

Practice Tests



Flash Cards



Study Planner



Review Exercises

CCNP and CCIE Data Center Core

DCCOR 350-601

2nd Edition

ciscopress.com

Somit Maloo

CCDE® No. 20170002, CCIE® No. 28603

Iskren Nikolov

CCIE® No. 20164, CCNP Data Center, CCSI® No. 32481

Firas Ahmed

CCIE® No. 14967

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

Copyright© 2024 Cisco Systems, Inc.

Published by:
Cisco Press

Hoboken, New Jersey

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

\$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.

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

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

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

Introduction xxxv

Part I Networking

- Chapter 1 Implementing Routing in the Data Center 2
- Chapter 2 Implementing Data Center Switching Protocols 90
- Chapter 3 Implementing Data Center Overlay Protocols 150
- Chapter 4 Describe Cisco Application Centric Infrastructure 172
- Chapter 5 Cisco Cloud Services and Deployment Models 240
- Chapter 6 Data Center Network Management and Monitoring 252
- Chapter 7 Describe Cisco Nexus Dashboard 314

Part II Storage

- Chapter 8 Implement Fibre Channel 352
- Chapter 9 Implement FCoE Unified Fabric 434
- Chapter 10 Describe NFS and NAS Concepts 478
- Chapter 11 Describe Software Management and Infrastructure Monitoring 488

Part III Compute

- Chapter 12 Cisco Unified Computing Systems Overview 530
- Chapter 13 Cisco Unified Computing Infrastructure Monitoring 628
- Chapter 14 Cisco Unified Compute Software and Configuration Management 658
- Chapter 15 Cisco HyperFlex Overview 702

Part IV Automation

- Chapter 16 Automation and Scripting Tools 730
- Chapter 17 Evaluate Automation and Orchestration Technologies 762

Part V Security

- Chapter 18 Network Security 798
- Chapter 19 Compute Security 874

Chapter 20 Storage Security 896

Chapter 21 Final Preparation 932

Chapter 22 *CCNP and CCIE Data Center Core DCCOR 350-601 Official Cert Guide*
Exam Updates 942

Appendix A Answers to the “Do I Know This Already?” Quizzes 946

Glossary 961

Index 984

Online Elements

Appendix B Memory Tables

Appendix C Memory Tables Answer Key

Appendix D Study Planner

Glossary

Contents

	Introduction	xxxv
Part I	Networking	
Chapter 1	Implementing Routing in the Data Center	2
	“Do I Know This Already?” Quiz	2
	Foundation Topics	5
	Routing Protocols Support on Cisco Nexus Devices	5
	OSPF	6
	OSPF Link-State Advertisements	7
	<i>OSPF Areas</i>	10
	<i>Designated Routers and Backup Designated Routers</i>	12
	OSPF Authentication	13
	OSPF Configurations and Verifications	13
	Border Gateway Protocol	24
	BGP Peering	25
	BGP Path Selection	26
	<i>Step 1: Comparing Pairs of Paths</i>	27
	<i>Step 2: Determining the Order of Comparisons</i>	28
	<i>Step 3: Determining the Best-Path Change Suppression</i>	29
	Multiprotocol BGP	29
	BGP Configurations and Verifications	30
	Bidirectional Forwarding Detection	37
	Rapid Detection of Failures	38
	BFD Configurations and Verifications	38
	Multicast	42
	Internet Group Management Protocol	43
	Switch IGMP Snooping	46
	Multicast Listener Discovery	46
	Multicast Distribution Trees	47
	Protocol Independent Multicast	49
	<i>PIM Rendezvous Points</i>	53
	<i>PIM Designated Routers/Forwarders</i>	54
	Multicast Forwarding	55
	Multicast Configurations and Verifications	56
	Hot Standby Router Protocol	69
	Virtual Router Redundancy Protocol	73

VRRP Operation	73
VRRP Groups	75
VRRP Router Priority and Preemption	76
VRRP Authentication	77
VRRP Tracking	77
IPv6 First Hop Redundancy	77
HSRP/VRRP Configurations and Verifications	79
Exam Preparation Tasks	87
Review All Key Topics	87
Memory Tables	88
Define Key Terms	88
References	88

