know I could not have done this without you.

—James Risler

Contents at a Glance

Online Elements

Contents

Online Elements

Command Syntax Conventions

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

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

Introduction

Congratulations! If you are reading this Introduction, then you have probably decided to obtain a Cisco certification and want to learn about VPN technology. As of February 24, 2020, in order to obtain a professional-level certification in security from Cisco, a candidate must pass two exams. One required milestone is the 350-701 SCOR core exam. The other exam is a concentration exam, and the Implementing Secure Solutions with Virtual Private Networks SVPN 300-730 exam is one option to meet the concentration exam requirement.

Obtaining a Cisco certification in VPN technology will ensure that you have a solid understanding of how to develop, configure, and support various types of VPN solutions. Securing communication has always been and will continue to be a critical topic for many organizations, and the skills covered in this book are extremely valuable. As more devices are provided network access and the concept of "work from anywhere" increases in popularity, knowledge of VPN technology will continue to be in demand. Protecting the confidentially, integrity, and availability of data is a fundamental requirement for every security program, and VPN technology is a tool commonly used to meet those objectives.

Professional certifications have been an important part of the computing industry for many years and will continue to become more important. Many reasons exist for these certifications, but the most popularly cited reason is credibility. All other factors being equal, a certified employee/consultant/job candidate is considered more valuable than one who is not certified. The SVPN 300-730 exam can be challenging, but this book can serve as a valuable tool for exam preparation to help you become certified in VPN technology. This book can also serve as a resource for those already in the field working with VPN solutions. After you pass the 300-730 SVPN exam, you earn the Cisco Certified Specialist - Network Security VPN Implementation, and you satisfy the concentration exam requirement for this professional-level certification.

Be sure to visit www.cisco.com to find the latest information on CCNP concentration requirements and to keep up to date on any new concentration exams that are announced.

Goals and Methods

The focus of this book is to teach how to develop and deliver Cisco VPN solutions. By accomplishing the learning objectives in this book, you will prepare yourself for taking the Implementing Secure Solutions with Virtual Private Networks SVPN 300-730 exam as well as deploying VPN technology. The goal of the book is to both help you pass the SVPN 300-730 exam and serve as a go-to resource when you are developing, deploying, and managing VPN technology. This book combines technical concepts with real-world experience, including tips and tricks for troubleshooting VPN deployment problems. Many parts of this book are inspired by our work with customers to deploy VPN technology.

One key methodology used in this book is to help you discover the exam topics that you need to review in more depth, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. Our goal is not to help you pass the SVPN 300-730 simply through memorization. The mixture of technology and lab concepts in this book is meant to help you truly learn and understand the VPN topics needed for both the exam and real-world deployments. This book will help you pass the SVPN 300-730 exam by using the following methods:

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

Who Should Read This Book?

This book is ideal for anybody interested in learning about VPN concepts and Cisco VPN technology, including those planning to take the SVPN 300-730 exam. However, anyone else who needs a resource for VPN concepts and Cisco VPN technology will also benefit from this book. We have a handful of objectives for writing this book, but the primary focus is to help you pass the exam.

Strategies for Exam Preparation

The strategy you use to study for the SVPN 300-730 exam might be slightly different than strategies used by other readers, depending on the skills, knowledge, and experience you have already obtained. For instance, if you have attended an SVPN 300-730 course, you might take a different approach than someone whose knowledge is based on job experience alone.

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

The Companion Website for Online Content Review

All the electronic review elements, as well as other electronic components of the book, exist on this book's companion website. To access the companion website, start by establishing a login at www.ciscopress.com and registering your book. To do so, simply go to www.ciscopress.com/register and enter the ISBN of the print book: 9780136660606. After you have registered your book, go to your account page and click the Registered Products tab. From there, click the Access Bonus Content link to get access to the book's companion website.

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

How to Access the Pearson Test Prep (PTP) App

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

- **Print book:** Look in the cardboard sleeve in the back of the book for a piece of paper with your book's unique access code.
- **Premium Edition:** If you purchase the Premium Edition eBook and Practice Test directly from the Cisco Press website, the code will be populated on your account page after purchase. Just log in at www.ciscopress.com, click Account to see details of your account, and click the Digital Purchases tab.
- **Amazon Kindle:** For those who purchase a Kindle edition from Amazon, the access code will be supplied directly by Amazon.
- **Other bookseller eBooks:** Note that if you purchase an eBook version from any other source, the practice test is not included because other vendors to date have not chosen to vend the required unique access code.

NOTE Do not lose the access code because it is the only means with which you can access the QA content with the book.

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

Step 1. Open this book's companion website.

Step 2. Click the **Practice Exams** button.

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

If you want to use the web app only at this point, just navigate to www.pearsontestprep.com, establish a free login if you do not already have one, and register this book's practice tests using the access code you just found. The process should take only a couple of minutes.

NOTE Amazon eBook (Kindle) customers: It is easy to miss Amazon's email that lists your Pearson Test Prep access code. Soon after you purchase the Kindle eBook, Amazon should send an email; however, the email uses very generic text and makes no specific mention of PTP or practice exams. To find your code, read every email from Amazon after you purchase the book. Also do the usual checks for ensuring your email arrives, like checking your spam folder.

NOTE Other eBook customers: As of the time of publication, only the publisher and Amazon supply Pearson Test Prep access codes when you purchase their eBook editions of this book.

How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need to more work with. Chapters 1 through 10 cover SVPN topics that are relevant for the SVPN 300-730 exam. These core chapters cover the following topics:

- **Chapter 1, "Understanding the Implementing Secure Solutions with Virtual Private Networks SVPN 300-730 Exam":** This chapter introduces drivers for getting certified in VPN technology as well as what is involved in getting certified at a professional level for Cisco security.
- **Chapter 2, "Introduction to Virtual Private Networks (VPNs)":** This chapter introduces fundamental VPN concepts, including an overview of the topics that covered in that book and a look at the Cisco technologies that offer VPN capabilities.
- **Chapter 3, "Site-to-Site VPNs":** This chapter takes a close look at site-to-site VPN technology and concepts you need to know to pass the SVPN 300-730 exam. This chapter also lays the groundwork for Chapters 4 through 6.
- **Chapter 4, "Group Encrypted Transport VPN (GETVPN)":** This chapter takes a closer look at a specific site-to-site VPN topic: GETVPN. This chapter covers everything from designing to managing GETVPN using Cisco technology.
- **Chapter 5, "Dynamic Multipoint Virtual Private Network (DMVPN)":** This chapter takes a deep dive into DMVPN. You need to master the deployment, management, and troubleshooting concepts covered in the chapter because they are heavily featured in the SVPN 300-730 exam.
- **Chapter 6, "FlexVPN Configuration and Troubleshooting":** This chapter covers various FlexVPN learning objectives outlined in the SVPN 300-730 exam blueprint as well as tips and tricks used in real-world FlexVPN deployments.

- **Chapter 7, "Remote Access VPNs":** This chapter examines remote access VPN technology. You will learn fundamental remote access VPN concepts, including which Cisco technologies support remote access VPNs. This chapter lays the groundwork for Chapters 8 through 10.
- **Chapter 8, "Clientless Remote Access SSL VPNs on the ASA":** This chapter focuses on clientless remote access VPN concepts specific to the Cisco ASA. Clientless VPNs continue to grow in popularity, and you need to understand them for the SVPN 300-730 exam.
- **Chapter 9, "AnyConnect VPNs on the ASA and IOS":** This chapter examines client-based remote access VPNs. The client you need to know for the SVPN 300-730 exam is Cisco AnyConnect, which is one of the VPN technologies deployed most widely in organizations around the world. This chapter covers how to deliver remote access VPNs using Cisco AnyConnect from both an appliance and IOS.
- **Chapter 10, "Troubleshooting Remote Access VPNs":** This chapter provides a wrap-up of the remote access VPN topics, with a focus on troubleshooting.
- **Chapter 11, "Final Preparation":** The final chapter covers how to prepare for the SVPN exam and resources you can use as a next step after reading this book.

The questions for each certification exam are a closely guarded secret. However, Cisco has published an exam blueprint that lists the topics you must know to successfully complete the exam. The blueprint for the SVPN 300-730 exam lists the following topics and the percentage of the exam that is dedicated to each of them:

15%	1.0 Site-to-site Virtual Private Networks on Routers and Firewalls 1.1 Describe GETVPN 1.2 Describe uses of DMVPN 1.3 Describe uses of FlexVPN
20%	2.0 Remote access VPNs 2.1 Implement AnyConnect IKEv2 VPNs on ASA and routers 2.2 Implement AnyConnect SSL VPN on ASA 2.3 Implement Clientless SSL VPN on ASA 2.4 Implement Flex VPN on routers
35%	3.0 Troubleshooting using ASDM and CLI 3.1 Troubleshoot IPsec 3.2 Troubleshoot DMVPN 3.3 Troubleshoot FlexVPN 3.4 Troubleshoot AnyConnect IKEv2 on ASA and routers 3.5 Troubleshoot SSL VPN and Clientless SSL VPN on ASA

30%	4.0 Secure Communications Architectures 4.1 Describe functional components of GETVPN, FlexVPN, DMVPN, and IPsec for site-to-site VPN solutions 4.2 Describe functional components of FlexVPN, IPsec, and Clientless SSL for remote access VPN solutions 4.3 Recognize VPN technology based on configuration output for site-to-site VPN solutions 4.4 Recognize VPN technology based on configuration output for remote access VPN solutions 4.5 Describe split tunneling requirements for remote access VPN solutions 4.6 Design site-to-site VPN solutions 4.6.a VPN technology considerations based on functional requirements 4.6.b High availability considerations 4.7 Design remote access VPN solutions 4.7.a VPN technology considerations based on functional requirements 4.7.b High availability considerations 4.7.c Clientless SSL browser and client considerations and requirements 4.8 Describe Elliptic Curve Cryptography (ECC) algorithms

You should be proficient with these topics for the exam as well as for designing and implementing Cisco VPN technology in the real world.

Each version of the exam can have topics that emphasize different functions or features, and some topics can be rather broad and generalized. The goal of this book is to provide the most comprehensive coverage to ensure that you are well prepared for the exam. Although some chapters might not address specific exam topics, they provide a foundation that is necessary for a clear understanding of important topics. Your short-term goal might be to pass this exam, but your long-term goal should be to become a qualified CCNP security engineer with an understanding of VPN technology.

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

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

Note that as VPN technologies continue to evolve, Cisco reserves the right to change the SVPN 300-730 exam topics without notice. Check Cisco.com to verify the actual list of topics to ensure that you are prepared before taking the exam. You can view the current exam topics on any current Cisco certification exam by visiting the Cisco.com website, choosing Menu, choosing Training & Events, and selecting from the Certifications list. Note also that, if needed, Cisco Press might post additional preparatory content on the web page associated with this book, at http://www.ciscopress.com/title/9780136660606. It's a good idea to check the website a couple of weeks before taking your exam to be sure that you have up-to-date content.

