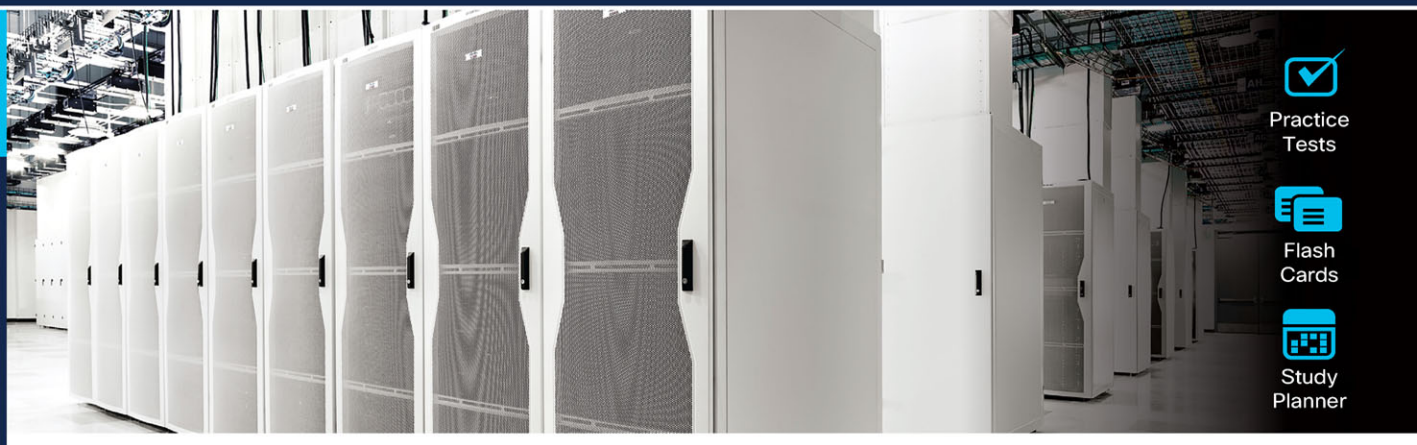
Official Cert Guide



Review Exercises

CCNP and CCIE Data Center Core

DCCOR 350-601

2nd Edition

Somit Maloo
CCDE® No. 20170002, CCIE® No. 28603
Iskren Nikolov
CCIE® No. 20164, CCNP Data Center, CCSI® No. 32481
Firas Ahmed
CCIE® No. 14967

ciscopress.com

FREE SAMPLE CHAPTER

CCNP and CCIE Data Center Core DCCOR 350-601 Official Cert Guide

Companion Website and Pearson Test Prep Access Code

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

To access the companion website, simply follow these steps:

1. Go to www.ciscopress.com/register.
2. Enter the print book ISBN: **9780138228088**.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

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

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

This page intentionally left blank

CCNP and CCIE Data Center Core DCCOR 350-601

Official Cert Guide

Second Edition

SOMIT MALOO, CCIE NO. 28603, CCDE NO. 20170002
ISKREN NIKOLOV, CCIE NO. 20164, CCSI NO. 32481
FIRAS AHMED, CCIE NO. 14967

Cisco Press

CCNP and CCIE Data Center Core DCCOR 350-601 Official Cert Guide, Second Edition

Somit Maloo, Iskren Nikolov, Firas Ahmed

Published by:
Cisco Press

Hoboken, New Jersey

$PrintCode

Library of Congress Control Number: 2023946984

ISBN-13: 978-0-13-822808-8

ISBN-10: 0-13-822808-6

Warning and Disclaimer

This book discusses the content and skills needed to pass the 350-601 CCNP Data Center Core certification exam, which is the prerequisite for CCNP as well as CCIE certification. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Trademark Acknowledgments

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

Special Sales

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

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

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

Feedback Information

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

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

We greatly appreciate your assistance.

Vice President, IT Professional: Mark Taub

Alliances Managers, Cisco Press: Jaci Featherly; James Risler

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: Chuck Hutchinson

Technical Editor: Donald S. Bacha

Editorial Assistant: Cindy Teeters

Cover Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Ken Johnson

Proofreader: Charlotte Kughen

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 Authors

Somit Maloo, CCIE No. 28603, CCDE No. 20170002, is a content architect from the data center team in the Learning & Certifications' organization. He holds a master's degree in telecommunication networks and a bachelor's degree in electronics and telecommunication engineering. He is also a penta CCIE in routing and switching, service provider, wireless, security, and data center technologies. Somit holds various industry-leading certifications, including CCDE, PMP, RHCSA, and VMware VCIX6 in Data Center and Network Virtualization. Somit has extensive experience in designing and developing various data center courses for the official Cisco curriculum. He started his career as a Cisco TAC engineer. Somit has more than 13 years of experience in the networking industry, working mostly with data center networks. You can reach Somit on Twitter: @somitmaloo.

Iskren Nikolov, CCIE No. 20164, CCSI No. 32481, MCT Alumni, content architect, engineer, and developer with the Cisco Learning & Certifications' Data Center & Cloud team. He is responsible for designing, developing, and reviewing Data Center Official Learning Cisco courses, including lab infrastructures and exercises. He holds a master's degree in computer systems and management from the Technical University-Sofia, Bulgaria. Iskren has more than 26 years of experience in designing, implementing, and supporting solutions based on the data center, security, storage, wide area networks, software-defined networks, cloud, hybrid, and multi-cloud technologies, including 11 years of teaching, and developing Cisco Data Center & Cloud and Microsoft Azure courses. The huge experience across technologies from multiple vendors such as Cisco Systems, VMware, Microsoft, and Barracuda, combined with the different perspectives gained from the different roles in his work and experience with customers from different industries, allow Iskren to have a unique view of the current data center technologies and the future trends. You can reach Iskren on LinkedIn: https://www.linkedin.com/in/iskrennikolov.

Firas Ahmed, CCIE No. 14967, is a solution architect on the data center technologies team at Nile. He completed a master's degree in systems and control engineering following a bachelor's degree in computer engineering. Firas holds CCIE certificates in routing and switching, collaboration, wireless, security, and data center technologies in addition to industry-based certifications, including CISSP, PMP, VMware VCP6.5-DCV, ITIL, and GICSP. Firas has more than 18 years of experience in designing, developing, and supporting various data centers for enterprise and IoT customers. Firas has additional experience as a seasonal instructor in a number of community colleges in Toronto, where he taught various computer networking courses. You can reach Firas on Twitter: @dccor_firas.

About the Technical Reviewer

Donald Bacha is an infrastructure manager with a health research organization in New York City. He's the technical lead responsible for designing and implementing network, compute, virtualization, storage, and disaster recovery solutions. During the past 18 years, Donald has supported Cloud Services Provider, Enterprise, and Data Center environments contributing to complex routing and switching, data center, storage, and virtualization projects in both greenfield and brownfield deployments. Donald's certifications include CCNP Data Center, CCNP Enterprise, and VCAP-DCV. Donald holds a master of science in network engineering from Southern Methodist University (SMU) Lyle School of Engineering and a master of business administration from the Commonwealth of Learning/University of Guyana. You can reach Donald on Twitter: @donald_bacha.

Dedications

Somit:

To my loving wife, Renuka, for her unending love and support.

To my wonderful parents, who supported me in every phase of my life.

To Navya and Namit, who agreed not to fight while Papa was working on the book.

To my aunt, Tara, for being the guiding angel in my life.

Iskren:

To my loving family—my wife, Petya, and my kids, Diana and Valentin—for their continued support and unconditional love!

Firas:

To my amazing wife, Nora, who has been extremely supportive throughout this process. Thanks for letting me spend long hours on my computer once again!

To Ibrahim and Maryam, you are growing so fast. Never give up on what you want. If at first you don't succeed, try and try again. I love you more than anything!

To my parents, you are still the guiding light that keeps me on the right path.

Acknowledgments

Somit Maloo:

I would like to thank my coauthors, Iskren Nikolov and Firas Ahmed, for working as a team to complete this book. Without their support, this book would not have been possible. I am thankful to all our professional editors, especially James Manly and Ellie Bru, for their patience and guidance at every step of the book process. I would also like to thank our technical editor, Donald Bacha, for his keen attention to detail and for agreeing to review the book, taking time out of his busy schedule.

Firas Ahmed:

I would like to thank my co-author, Somit Maloo, for taking the initiative to form this partnership and for his dedication in putting together the outline of this book. Thank you for your valuable input and continuous support throughout the process.

Thanks to the Cisco Press team, especially James Manly, for believing in us, and Ellie Bru, for her guidance and extreme patience while editing and amending the chapters of the book.

A special credit to Hazim Dahir, distinguished engineer at Cisco Systems, for his help and support with the technical review of the book.

In addition, I want to thank my colleague Naveen Chapa for reviewing and providing constructive feedback that helped enhance the ACI chapter.

Iskren Nikolov:

I would like to thank my co-author, Somit Maloo—it's not that often one can work effortlessly as a team with someone. I am thankful to the whole production team, especially James Manly and Ellie Bru, for their professionalism and endless patience with me! Special thanks also to our technical editor, Donald Bacha, for providing this precious other perspective on how we can tell a better story about the technology!

Contents at a Glance

Online Elements

Contents

Online Elements

Other Features

In addition to the features in each of the core chapters, this book has additional study resources on the companion website, including the following:

Practice exams: The companion website contains an exam engine that enables you to review practice exam questions. Use these questions to prepare with a sample exam and to pinpoint topics where you need more study.

An online interactive Flash Cards application to help you drill on Key Terms by chapter.