Chapter 2 Implementing Data Center Switching Protocols 90

“Do I Know This Already?” Quiz	90
Foundation Topics	93
Spanning Tree Protocols	93
STP Topology	93
STP Port Types	94
STP Extensions	94
<i>STP Bridge Assurance</i>	95
<i>BPDU Guard</i>	96
<i>BPDU Filter</i>	96
<i>Loop Guard</i>	96
<i>Root Guard</i>	97
Unidirectional Link Detection	97
Rapid PVST+	98
<i>Rapid PVST+ Ports</i>	100
Spanning Tree Configurations and Verifications	102
Port Channels	117
<i>Port Channel Load Balance</i>	120
Virtual Port Channel	122
vPC Traffic Flows	125
vPC Dual-Control Plane	126
vPC Primary and Secondary Roles	127
vPC Configuration Consistency	128
vPC Duplicate Frames Prevention Mechanism	129
vPC HSRP Gateway Considerations	131

	vPC ARP Synchronization	131
	vPC Peer Gateway	131
	Port Channel Configurations and Verifications	132
	Exam Preparation Tasks	146
	Review All Key Topics	146
	Memory Tables	147
	Define Key Terms	147
	References	148
Chapter 3	Implementing Data Center Overlay Protocols	150
	“Do I Know This Already?” Quiz	150
	Foundation Topics	151
	Virtual Extensible LAN (VXLAN) Overview	151
	VXLAN Encapsulation and Packet Format	152
	VXLAN Tunnel Endpoint	152
	Virtual Network Identifier	153
	VXLAN Control Plane	154
	<i>VXLAN Flood and Learn Multicast-Based Control Plane</i>	154
	<i>VXLAN MPBGP EVPN Control Plane</i>	156
	VXLAN Gateways	157
	VXLAN High Availability	157
	VXLAN Tenant Routed Multicast	159
	VXLAN Configurations and Verifications	159
	Exam Preparation Tasks	169
	Review All Key Topics	169
	Define Key Terms	170
	References	170
Chapter 4	Describe Cisco Application Centric Infrastructure	172
	“Do I Know This Already?” Quiz	172
	Foundation Topics	174
	Cisco Application Centric Infrastructure (ACI) Overview	174
	Cisco Application Policy Infrastructure Controller	176
	Cisco Nexus 9000 Series Spine and Leaf Switches for Cisco ACI	179
	Cisco ACI Initial Setup, Fabric Discovery, Fabric Upgrade, and Fabric Access Policies	182
	Cisco ACI Initial Setup	182
	Cisco ACI Fabric Discovery	187

Startup with Cisco ACI Fabric Discovery and Configuration	188
Fabric Upgrade	189
Cisco ACI Fabric Access Policies	190
Cisco ACI Fabric Building Blocks, Policy Model, and VMM Domains	195
ACI Policy Model	197
Cisco ACI Tenants	198
<i>Virtual Routing and Forwarding</i>	200
<i>Bridge Domain and Subnets</i>	200
<i>Endpoint Group</i>	202
<i>Cisco ACI Virtual Machine Manager Domains</i>	203
<i>Cisco ACI Integration with Microsoft SCVMM</i>	204
<i>Cisco ACI Integration with VMware vCenter</i>	205
<i>Cisco ACI Virtual Edge</i>	206
<i>Integrating VMware Overlays with the Cisco ACI</i>	206
<i>Application Profiles</i>	206
<i>Microsegmentations</i>	207
<i>Attachable Entity Profile</i>	207
<i>ACI Contract</i>	208
Taboo Contracts	209
vzAny Rule	210
Filters and Subjects	213
Management Tenant	213
In-Band Management Access	214
<i>Out-of-Band Management Access</i>	214
ACI VXLAN	215
ACI Intersubnet Tenant Traffic	217
Policy Identification and Enforcement	218
ACI Fabric Traffic Storm Control	219
ACI Fabric Traffic Load Balance	219
ACI Fabric Loop Detection	220
ACI Design Best Practices	221
ACI LAB Configurations Example	221
Building ACI Fabric	224
Creating Tenant	227
Creating Contract and Filter	230
Deploying a Three-Tier Application	233
Integrating with vCenter	235