Figure Credits

Figure 1-1, WiFi Pineapple, from Hak5, LLC

Figure 1-3, Karma log within WiFi Pineapple, from Hak5, LLC

Figure 1-4, Masscan Ran Again a Target, from Robert David Graham

Figure 2-1, An Advertisement for the TunnelBear VPN Service, from TunnelBear LLC

Figure 2-8, Brute Force Attack Using Thc-pptp-bruter, from OffSec Services Limited

Figure 2-10, Splunk Managing Cisco AnyConnect Logs, from Splunk, Inc

Figure 2-14, TunnelBear Data Collection and Use Policy, from TunnelBear LLC

Figure 3-5, Certificate Warning Example, from Mozilla.org

Figure 7-53, Mobile Device Setup to use Meraki Remote Access VPN, from Apple, Inc

CHAPTER 5

Dynamic Multipoint Virtual Private Network (DMVPN)

"If you read someone else's diary, you get what you deserve."

—David Sedaris

This chapter covers the following subjects:

DMVPN Overview: This section provides an overview of the advantages DMVPN provides and compares DMVPN to the legacy site-to-site crypto map solution.

DVMPN Network Components: This section examines the components of DMPVN and how they work together to create a dynamic solution.

DMVPN Design Considerations: This section discusses design issues that must be considered before deploying a DMVPN solution as well as the differences between DMVPN phase 1, DMVPN phase 2, and DMVPN phase 3 configuration.

DMVPN Hub-and-Spoke Implementation for IPv4: This section steps through a basic DMVPN hub-and-spoke IPv4 configuration. Examples demonstrate how the DMVPN components interact to provide a comprehensive three-router solution.

DMVPN Hub-and-Spoke Implementation for IPv6: This section steps through a basic DMVPN hub-and-spoke IPv6 configuration.

DMVPN Troubleshooting: This section discusses how to troubleshoot DMVPN components and provides potential solutions.

This chapter covers the following exam objectives:

- 1.0 Site-to-site Virtual Private Networks on Routers and Firewalls
  - 1.2 Describe uses of DMVPN
- 3.0 Troubleshooting using ASDM and CLI
  - 3.1 Troubleshoot IPsec
  - 3.2 Troubleshoot DMVPN
- 4.0 Secure Communications Architectures
  - 4.1 Describe functional components of GETVPN, FlexVPN, DMVPN, and IPsec for site-to-site VPN solutions
  - 4.3 Recognize VPN technology based on configuration output for site-to-site VPN solutions
  - 4.6 Design site-to-site VPN solutions

Learning beyond the SVPN concepts:

- DMVPN Overview
- DMVPN Foundational Concepts
- DMVPN Design Considerations

In earlier chapters of this book, you have seen that secure VPN technology varies and has been adapted to be used in many different architectures by vastly different organizations. This chapter explores a dynamic adaptation of the site-to-site VPN solution. Traditional site-to-site VPNs did not scale easily, and Dynamic Multipoint Virtual Private Network (DMVPN) was designed to dynamically establish connections with minimal administrative overhead. Furthermore, traditional site-to-site VPNs had various challenges in supporting dynamic routing protocols, voice over IP (VoIP), and streaming video. All of these technologies are needed to support large-scale telecommuter and remote branch networks. In addition, the dynamic nature of DMVPN enables optimization of network paths, which in turn reduces latency and jitter, which are detrimental to VoIP and video. Organizations are finding that dedicated WAN circuits are no longer necessary for remote connectivity. In its place, organizations are using the Internet and secure communication through VPN technology to achieve the same benefits at a fraction of the cost.

A short summary of the value of DMVPN is that it can lower capital and operation expenses, simplify branch communications, reduce deployment complexity, and improve business resiliency. This is why DMVPN is a widely used VPN option and one you will need to master before attempting the SVPN exam. The SVPN exam expects you to be able to describe the components within a DMVPN deployment, recognize DMVPN configuration components, and troubleshoot a DMVPN deployment.

NOTE On the exam, you might see a configuration that includes a misconfigured or broken DMVPN solution. In such a situation, you will need to be able to determine what is wrong, and you will need to know the proper commands to fix the configuration. One of the best ways to learn and prepare for the exam is by getting hands-on experience. Reading this book and working with three routers to try out the examples shown in this chapter is a good way to prepare for the exam.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read the entire chapter. If you miss no more than one of these self-assessment questions, you might want to move ahead to the "Exam Preparation Tasks" section of the chapter. Table 5-1 lists the major headings in this chapter and the "Do I Know This Already?" quiz questions related to the material in each of those sections to help you assess your knowledge of these specific areas. The answers to the "Do I Know This Already?" quiz appear in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 5-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
DMVPN Overview	1–3
DMVPN Network Components	4–6
DMVPN Design Considerations	7–10
DMVPN Hub-and-Spoke Implementation	11, 12
DMVPN Troubleshooting	13

1. What are some of the benefits of DMVPN technology compared to legacy site-to-site VPN solutions? (Choose three.)
   - **a.** Multicast support
   - **b.** Crypto map enhancement
   - **c.** QoS support
   - **d.** Dynamic routing protocol capabilities
   - **e.** Complex administrative overhead
2. What is the primary reason companies select DMVPN over a legacy crypto map VPN solution?
   - **a.** Static Internet addresses
   - **b.** Dynamic Internet addresses
   - **c.** Complex configuration overhead
   - **d.** GRE support
3. What advantages does DMVPN offer that a crypto map–based VPN does not? (Choose two.)
   - **a.** Scalability
   - **b.** Lack of routing protocol support
   - **c.** Reduced configuration overhead
   - **d.** Increased bandwidth requirements
4. What are the key components of DMVPN? (Choose all that apply.)
   - **a.** mGRE
   - **b.** OSPF
   - **c.** NHRP
   - **d.** Static routes
   - **e.** IPsec
   - **f.** Routing protocols
5. Which DMVPN component is responsible for mapping the tunnel IP address to an external IP address?
   - **a.** OSPF
   - **b.** NHRP
   - **c.** ISAKMP
   - **d.** mGRE

6. Which DMPVN component enables the use of dynamic routing protocols across an IPsec tunnel?
   a. OSPF
   b. NHRP
   c. IPsec
   d. GRE
7. Which of the routing protocols used with DMVPN face a split-horizon issue? (Choose two.)
   a. OSPF
   b. EIGRP
   c. BGP
   d. RIP
8. Which routing protocol for use with DMVPN faces a non-broadcast multiple-access (NBMA) challenge that must be addressed?
   a. OSPF
   b. EIGRP
   c. BGP
   d. RIP
9. Which design considerations must you consider for DMVPN? (Choose two.)
   a. The number of IP address ranges
   b. The number of remote sites
   c. External IP addresses
   d. The need for quality of service (QoS) in applications
10. What is the difference between DMVPN phase 2 and DMVPN phase 3?
    a. There is no difference; they both support only hub-and-spoke solutions.
    b. DMVPN phase 2 supports hub-and-spoke solutions, and DMVPN phase 3 also supports spoke-to-spoke.
    c. DMVPN phase 2 has smaller routing tables.
    d. DMVPN phase 3 has smaller routing tables.
11. What key word on a hub router enables connections from any remote spokes?
    a. **multicast**
    b. **dynamic**
    c. **host**
    d. **map**
12. Which command for EIGRP prevents a hub router from setting the router advertisement out to a spoke to its own IP address?
    a. **no ip split-horizon eigrp 1**
    b. **ip eigrp 1 non-broadcast**
    c. **no ip broadcast eigrp 1**
    d. **no ip next-hop-self eigrp 1**

13. Which command would show whether the spoke router is registered with the NHS?
    a. show ip nhrp detail
    b. show ip nhs detail
    c. show ip nhrp nhs detail
    d. show ip nhrp client

Foundation Topics

Dynamic Multipoint Virtual Private Network (DMVPN) enables different branch locations to communicate in a direct and secure manner using either a public or a private network. DMVPN accomplishes this by utilizing a centralized architecture to ease implementation and management. This enables branch locations to communicate directly with one another, such as when using voice or video between offices, while also not requiring a permanent VPN tunnel between offices.

DMVPN creates a mesh VPN network that is applied selectively based on the connections being utilized by the organization. Each different location, or "spoke," can connect to any another location in a secure manner. The components involved include GRE tunnel interfaces, IPsec tunnel endpoint discovery, routing protocols for dynamically building the network, and NHRP for locating spokes. We dive into all these topics in this chapter, including supporting both IPv4 and IPv6 as well as troubleshooting your deployment.

The following highlight some of the key benefits of using DMVPN compared to a traditional MPLS network.

- It has the potential for high-performance VPN access at Internet speeds.
- It reduces the cost of secure communications and connections between branch locations by integrating VPN with communication technology (voice and video).
- The centralized system simplifies branch-to-branch connections.
- It reduces the risk of downtime by securing routing with IPsec technology.

DMVPN Overview

Many companies use DMVPN for their wide area network connectivity for one primary reason: It enables remote sites to have dynamic Internet addressing and yet still access corporate data in a cryptographically secure manner. With legacy VPN solutions, companies had to order static IP addresses at each remote site, thereby incurring an extra charge from the ISP and adding to the overall cost of the solution. Furthermore, as you added remote sites to such a solution, the hub router configuration grew exponentially. The days of configuring crypto maps, access control lists (ACLs), policies, and generic routing encapsulation (GRE) tunnels for each remote site have been replaced by the use of more mature and flexible VPN solutions. DMVPN specifically resolved the issues of static routing and cumbersome configuration with the use of an IPsec profile. In the legacy VPN configurations shown in Chapter 3, "Site-to-Site VPNs," you had to configure one crypto map with multiple policies, each with its own ACL, to indicate which traffic was permitted to go to which destination through the tunnel and what transform set would be used for the traffic. Each time you added another site-to-site VPN, you added to the policy and, potentially, to the non-NAT ACL.

Legacy Crypto Map VPN Solutions

Figure 5-1 shows an example of a legacy crypto map VPN tunnel solution. This solution requires specific configuration for each site; DMVPN does not require this much configuration. In addition, the legacy solution does not support spoke-to-spoke communication, whereas DMVPN does.