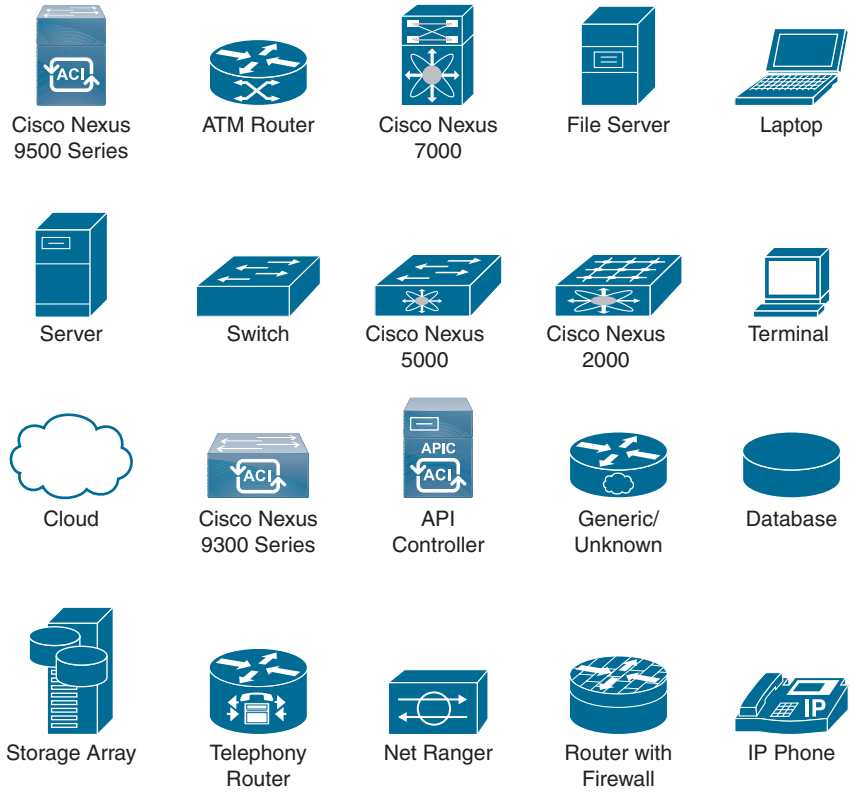
Glossary quizzes: The companion website contains interactive quizzes that enable you to test yourself on every glossary term in the book.

More than two hours of video training: The companion website contains multiple hours of unique test-prep videos.

To access this additional content, simply register your product. To start the registration process, go to www.ciscopress.com/register and log in or create an account*. Enter the product ISBN 9780138228088 and click **Submit**. After the process is complete, you will find any available bonus content under Registered Products.

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

Icons Used in This Book



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

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 that of credibility. All other considerations held equal, the certified employee/consultant/job candidate is considered more valuable than one who is not.

Goals and Methods

The most important and somewhat obvious goal of this book is to help you pass the 350-601 CCNP Data Center Core Exam. In fact, if the primary objective of this book were different, the book's title would be misleading; however, the methods used in this book to help you pass the 350-601 CCNP Data Center Core Exam are designed to also make you much more knowledgeable about how to do your job. Although this book and the companion website together have more than enough questions to help you prepare for the actual exam, the method in which they are used is not simply to make you memorize as many questions and answers as you possibly can.

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. So, this book does not try to help you pass by memorization, but helps you truly learn and understand the topics. The Data Center Core Exam is just one of the foundation topics in the CCNP and CCIE certification, and the knowledge contained within is vitally important to consider yourself a truly skilled data center engineer or specialist. This book would do you a disservice if it didn't attempt to help you learn the material. To that end, the book will help you pass the Data Center Core Exam by using the following methods:

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

Who Should Read This Book?

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

So why should you want to pass the CCNP Data Center Core Exam? Because it's one of the milestones toward getting the CCNP and CCIE certification—no small feat in itself.

What would getting the CCNP or CCIE mean to you? A raise, a promotion, recognition? How about to enhance your resume? To demonstrate that you are serious about continuing the learning process and that you're not content to rest on your laurels. To please your reseller-employer, who needs more certified employees for a higher discount from Cisco. Or one of many other reasons.

Strategies for Exam Preparation

The strategy you use for the CCNP Data Center Core Exam might be slightly different from strategies used by other readers, mainly based on the skills, knowledge, and experience you already have obtained. For instance, if you have attended the DCFNDU course, you might take a different approach than someone who learned data center technologies via on-the-job training.

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

The Companion Website for Online Content Review

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

How to Access the Companion Website

To access the companion website, which gives you access to the electronic content with this book, start by establishing a login at ciscopress.com and register your book. To do so, simply go to ciscopress.com/register and enter the ISBN of the print book: 9780138228088. After you have registered your book, go to your account page and click the **Registered Products** tab. From there, click the **Access Bonus Content** link to get access to the book's companion website.

Note that if you buy the Premium Edition eBook and Practice Test version of this book from Cisco Press, your book will automatically be registered on your account page.

Simply go to your account page, click the **Registered Products** tab, and select **Access Bonus Content** to access the book's companion website.

How to Access the Pearson Test Prep (PTP) App

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

- **Print book or bookseller eBook versions:** You can get your access code by registering the print ISBN (9780138228088) on ciscopress.com/register. Make sure to use the

print book ISBN regardless of whether you purchased an eBook or the print book. Once you register the book, your access code will be populated on your account page under the Registered Products tab. Instructions for how to redeem the code are available on the book's companion website by clicking the Access Bonus Content link.

- **Premium Edition:** If you purchase the Premium Edition eBook and Practice Test directly from the Cisco Press website, the code will be populated on your account page after purchase. Just log in at www.ciscopress.com, click Account to see details of your account, and click the digital purchases tab.

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

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

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

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

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

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

How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with.

The core chapters, Chapters 1 through 20, cover the following topics:

- **Chapter 1, "Implementing Routing in the Data Center":** This chapter discusses data center Layer 3 routing protocols, focusing on OSPF and BGP routing protocols. It also discusses multicast and First Hop Redundancy Protocols such as HSRP and VRRP.
- **Chapter 2, "Implementing Data Center Switching Protocols":** This chapter discusses data center Layer 2 switching protocols, focusing on spanning tree and multiport aggregation. It also discusses virtual port channels (multichassis port channels).
- **Chapter 3, "Implementing Data Center Overlay Protocols":** This chapter discusses data center overlay protocol Virtual Extensible LAN (VXLAN).

- **Chapter 4, "Describe Cisco Application Centric Infrastructure":** This chapter discusses various aspects of Cisco ACI, including but not limited to fabric discovery, fabric access policies, fabric packet flow, tenants, and VMM domains.
- **Chapter 5, "Cisco Cloud Services and Deployment Models":** This chapter discusses an overview of what cloud computing is along with cloud service models per the NIST 800-145 definition, such as Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). It also discusses various cloud deployment models per the NIST 800-145 definition, such as public, private, community, and hybrid cloud.
- **Chapter 6, "Data Center Network Management and Monitoring":** This chapter discusses data center network disruptive/nondisruptive upgrade procedures, network configurations, and infrastructure monitoring aspects in detail. It also discusses data center network assurance and data telemetry.
- **Chapter 7, "Describe Cisco Nexus Dashboard":** This chapter discusses various services/applications for the Cisco Nexus Dashboard platform including Cisco Nexus Dashboard Insights (NDI), Cisco Nexus Dashboard Orchestrator (NDO), Cisco Nexus Dashboard Fabric Controller (NDFC), and Cisco Nexus Dashboard Data Broker (NDDB), along with their features and benefits. It also discusses various form factors, node types, and network types for Cisco Nexus Dashboard deployment along with a graphical user interface (GUI) overview of the Cisco Nexus Dashboard platform.
- **Chapter 8, "Implement Fibre Channel":** This chapter discusses the MDS 9000 Series Hardware and Fibre Channel protocol in detail. It discusses Fibre Channel topologies, port types, switched fabric initialization, CFS distribution, VSAN, zoning, device alias, FLOGI, and FCNS databases. It also discusses NPV and NPIV features in detail.
- **Chapter 9, "Implement FCoE Unified Fabric":** This chapter discusses the FCoE Unified Fabric Protocol in detail. It discusses various Ethernet enhancements that enable FCoE support on Ethernet interfaces. It also discusses FCoE topology options and various FCoE implementations—for example, FCoE over FEX and FCoE NPV.
- **Chapter 10, "Describe NFS and NAS Concepts":** This chapter discusses NFS basics along with various NFS versions. It also discusses NAS basics with an overview of the Cisco UCS S-Series Storage Servers.
- **Chapter 11, "Describe Software Management and Infrastructure Monitoring":** This chapter discusses how the Cisco MDS NX-OS Setup Utility helps to build an initial configuration file using the System Configuration dialog. It also discusses Cisco MDS NX-OS software upgrade and downgrade procedures, along with infrastructure monitoring features such as SPAN, RSPAN, RMON, and Call Home.
- **Chapter 12, "Cisco Unified Computing Systems Overview":** This chapter discusses the Cisco Unified Computing System (UCS) architecture. It also discusses in detail UCS initial setup, along with network management aspects of Cisco UCS, such as identity pools, policies, QoS, and templates.

- **Chapter 13, "Cisco Unified Computing Infrastructure Monitoring":** This chapter discusses Cisco Unified Compute traffic monitoring and Intersight cloud management.
- **Chapter 14, "Cisco Unified Compute Software and Configuration Management":** This chapter discusses Cisco UCS configuration management such as backup and restore. It also discusses aspects of firmware and software updates on Cisco UCS.
- **Chapter 15, "Cisco HyperFlex Overview":** This chapter discusses the Cisco Hyperflex solution and benefits. It also discusses edge solutions that enable any application to be deployed, monitored, and managed anywhere.
- **Chapter 16, "Automation and Scripting Tools":** This chapter discusses various automation and scripting tools. It discusses the Embedded Event Manager (EEM), Scheduler, Bash Shell, and Guest Shell for Cisco NX-OS software, and various data formats such as XML and JSON. It also discusses how the REST API can be used to configure Cisco NX-OS devices.
- **Chapter 17, "Evaluate Automation and Orchestration Technologies":** This chapter discusses various automation and orchestration technologies. It discusses how Ansible, Python, and Terraform can be used to automate Cisco Data Center products. It also discusses the PowerOn Auto Provisioning (POAP) process, along with the UCS PowerShell modules, also referred to as UCS PowerTool Suite.
- **Chapter 18, "Network Security":** This chapter discusses network authentication, authorization, and accounting (AAA) and user role-based access control (RBAC). It also discusses various network security protocols in detail, including control plan policing, dynamic ARP inspection, DHCP snooping, and port security, along with the keychain authentication method.
- **Chapter 19, "Compute Security":** This chapter discusses Cisco UCS authentication and user role-based access control.
- **Chapter 20, "Storage Security":** This chapter discusses various storage security features in detail. It discusses authentication, authorization, and accounting (AAA), user accounts, and RBAC. It also discusses configuration and verification of port security and fabric binding features on the Cisco MDS 9000 Series switches.
- **Chapter 21, "Final Preparation":** This chapter suggests a plan for final preparation after you have finished the core parts of the book, in particular explaining the many study options available in the book.