Exam Preparation Tasks 238

Review All Key Topics 238

Define Key Terms 239

References 239

Chapter 5 Cisco Cloud Services and Deployment Models 240

“Do I Know This Already?” Quiz 240

Foundation Topics 242

What Is Cloud Computing? 242

Cloud Service Models 245

 Software as a Service 245

 Platform as a Service 246

 Infrastructure as a Service 246

Cloud Deployment Models 248

 Private Cloud 248

 Public Cloud 248

 Hybrid Cloud 249

 Community Cloud 250

Exam Preparation Tasks 250

Review All Key Topics 250

Define Key Terms 251

References 251

Chapter 6 Data Center Network Management and Monitoring 252

“Do I Know This Already?” Quiz 252

Foundation Topics 254

Cisco Nexus NX-OS Software Installation, Updates, and Their Impacts 254

 PowerOn Auto Provisioning (POAP) 259

 Data Center Infrastructure Software Lifecycle Management 263

 Nexus Nondisruptive In-Service Software Upgrade 263

 Nexus Disruptive and Nondisruptive Upgrade/Downgrade Procedure 265

 Programmable Logical Devices Upgrade 269

Nexus Configuration Management 271

 NX-OS Configuration Save and Backup 272

 Nexus Config Rollback and Checkpoint 272

Network Time Management 274

 Network Time Protocol 275

 Precision Time Protocol 280

Network Infrastructure Monitoring	284
NX-OS System Message Logging	284
NX-OS Simple Network Management Protocol	286
Nexus Smart Call Home	292
Nexus NetFlow	293
Switched Port Analyzer	298
Streaming Telemetry	306
Network Assurance Concept	310
Exam Preparation Tasks	312
Review All Key Topics	312
Memory Tables	313
Define Key Terms	313
References	313

Chapter 7 Describe Cisco Nexus Dashboard 314

“Do I Know This Already?” Quiz	314
Foundation Topics	316
Cisco Nexus Dashboard	316
Cisco Nexus Dashboard Insights	318
<i>Cisco Nexus Dashboard Insights Features and Benefits</i>	318
<i>Cisco Nexus Dashboard Insights GUI Overview</i>	320
Cisco Nexus Dashboard Orchestrator	323
<i>Cisco Nexus Dashboard Orchestrator Features and Benefits</i>	324
Cisco Nexus Dashboard Fabric Controller	325
<i>Cisco Nexus Dashboard Fabric Controller Features and Benefits</i>	326
<i>Cisco Nexus Dashboard Fabric Controller GUI Overview</i>	331
Cisco Nexus Dashboard Data Broker	335
<i>Cisco Nexus Dashboard Data Broker Features and Benefits</i>	337
Cisco Nexus Dashboard Platforms	337
Cisco Nexus Dashboard Cluster Nodes	339
Cisco Nexus Dashboard External Networks	341
Cisco Nexus Dashboard GUI Overview	342
One View Page	343
Admin Console Page	343
<i>Overview Page</i>	344
<i>Sites Page</i>	345
<i>Services Page</i>	345
<i>System Resources Pages</i>	346

Operations Pages 347
Infrastructure Pages 348
Administrative Pages 348

Exam Preparation Tasks 348
 Review All Key Topics 348
 Memory Tables 349
 Define Key Terms 349
 References 349

Part II Storage

Chapter 8 Implement Fibre Channel 352

“Do I Know This Already?” Quiz 353
 Foundation Topics 356
 Cisco MDS 9000 Series Hardware 356
 Cisco MDS 9700 Series Multilayer Directors 356
 Cisco MDS 9300 Series Multilayer Fabric Switches 360
 Cisco MDS 9200 Series Multiservice Switches 361
 Cisco MDS 9100 Series Multilayer Fabric Switches 362
 Fibre Channel Basics 365
 Fibre Channel Topologies 365
 Fibre Channel Port Types 368
 E Port 369
 F Port 369
 NP Ports 369
 TE Port 369
 TF Port 370
 TNP Port 370
 Fx Port 370
 Auto Mode 370
 Fibre Channel Addressing 371
 Flow Control 372
 Switched Fabric Initialization 373
 Principal Switch Selection 374
 Domain ID Distribution 375
 FCID Allocation 377
 Fabric Reconfiguration 377
 Device Registration: FLOGI, PLOGI, PRLI 378
 FLOGI and FCNS Databases 378