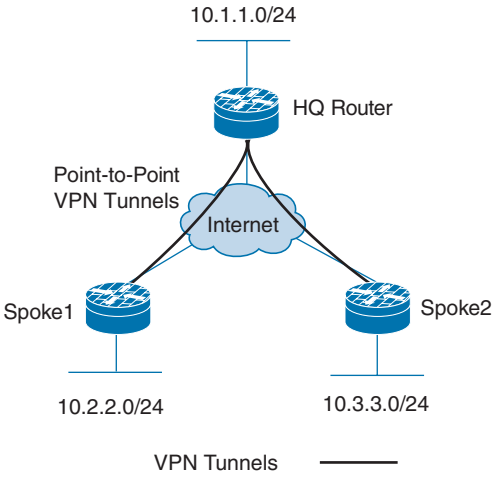

Figure 5-1 *Legacy VPN Tunnels*

Modern VPN Needs

As shown in Figure 5-2, companies today are using VPNs for a variety of services. In this diagram you can see a mobile user who may be using a video conferencing software package on a laptop in order to communicate. In addition, you can see a remote office that might have multiple users who all have VoIP phones behind the main router; they might need to be able to use the DMVPN solution for not only data but voice and video conferencing. We could expand this diagram by adding another remote office on the DMVPN network, and users from one office would be able to call users in another office by using VoIP rather than traditional dedicated phone circuits from the local provider.

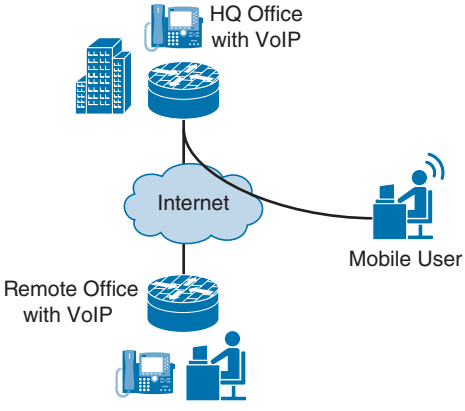

Figure 5-2 *A Telecommuter and a Remote Office with VoIP*

DMVPN Risks

Although DMVPN provides secure connectivity, it does not make you immune to attacks. Simply adding remote sites to a corporate network increases your organization's security risk. For example, if a teleworker's remote machine is infected with ransomware, it might be possible for that ransomware to find other clients to infect through the network. In a fully meshed DMVPN solution, such an attack could cripple an organization's capability to run its business (see Figure 5-3). So, as you are building out a VPN security solution, you should consider best practices for restricting, monitoring, and policing VPN traffic. Some examples of best practices would be to establish east–west access control and to monitor communications using traffic capture or NetFlow. In terms of packet monitoring security, implementing breach detection capabilities such as IPS/IDS technology should be considered essential.

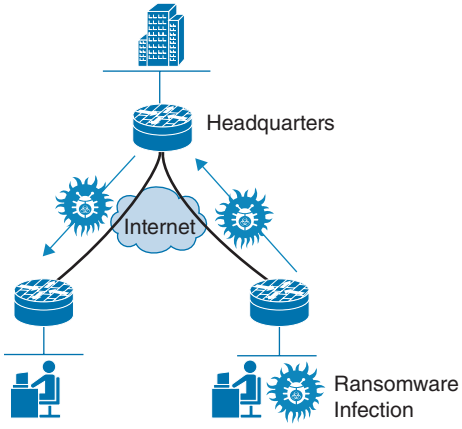

Figure 5-3 *Ransomware Infection*

DMVPN Core Concepts

The features available in a DMVPN solution are similar to those available with both GETVPN and FlexVPN. However, like those types of VPN architectures, DMVPN has its own components and terminology. For example, you need to know and understand GRE tunnels and **Next Hop Resolution Protocol (NHRP)**, which enable DMVPN to scale up to thousands of remote connections and reduce the need for complex administration.

DMVPN Example

Figure 5-4 shows an example of a DMVPN solution where each spoke can communicate with the hub router. In addition, Spoke1 and Spoke2 establish a VPN tunnel directly between themselves.

A critical piece of this solution is that GRE and NHRP work together to resolve the peer destination IP address. In essence, the NHRP configuration on a spoke router forces a registration process that maps the GRE tunnel IP address to the Internet IP address for the spoke on the hub NHRP database. Another critical piece of this solution is **multipoint Generic Routing Encapsulation (mGRE)**. We will look more closely at these two components in the next section.

DMVPN, as its name implies, also supports IPsec. The configuration combinations for IPsec are quite extensive, and this chapter covers only some of the key ones; in other chapters, you will see many other configurations that include IPsec. Let's look at the components of a DMVPN deployment.

Key Topic

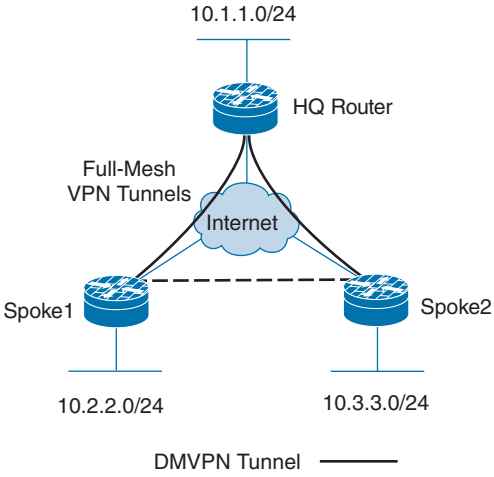

Figure 5-4 *A Full-Mesh DMVPN Tunnel*

DVMPN Network Components

As mentioned in the previous section of this chapter, DMVPN uses several components to achieve either a hub-and-spoke or a spoke-to-spoke solution: mGRE, NHRP, and IPsec. This section examines these components as well as the routing protocols that DMVPN supports. Make sure you are familiar with each of these components before moving to the next part of this chapter. First, we need to understand mGRE.

mGRE

mGRE enables routers to support multiple GRE tunnels on a single interface. This single interface can receive inbound GRE connections from dynamically addressed remote site locations and simultaneously support dynamic routing protocols, IP Multicast, and non-IP protocols. Both GRE and mGRE have a 24-bit header; in some situations, this header can impact application functionality. (We will examine this later in this chapter.) The advantage of using mGRE is that it enables the DMVPN network to replicate the function of a non-broadcast multiple-access (NBMA) multipoint Frame Relay solution (see Figure 5-5). Such solutions were more common in the past, when companies would purchase a Frame Relay WAN architecture from a telephone company and request that it be configured as multipoint. In Figure 5-5, which provides an example of the components in a DMVPN configuration, you can see that, in addition to a VPN tunnel, there are also GRE tunnels configured between sites.

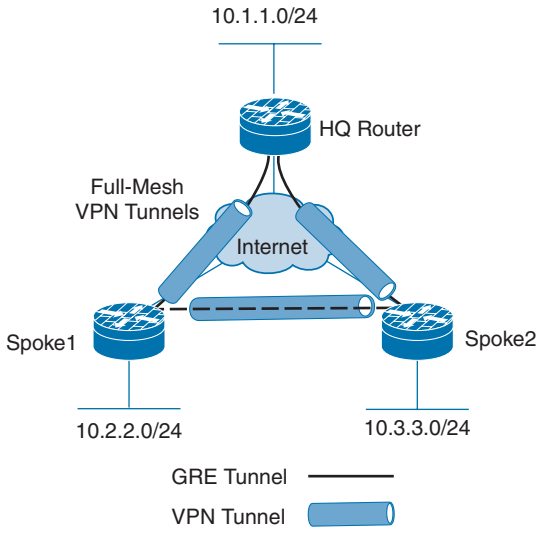

Figure 5-5 *GRE Tunnels*

GRE and mGRE Advantages

GRE and mGRE have many advantages both with DMVPN and in other solutions. For example, you can use a GRE tunnel to repair network routing links between OSPF areas that have become disconnected, causing routing updates between them to stop. Because GRE uses the IP protocol 47 and encapsulates the entire original IP payload, it supports nontraditional protocols as well as multicast and the use of routing protocols across a VPN tunnel.

GRE has a few limitations, but they are significant:

- GRE is not a cryptographic protocol, and it does not provide data protection.
- GRE can be CPU intensive, and you need to consider this during design.
- The IP MTU and fragmentation issue mentioned earlier might occur with some applications.
- Vendor GRE solutions are not all alike, and integration can be challenging.

NHRP

NHRP is used as the primary communication system for DMVPN hubs to inform spoke devices about other registered spokes. This is a classic client and server protocol: The server (hub) maintains the database of the spokes (clients) that have successfully registered. During the registration process, each spoke provides the server with its public IP address and the internal IP address of its GRE tunnel. The NHRP hub stores that information in the NHRP database so that other spokes can query the database for that information. Notice in Figure 5-6 that the NHRP registration occurs over the tunnel, and the NHRP packet includes the source address of the device that sent the tunnel, the destination address of the tunnel, and the NBMA address (public) of the destination device.

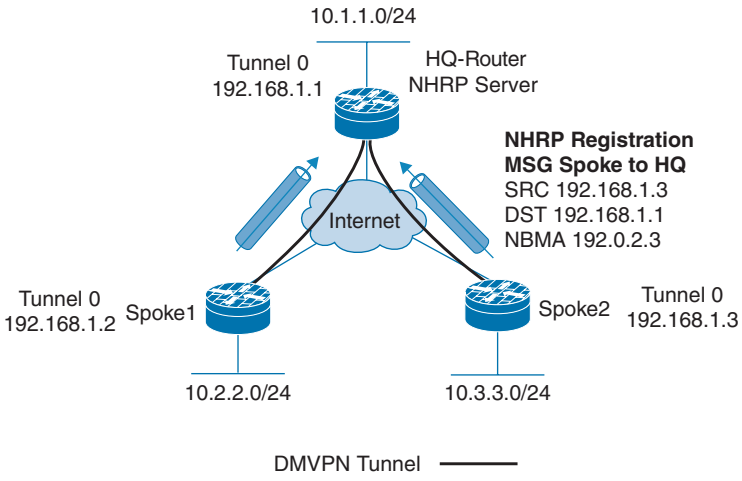

Figure 5-6 *NHRP Registration Process*

NHRP Example

Figure 5-6 shows IPsec tunnels, the GRE tunnel, and NHRP configured. It shows that the NHRP database on the NHRP server provides both the tunnel and the external IP address of a spoke router. This information is gathered during the spoke registration process.

Remaining DMVPN Components

IPsec is used to secure traffic going across a tunnel. Depending on the architecture of a DMVPN topology, it is possible for spokes to dynamically establish VPN tunnels with other spokes.

Routing is an often-overlooked piece of a DMVPN solution. However, routing is key because it enables a remote site to reach another remote spoke network that it did not initially have in its routing table prior to registration. Understanding DMVPN routing configuration comes down to understanding the shortfalls of routing protocols such as EIGRP and the split-horizon feature. With OSPF, an engineer would need to address the issue of NBMA with a multipoint OSPF configuration or set up a broadcast network.

Solution Breakdown

In studying and preparing for the SVPN 300-730 exam, a good approach would be to break down the components of a solution down into sub pieces. When you have mastered all the components, troubleshooting DMVPN will be much easier. Table 5-2 will help you study and focus on the key components of a DMVPN configuration.