Certification Exam Topics and This Book

The questions for each certification exam are a closely guarded secret. However, we do know which topics you must know to *successfully* complete this exam. Cisco publishes them as an exam blueprint for the Implementing Cisco Data Center Core Technologies (DCCOR 350-601) Exam. Table I-1 lists each exam topic listed in the blueprint along with a reference to the book chapter that covers the topic. These are the same topics you should be proficient in when working with Cisco data center technologies in the real world.

Table I-1 DCCOR Exam 350-601 Topics and Chapter References

DCCOR 350-601 Exam Topic	Chapter(s) in Which Topic Is Covered
1.0 Network	
1.1 Apply routing protocols	1
1.1.a OSPFv2, OSPFv3	1
1.1.b MP-BGP	1
1.1.c PIM	1
1.1.d FHRP	1
1.2 Apply switching protocols such as RSTP+, LACP and vPC	2
1.3 Apply overlay protocols such as VXLAN EVPN	3
1.4 Apply ACI concepts	4
1.4.a Fabric setup	4
1.4.b Access policies	4
1.4.c VMM	4
1.5 Analyze packet flow (unicast, multicast, and broadcast)	4
1.6 Describe Cloud service and deployment models (NIST 800-145)	5
1.7 Describe software updates and their impacts	6
1.7.a Disruptive/nondisruptive	6
1.7.b EPLD	6
1.7.c Patches	6
1.8 Implement network configuration management	6
1.9 Implement infrastructure monitoring such as NetFlow and SPAN	6
1.10 Explain network assurance concepts such as streaming telemetry	6
1.11 Describe the capabilities and features of Nexus Dashboard	7
2.0 Compute	
2.1 Implement Cisco Unified Compute System Rack Servers	12
2.2 Implement Cisco Unified Compute System Blade Chassis	12
2.2.a Initial setup	12
2.2.b Infrastructure management	12
2.2.c Network management (VLANs, pools and policies, templates, QoS)	12
2.2.d Storage management (SAN connectivity, Fibre Channel zoning, VSANs, WWN pools, SAN policies, templates)	12
2.2.e Server management (Server pools and boot policies)	12

DCCOR 350-601 Exam Topic	Chapter(s) in Which Topic Is Covered
2.3 Explain HyperFlex Infrastructure concepts and benefits (Edge and Hybrid Architecture vs all-flash)	15
2.4 Describe firmware and software updates and their impacts on B-Series and C-Series servers	14
2.5 Implement compute configuration management (Backup and restore)	14
2.6 Implement infrastructure monitoring such as SPAN and Cisco Intersight	13
3.0 Storage Network	
3.1 Implement Fibre Channel	8
3.1.a Switch fabric initialization	8
3.1.b Port channels	8
3.1.c FCID	8
3.1.d CFS	8
3.1.e Zoning	8
3.1.f FCNS	8
3.1.g Device alias	8
3.1.h NPV and NPIV	8
3.1.i VSAN	8
3.2 Implement FCoE Unified Fabric	9
3.3 Describe NFS and NAS concepts	10
3.4 Describe software updates and their impacts (Disruptive/ nondisruptive and EPLD)	11
3.5 Implement infrastructure monitoring	11
4.0 Automation	
4.1 Implement automation and scripting tools	16
4.1.a EEM	16
4.1.b Scheduler	16
4.1.c Bash Shell and Guest Shell for NX-OS	16
4.1.d REST API (NX-API, JSON, and XML encodings)	16
4.1.e On-box Python	17
4.2 Evaluate automation and orchestration technologies	17
4.2.a Ansible	17
4.2.b Python	17
4.2.c POAP	17
4.2.d Cisco Nexus Dashboard Fabric Controller	7

DCCOR 350-601 Exam Topic	Chapter(s) in Which Topic Is Covered
4.2.e PowerShell	17
4.2.f Terraform	17
5.0 Security	
5.1 Apply network security	18
5.1.a AAA and RBAC	18
5.1.b ACI contracts and microsegmentation	18
5.1.c First-hop security features	18
5.1.d Keychain authentication	18
5.2 Apply compute security	19
5.2.a AAA and RBAC	19
5.3 Apply storage security	20
5.3.a AAA and RBAC	20
5.3.b Port security	20
5.3.c Fabric binding	20

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 data center professional.

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

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

Note that as data center technologies continue to develop, Cisco reserves the right to change the exam topics without notice. Although you can refer to the list of exam topics in Table I-1, always check Cisco.com to verify the actual list of topics to ensure that you are prepared before taking the exam. You can view the current exam topics on any current Cisco certification exam by visiting the Cisco.com website, choosing **Menu**, and **Training & Events**, then 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/9780138228088. 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.

Taking the CCNP Data Center Core Exam

As with any Cisco certification exam, you should strive to be thoroughly prepared before taking the exam. There is no way to determine exactly what questions are on the exam, so the best way to prepare is to have a good working knowledge of all subjects covered on the exam. Schedule yourself for the exam and be sure to be rested and ready to focus when taking the exam.

The best place to find out the latest available Cisco training and certifications is under the Training & Events section at Cisco.com.

Tracking Your Status

You can track your certification progress by checking http://www.cisco.com/go/certifications/login. You must create an account the first time you log in to the site.

How to Prepare for an Exam

The best way to prepare for any certification exam is to use a combination of the preparation resources, labs, and practice tests. This guide has integrated some practice questions and sample scenarios to help you better prepare. If possible, get some hands-on experience with ACI, Nexus, and UCS equipment. There is no substitute for real-world experience; it is much easier to understand the designs, configurations, and concepts when you can actually work with a live data center network.

Cisco.com provides a wealth of information about Application Centric Infrastructure (ACI), Nexus switches, and Unified Computing System—Blade and Rack servers, and data center LAN technologies and features.

Assessing Exam Readiness

Exam candidates never really know whether they are adequately prepared for the exam until they have completed about 30 percent of the questions. At that point, if you are not prepared, it is too late. The best way to determine your readiness is to work through the "Do I Know This Already?" quizzes at the beginning of each chapter and review the foundation and key topics presented in each chapter. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

Cisco Data Center Certifications in the Real World

Cisco is one of the most recognized names on the Internet. Cisco Certified data center specialists can bring quite a bit of knowledge to the table because of their deep understanding of data center technologies, standards, and networking devices. This is why the Cisco certification carries such high respect in the marketplace. Cisco certifications

demonstrate to potential employers and contract holders a certain professionalism, expertise, and dedication required to complete a difficult goal. If Cisco certifications were easy to obtain, everyone would have them.

Exam Registration

The 350-601 CCNP Data Center Core Exam is a computer-based exam, with around 100 to 110 multiple-choice, fill-in-the-blank, list-in-order, and simulation-based questions. You can take the exam at any Pearson VUE (http://www.pearsonvue.com) testing center. According to Cisco, the exam should last about 120 minutes. Be aware that when you register for the exam, you might be told to allow a certain amount of time to take the exam that is longer than the testing time indicated by the testing software when you begin. The reason for this discrepancy is that the testing center will want you to allow for some time to get settled and take the tutorial about the test engine.

Book Content Updates

Because Cisco occasionally updates exam topics without notice, Cisco Press might post additional preparatory content on the web page associated with this book at http://www.ciscopress.com/title/9780138228088. It is a good idea to check the website a couple of weeks before taking your exam to review any updated content that might be posted online. We also recommend that you periodically check back to this page on the Cisco Press website to view any errata or supporting book files that may be available.

Figure Credits

Figures 17-5 through 17-8: HashiCorp

This page intentionally left blank

CHAPTER 3

Implementing Data Center Overlay Protocols

The adoption of server virtualization has been increasing rapidly. Server virtualization provides flexibility and agility in provisioning and placement of computing workloads. However, network connectivity has not kept pace with such innovations in the computing environment, although it still offers a rigid approach to provisioning transport services.

As a solution, network overlays abstract the details of the physical network, making it much faster to connect virtual machines (VMs) and other devices. Rather than provision paths on physical devices, overlays encapsulate traffic using protocols such as Overlay Transport Virtualization (OTV) or Virtual Extensible LAN (VXLAN) across the physical network. These newer protocols allow operators to move beyond the limitations of VLANs, which support only 4096 virtual networks, so that they can better support multitenant services.

This chapter covers the following key topics:

Virtual Extensible LAN (VXLAN) Overview: This section discusses the Layer 2 VLAN extension to provide multitenant flexibility, high segment scalability, and Layer 2 spanning tree improvement, along with a configuration example.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 3-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 3-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Virtual Extensible LAN (VXLAN) Overview	1–3

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

1. In current data center networking architecture, which network layer is used to transmit VXLAN packets or other overlay packets?
   a. Overlay network
   b. SD-WAN
   c. Underlay network
   d. MPLS
2. How many available IDs can be assigned to a VXLAN at any given time?
   a. 4096
   b. 160,000
   c. 1 million
   d. 16 million
3. Which statement about VXLAN high availability is correct?
   a. For an anycast IP address, vPC VTEP switches can use the same VTEP IP address.
   b. For an anycast IP address, vPC VTEP switches must use the same secondary IP address on the loopback interface.
   c. Distributed anycast gateways must be connected with vPC.
   d. VTEP high availability will use unicast instead of multicast communications.