CFS	380
CFS Features	381
CFS Fabric Lock	382
CFSoIP and CFSoFC	382
CFS Merge	384
CFS Regions	384
VSAN	386
VSAN Features	386
VSAN Attributes	387
VSAN Advantages	388
Dynamic Port VSAN Membership (DPVM)	388
VSAN Trunking	389
SAN Port Channels	396
Types of SAN Port Channels	396
Port Channel Load Balancing	398
Port Channel Modes	399
Zoning	404
Zoning Features	404
Zone Enforcement	406
Full and Active Zone Set	407
Autozone	410
Zone Merge	410
Smart Zoning	411
Enhanced Zoning	412
Device Alias	418
Device Alias Features	419
Device Alias Modes	419
Device Alias Distribution	420
Zone Aliases (FC Aliases) Versus Device Aliases	421
NPIV and NPV	424
Exam Preparation Tasks	431
Review All Key Topics	431
Memory Tables	432
Define Key Terms	432
References	433

Chapter 9	Implement FCoE Unified Fabric	434
	“Do I Know This Already?” Quiz	434
	Foundation Topics	436
	FCoE Overview	436
	Ethernet Enhancements	438
	<i>Priority-Based Flow Control (PFC)</i>	438
	<i>Enhanced Transmission Selection (ETS)</i>	439
	<i>Data Center Bridging Exchange (DCBX)</i>	440
	FCoE Frame Format	442
	Virtual Fibre Channel (VFC)	444
	FCoE Elements and Port Types	445
	FCoE Addressing and Forwarding	447
	FCoE Initialization Protocol (FIP)	448
	Benefits of FCoE	451
	FCoE Topology Options	451
	FCoE Single-Hop Topology	451
	<i>FCoE Direct-Attached Topology</i>	452
	<i>FCoE FEX Topology</i>	453
	<i>FCoE Remote-Attached Topology</i>	454
	FCoE Multi-Hop Topology	454
	FCoE Implementations	455
	FCoE Configuration on Cisco Nexus 7000 Series Switches	456
	<i>Miscellaneous FCoE Configuration</i>	457
	FCoE Configuration on Cisco Nexus 5000 Series Switches	458
	FCoE Configuration on Cisco Nexus 9000 Series Switches	459
	FCoE over FEX	461
	FCoE NPV	463
	FCoE Verification	466
	Exam Preparation Tasks	475
	Review All Key Topics	475
	Memory Tables	476
	Define Key Terms	476
	References	476
Chapter 10	Describe NFS and NAS Concepts	478
	“Do I Know This Already?” Quiz	478
	Foundation Topics	479
	Describe NFS Concepts	479

Describe NAS Concepts	481
NAS Benefits	483
Cisco UCS S-Series Storage Servers	483
Exam Preparation Tasks	485
Review All Key Topics	485
Define Key Terms	485
References	486

Chapter 11 Describe Software Management and Infrastructure Monitoring 488

“Do I Know This Already?” Quiz	488
Foundation Topics	490
Cisco MDS NX-OS Setup Utility	490
Cisco MDS NX-OS Software Upgrade and Downgrade	498
Nondisruptive Upgrade on a Cisco MDS Fabric Switch	500
Disruptive Upgrade on a Cisco MDS Fabric Switch	505
Nondisruptive Downgrade on a Cisco MDS Fabric Switch	508
Disruptive Downgrade on a Cisco MDS Fabric Switch	513
EPLD Upgrade on Cisco MDS 9000 Series Switches	515
Infrastructure Monitoring	521
System Messages	521
Call Home	521
Embedded Event Manager	522
RMON	523
SPAN	523
<i>SPAN Configuration Example</i>	526
<i>Remote SPAN</i>	526
Exam Preparation Tasks	528
Review All Key Topics	528
Define Key Terms	529
References	529

Part III Compute

Chapter 12 Cisco Unified Computing Systems Overview 530

“Do I Know This Already?” Quiz	530
Foundation Topics	532
Cisco UCS Architecture	532
Cisco UCS Components and Connectivity	534
Cisco UCS 5108 Blade Server Chassis	536