Table 5-2 Basic DMVPN Configuration Components

Component	Requirement
Crypto configuration	Commands for ISAKMP and IPsec
Tunnel configuration	Commands to set up a tunnel interface
Next Hop Resolution Protocol	Commands to configure NHRP on both hub and spoke routers
Routing protocol configuration	Commands to configure a routing protocol for hub-and-spoke or spoke-to-spoke communications

DMVPN Design Considerations

Before you start designing a DMVPN network, it is critical to establish a goal for the solution. Just like with any VPN technology, you first need to understand what business problems you are going to solve. Once you have determined the goal, you can work back from the goal to the solution. We performed a similar exercise in the last chapter when covering design considerations for deploying GETVPN.

This section looks at some of the common design challenges and issues that security engineers must consider. In addition, equipment has a significant impact on a solution, and you might need to upgrade some of your equipment to support DMVPN, especially if you are trying to reuse existing equipment for remote site deployments. (Chapter 3 includes a list of pre-design questions that a team should consider before deploying DMVPN. Many of them specifically address equipment issues.)

DMVPN Planning

During the DMVPN design phase, a key constraint would be what applications will be running over the DMVPN links. Are you deploying VoIP or video conferencing solutions? Such low-latency applications might require QoS and priority over other applications. In addition, what level of fault tolerance is needed at the headend (hub) site to which the DMVPN remote sites connect? Will multicast traffic need to traverse the VPN links? What type of routing protocol will you use? The routing protocol setup requires some serious consideration. You should think about the following questions before configuring your routing protocol:

- What network IP blocks need to be accessible from the remote sites?
- Do remote site IP blocks need to be accessible from other locations?
- Does traffic need to be filtered for specific IP address ranges?
- Is QoS required?

Based on the answers to these questions, you might need to configure spoke-to-spoke communication across the VPN tunnel. If the objective of your design is to create spoke-to-spoke communication, you will need to answer another question: Will that traffic go through the headend router, or will it travel directly to the spoke? The answer impacts the configuration of your solution.

You need to think about all the questions posed so far, but these are just a few of the many considerations. Later in this chapter, you will see how to configure traffic from one spoke destined for another to be routed through the hub. You will also see how to configure a solution in which the spoke router can establish a direct VPN link to the other spoke router, thus reducing the overhead on the headend router.

NOTE Cisco has a DMVPN Design and Implementation guide available at https://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/dmvpn_design_guide.pdf?dtid=osscdc000283. We highly recommend that you review it before you deploy DMVPN.

DMVPN Fault Tolerance Considerations

We would be remiss if we did not talk about fault tolerance in this or any section that involves design considerations. Even though we do not focus on fault tolerance/high availability in our examples in this chapter, having multiple hub sites should be part of your design for high-availability purposes. Including multiple hub sites will add to the configuration on the spoke routers, but that additional work will not be a significant amount, and it could also increase the available bandwidth at the hub site. The level of fault tolerance your organization requires will impact your solution and its cost. As stated in the last chapter, we find cost is the number one factor that impacts how an organization will include fault tolerance within its VPN design.

Key DMVPN Considerations

One best practice we will continue to use in this chapter is creating a design on paper first. We recommend you share your design with your peers to validate and assess the design before moving forward with any deployment. The following are some of the many factors that should be documented and discussed before an implementation. You find this list to be similar to the one used in the last chapter.

- IOS requirements
- Platform capabilities (and upgrade options)
- IP address scheme: IPv4, IPv6, or both
- Tunnel addresses
- External (public) addresses
- DMVPN hub-and-spoke or partial mesh
- Routing requirements
- Authentication method: RSA signature, PKI, or pre-shared key
- Encryption scheme
- Deployment strategy
- Application requirements

DMVPN Phases

DMVPN comes in three different designs, referred to as DMVPN phase 1, DMVPN phase 2, and DMVPN phase 3. The DMVPN phase you choose determines how spokes communicate with one another as well as the routing configuration. In the next three sections we discuss the differences between each phase and the major configuration differences between them.

DMVPN Phase 1

DMVPN phase 1 is the first phase that was defined when this technology was implemented by Cisco and is strictly designed for hub-and-spoke communications only. Spoke-to-spoke traffic flows will need to reach the hub and then be transported to the other spoke. This is the same traffic flow as a hub-and-spoke design in Frame Relay or ATM. For example, consider the topology shown in Figure 5-7.

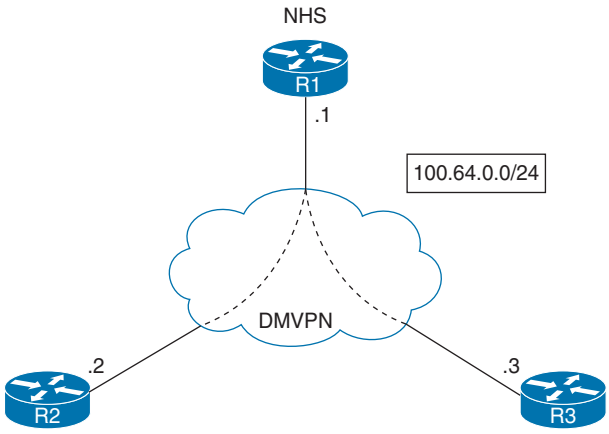

Figure 5-7 *Basic DMVPN Hub-and-Spoke Example*

R1 is acting as the DMVPN hub for this network and is therefore the NHS for NHRP registration of the spokes. In DMVPN phase 1 the GRE tunnels shown are multipoint GRE on the hub and point-to-point on the spokes. This forces hub-and-spoke traffic flows on the spokes. In addition to this, the next-hop value of any routes sent from the hub to spoke show the hub as the next hop. Therefore, a spoke has no knowledge of other spokes and sends all traffic destined to another spoke via the hub.

DMVPN Phase 2

In DMVPN phase 2, spoke-to-spoke traffic flow is now permitted, and all spoke routers implement multipoint GRE. Equally, resolution request NHRP messages are now sent to resolve a spoke's VPN address to its NBMA address. However, this function relies heavily on your routing design and in ensuring that the next-hop address is preserved during advertisement from the hub down to other spokes, much like how the next hop is preserved on an ethernet switch to allow more efficient traffic flows. To demonstrate this, the topology in Figure 5-8 has been updated to reflect this change.

In DMVPN phase 2, when a spoke router wants to communicate with another spoke router it will look at its routing table to determine the next-hop address. When routes are advertised from the hub, the next hop address is preserved. One downside of this is that each spoke has to hold the full network routing table for all spokes on the DMVPN network. This downside is because the routing and NHRP tables are unable to exchange information in DMVPN phase 2. In Figure 5-8, if Spoke1 had a change in its routing table with the failed link that triggered an update, Spoke2 would see this change and update its routing table. The reason is that the Spoke2 routing table has received routes from Spoke1 via the hub router, including the next hop of the tunnel address, which is 192.168.1.2 (Spoke1). Spoke1 only knows of Spoke2 through the tunnel address 192.168.1.3; it is not aware of the NBMA address (public) that lies in between. The hub router knows of the Spoke2 NBMA address and would forward the route update to Spoke2. You need to understand that changes or queries by any spoke of another spoke would, at a minimum, generate an NHRP resolution request to the hub. In this example, a failed link would generate not only an NHRP resolution request but also a routing protocol update packet.

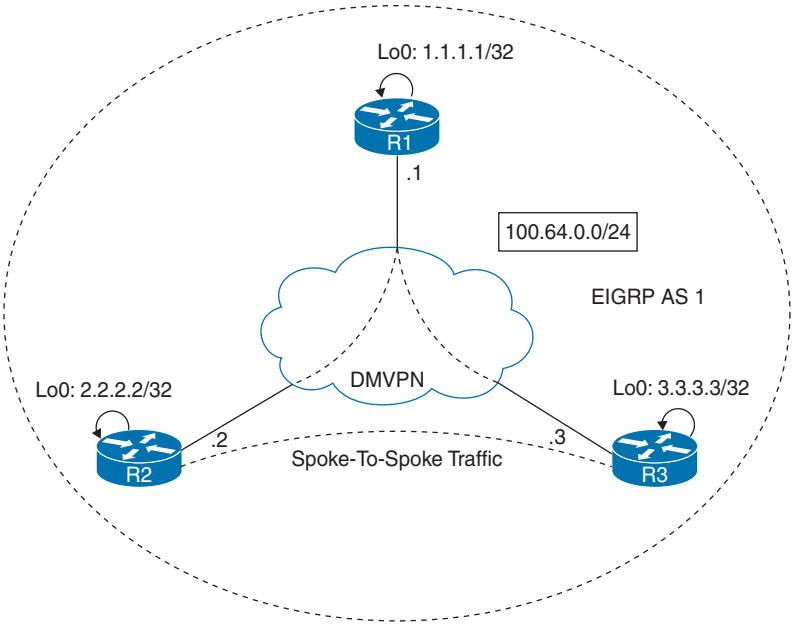

Figure 5-8 *Spoke-to-Spoke Added*

Figure 5-9 shows that a link on Spoke1 has failed. This figure demonstrates that in a DMVPN phase 2 solution, a failed link such as the one on Spoke1 will trigger a routing update being sent to Spoke2 to notify that router of the change.

Key Topic

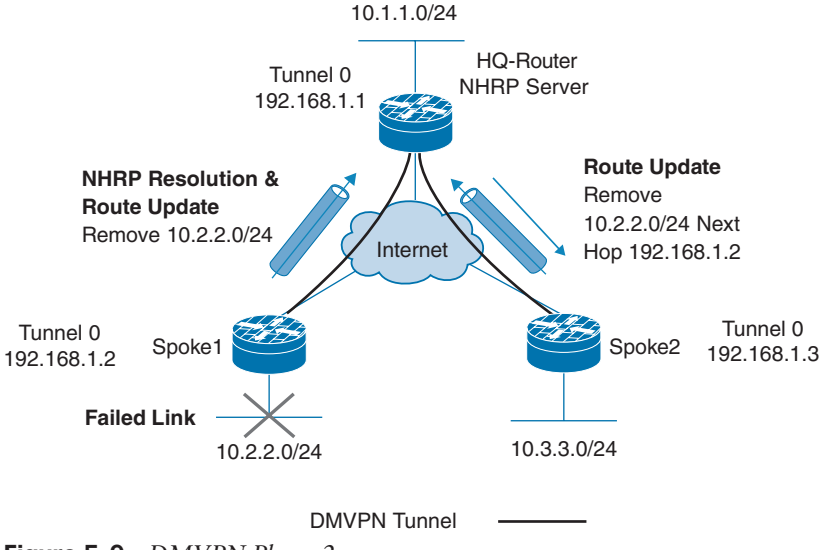

Figure 5-9 *DMVPN Phase 2*

DMVPN Phase 3

With DMVPN phase 3, Cisco modified the Cisco Express Forwarding (CEF) table and the NHRP table so that they can work together. This enables the NHRP table to resolve the next

hop information and the CEF table to route the packets. This change enables the hub router to set the next hop to itself and advertise summarized routes to all of the spokes. This configuration option supports the use of smaller spoke routers by eliminating the need to support the entire corporate routing table.