Foundation Topics

Virtual Extensible LAN (VXLAN) Overview

In partnership with other leading vendors, Cisco proposed the VXLAN standard to the Internet Engineering Task Force (IETF) as a solution to the data center network challenges posed by the traditional VLAN technology. The VXLAN standard provides for flexible workload placement and the higher scalability of Layer 2 segmentation that is required by modern application demands. VXLAN is an extension to the Layer 2 VLAN. It was designed to provide the same VLAN functionality with greater extensibility and flexibility. VXLAN offers the following benefits:

- **VLAN flexibility in multitenant segments:** It provides a solution to extend Layer 2 segments over the underlying network infrastructure so that tenant workload can be placed across physical pods in the data center.
- **Higher scalability:** VXLAN uses a 24-bit segment ID known as the VXLAN network identifier (VNID), which enables up to 16 million VXLAN segments to coexist in the same administrative domain.
- **Improved network utilization:** VXLAN solved Layer 2 STP limitations. VXLAN packets are transferred through the underlying network based on its Layer 3 header and can take complete advantage of Layer 3 routing, equal-cost multipath (ECMP) routing, and link aggregation protocols to use all available paths.

VXLAN Encapsulation and Packet Format

VXLAN is a solution to support a flexible, large-scale multitenant environment over a shared common physical infrastructure. The transport protocol over the physical data center network is IP plus UDP.

VXLAN defines a MAC-in-UDP encapsulation scheme where the original Layer 2 frame has a VXLAN header added and is then placed in a UDP-IP packet. With this MAC-in-UDP encapsulation, VXLAN tunnels the Layer 2 network over the Layer 3 network. The VXLAN packet format is shown in Figure 3-1.

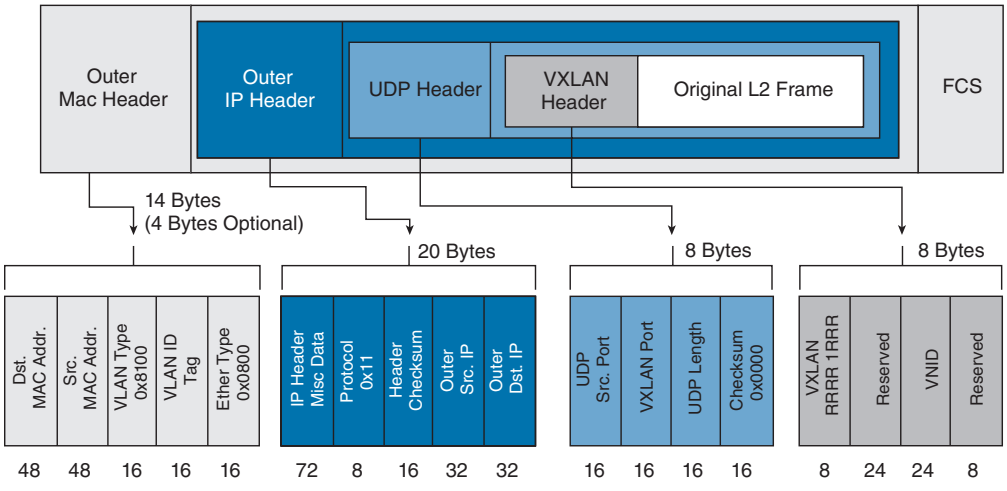


Figure 3-1 *VXLAN Packet Format*

As shown in Figure 3-1, VXLAN introduces an 8-byte VXLAN header that consists of a 24-bit VNID and a few reserved bits. The VXLAN header together with the original Ethernet frame goes in the UDP payload. The 24-bit VNID is used to identify Layer 2 segments and to maintain Layer 2 isolation between the segments. With all 24 bits in VNID, VXLAN can support 16 million LAN segments.

VXLAN Tunnel Endpoint

VXLAN uses the VXLAN tunnel endpoint (VTEP) to map tenants' end devices to VXLAN segments and to perform VXLAN encapsulation and decapsulation. Each VTEP function has two interfaces: one is a switch interface on the local LAN segment to support local endpoint communication, and the other is an IP interface to the transport IP network.

Infrastructure VLAN is a unique IP address that identifies the VTEP device on the transport IP network. The VTEP device uses this IP address to encapsulate Ethernet frames and transmits the encapsulated packets to the transport network through the IP interface.

A VTEP device also discovers the remote VTEPs for its VXLAN segments and learns remote MAC Address-to-VTEP mappings through its IP interface. The functional components of VTEPs and the logical topology that is created for Layer 2 connectivity across the transport IP network are shown in Figure 3-2.

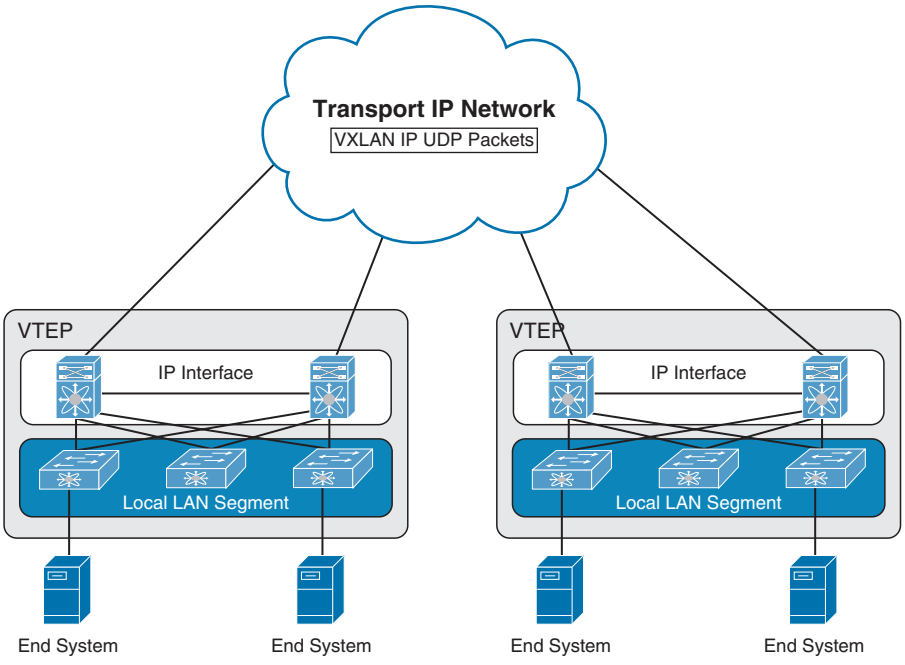


Figure 3-2 *VXLAN Tunnel Endpoint (VTEP)*

The VXLAN segments are independent of the underlying network topology; conversely, the underlying IP network between VTEPs is independent of the VXLAN overlay. It routes the encapsulated packets based on the outer IP address header, which has the initiating VTEP as the source IP address and the terminating VTEP as the destination IP address.

Virtual Network Identifier

A virtual network identifier (VNI) is a value that identifies a specific virtual network in the data plane. It is typically a 24-bit value part of the VXLAN header, which can support up to 16 million individual network segments. (Valid VNI values are from 4096 to 16,777,215.) There are two main VNI scopes:

- **Network-wide scoped VNIs:** The same value is used to identify the specific Layer 3 virtual network across all network edge devices. This network scope is useful in environments such as within the data center where networks can be automatically provisioned by central orchestration systems.

  Having a uniform VNI per VPN is a simple approach, while also easing network operations (such as troubleshooting). It also means simplified requirements on network edge devices, both physical and virtual devices. A critical requirement for this type of approach is to have a very large number of network identifier values given the network-wide scope.

- **Locally assigned VNIs:** In an alternative approach supported as per RFC 4364, the identifier has local significance to the network edge device that advertises the route.

In this case, the virtual network scale impact is determined on a per-node basis versus a network basis.

When it is locally scoped and uses the same existing semantics as an MPLS VPN label, the same forwarding behaviors as specified in RFC 4364 can be employed. This scope thus allows a seamless stitching together of a VPN that spans both an IP-based network overlay and an MPLS VPN.

This situation can occur, for instance, at the data center edge where the overlay network feeds into an MPLS VPN. In this case, the identifier may be dynamically allocated by the advertising device.

It is important to support both cases and, in doing so, ensure that the scope of the identifier be clear and the values not conflict with each other.

VXLAN Control Plane

Two widely adopted control planes are used with VXLAN: the VXLAN Flood and Learn Multicast-Based Control Plane and the VXLAN MPBGP EVPN Control Plane.

VXLAN Flood and Learn Multicast-Based Control Plane

Cisco Nexus switches utilize existing Layer 2 flooding mechanisms and dynamic MAC address learning to

- Transport broadcast, unknown unicast, and multicast (BUM) traffic
- Discover remote VTEPs
- Learn remote-host MAC addresses and MAC-to-VTEP mappings for each VXLAN segment

IP multicast is used to reduce the flooding scope of the set of hosts that are participating in the VXLAN segment. Each VXLAN segment, or VNID, is mapped to an IP multicast group in the transport IP network. Each VTEP device is independently configured and joins this multicast group as an IP host through the Internet Group Management Protocol (IGMP). The IGMP joins trigger Protocol Independent Multicast (PIM) joins and signaling through the transport network for the particular multicast group. The multicast distribution tree for this group is built through the transport network based on the locations of participating VTEPs. The multicast tunnel of a VXLAN segment through the underlying IP network is shown in Figure 3-3.

The multicast group shown in Figure 3-4 is used to transmit VXLAN broadcast, unknown unicast, and multicast traffic through the IP network, limiting Layer 2 flooding to those devices that have end systems participating in the same VXLAN segment. VTEPs communicate with one another through the flooded or multicast traffic in this multicast group.