UCS Blade Servers	536
Cisco UCS Rack Servers	537
Cisco UCS Storage Servers	537
Cisco UCS Mini	539
Cisco UCS Fabric Infrastructure	539
Cisco UCS 6536 Fabric Interconnect	540
Cisco UCS 6454 Fabric Interconnect	541
Cisco UCS 6300 Series Fabric Interconnects	543
Fabric Interconnect and Fabric Extender Connectivity	544
Cisco UCS Virtualization Infrastructure	550
Cisco UCS-X System	555
Cisco UCS Initial Setup and Management	557
Fabric Interconnect Connectivity and Configurations	565
<i>Uplink Connectivity</i>	566
<i>Downlink Connectivity</i>	567
Fabric Interconnect Port Modes	567
Fabric Failover for Ethernet: High-Availability vNIC	569
Ethernet Switching Mode	570
UCS Device Discovery	577
Chassis/FEX Discovery	577
Rack Server Discovery Policy	577
Initial Server Setup for Standalone UCS C-Series	578
Cisco UCS Network Management	584
UCS Virtual LAN	584
<i>Named VLANs</i>	586
UCS Identity Pools	591
<i>Universally Unique Identifier Suffix Pools</i>	591
<i>MAC Pools</i>	593
<i>IP Pools</i>	593
<i>Server Pools</i>	596
Service Profiles	596
UCS Server Policies	599
UCS Service Profile Templates	602
Quality of Service	608
<i>QoS System Classes</i>	608
<i>QoS System Classes Configurations</i>	609
<i>Configuring Quality of Service Policies</i>	610

- Cisco UCS Storage 611
 - UCS SAN Connectivity 611
 - UCS SAN Configuration 615
 - Virtual Storage-Area Networks 616
 - Named VSANs Configurations* 616
 - Zones and Zone Sets* 618
 - World Wide Name Pool 621
 - SAN Connectivity Policies 624
- Exam Preparation Tasks 625
- Review All Key Topics 625
- Define Key Terms 626
- References 626

Chapter 13 Cisco Unified Computing Infrastructure Monitoring 628

- “Do I Know This Already?” Quiz 628
- Foundation Topics 630
- Cisco UCS System Monitoring 630
 - Data Management Engine 631
 - Application Gateway 631
 - Northbound Interfaces 631
 - Cisco UCS Monitoring Events and Logs 632
 - Cisco UCS Monitoring Policies 634
 - Cisco UCS Simple Network Management Protocol* 636
 - Cisco UCS Call Home and Smart Call Home* 636
 - Cisco UCS Manager Database Health and Hardware Monitoring* 638
 - Cisco UCS NetFlow Monitoring* 638
 - Traffic Monitoring 640
 - Traffic Monitoring Across Ethernet* 641
 - Traffic Monitoring Across Fibre Channel* 642
- Cisco Intersight 647
 - Intersight Management as a Service 648
 - Intersight as a Telemetry Data Collection 650
 - Cisco Intersight Supported Software 650
 - Cisco Intersight Licensing 652
- Exam Preparation Tasks 656
- Review All Key Topics 656
- Define Key Terms 657
- References 657

Chapter 14 Cisco Unified Compute Software and Configuration Management 658

- “Do I Know This Already?” Quiz 658
- Foundation Topics 660
- Cisco UCS Configuration Management 660
 - Creating and Running a Backup Operation 661
 - Backup Policies 666
 - Backup Policy Configuration 666
 - Import Backups 668
 - Enable the Import Operation 669
 - System Restore 670
 - Restoring the Configuration for a Fabric Interconnect 671
- UCS Firmware and Software Updates 672
 - Firmware Version Terminology 679
 - Firmware Upgrades Through Auto Install 680
 - Direct Upgrade After Auto Install Procedure 684
 - Install Infrastructure Firmware Procedure 688
 - Upgrading the Server Firmware with Auto Install 691
 - Standalone Cisco UCS C-Series Server Firmware Upgrade Using the Host Upgrade Utility (HUU) 693
 - Downloading and Preparing the ISO for an Upgrade 694
- Exam Preparation Tasks 700
- Review All Key Topics 700
- Define Key Terms 700
- References 700