Now that we have tackled all the design concepts behind DMVPN, we next learn what is involved with deploying DMVPN. Let's first start with a look at a hub-and-spoke implementation.

DMVPN Phase 1 Hub-and-Spoke Implementation

Now it is time to dive into DMVPN implementations. The best way to address learning how technology is configured is to break it down into manageable parts. This section shows the implementation of a basic hub-and-spoke DMVPN design for both IPv4 and IPv6 by breaking down the process into four parts. We highly recommend that you understand how each part works as you study DMVPN technology because you will see questions about the different parts of a DMVPN configuration on the SVPN exam. The following are the four parts of a DMVPN configuration:

- Crypto IPsec policy configuration
- GRE tunnel configuration
- NHRP hub-and-spoke configuration
- Routing configuration

Breaking down the process into these four parts will make it easier to troubleshoot which part of the configuration is incorrect and which parts are correct. It will also help with identifying wrong answers for questions about specific parts of a DMVPN configuration. For example, if you are dealing with a routing issue, any answer regarding the GRE tunnel configuration could be eliminated.

Figure 5-10 shows the topology and IPv4 design, and Figure 5-11 shows the topology and IPv6 design for the following configuration examples. Use this as a reference for this next section.

Key Topic

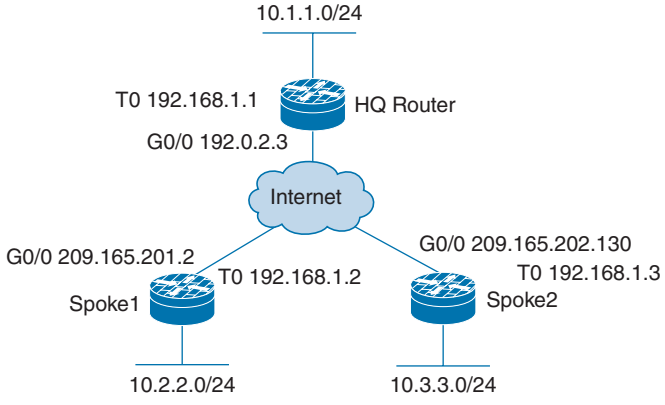

Figure 5-10 *DMVPN IPv4 Solution*

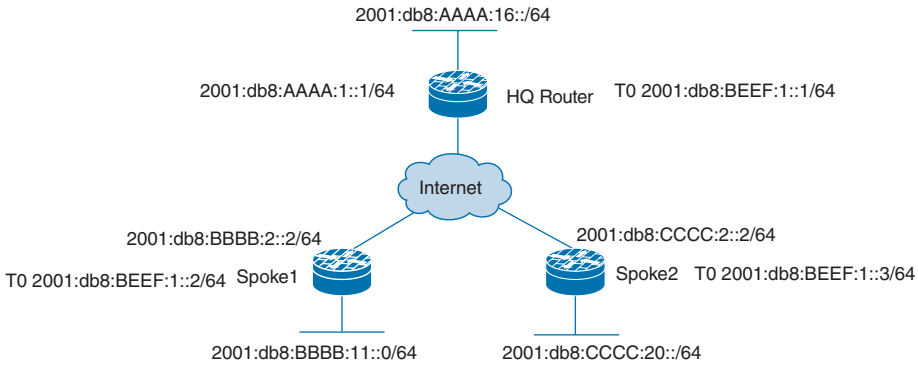

Figure 5-11 *DMVPN IPv6 Solution*

Crypto IPsec Policy Configuration

As discussed in earlier chapters, the Internet Key Exchange (IKE) management protocol is primarily used to authenticate IPsec peers. Configuring a crypto IPsec policy can be broken into the following three steps:

- Creating an IKE Policy
- Creating Pre-shared Key Authentication Credentials
- Creating a Profile and Transform Set

This section works through each of these three steps starting with creating an IKE Policy.

Creating an IKE Policy

In Example 5-1, the IKE management protocol is used by the two spoke routers and the hub router to authenticate, negotiate, and distribute IPsec encryption keys. Today, this is optional on some Cisco platforms because there is a default IKE policy; however, your organization may require a more secure policy. In this example, this policy will be repeated on the two remote site routers (spokes) and must match the HQ router policy. Let's work through each step of the IKE policy configuration. We will break this into steps as well to clearly work through how the configuration is performed.

Example 5-1 shows the basic crypto IKE policy used by all the routers in Figures 5-8 and 5-9.

Example 5-1 *Creating an IKE Policy*

```
HQ-Router(config)# crypto isakmp policy 10
HQ-Router(config-isakmp)# encryption aes 192
HQ-Router(config-isakmp)# hash sha256
HQ-Router(config-isakmp)# authentication pre-share
HQ-Router(config-isakmp)# group 5
```

The policy shown in Example 5-1 is policy number 10. You can have policies from 1 to 65,535, ordered by priority. If you establish a VPN with another router that does not have a policy matching this one, your router could potentially find another policy that might match

the remote side. If, during troubleshooting, you notice that the IKE policy fails to negotiate, the first place to look is at the IKE policy parameters on both routers.

Example 5-1 shows the use of AES-192 encryption and the hash policy SHA-256. Notice in this example that the authentication in use is pre-shared. This means that you are going to have to manually set up authentication keys on all the DMVPN routers. Another option would be to use certificate authority (CA) signatures. The third method for authentication would be to use encrypted nonces. (Both forms of certificate authentication are discussed in Chapter 3.) We recommend that you take the time to learn how to use certificates for authentication because this process is critical for large-scale deployments. By using certificates, you remove the need to keep track of pre-shared keys, which significantly improves security.

Finally, Example 5-1 specifies group 5 for the Diffie-Hellman key algorithm, which uses a 1536-bit modulus, which in turn uses 2048 bits to create a prime and generate numbers as security association (SA) keys. Depending on your router and its IOS version, you might be able to create a more secure solution by increasing the AES encryption to AES-256 with SHA-512. Chapter 7, "Remote Access VPNs," covers encryption in more detail.

Creating Pre-shared Key Authentication Credentials

The next step is creating a pre-shared key. Example 5-2 shows an implementation of IPv4 pre-shared keys for the two remote spoke routers.

Example 5-2 *Creating Pre-shared Key Authentication Credentials, IPv4*

```
HQ-Router(config)# crypto isakmp key TESTKEY address 209.165.201.2
HQ-Router(config)# crypto isakmp key TESTKEY address 209.165.202.130
```

On the main router, you need to reference the remote site routers or, in this case, the spokes. It is critical that you reference the public IP address of the router or the address that is reachable by the router if you are implementing a DMVPN solution on a private network. The spoke routers at first have just one crypto pre-shared key configuration line. With spoke-to-spoke configuration, this changes, as you'll see later in this chapter.

Example 5-3 shows an implementation of IPv6 pre-shared keys for the two remote spoke routers.

Example 5-3 *Creating Pre-shared Key Authentication Credentials, IPv6*

```
HQ-Router(config)# crypto isakmp key TESTKEY address ipv6 2001:db8:bbbb:2::2/64
HQ-Router(config)# crypto isakmp key TESTKEY address ipv6 2001:db8:cccc:2::2/64
```

Notice in Example 5-3 that the IPv6 command has similar syntax to the IPv4 command, and both reference the public endpoint IP addresses of the devices that are authenticating.

Example 5-4 shows the IPv4 pre-shared key used by the spoke to authenticate to the hub router.

Example 5-4 *Spoke Router Pre-shared Key in IPv4*

```
Spoke1(config)# crypto isakmp key TESTKEY address 192.0.2.3
```

Similarly, with IPv6, the spoke would reference the public IPv6 address of the hub router. Example 5-5 shows the IPv6 pre-shared key used by the spoke to authenticate to the hub router.

Example 5-5 *Spoke Router Pre-shared Key in IPv6*

```
Spoke1(config)# crypto isakmp key TESTKEY address 2001:db8:aaaa:1::1/64
```

Creating a Profile

Next, you need to create a profile and transform set. Example 5-6 shows the implementation of a profile and transform set, which is the same for IPv4 and IPv6 and the same on both the hub and the spoke.

Example 5-6 *Creating a Profile and a Transform Set for IPv4 or IPv6*

```
HQ-Router(config)# crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
HQ-Router(cfg-crypto-trans)# mode tunnel
HQ-Router(cfg-crypto-trans)# crypto ipsec profile MYIPSECPROFILE
HQ-Router(ipsec-profile)# set transform-set MYSET
```


Notice that these two commands are tied together by the crypto profile referencing the transform set. You will see later how the profile is used by the DMVPN configuration. As discussed in Chapter 3, the transform set is for IKE Phase 2 negotiation of the encrypted tunnel. As with the IKE policy, some IOS versions now include a default transform set, as you can see with the command **show crypto ipsec profile** in Example 5-7. The key pieces of the transform set are the encryption method, the hash type, and whether Perfect Forward Security (PFS) is used. These must all match except for the security association lifetime. The two sides select the SA lifetime with the smallest size and use that for the tunnel.

In Example 5-7, the command **show crypto ipsec profile** validates your previous profile configuration steps.

Example 5-7 *Output Crypto IPsec Profile*

```
HQ-Router(config)# show crypto ipsec profile
IPSEC profile MYIPSECPROFILE
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                MYSET:  { esp-aes esp-sha-hmac  } ,
        }
IPSEC profile default
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Mixed-mode : Disabled
        Transform sets={
                default:  { esp-aes esp-sha-hmac  } ,
        }
```

Creating a Transform Set

The transform set is a collection of individual IPsec parameters designed to implement the security policy on the traffic that is transmitted across the tunnel. During ISAKMP IPsec security association negotiation, the two routers need to agree on the parameters; if the parameters are not the same, the tunnel setup fails. For example, if one side has transport mode set to AH and the other side only supports ESP, the negotiation will fail.

Example 5-8 shows how to verify the transform set configuration. It is important that both sides of the tunnel solution have a match.