Key Topic

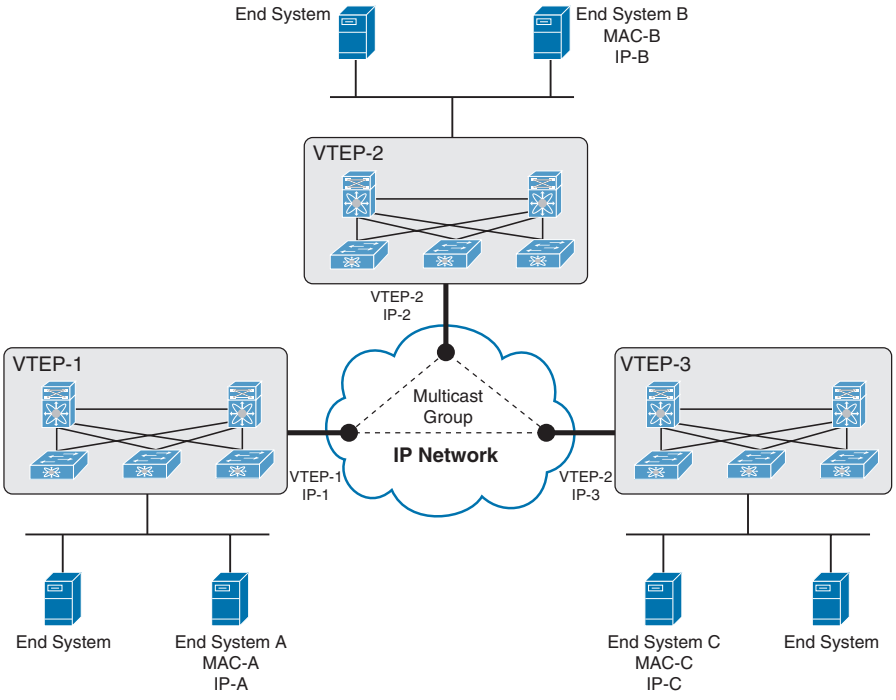


Figure 3-3 *VXLAN Multicast Group in Transport Network*

Key Topic

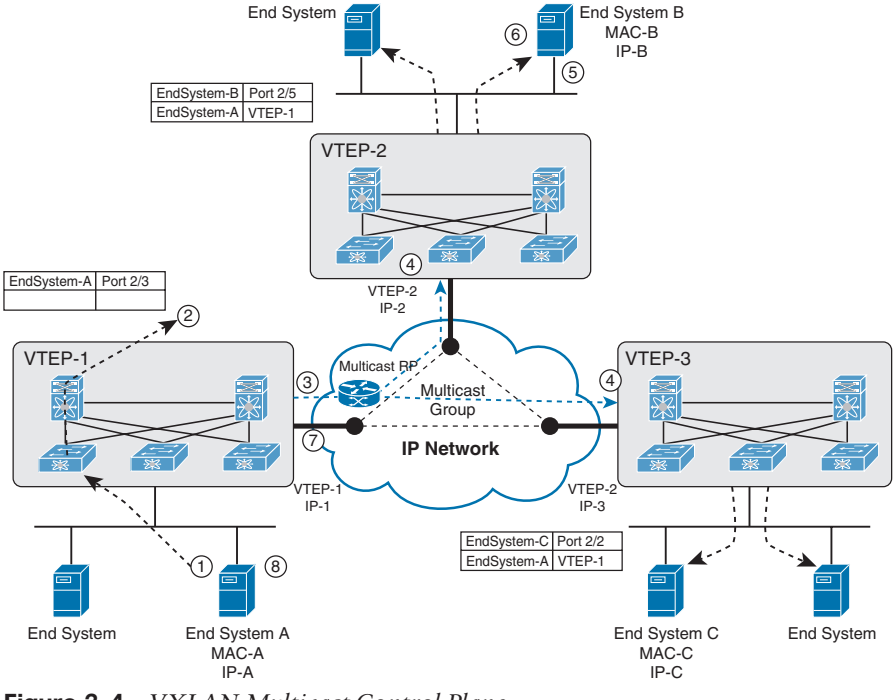


Figure 3-4 *VXLAN Multicast Control Plane*

As an example, if End System A wants to talk to End System B, it does the following:

1. End System A generates an ARP request trying to discover the End System B MAC address.
2. When the ARP request arrives at SW1, it will look up its local table, and if an entry is not found, it will encapsulate the ARP request over VXLAN and send it over the multicast group configured for the specific VNI.
3. The multicast RP receives the packet, and it forwards a copy to every VTEP that has joined the multicast group.
4. Each VTEP receives and deencapsulates the packet VXLAN packet and learns the System A MAC address pointing to the remote VTEP address.
5. Each VTEP forwards the ARP request to its local destinations.
6. End System B generates the ARP reply. When SW2 VTEP2 receives it, it looks up its local table and finds an entry with the information that traffic destined to End System A 180 must be sent to VTEP1 address. VTEP2 encapsulates the ARP reply with a VXLAN header and unicasts it to VTEP1.
7. VTEP1 receives and deencapsulates the packet and delivers it to End System A.
8. When the MAC address information is learned, additional packets are fed to the corresponding VTEP address.

VXLAN MPBGP EVPN Control Plane

The EVPN overlay specifies adaptations to the BGP MPLS-based EVPN solution so that it is applied as a network virtualization overlay with VXLAN encapsulation where

- The PE node role described in BGP MPLS EVPN is equivalent to the VTEP/network virtualization edge (NVE) device.
- VTEP information is distributed via BGP.
- VTEPs use control plane learning/distribution via BGP for remote MAC addresses instead of data plane learning.
- Broadcast, unknown unicast, and multicast (BUM) data traffic is sent using a shared multicast tree.
- A BGP route reflector (RR) is used to reduce the full mesh of BGP sessions among VTEPs to a single BGP session between a VTEP and the RR.
- Route filtering and constrained route distribution are used to ensure that the control plane traffic for a given overlay is distributed only to the VTEPs that are in that overlay instance.
- The host (MAC) mobility mechanism ensures that all the VTEPs in the overlay instance know the specific VTEP associated with the MAC.
- Virtual network identifiers (VNIs) are globally unique within the overlay.

The EVPN overlay solution for VXLAN can also be adapted to enable it to be applied as a network virtualization overlay with VXLAN for Layer 3 traffic segmentation. The adaptations for Layer 3 VXLAN are similar to L2 VXLAN, except the following:

- VTEPs use control plane learning/distribution via BGP of IP addresses (instead of MAC addresses).
- The virtual routing and forwarding instances are mapped to the VNI.
- The inner destination MAC address in the VXLAN header does not belong to the host but to the receiving VTEP that does the routing of the VXLAN payload. This MAC address is distributed via the BGP attribute along with EVPN routes.

VXLAN Gateways

VXLAN gateways are used to connect VXLAN and classic VLAN segments to create a common forwarding domain so that tenant devices can reside in both environments. The types of VXLAN gateways are

- **Layer 2 Gateway:** A Layer 2 VXLAN gateway is a device that encapsulates a classical Ethernet (CE) frame into a VXLAN frame and decapsulates a VXLAN frame into a CE frame. A gateway device transparently provides VXLAN benefits to a device that *does not support* VXLAN; that device could be a physical host or a virtual machine. The physical hosts or VMs are completely unaware of the VXLAN encapsulation.
- **VXLAN Layer 3 Gateway:** Similar to traditional routing between different VLANs, a VXLAN router is required for communication between devices that are in different VXLAN segments. The VXLAN router translates frames from one VNI to another. Depending on the source and destination, this process might require decapsulation and re-encapsulation of a frame. The Cisco Nexus device supports all combinations of decapsulation, route, and encapsulation. The routing can also be done across native Layer 3 interfaces and VXLAN segments.

  You can enable VXLAN routing at the aggregation layer or on Cisco Nexus device aggregation nodes. The spine forwards only IP-based traffic and ignores the encapsulated packets. To help scaling, a few leaf nodes (a pair of border leaves) perform routing between VNIs. A set of VNIs can be grouped into a virtual routing and forwarding (VRF) instance (tenant VRF) to enable routing among those VNIs. If routing must be enabled among a large number of VNIs, you might need to split the VNIs between several VXLAN routers. Each router is responsible for a set of VNIs and a respective subnet. Redundancy is achieved with FHRP.

VXLAN High Availability

For high availability, a pair of virtual port channel (vPC) switches can be used as a logical VTEP device sharing an anycast VTEP address (shown in Figure 3-5).

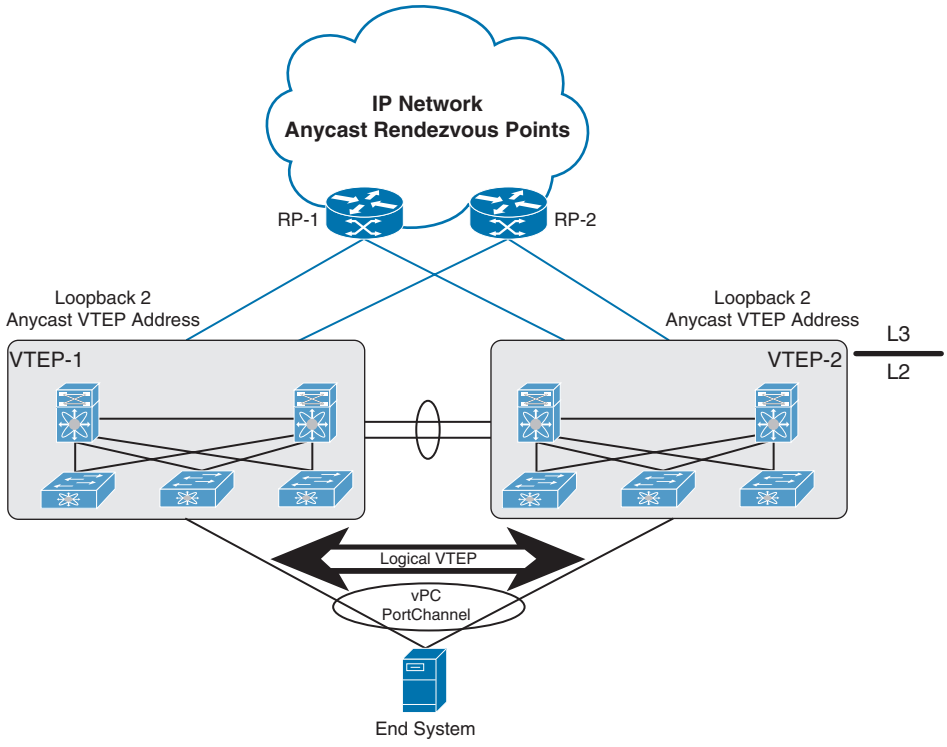


Figure 3-5 *VXLAN High Availability*

The vPC switches provide vPCs for redundant host connectivity while individually running Layer 3 protocols with the upstream devices in the underlay network. Both will join the multicast group for the same VXLAN VNI and use the same anycast VTEP address as the source to send VXLAN-encapsulated packets to the devices in the underlay network, including the multicast rendezvous point and the remote VTEP devices. The two vPC VTEP switches appear to be one logical VTEP entity.

vPC peers must have the following identical configurations:

- Consistent mapping of the VLAN to the virtual network segment (VN-segment)
- Consistent NVE binding to the same loopback secondary IP address (anycast VTEP address)
- Consistent VNI-to-group mapping

For the anycast IP address, vPC VTEP switches must use a secondary IP address on the loopback interface bound to the VXLAN NVE tunnel. The two vPC switches need to have the exact same secondary loopback IP address.