Chapter 15 Cisco HyperFlex Overview 702

- “Do I Know This Already?” Quiz 702
- Foundation Topics 704
- Cisco HyperFlex Solution and Benefits 704
 - HyperFlex Benefits 707
 - Intelligent End-to-End Automation* 708
 - Unified Management for All Workloads* 709
 - Independent Resource Scaling* 710
 - Superior Virtual Machine Density with Lower and Consistent Latency* 711
- HyperFlex as an Edge, Hybrid, and All-Flash Nodes 712
 - HyperFlex as an Edge Device 712

HyperFlex Hyperconverged Multicloud Platform (Hybrid or All-Flash)	714
HyperFlex All NVMe	715
Cisco HyperFlex Data Platform	716
<i>HX Storage Cluster Physical Components</i>	717
<i>HX Data Platform High Availability</i>	718
<i>HX Data Platform Cluster Tolerated Failures</i>	719
<i>HX Data Platform Ready Clones</i>	719
<i>HX Data Platform Native Snapshots</i>	719
<i>HX Cluster Interfaces</i>	720
<i>HX Self-Encrypting Drives</i>	720
<i>Configuring a Local Encryption Key</i>	721
<i>Managing HX Disks in the Cluster</i>	721
<i>Managing HX Datastores</i>	724
<i>Expand Cisco HX System Clusters</i>	725
<i>Enabling HX Logical Availability Zones</i>	726
Exam Preparation Tasks	728
Review All Key Topics	728
Define Key Terms	728
References	728

Part IV Automation

Chapter 16 Automation and Scripting Tools 730

“Do I Know This Already?” Quiz	730
Foundation Topics	733
EEM Overview	733
Policies	733
Event Statements	734
Action Statements	734
Configuring EEM	735
Verifying the EEM Configuration	736
Scheduler	736
Configuring Scheduler	737
Verifying Scheduler Configuration	739
Bash Shell for Cisco NX-OS	740
Managing Feature RPMs	742
Managing Patch RPMs	742
Guest Shell for Cisco NX-OS	743

Accessing the Guest Shell	743
Resources Used for the Guest Shell	744
Capabilities in the Guest Shell	744
Managing the Guest Shell	746
XML	748
Example	749
XML Syntax	750
JSON	751
Rest API	752
Authentication	753
Response	754
NX-API	755
NX-API Request and Response Elements	757
NX-API Developer Sandbox	759
Exam Preparation Tasks	760
Review All Key Topics	760
Memory Tables	761
Define Key Terms	761
References	761
Chapter 17 Evaluate Automation and Orchestration Technologies	762
“Do I Know This Already?” Quiz	762
Foundation Topics	764
Ansible	764
Ansible Components	765
Important Ansible Concepts	766
Ansible CLI Tools	767
Cisco NX-OS and Ansible Example	767
Python	768
Python Package for Cisco	769
Using the CLI Command APIs	771
Python in Interactive Mode	772
Python in Noninteractive Mode	773
UCS Manager Python SDK	775
Convert to UCS Python	777
PowerOn Auto Provisioning (POAP)	777
Limitations of POAP	778
Network Requirements for POAP	778

POAP Configuration Script	778
POAP Process	779
<i>Power-Up Phase</i>	779
<i>USB Discovery Phase</i>	779
<i>DHCP Discovery Phase</i>	781
<i>Script Execution Phase</i>	782
<i>Post-Installation Reload Phase</i>	782
Configuring a Switch Using POAP	782
HashiCorp Terraform	783
Terraform Concept	784
Terraform Components	784
Terraform Commands	786
PowerShell	789
Exam Preparation Tasks	795
Review All Key Topics	795
Memory Tables	796
Define Key Terms	796
References	797

Part V Security

Chapter 18 Network Security 798

“Do I Know This Already?” Quiz	798
Foundation Topics	801
Authentication, Authorization, and Accounting	801
AAA Service Configuration Options	802
Authentication and Authorization User Login Process	803
AAA NX-OS Configurations	804
Role-Based Access Control	807
NX-OS User Roles and Rules	809
NX-OS RBAC Configurations	811
Nexus First-Hop Security	815
Nexus Dynamic ARP Inspection	816
NX-OS DAI Configurations	819
NX-OS DHCP Snooping	827
<i>DHCP Snooping Trusted and Untrusted Sources</i>	827
<i>DHCP Snooping Packet Validation</i>	828
<i>DHCP Snooping Option 82 Data Insertion</i>	829