Example 5-8 *Verifying the IPsec Transform Set*

```
HQ-Router(config)# show crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set MYSET: { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

In the default configuration, transport mode only protects the upper layer protocols with payload encapsulation mode, and tunnel mode protects the entire IP datagram.

GRE Tunnel Configuration

A GRE tunnel is required for a DMVPN network. If you think about it, the tunnel interface allows the consolidation of numerous remote site point-to-point links into one interface. In some of the legacy Cisco site-to-site configurations, you would have one crypto map on the outside interface with multiple configuration sections for each remote site VPN link. That would cause the router configuration to be extensive and possibly complex to troubleshoot. With the GRE tunnel solution, you have one tunnel interface scaling to support hundreds of remote site locations. The tunnel interface is designated as a multipoint interface, resulting in an NBMA network. Typically, when you configure a GRE tunnel, the source and destination IP addresses are configured so that the tunnel can be established; however, with DMVPN, you do not need this because you use NHRP to solve endpoint address resolution.

A GRE tunnel configuration on the hub consists of a single step, which is creating a multipoint GRE tunnel.

Creating a Multipoint GRE Tunnel on the Hub

Example 5-9 shows how to build a basic DMVPN hub router tunnel configuration. The key to this configuration is the **tunnel** command, which sets the mode to **multipoint**. This tunnel configuration works for both IPv4 and IPv6.

Example 5-9 *Creating a Multipoint GRE Tunnel on a Hub Router for IPv4 or IPv6*

```
HQ-Router(config)# interface tunnel0
HQ-Router(config-if)# ip address 192.168.1.1 255.255.255.0
HQ-Router(config-if)# ipv6 address 2001:db8:aaaa:1::1/64
HQ-Router(config-if)# tunnel source GigabitEthernet1
HQ-Router(config-if)# tunnel mode gre multipoint
HQ-Router(config-if)# tunnel key 12345
```

Notice that Example 5-9 has both an IPv4 address and an IPv6 address on the tunnel interface. That means you can configure it for either solution, and you can select the one you need for your environment. If IPv6 is used, the command **tunnel mode gre multipoint** must be changed to **tunnel mode gre multipoint ipv6**. It is possible to use the **tunnel mode** command without the **ipv6** keyword, but without this keyword, your IPv6 configuration will not work. The tunnel source is the outside interface (that is, the interface of the router in this example).

NOTE We cannot stress enough the importance of using the **ipv6** keyword with the **tunnel mode** command for IPv6 because it is critical.

The command **tunnel mode gre multipoint** in Example 5-9 makes the GRE tunnel a multipoint GRE (mGRE) tunnel, which allows multiple remote sites to be grouped into a single multipoint interface. The **tunnel key** command provides a weak form of security, but it could help prevent misconfiguration of a remote site from impacting a large-scale DMVPN environment.

Creating a GRE Tunnel on the Spoke

Unlike the hub, in DMVPN phase 1 the spoke uses a point-to-point tunnel. To put it another way, the command **tunnel mode gre multipoint** is replaced with the command **tunnel destination** *ip_address*, where *ip_address* is the public IP address of the hub router, as shown in Example 5-10.

Example 5-10 *Configuring a Spoke Router for IPv4*

```
Spoke1(config)# interface tunnel0
Spoke1(config-if)# ip address 192.168.1.2 255.255.255.0
Spoke1(config-if)# tunnel source GigabitEthernet0
Spoke1(config-if)# tunnel destination 192.0.2.3
Spoke1(config-if)# tunnel key 12345
```

Example 5-11 shows the IPv6 configuration of a spoke router tunnel interface.

Example 5-11 *Configuring a Spoke Router for IPv6*

```
Spoke1(config)# interface tunnel0
Spoke1(config-if)# ipv6 address 2001:db8:beef:4::2/64
Spoke1(config-if)# tunnel source GigabitEthernet0
Spoke1(config-if)# tunnel destination 2001:db8:aaaa:1::1
Spoke1(config-if)# tunnel key 12345
```

The tunnel configuration for the spoke router references the outside interface with the **tunnel source** command. Because GRE is the default tunnel mode, no specific tunnel mode command is required to support both unicast and multicast traffic. It will be important that the tunnel supports the use of multicast communication mechanisms later, when you want to run routing protocols such as OSPF. As mentioned earlier, the **tunnel key** command provides

a weak form of security, preventing misconfiguration of a spoke router from impacting a production DMVPN network.

NHRP Hub-and-Spoke Configuration

The next part of the configuration is the NHRP hub-and-spoke configuration. Configuring NHRP for hub-and-spoke is a three-step process on the hub:

- Configure NHRP
- Configure the tunnel
- Configure tunnel optional parameters

Configure NHRP on the Hub

Let's start by setting up NHRP using IPv4. Example 5-12 shows the required commands for NHRP on a hub router tunnel interface with IPv4.

Key Topic

Example 5-12 *Setting Up NHRP IPv4 Server Parameters on the mGRE Tunnel*

```
HQ-Router(config)# interface tunnel0
HQ-Router(config-if)# ip nhrp authentication KEY123
HQ-Router(config-if)# ip nhrp map multicast dynamic
HQ-Router(config-if)# ip nhrp network-id 1
```

Example 5-13 shows the required commands for NHRP on a hub router tunnel interface for IPv6. Notice that these two examples are almost the same; the only difference is the addition of **ipv6** at the start of the commands in Example 5-13.

Example 5-13 *Setting Up NHRP IPv6 Server Parameters on the mGRE Tunnel*

```
HQ-Router(config)# interface tunnel0
HQ-Router(config-if)# ipv6 nhrp authentication KEY123
HQ-Router(config-if)# ipv6 nhrp map multicast dynamic
HQ-Router(config-if)# ipv6 nhrp network-id 1
```

The tunnel interface is set up as NBMA. You need a mechanism to allow the remote sites to communicate with the hub router. NHRP acts like dynamic DNS, as it allows remote sites to communicate and register with the DMVPN hub router. The command **map multicast dynamic** in Example 5-12 and Example 5-13 enables the DMVPN hub router to receive inbound registration requests from any spoke router IP address. Furthermore, the **dynamic** command enables the replication of multicast packets to each of the spoke routers through the single tunnel interface. Think of this in terms of the hub router referencing the NHRP database, and for each entry, it sends a unicast/multicast packet to that spoke IP address. It does this until each spoke has received the routing update. This way, the router is able to establish dynamic routing protocol adjacencies by utilizing the database to map the multicast endpoints.

Configure NHRP on the Spoke

The configuration of NHRP on the spoke router is different from the configuration on the hub router. Notice that there are a few more commands, and you must specify the IP address of the next hop server. In this case, you provide the tunnel IP address for the hub router.

In addition, you add an NBMA address that can receive the broadcast or multicast packets you send out the tunnel interface. Finally, the key to mapping the NHRP tunnel address to the outside public address is to provide the mapping of the NHS tunnel IP address (192.168.1.1) to the NBMA IP address (192.0.2.3).

Example 5-14 shows a basic IPv4 NHRP configuration setup.

Key Topic

Example 5-14 *Configuring NHRP on a Spoke Router for IPv4*

```
Spoke1(config)# interface tunnel0
Spoke1(config-if)# ip nhrp authentication KEY123
Spoke1(config-if)# ip nhrp network-id 1
Spoke1(config-if)# ip nhrp nhs 192.168.1.1
Spoke1(config-if)# ip nhrp map multicast 192.0.2.3
Spoke1(config-if)# ip nhrp map 192.168.1.1 192.0.2.3
```

The IPv6 configuration of NHRP on the spoke is different from the configuration on the hub router, just as it is for IPv4. You use a few more commands and must specify the IP address of the NHS. In this case, you provide the tunnel IP address for the hub router (2001:db8:beef:1::1). In addition, you add an NBMA address that can receive the broadcast or multicast packets you send out the tunnel interface. Finally, it is critical to provide the mapping of the NHS tunnel IP address (192.168.1.1) to the NBMA IP address (192.0.2.3).

Example 5-15 shows a basic IPv6 NHRP configuration setup.

Example 5-15 *Configuring NHRP on a Spoke Router for IPv6*

```
Spoke1(config)# interface tunnel0
Spoke1(config-if)# ipv6 nhrp authentication KEY123
Spoke1(config-if)# ipv6 nhrp network-id 1
Spoke1(config-if)# ipv6 nhrp nhs 2001:db8:beef:1::1
Spoke1(config-if)# ipv6 nhrp map multicast 2001:db8:aaaa:1::1
Spoke1(config-if)# ipv6 nhrp map 2001:db8:beef:1::1/64 2001:db8:aaaa:1::1
```

Configure Tunnel Protection

Now we need to configure the tunnel interface. Example 5-16 shows the configuration required to encrypt the traffic passing through the tunnel. This same configuration should be applied to both the hubs and the spokes.

Example 5-16 *Configuring the Tunnel Interface with IPsec Profile Protection*

```
HQ-Router(config)# interface tunnel0
HQ-Router(config-if)# tunnel protection ipsec profile MYIPSECPROFILE
```

The **tunnel protection ipsec profile** command applies the IPsec profile created previously to the tunnel interface. No crypto map is required. All traffic that passes through the tunnel will be encrypted with IPsec, and traffic outside the tunnel will not be encrypted. The use of tunnel protection and an IPsec profile significantly simplifies the IPsec configuration when compared to crypto maps.

Configure Tunnel Optional Parameters

Next, we need to address issues such as MTU size and the maximum segment size that is negotiated during the TCP synchronization handshake. For any TCP packet going through the tunnel, the router will adjust the maximum segment size (MSS) in the TCP header to match the value you have set it to. This will force the end hosts to also adjust their setting to this value. The **mtu** and **adjust-mss** commands help resolve issues with most TCP-based applications that need to traverse the DMVPN tunnel.

Example 5-17 shows additional commands to prevent applications from failing to function across the DMVPN tunnel.

Example 5-17 *Configuring the Tunnel Interface with Optional IP Parameters*

```
HQ-Router(config)# interface tunnel0
HQ-Router(config-if)# ip mtu 1400
HQ-Router(config-if)# ip tcp adjust-mss 1360
```

IPv6 has a different header than with IPv4. You still have to be concerned about the MTU size, but with IPv6, the fragmentation and reassembly process is improved; thus, most hops can handle average IP datagrams along the path without needing to fragment packets.

IPv6 has built-in solutions to address fragmentation, and Example 5-18 shows that you only need to adjust the MTU size.

Example 5-18 *Sample IPv6 Configuration of the Tunnel Interface*

```
HQ-Router(config)# interface tunnel0
HQ-Router(config-if)# ipv6 mtu 1400
```

Routing Protocol Configuration

Routing protocol configuration is the final part in setting up a DMVPN solution. During the design phase, you needed to determine which routing protocol you would select. There are a few options, such as EIGRP or OSPF. This section walks you through an example of configuring EIGRP. (For other configuration examples, such as OSPF, please refer to the documentation links included at the end of this chapter.)

Configure Routing on the Hub

With DMVPN, the NHRP database enables the hub router to replicate the individual multicast packets needed by the routing protocol to each site, one by one. In DMVPN, the routing protocol neighbor relationship is only established between the hub and the spoke routers. Thus, the hub is responsible for distributing routes learned from one spoke back out to another spoke. Thus, you run into an issue where a feature in the link state routing protocols, split horizon, works against you. With split horizon, any network learned on an EIGRP interface is not advertised back out the same interface. With DMVPN, you must disable this so that routes propagate successfully to all of the spoke routers.

Example 5-19 shows how to configure EIGRP for IPv4. Notice the commands **no auto-summary** and **no ip split-horizon eigrp 1**.

Example 5-19 *IPv4 Hub Router Configuration*