Both devices will advertise this anycast VTEP address on the underlay network so that the upstream devices learn the /32 route from both vPC VTEPs and can load-share VXLAN unicast-encapsulated traffic between them.

In the event of vPC peer-link failure, the vPC operational secondary switch will shut down its loopback interface bound to VXLAN NVE. This shutdown will cause the secondary vPC switch to withdraw the anycast VTEP address from its IGP advertisement so that the upstream devices in the underlay network start to send all traffic just to the primary vPC switch. The purpose of this process is to avoid a vPC active-active situation when the peer link is down. With this mechanism, the orphan devices connected to the secondary vPC switch will not be able to receive VXLAN traffic when the vPC peer link is down.

VXLAN Tenant Routed Multicast

Tenant Routed Multicast (TRM) brings the efficiency of multicast delivery to VXLAN overlays. It is based on standards-based next-gen control plane (ngMVPN) described in IETF RFCs 6513 and 6514. TRM enables the delivery of customer Layer 3 multicast traffic in a multitenant fabric, and this in an efficient and resilient manner.

While BGP EVPN provides a control plane for unicast routing, as shown in Figure 3-6, ngMVPN provides scalable multicast routing functionality. It follows an "always route" approach where every edge device (VTEP) with distributed IP Anycast Gateway for unicast becomes a designated router (DR) for multicast. Bridged multicast forwarding is present only on the edge devices (VTEP) where IGMP snooping optimizes the multicast forwarding to interested receivers. All other multicast traffic beyond local delivery is efficiently routed.

With TRM enabled, multicast forwarding in the underlay is leveraged to replicate VXLAN-encapsulated routed multicast traffic. A Default Multicast Distribution Tree (Default-MDT) is built per VRF. This is an addition to the existing multicast groups for Layer 2 VNI broadcast, unknown unicast, and Layer 2 multicast replication group. The individual multicast group addresses in the overlay are mapped to the respective underlay multicast address for replication and transport. The advantage of using a BGP-based approach is that TRM can operate as a fully distributed overlay rendezvous point (RP), with the RP presence on every edge device (VTEP).

A multicast-enabled data center fabric is typically part of an overall multicast network. Multicast sources, receivers, and even the multicast RP might reside inside the data center but might also be inside the campus or externally reachable via the WAN. TRM allows seamless integration with existing multicast networks. It can leverage multicast RPs external to the fabric. Furthermore, TRM allows for tenant-aware external connectivity using Layer 3 physical interfaces or subinterfaces.

VXLAN Configurations and Verifications

VXLAN requires a license. Table 3-2 shows the NX-OS feature license required for VXLAN. For more information, visit the Cisco NX-OS Licensing Guide.

Table 3-2 VXLAN Feature-Based Licenses for Cisco NX-OS

Platform	Feature License	Feature Name
Cisco Nexus 9000 Series switches	LAN_ENTERPRISE_SERVICES_PK	Cisco programmable fabric spine, leaf, or border leaf

Tables 3-3 through 3-6 show the most-used VXLAN configuration commands along with their purpose. For full commands, refer to the Nexus VXLAN Configuration Guide.

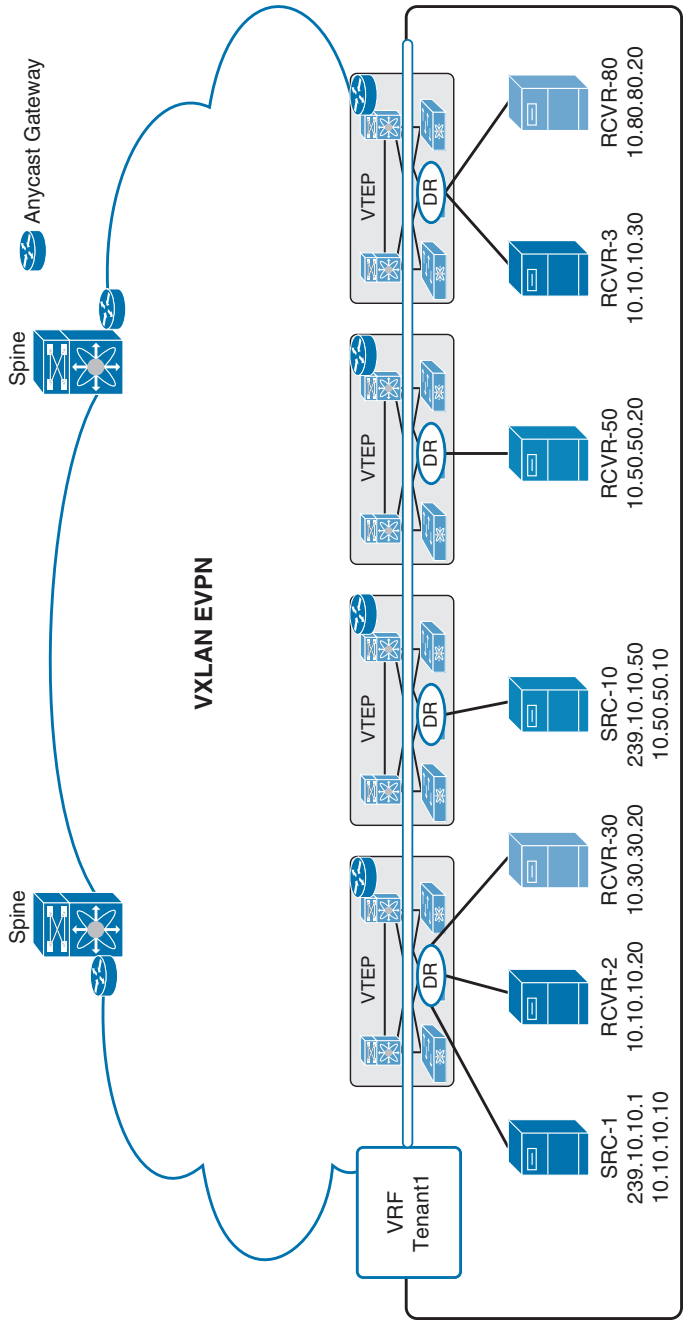


Figure 3-6 *Tenant Routed Multicast (TRM)*

Table 3-3 VXLAN Global-Level Commands

Command	Purpose
feature nv overlay	Enables the VXLAN feature.
feature vn-segment-vlan-based	Configures the global mode for all VXLAN bridge domains.
vlan *vlan-id*	Specifies VLAN.
vn-segment *vnid*	Specifies VXLAN virtual network identifier (VNID).
bridge-domain *domain*	Enters the bridge domain configuration mode. It will create a bridge domain if it does not yet exist. Use from the global configuration mode.
dot1q *vlan* **vni** *vni*	Creates mapping between VLAN and VNI. Use from the encapsulation profile configuration mode.
encapsulation profile *name_of_profile* **default**	Applies an encapsulation profile to a service profile. Use from the service instance configuration mode.
encapsulation profile vni *name_of_profile*	Creates an encapsulation profile. Use from the global configuration mode.
service *instance* **instance** *vni*	Creates a service instance. Use from the interface configuration mode.
interface nve *x*	Creates a VXLAN overlay interface that terminates VXLAN tunnels.
mac address-table static *mac-address* **vni** *vni-id* **interface nve** *x* **peer-ip** *ip-address*	Specifies the MAC address pointing to the remote VTEP. **NOTE:** Only 1 NVE interface is allowed on the switch.
ip igmp snooping vxlan	Enables IGMP snooping for VXLAN VLANs. You have to explicitly configure this command to enable snooping for VXLAN VLANs.
ip igmp snooping disable-nve-static-router-port	Configures IGMP snooping over VXLAN so that it does not include NVE as a static multicast router (mrouter) port using this global CLI command. The NVE interface for IGMP snooping over VXLAN is the mrouter port by default.

Table 3-4 Interface-Level Commands

Command	Purpose
switchport vlan mapping enable	Enables VLAN translation on the switch port. VLAN translation is disabled by default. **NOTE:** Use the **no** form of this command to disable VLAN translation.
switchport vlan mapping *vlan-id translated-vlan-id*	Translates a VLAN to another VLAN. The range for both the *vlan-id* and *translated-vlan-id* arguments is from 1 to 4094. ■ You can configure VLAN translation between the ingress (incoming) VLAN and a local (translated) VLAN on a port. For the traffic arriving on the interface where VLAN translation is enabled, the incoming VLAN is mapped to a translated VLAN that is VXLAN enabled.

Command	Purpose
	■ On the underlay, this is mapped to a VNI; the inner dot1q is deleted and switched over to the VXLAN network. On the egress switch, the VNI is mapped to a translated VLAN. On the outgoing interface, where VLAN translation is configured, the traffic is converted to the original VLAN and egress out. **NOTE:** Use the **no** form of this command to clear the mappings between a pair of VLANs.
switchport vlan mapping all	Removes all VLAN mappings configured on the interface.