<i>NX-OS DHCP Snooping Configuration</i>	829
Port Security	832
Nexus Port Secure MAC Address Maximum and Dynamic Address Aging	833
Port Security Violations and Actions	834
Nexus Port Types and Port Security	835
NX-OS Port Security Configuration	835
Nexus Control Plane Policing	837
Control Plane Packet	839
Classification for CoPP	840
<i>Rate-Controlling Mechanisms</i>	840
<i>Modular QoS Command-Line Interface</i>	842
NX-OS CoPP Configuration	844
Cisco ACI Contracts	851
Cisco ACI Contract Configuration Parameters	853
Create, Modify, or Remove Regular Contracts	854
Apply or Remove VRF Contracts	856
Inter-Tenant Contracts	857
Inter-Private Network Contracts Communication	858
Single Contract Bidirectional Reverse Filter	859
Single Contract Unidirectional with Multiple Filters	859
Multiple Contracts Unidirectional Single Filter	860
ACI Microsegmentation	860
Example: ACI Microsegmentation with VMs from a Single Application EPG	862
Example: ACI Microsegmentation with VMs in Different Application EPGs	863
ACI Microsegmentation Configurations	864
Keychain Authentication	868
NX-OS Keychain Configurations	868
Key Selection	871
Exam Preparation Tasks	872
Review All Key Topics	872
Define Key Terms	873
References	873

Chapter 19 Compute Security 874

- “Do I Know This Already?” Quiz 874
- Foundation Topics 875
- Securing UCS Management Using Authentication, Authorization, and Accounting 875
 - User RADIUS and TACACS+ Attributes 876
 - Two-Factor Authentication 879
 - UCS Web Session Refresh and Session Timeout Period 879
 - UCS LDAP Providers and Groups 879
 - LDAP Group Mapping* 885
 - RADIUS and TACACS+ Authentication Configurations 888
 - UCS Remote Users Role Policy 892
 - Multiple Authentication Services Configuration 894
- Exam Preparation Tasks 895
- Review All Key Topics 895
- Define Key Terms 895
- References 895

Chapter 20 Storage Security 896

- “Do I Know This Already?” Quiz 896
- Foundation Topics 898
- Authentication, Authorization, and Accounting 898
 - Authentication 899
 - Authorization 899
 - Accounting 900
 - Server Groups 900
 - AAA Service Configuration Options 900
 - AAA Server Monitoring 900
 - Remote AAA Services 901
 - RADIUS* 902
 - TACACS+* 904
 - LDAP* 907
 - Local AAA Services 911
 - AAA Authentication and Authorization Process 912
 - AAA Server Distribution 913
 - Merging RADIUS and TACACS+ Configurations 914
- User Accounts and RBAC 914
 - User Roles 915

	Rules	915
	User Role Policies	917
	RBAC Sample Configuration	918
	Port Security	919
	Port Security Configuration	921
	<i>Method 1: Manual Database Configuration</i>	921
	<i>Method 2: Auto-Learning Without CFS Distribution</i>	922
	<i>Method 3: Auto-Learning with CFS Distribution</i>	923
	Verification of Port Security	924
	Fabric Binding	926
	Fabric Binding Configuration	926
	Port Security Versus Fabric Binding	928
	Exam Preparation Tasks	929
	Review All Key Topics	929
	Memory Tables and Lists	930
	Define Key Terms	930
	References	930
Chapter 21	Final Preparation	932
	Getting Ready	932
	Tools for Final Preparation	933
	Pearson Test Prep Practice Test Software and Questions on the Website	933
	How to Access the Pearson Test Prep (PTP) App	933
	Customizing Your Exams	934
	Updating Your Exams	935
	<i>Premium Edition</i>	935
	Chapter-Ending Review Tools	935
	Learn the Question Types Using the Cisco Certification Exam Tutorial	935
	Suggested Plan for Final Review/Study	940
	Summary	940
Chapter 22	CCNP and CCIE Data Center Core DCCOR 350-601 Official Cert Guide Exam Updates	942
	The Purpose of This Chapter	942
	About Possible Exam Updates	943
	Impact on You and Your Study Plan	943
	News About the Next Exam Release	944
	Updated Technical Content	944

Appendix A Answers to the “Do I Know This Already?” Quizzes 946

Glossary 961

Index 984

Online Elements

Appendix B Memory Tables

Appendix C Memory Tables Answer Key

Appendix D Study Planner

Glossary

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.