```
HQ-Router(config)# router eigrp 1
HQ-Router(config-router)# no auto-summary
HQ-Router(config-router)# network 10.1.1.0 0.0.0.255
HQ-Router(config-router)# network 192.168.1.0 0.0.0.255

HQ-Router(config-router)# interface tunnel 0
HQ-Router(config-router)# no ip split-horizon eigrp 1
```

Notice that Example 5-19 includes a command under the tunnel interface that disables split horizon. In addition, you can (for EIGRP) disable route summarization on the hub so that the hub router will send complete spoke route information out to each spoke rather than summarizing it.

Configure Routing on the Spoke Using IPV4

Example 5-20 shows the IPv4 spoke router configuration for EIGRP.

Example 5-20 *IPv4 Spoke Router Configuration*

```
Spoke1(config)# router eigrp 1
Spoke1(config-router)# no auto-summary
Spoke1(config-router)# network 10.2.2.0 0.0.0.255
Spoke1(config-router)# network 192.168.1.0 0.0.0.255
```

The spoke routers have a simple EIGRP configuration that identifies the GRE tunnel IP network and the inside network that you need propagated to the hub routing table.

Example 5-21 shows the IPv6 configuration of EIGRP on the hub router.

Example 5-21 *IPv6 Hub Router Configuration*

```
HQ-Router(config)# ipv6 unicast routing
HQ-Router(config)# ipv6 cef
HQ-Router(config)# ipv6 router eigrp 1
HQ-Router(config-rtr)# eigrp router-id 192.0.2.3
HQ-Router(config-rtr)# interface tunnel 1
HQ-Router(config-if)# ipv6 eigrp 1
```

Configure Routing on the Spoke Using IPV6

For the IPv6 configuration, we show you an example of enabling IPv6 unicast routing on the router and then configuring the IPv6 router with an EIGRP router ID. It is a good practice to control the router ID; in this case, you are using the outside IPv4 address of the HQ router, which is 192.0.2.3. (Yes, in an IPv6 configuration, you can use an IPv4 address as an identifier.)

Next, on the interface tunnel, you enable EIGRP routing by specifying IPv6 EIGRP with the autonomous system number you set up, which in this case is 1.

Example 5-22 shows the IPv6 EIGRP configuration on the spoke router.

Example 5-22 *IPv6 Spoke Router Configuration*

```
Spoke1(config)# ipv6 unicast routing
Spoke1(config)# ipv6 cef
Spoke1(config)# ipv6 router eigrp 1
Spoke1(config-rtr)# eigrp router-id 2.2.2.2
Spoke1(config-rtr)# interface tunnel 1
Spoke1(config-if)# ipv6 eigrp 1
```

For the IPv6 configuration, you configure the spoke with IPv6 unicast routing and then configure the IPv6 router with the EIGRP router ID 2.2.2.2. Again, in this case, you do this simply to identify the router when looking at the EIGRP neighbors.

That wraps up our DMVPN hub-and-spoke configuration walkthrough. Next, let's look at a DMVPN phase 2 spoke-to-spoke configuration.

DMVPN Phase 2 Spoke-to-Spoke Implementation

To enable spoke-to-spoke communication, you need to focus on two configuration changes versus what we worked through when deploying a hub-and-spoke DMVPN deployment. First, you need to make sure that the two routers can communicate via IPsec. This means that any spoke that needs to talk to another spoke needs to include an additional **crypto isakmp key** statement. You also need to enable routing to use the correct next hop IP address. Let's first look at the IPsec configuration.

IPsec for Spoke-to-Spoke

Example 5-23 shows the addition of extra IPv4 ISAKMP keys on Spoke1. You need to add these keys on both spokes so that they can encrypt and decrypt the traffic when they communicate directly with one another. After adding the second crypto map statement to the Spoke1 router, you need to also add it to the Spoke2 router.

Example 5-23 *IPv4 Additional Spoke Crypto Keys*

```
Spoke1(config)# crypto isakmp key TESTKEY address 209.0.2.3
Spoke1(config)# crypto isakmp key TESTKEY address 209.165.202.130
```

In IPv6, you do a similar configuration. Example 5-24 shows the addition of extra IPv6 ISAKMP keys on Spoke1.

Example 5-24 *IPv6 Additional Spoke Crypto Keys*

```
Spoke1(config)# crypto isakmp key TESTKEY address 2001:db8:aaaa:1::1/64
Spoke1(config)# crypto isakmp key TESTKEY address 2001:db8:cccc:2::2/64
```

Spoke-to-Spoke Routing

In spoke-to-spoke routing configuration, spokes do not directly exchange routing information with each other, even though they may be on the same logical subnet (that is tunnel IP address range) with each other. You need to enable a few commands to ensure that routing functions correctly and spokes use the correct next hop IP address.

Example 5-25 expands the EIGRP configuration for spoke-to-spoke communications by resolving the issue of the hub router setting the next hop address to its own IPv4 address.

Example 5-25 *IPv4 Additional EIGRP Configuration*

```
HQ-Router(config)# router eigrp 1
HQ-Router(config-router)# no auto-summary
HQ-Router(config-router)# network 10.1.1.0 0.0.0.255
HQ-Router(config-router)# network 192.168.1.0 0.0.0.255

HQ-Router(config-router)# interface tunnel 0
HQ-Router(config-router)# no ip split-horizon eigrp 1
HQ-Router(config-router)# no ip next-hop-self eigrp
```

Notice the addition of the command **no ip next-hop-self eigrp**. This command tells the hub router that, when it redistributes the subnets received from one spoke back out to other spokes, it should not replace its own next hop address but should leave the original address provided by the spoke.

IPv6 Spoke-to-Spoke Routing Configuration

The IPv6 spoke-to-spoke routing configuration is not very complex in terms of DMVPN phase 3 support. You only need to add a command to disable the split horizon associated with EIGRP. Example 5-26 also includes the **ipv6 summary** command to expose some options for simplifying routing tables.

As you can see in Example 5-26, with IPv6 you address the split horizon issue but do not have to address the next-hop-self challenge that occurs in IPv4.

Example 5-26 *IPv6 Additional EIGRP Configuration*

```
HQ-Router(config)# interface tunnel 1
HQ-Router(config-if)# no ipv6 split-horizon eigrp 1
HQ-Router(config-if)# ipv6 summary-address eigrp 1 2001:db8:AAAA::/48
```

DMVPN Phase 3 Spoke-to-Spoke Implementation

As mentioned earlier in this chapter, DMVPN phase 2 suffers from scale limitations that are addressed in DMVPN phase 3. To transition from DMVPN phase 2 to DMVPN phase 3, we will make two simple changes on the hub-and-spoke routers.

Enable NHRP Redirects on the Hub

On the hub router, enable NHRP redirects with the command **ip nhrp redirect**. The **redirect** command enables the hub to issue redirects, informing the spoke of a better path if such a path exists. Example 5-27 shows an example of doing this on the hub router.

Example 5-27 *Enabling NHRP Redirects on the Hub Router*

```
HQ-Router(config)# interface tunnel 1
HQ-Router(config-if)# ip nhrp redirect
```

Enable NHRP Shortcuts on the Spoke

On the spoke router, enable NHRP shortcuts with the command **ip nhrp shortcut**. The **shortcut** command enables the spoke to accept redirect messages issues by the hub. Example 5-28 shows an example of doing this on a spoke router.

Example 5-28 *Enabling NHRP Shortcuts on the Spoke Router*

```
Spoke1(config)# interface tunnel 1
Spoke1(config-if)# ip nhrp shortcut
```

DMVPN Troubleshooting

This final section of the chapter discusses troubleshooting DMVPN in terms of the same four steps used to configure DMVPN earlier in this chapter. You are expected to not only be able to build DMVPNs but also identify why a DMVPN is not working, which is why we stress how important it is for you to understand troubleshooting. We concluded Chapter 4, "Group Encrypted Transport VPN (GETVPN)," with steps to validate whether the VPN deployment is running, but in this chapter we skip validation and move right into troubleshooting because there are many overlapping steps with validation and troubleshooting. Know that the process used in this section is similar to validating or troubleshooting other site-to-site VPN deployments.

You can break troubleshooting into four parts that mirror the four configuration parts covered earlier in this chapter:

- Troubleshooting the crypto IPsec policy configuration
- Troubleshooting the GRE tunnel configuration
- Troubleshooting the NHRP hub-and-spoke configuration
- Troubleshoot the routing configuration

NOTE An interesting thing about configuring DMVPN is that you must have at least three of the steps done on the hub-and-spoke routers before you start troubleshooting your configuration. So, for example, if you configure just the crypto policy on the hub and spoke, you do not see either side attempt to establish the VPN tunnel.

Troubleshooting the Crypto IPsec Policy Configuration

There are some key commands you can use to determine whether the crypto configuration is functioning correctly. To see whether IKE Phase 1 or IKE Phase 2 of the ISAKMP process is working, you issue the command **show crypto isakmp sa** on the hub router, as shown in Figure 5-12. This command determines whether IKE Phase 1 of the IPsec tunnel is up.

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.0.2.3       209.165.202.130 QM_IDLE          29058 ACTIVE
192.0.2.3       209.165.201.2   QM_IDLE          29059 ACTIVE
```

Figure 5-12 *Output of the Command* **show crypto isakmp sa**

The output **QM_IDLE** indicates that the VPN peers are authenticated, and the policy between the two devices has been accepted. This indicates that there is a match. If you see **MM_Active**, IKE Phase 1 failed, and you must validate your IKE policy on both sides of the link.

Troubleshooting IKE Phase 2

To troubleshoot IKE Phase 2, use these two commands:

- **show crypto ipsec sa**
- **show crypto session detail**

Figure 5-13 demonstrates the use of the first command, **show crypto ipsec sa**, to learn some important information, such as the crypto endpoints of both sides of the tunnel configuration. Data encapsulating (**encaps**) but not returning (**decaps**) indicates that you have a one-way tunnel, which typically means an ACL or NAT on either side of the tunnel is misconfigured.