Table 3-5 Network Virtual Interface (NVE) Config Commands

Command	Purpose
source-interface *src-if*	The source interface must be a loopback interface that is configured on the switch with a valid /32 IP address. The transient devices in the transport network and the remote VTEPs must know this /32 IP address. This is accomplished by advertising it through a dynamic routing protocol in the transport network.
member vni *vni*	Associates VXLAN virtual network identifiers (VNIs) with the NVE interface.
mcast-group *start-address* [*end-address*]	Assigns a multicast group to the VNIs. **NOTE:** Used only for BUM traffic.
ingress-replication protocol bgp	Enables BGP EVPN with ingress replication for the VNI.
ingress-replication protocol static	Enables static ingress replication for the VNI.
peer-ip *n.n.n.n*	Enables peer IP for static ingress-replication protocol.

Table 3-6 VXLAN Global-Level Verification Commands

Command	Purpose
show tech-support vxlan [platform]	Displays related VXLAN tech-support information.
show bridge-domain	Shows the bridge domain.
show logging level nve	Displays the logging level.
show tech-support nve	Displays related NVE tech-support information.
show run interface nve x	Displays NVE overlay interface configuration.
show nve interface	Displays NVE overlay interface status.
show nve peers	Displays NVE peer status.
show nve peers *peer_IP_address* **interface** *interface_ID counters*	Displays per-NVE peer statistics.
clear nve peer-ip *peer-ip-address*	Clears stale NVE peers. Stale NVE peers are those that do not have MAC addresses learned behind them.
show nve vni	Displays VXLAN VNI status.
show nve vni ingress-replication	Displays the mapping of VNI to an ingress-replication peer list and uptime for each peer.
show nve vni *vni_number* **counters**	Displays per-VNI statistics.
show nve vxlan-params	Displays VXLAN parameters, such as VXLAN destination or UDP port.

Figure 3-7 shows the VXLAN network topology with configurations.

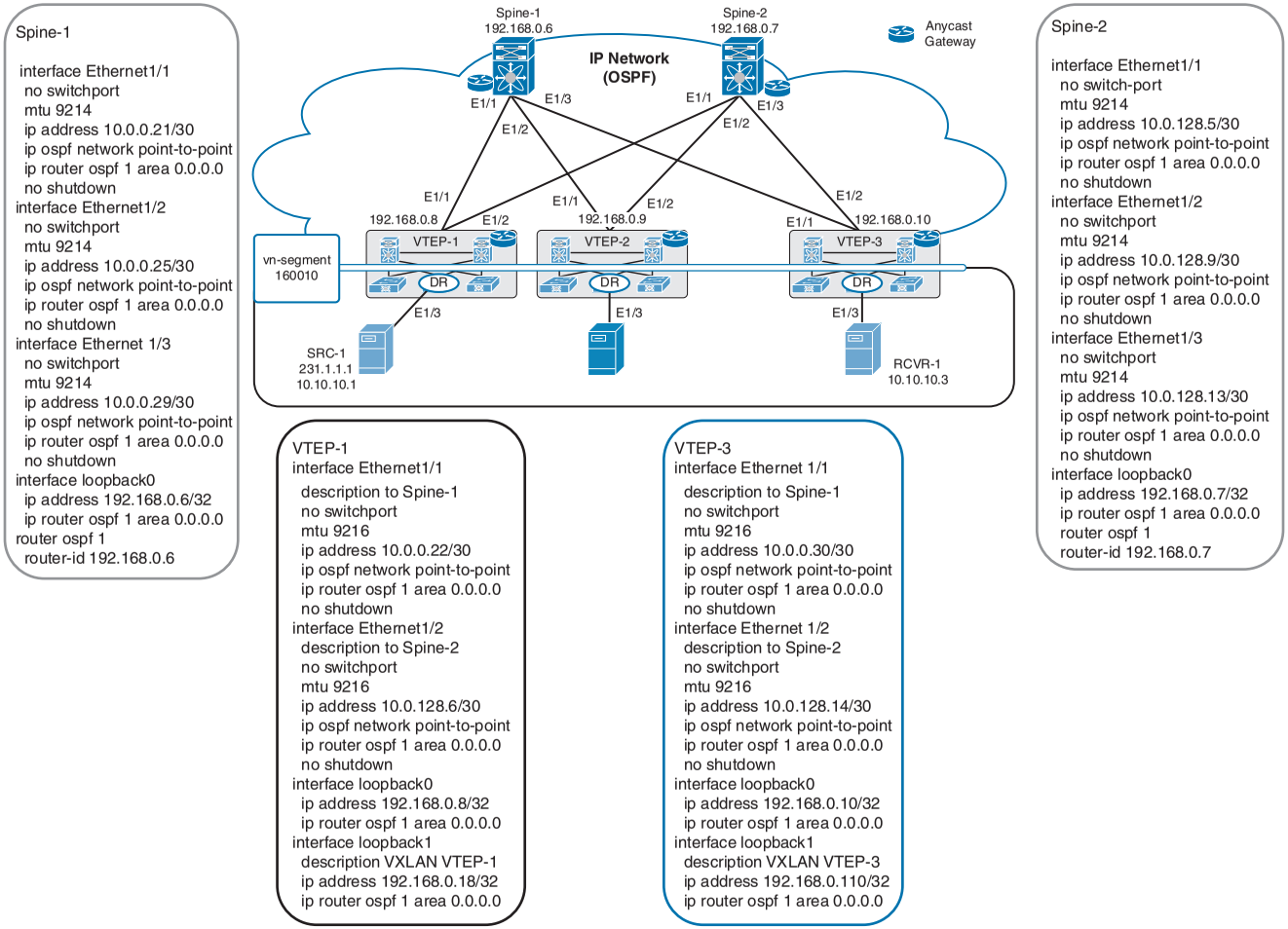


Figure 3-7 *VXLAN Control Plane Topology*

Example 3-1 shows the spine router (Spine-1 and Spine-2) OSPF and multicast routing configuration, VTEP (VTEP-1 and VTEP-3) multicast routing configuration, and multicast routing verification.

Example 3-1 *PIM Multicast Configurations and Verifications*

```
Spine-1 Config
Spine-1(config)# feature pim
Spine-1(config)# interface loopback1
Spine-1(config-if)# ip address 192.168.0.100/32
Spine-1(config-if)# ip pim sparse-mode
Spine-1(config-if)# ip router ospf 1 area 0.0.0.0
Spine-1(config)# ip pim rp-address 192.168.0.100
Spine-1(config)# ip pim anycast-rp 192.168.0.100 192.168.0.6
Spine-1(config)# ip pim anycast-rp 192.168.0.100 192.168.0.7
Spine-1(config)# interface E1/1
Spine-1(config-if)# ip pim sparse-mode
Spine-1(config)# interface E1/2
Spine-1(config-if)# ip pim sparse-mode
Spine-1(config)# interface E1/3
Spine-1(config-if)# ip pim sparse-mode
Spine-1(config)# interface loopback0
Spine-1(config-if)# ip pim sparse-mode
Spine-2 Config (PIM Redundancy)
Spine-2(config)# feature pim
Spine-2(config)# interface loopback1
Spine-2(config-if)# ip address 192.168.0.100/32
Spine-2(config-if)# ip pim sparse-mode
Spine-2(config-if)# ip router ospf 1 area 0.0.0.0
Spine-2(config)# ip pim rp-address 192.168.0.100
Spine-2(config)# ip pim anycast-rp 192.168.0.100 192.168.0.6
Spine-2(config)# ip pim anycast-rp 192.168.0.100 192.168.0.7
Spine-2(config)# interface E1/1
Spine-2(config-if)# ip pim sparse-mode
Spine-2(config)# interface E1/2
Spine-2(config-if)# ip pim sparse-mode
Spine-2(config)# interface E1/3
Spine-2(config-if)# ip pim sparse-mode
Spine-2(config)# interface loopback0
Spine-2(config-if)# ip pim sparse-mode
VTEP-1 PIM Config
VTEP-1(config)# feature pim
VTEP-1(config)# ip pim rp-address 192.168.0.100
VTEP-1 (config)# interface E1/1
VTEP-1 (config-if)# ip pim sparse-mode
VTEP-1 (config)# interface E1/2
VTEP-1 (config-if)# ip pim sparse-mod
```

```
VTEP-1 (config)# interface loopback0
VTEP-1 (config-if)# ip pim sparse-mode
VTEP-1 (config)# interface loopback1
VTEP-1 (config-if)# ip pim sparse-mode
VTEP-3 PIM Config
VTEP-3(config)# feature pim
VTEP-3(config)# ip pim rp-address 192.168.0.100
VTEP-3(config)# interface E1/1
VTEP-3(config-if)# ip pim sparse-mode
VTEP-3(config)# interface E1/2
VTEP-3(config-if)# ip pim sparse-mode
VTEP-3(config)# interface loopback0
VTEP-3(config-if)# ip pim sparse-mode
VTEP-3(config)# interface loopback1
VTEP-3(config-if)# ip pim sparse-mode
Spine 1 Verifications
Spine-1# show ip pim neighbor
PIM Neighbor Status for VRF "default"
Neighbor         Interface         Uptime   Expires       DR        Bidir-   BFD
                                                          Priority  Capable  State
10.0.0.22        Ethernet1/1      00:02:21 00:01:23        1        yes      n/a
10.0.0.26        Ethernet1/2      00:01:50 00:01:20        1        yes      n/a
10.0.0.30        Ethernet1/3      00:00:37 00:01:38        1        yes      n/a
Spine-1# show ip pim rp
PIM RP Status Information for VRF "default"
BSR disabled
Auto-RP disabled
BSR RP Candidate policy: None
BSR RP policy: None
Auto-RP Announce policy: None
Auto-RP Discovery policy: None
Anycast-RP 192.168.0.100 members:
  192.168.0.6* 192.168.0.7
RP: 192.168.0.100*, (0),
 uptime: 00:04:29 priority: 255,
 RP-source: (local),
 group ranges:
 224.0.0.0/4
Spine 2 Verifications
Spine-2# show ip pim neighbor
PIM Neighbor Status for VRF "default"
Neighbor         Interface        Uptime   Expires       DR        Bidir-    BFD
                                                         Priority  Capable   State
10.0.128.6       Ethernet1/1      00:02:21 00:01:23       1         yes       n/a
10.0.128.10      Ethernet1/2      00:01:50 00:01:20       1         yes       n/a
10.0.128.14      Ethernet1/3      00:00:37 00:01:38       1         yes       n/a
```

```
Spine-2# show ip pim rp
PIM RP Status Information for VRF "default"
BSR disabled
Auto-RP disabled
BSR RP Candidate policy: None
BSR RP policy: None
Auto-RP Announce policy: None
Auto-RP Discovery policy: None
Anycast-RP 192.168.0.100 members:
  192.168.0.6 192.168.0.7*
RP: 192.168.0.100*, (0),
 uptime: 00:04:16 priority: 255,
 RP-source: (local),
 group ranges:
 224.0.0.0/4
VTEP-1 Verifications
VTEP-1# show ip pim neighbor
PIM Neighbor Status for VRF "default"
Neighbor         Interface           Uptime    Expires   DR       Bidir-   BFD
                                                         Priority Capable  State
10.0.0.21        Ethernet1/1         00:03:47  00:01:32   1        yes     n/a
10.0.128.5       Ethernet1/2         00:03:46  00:01:37   1        yes     n/a

VTEP-1# show ip pim rp
PIM RP Status Information for VRF "default"
BSR disabled
Auto-RP disabled
BSR RP Candidate policy: None
BSR RP policy: None
Auto-RP Announce policy: None
Auto-RP Discovery policy: None
RP: 192.168.0.100, (0),
 uptime: 00:03:53 priority: 255,
 RP-source: (local),
 group ranges:
 224.0.0.0/4
VTEP-3 Verifications
VTEP-3# show ip pim neighbor
PIM Neighbor Status for VRF "default"
Neighbor        Interface            Uptime    Expires   DR       Bidir-  BFD
                                                         Priority Capable State
10.0.0.29       Ethernet1/1          00:03:06  00:01:21  1        yes     n/a
10.0.128.13     Ethernet1/2          00:02:48  00:01:35  1        yes     n/a
```

```
VTEP-3(config)# show ip pim rp
PIM RP Status Information for VRF "default"
BSR disabled
Auto-RP disabled
BSR RP Candidate policy: None
BSR RP policy: None
Auto-RP Announce policy: None
Auto-RP Discovery policy: None
RP: 192.168.0.100, (0),
 uptime: 00:03:11 priority: 255,
 RP-source: (local),
 group ranges:
 224.0.0.0/
```


Example 3-2 shows the VTEP (VETP-1 and VTEP-3) VXLAN and VXLAN Network Virtual Interface (NVE) configuration and status verification.

Example 3-2 *VXLAN Configurations and Verifications*

```
VTEP-1 Config
VTEP-1(config)# feature vn-segment-vlan-based
VTEP-1(config)# feature vn overlay
VTEP-1(config)# vlan 10
VTEP-1(config-vlan)# vn-segment 160010
VTEP-1(config)# vlan 20
VTEP-1(config-vlan)# vn-segment 160020
VTEP-1(config)# interface nve1
VTEP-1 (config-if)# source-interface loopback1
VTEP-1 (config-if)# member vni 160010 mcast-group 231.1.1.1
VTEP-1 (config-if)# member vni 160020 mcast-group 231.1.1.1
VTEP-1 (config-if)# no shutdown
VTEP-3 Config
VTEP-3(config)# feature vn-segment-vlan-based
VTEP-3(config)# feature vn overlay
VTEP-3(config)# vlan 10
VTEP-3(config-vlan)# vn-segment 160010
VTEP-3(config)# vlan 20
VTEP-3(config-vlan)# vn-segment 160020
VTEP-3(config)# interface nve1
VTEP-3(config-if)# source-interface loopback1
VTEP-3(config-if)# member vni 160010 mcast-group 231.1.1.1
VTEP-3(config-if)# member vni 160020 mcast-group 231.1.1.1
VTEP-3(config-if)# no shutdown
VTEP-1 Verifications
VTEP-1# show nve vni
```

```
Codes: CP - Control Plane        DP - Data Plane
       UC - Unconfigured         SA - Suppress ARP
       SU - Suppress Unknown Unicast
Interface VNI      Multicast-group    State Mode Type [BD/VRF]      Flags
--------- -------- -----------------  ----- ---- ------------------ -----
nve1      160010   231.1.1.1          Up    DP   L2    [10]
nve1      160020   231.1.1.1          Up    DP   L2    [20]

VTEP-1# show vxlan
Vlan            VN-Segment
====            ==========
10              160010
20              160020
VTEP-1# ping 10.10.10.3
PING 10.10.10.3 (10.10.10.3) : 56 data bytes
64 bytes from 10.10.10.3: icmp_seq=0 ttl=254 time=8.114 ms
64 bytes from 10.10.10.3: icmp_seq=1 ttl=254 time=5.641 ms
64 bytes from 10.10.10.3: icmp_seq=2 ttl=254 time=6.213 ms
64 bytes from 10.10.10.3: icmp_seq=3 ttl=254 time=6.119 ms
VTEP-1# show nve peers
Interface Peer-IP          State LearnType Uptime     Router-Mac
--------- ---------------  ----- --------- --------   -----------------
nve1      192.168.0.110    Up    DP        00:09:08   n/a
VTEP-1# show ip mroute
IP Multicast Routing Table for VRF "default"
(*, 231.1.1.1/32), uptime: 00:10:38, nve ip pim
  Incoming interface: Ethernet1/1, RPF nbr: 10.0.0.29
  Outgoing interface list: (count: 1)
    nve1, uptime: 00:10:38, nve
(192.168.0.18/32, 231.1.1.1/32), uptime: 00:02:34, ip mrib pim
  Incoming interface: Ethernet1/2, RPF nbr: 10.0.128.13
  Outgoing interface list: (count: 1)
    nve1, uptime: 00:02:34, mrib
(*, 232.0.0.0/8), uptime: 00:17:03, pim ip
  Incoming interface: Null, RPF nbr: 0.0.0.0
  Outgoing interface list: (count: 0)
VTEP-3 Verifications
VTEP-3# show nve vni
Codes: CP - Control Plane        DP - Data Plane
       UC - Unconfigured         SA - Suppress ARP
       SU - Suppress Unknown Unicast
Interface  VNI      Multicast-group  State Mode Type [BD/VRF]      Flag
---------  -------- ---------------- ----- ---- ------------------ -----
nve1       160010   231.1.1.1        Up    DP   L2    [10]
nve1       160020   231.1.1.1        Up    DP   L2    [20]
```

```
VTEP-3# show vxlan
Vlan             VN-Segment
====             ==========
10               160010
20               160020
VTEP-3# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) : 56 data bytes
64 bytes from 10.10.10.1: icmp_seq=0 ttl=254 time=7.212 ms
64 bytes from 10.10.10.1: icmp_seq=1 ttl=254 time=6.243 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=254 time=5.268 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=254 time=6.397 ms
VTEP-1# show nve peers
Interface  Peer-IP          State  LearnType  Uptime    Router-Mac
---------  ---------------  -----  ---------  --------  -----------------
nve1       192.168.0.18     Up     DP         00:09:08  n/a
VTEP-3# show ip mroute
IP Multicast Routing Table for VRF "default"
(*, 231.1.1.1/32), uptime: 00:10:38, nve ip pim
 Incoming interface: Ethernet1/1, RPF nbr: 10.0.0.29
  Outgoing interface list: (count: 1)
    nve1, uptime: 00:10:38, nve
(192.168.0.18/32, 231.1.1.1/32), uptime: 00:02:34, ip mrib pim
  Incoming interface: Ethernet1/2, RPF nbr: 10.0.128.13
  Outgoing interface list: (count: 1)
    nve1, uptime: 00:02:34, mrib
(192.168.0.110/32, 231.1.1.1/32), uptime: 00:10:38, nve mrib ip pim
  Incoming interface: loopback1, RPF nbr: 192.168.0.110
  Outgoing interface list: (count: 1)
    Ethernet1/2, uptime: 00:09:39, pim
(*, 232.0.0.0/8), uptime: 00:17:03, pim ip
  Incoming interface: Null, RPF nbr: 0.0.0.0
  Outgoing interface list: (count: 0)
```

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 21, "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 topic icon in the outer margin of the page. Table 3-7 lists a reference to these key topics and the page numbers on which each is found.

Key Topic

Table 3-7 Key Topics for Chapter 3

Key Topic Element	Description	Page
Section	VXLAN Encapsulation and Packet Format	152
Figure 3-1	VXLAN Packet Format	152
Figure 3-2	VXLAN Tunnel Endpoint (VTEP)	153
Section	Virtual Network Identifier (VNI)	153
Section	VXLAN Control Plane	154
Figure 3-3	VXLAN Multicast Group in Transport Network	155
Figure 3-4	VXLAN Multicast Control Plane	155
Section	VXLAN MPBGP EVPN Control Plane	156

Define Key Terms

Define the following key terms from this chapter, and check your answers in the Glossary.

Address Resolution Protocol (ARP); broadcast, unknown unicast, and multicast (BUM); Cisco Nexus; Cisco NX-OS; equal-cost multipath (ECMP); Ethernet VPN (EVPN); Internet Group Management Protocol (IGMP); local-area network (LAN); Media Access Control (MAC); Protocol Independent Multicast (PIM); User Datagram Protocol (UDP); virtual LAN (VLAN); virtual port channels (vPCs); virtual private network (VPN); virtual routing and forwarding (VRF); wide-area network (WAN)

References

Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 10.3(x): https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/103x/configuration/vxlan/cisco-nexus-9000-series-nx-os-vxlan-configuration-guide-release-103x.html

Relevant CiscoLive Presentations: https://ciscolive.com

A Summary of Cisco VXLAN Control Planes: Multicast, Unicast, MP-BGP EVPN: https://blogs.cisco.com/perspectives/a-summary-of-cisco-vxlan-control-planes-multicast-unicast-mp-bgp-evpn-2

This page intentionally left blank

Index

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