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.0.2.3

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.0.2.3/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (209.165.201.2/255.255.255.255/47/0)
   current_peer 209.165.201.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14592, #pkts encrypt: 14592, #pkts digest: 14592
    #pkts decaps: 28935, #pkts decrypt: 28935, #pkts verify: 28935
    #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.: 192.0.2.3, remote crypto endpt.: 209.165.201.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0xDFB0D10(234556688)
     PFS (Y/N): Y, DH group: none
```

Figure 5-13 *Output of the Command* **show crypto ipsec sa**

With each of the commands shown in Figure 5-12 and Figure 5-13, if you add the word **detail** at the end, the output shows more detailed counters. (For more troubleshooting commands and techniques, see the IPsec troubleshooting documentation listed at the end of the chapter.)

Troubleshooting the GRE Tunnel Configuration

The configuration of a tunnel in a DMVPN solution is somewhat different from the configuration of a tunnel used to repair a discontinuous OSPF area. In DMVPN tunnel configuration on the hub, you only have a tunnel source and not a tunnel destination. This is because the tunnel is configured to support NHRP configuration. The hub is dynamic, so it is waiting for inbound registrations and does not need a tunnel destination. The spokes have the destination of the tunnel endpoint mapped to the public IP address in the **nhrp** command in Example 5-12 for IPv4 and Example 5-13 for IPv6.

Validating the Tunnel

You must validate that the tunnel state is up/up after you apply the **tunnel source** command and enable the tunnel interface. You need to make sure you have selected the correct tunnel source interface. In Example 5-11, it is the outside IP address. (This is a common mistake in configuring tunnel interfaces.) In addition, you need to make sure you have the tunnel configured as an mGRE tunnel, especially on the hub side. If you're using a tunnel key, both sides need to be the same.

Figure 5-14 shows the command **show ip interface brief** executed on the Spoke1 router. This validates that the Tunnel1 interface is in the up/up state.

```
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         209.165.201.2   YES NVRAM  up                    up
GigabitEthernet0/1         10.11.11.1      YES NVRAM  up                    up
GigabitEthernet0/2         unassigned      YES NVRAM  administratively down down
Tunnel1                    192.168.1.2     YES NVRAM  up                    up
```

Figure 5-14 *Output of the Command* **show ip interface brief** *on an IPv4 Interface*

Troubleshooting the NHRP Hub-and-Spoke Configuration

NHRP troubleshooting starts with issuing two basic commands on the spoke router. First, you need to determine if the VPN tunnel is up and functioning correctly. If it isn't, you need to determine whether IKE Phase 1 or IKE Phase 2 is failing. If the tunnel is up when you issue **show crypto isakmp sa**, you should see **QM_IDLE**. If you see only encapsulations and not decapsulations, you know you have either a crypto IKE Phase 2 problem or an NHRP registration issue.

NHRP Registration

You must determine whether the NHRP spoke is registering. The command **show ip nhrp nhs detail**, shown in Figure 5-15, tells you whether you have both sent and received packets from the NHRP NHS. If you see that the request has been sent (**req-sent**) but no replies have been received (**repl-recv**) and the request failed (**req-failed**) count is increasing, then you know you have an NHRP spoke that is unable to register with the NHS.

```
R2#sh ip nhrp nhs detail
Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel1:
192.168.1.1  RE priority = 0 cluster = 0  req-sent 281  req-failed 1  repl-recv 206 (00:03:05 ago)
```

Figure 5-15 *Output of the Command* **show ip nhrp nhs detail**

Tunnel Configuration

It is important to validate that the configuration of the tunnel interface is correct. Take a look at Figure 5-15, and make sure you have the correct information on the NHS, which in this example is the IP address of the tunnel interface of the hub router. This is the first area that might be misconfigured. Check your documentation and make sure this address is correct. Then verify that the command **ip nhrp map** references the tunnel address first, followed by the outside IP address (NBMA) of the hub router.

Figure 5-16 shows the command **show ipv6 nhrp nhs detail** executed on the Spoke1 router. The output provides information on the IPv6 address of the tunnel interface for the NHRP server. It validates that the NHRP configuration information on the spoke is valid.

```
R2#sh ipv6 nhrp nhs detail
Legend: E=Expecting replies, R=Responding, W=Waiting
Tunnel1:
2001:DB8:BEEF:1::1   E priority = 0 cluster = 0  req-sent 0  req-failed 8937  repl-recv 0
```

Figure 5-16 *Output of the Command* **show ipv6 nhrp nhs detail**

Debugging

If you determine that so far everything is correct, you can turn on debugging for NHRP packets on the hub router to see if they are being received by the NHS and why the NHS cannot respond. You can force a registration attempt by shutting down the tunnel interface on the spoke router and then reenabling it. If you have debugging enabled on the hub router, you should see an inbound registration request.

Figure 5-17 shows the command **debug nhrp packet** executed on the NHRP server router. This also validates that the spoke router is attempting to register with the NHRP server. If you do not see inbound registration requests, then there is probably a misconfiguration of the NHRP server parameters on the spoke router.

```
Jan 20 18:21:56.326: NHRP: Receive Registration Request via Tunnel1 vrf 0,
packet size: 104
Jan 20 18:21:56.326:  (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
Jan 20 18:21:56.326:      shtl: 4(NSAP), sstl: 0(NSAP)
Jan 20 18:21:56.326:      pktsz: 104 extoff: 52
Jan 20 18:21:56.326:  (M) flags: "unique nat ", reqid: 65583
Jan 20 18:21:56.326:      src NBMA: 209.165.201.2
Jan 20 18:21:56.326:      src protocol: 192.168.1.2, dst protocol:
192.168.1.1
Jan 20 18:21:56.326:  (C-1) code: no error(0)
Jan 20 18:21:56.326:        prefix: 32, mtu: 17870, hd_time: 7200
Jan 20 18:21:56.326:        addr_len: 0(NSAP), subaddr_len: 0(NSAP),
proto_len: 0, pref: 0
```

Figure 5-17 *Output of the Command* **debug nhrp packet**

In the debug screen shown in Figure 5-17, you can see that the inbound registration request comes via the tunnel interface and includes the source NBMA IP address (the outside address) and the source protocol IP address (the tunnel address). In addition, it includes the destination protocol addresses. Each of these fields provides a good indication about whether the configuration on the host side is aligned with the hub router configuration.

Troubleshoot the Routing Configuration

Troubleshooting the routing protocol part of the DMVPN tunnel is not very complex. The challenge is whether you are able to see routes of other remote sites in the routing table. The first command to issue is **show ip protocol**. This command shows what IP blocks are being advertised. You should compare the spoke side to what the hub side is seeing in the routing table. If you execute **show ip route** and do not see the route in the table, then you should verify both the EIGRP autonomous system number and whether you have any security on

the route exchanges. In addition, you should check to see if the hub router is summarizing the routes into a larger block. Finally, you should check to see what EIGRP neighbors the hub router identifies.

DMVPN Troubleshooting Summary

Table 5-3 consolidates some of the key commands covered so far, as well as a few more that are valuable for troubleshooting. The commands are organized in this table in the same parts as the DMVPN implementation shown in this chapter. Even if you configure your solution correctly the first time, it is good to use these commands to understand what the Cisco routers are doing in each of the phases.

Key Topic

Table 5-3 DMVPN Troubleshooting Commands

Troubleshooting Part	Commands
Crypto configuration (ISAKMP/IPSEC)	**show crypto isakmp sa** **show crypto ipsec sa** **debug crypto isakmp** **debug crypto ipsec**
Tunnel configuration	**show ip interface tunnel** *interface_number* **show ipv6 interface tunnel** *interface_number*
NHRP configuration	**show ip nhrp nhs detail** **show ipv6 nhrp nhs detail** **debug nhrp**
Routing configuration	**show ip protocol** **show ip route** **debug ip eigrp** **debug ip ospf adj** **debug ip ospf hello** **debug ip ospf packet**

That wraps up troubleshooting DMVPN troubleshooting fundamentals. Keep in mind that troubleshooting makes up a major part of the SVPN exam.

Summary

This chapter introduced DMVPN technology and its features. It also described the components needed for DMVPN and looked at two of the key components: mGRE and NHRP. We covered the features, benefits, and limitations of mGRE and NHRP, especially related to routing and security. We discussed both IPv4 and IPv6 DMVPN configuration because both are deployed and could be found within the SVPN exam. Finally, this chapter covered some potential pitfalls and challenges related to deploying a DMVPN solution.

At this point, you should have a strong foundation for planning, configuring, and managing GETVPN as well as DMVPN deployments. Next up is a deep dive into FlexVPN, wrapping up our focus on site-to-site VPN concepts.

References

Brandom, Russel (May 12, 2017). UK Hospitals Hit with a Massive Ransomware Attack. Retrieved from https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin

Coran, Matt, Design Guide | DMVPN Phases. Retrieved from https://network-insight.net/2015/02/design-guide-dmvpn-phases/

Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15S. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-s/sec-conn-dmvpn-15-s-book/ip6-dmvpn.html#GUID-AE87E1CC-DF83-426D-885C-2E00CF365833

Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15M&T. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-tun-mon.html#GUID-E968E183-0022-4E8C-89A6-69AE3AE2AFF9

GRE Tunnel Interface States and What Impacts Them, Retrieved from https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/118361-technote-gre-00.html

IP Addressing: NHRP Configuration Guide. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nhrp/configuration/xe-3s/nhrp-xe-3s-book/config-nhrp.html

IPsec Troubleshooting: Understanding and using debug Commands. Retrieved from https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html

Kingsbury, Josh, DMVPN – Concepts & Configuration. Retrieved from https://learningnetwork.cisco.com/s/article/dmvpn-concepts-amp-configuration

Scalable DMVPN Design and Implementation Guide. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/dmvpn_design_guide.pdf?dtid=osscdc000283

Transform Set Configuration. Retrieved from https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21/IPSec/21_IPSec-Reference/b_21_IPSec_chapter_0100.pdf

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 11, "Final Preparation," and the exam simulation questions in the Pearson Test Prep software online.

Review All Key Topics

Review the most important topics in the chapter, noted with the key topics icon in the outer margin of the page. Table 5-4 lists these key topics and the page number on which each is found.

Key Topic

Table 5-4 Key Topics for Chapter 5

Key Topic Element	Description	Page Number
Figure 5-4	A Full-Mesh DMVPN Tunnel	137
Figure 5-5	GRE Tunnels	138
List	GRE limitations	138
Figure 5-6	NHRP Registration Process	139
Table 5-2	Basic DMVPN Configuration Components	139
Figure 5-9	DMVPN Phase 2	143
Figure 5-10	DMVPN IPv4 Solution	144
Figure 5-11	DMVPN IPv6 Solution	145
Example 5-12	Setting Up NHRP IPv4 Server Parameters on the mGRE Tunnel	150
Example 5-14	Configuring NHRP on a Spoke Router for IPv4	151
Table 5-3	DMVPN Troubleshooting Commands	160

Complete Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the companion website), or at least the section for this chapter and complete the tables and lists from memory. Appendix D, "Memory Tables Answer Key" (also on the companion website), includes completed tables and lists to check your work.

Define Key Terms

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

Next Hop Resolution Protocol (NHRP), multipoint Generic Routing Encapsulation (mGRE)

This page intentionally left blank

Index

Numbers

A

B

C

D

E

F

G

H

I

J - K

L

M

N

O

P

Q

R

S

T

U

V

W - X - Y - Z