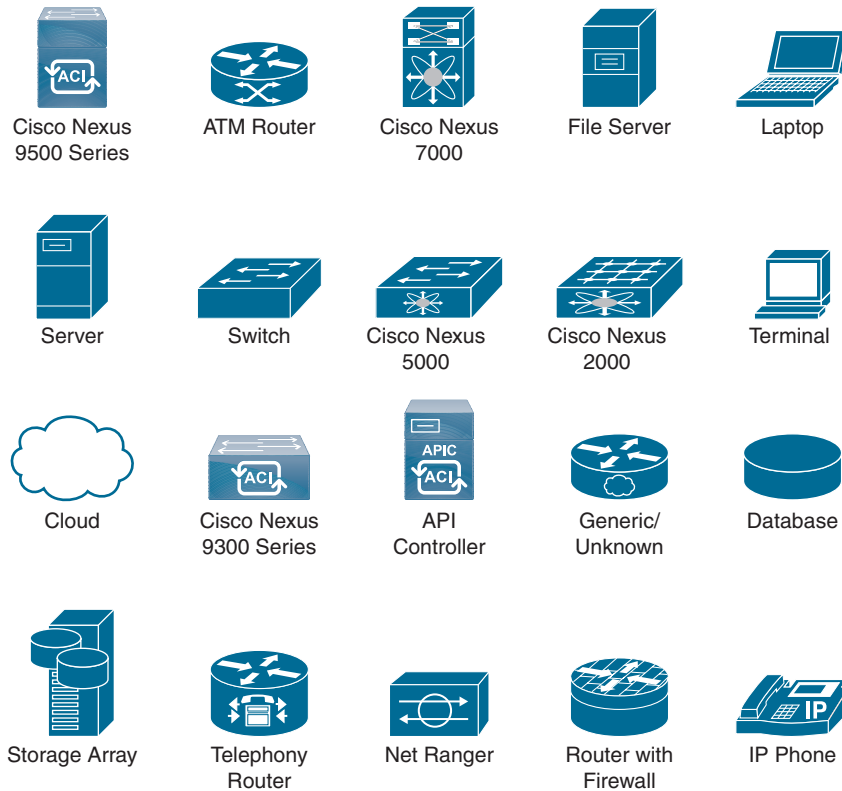
Glossary quizzes: The companion website contains interactive quizzes that enable you to test yourself on every glossary term in the book.

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 (NDDDB), 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

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.

Key Topic**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.

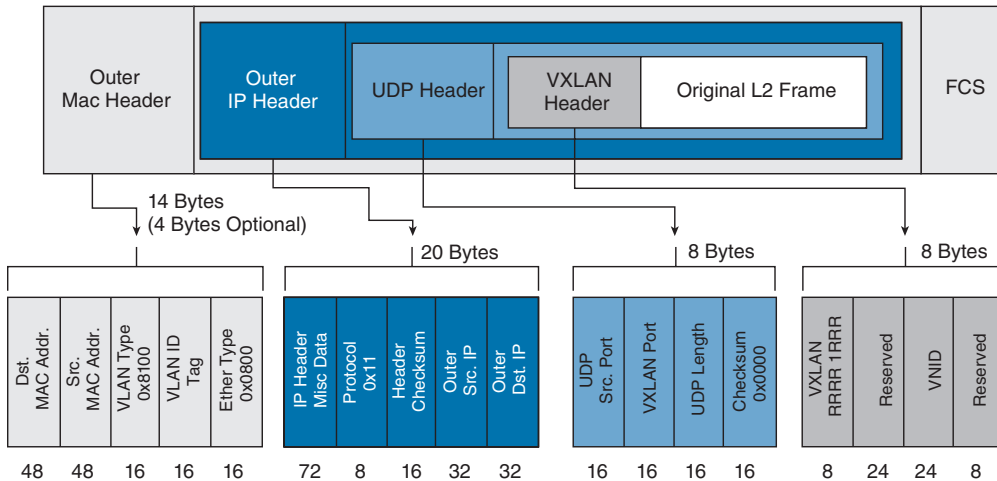
Key Topic

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 end-point 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.

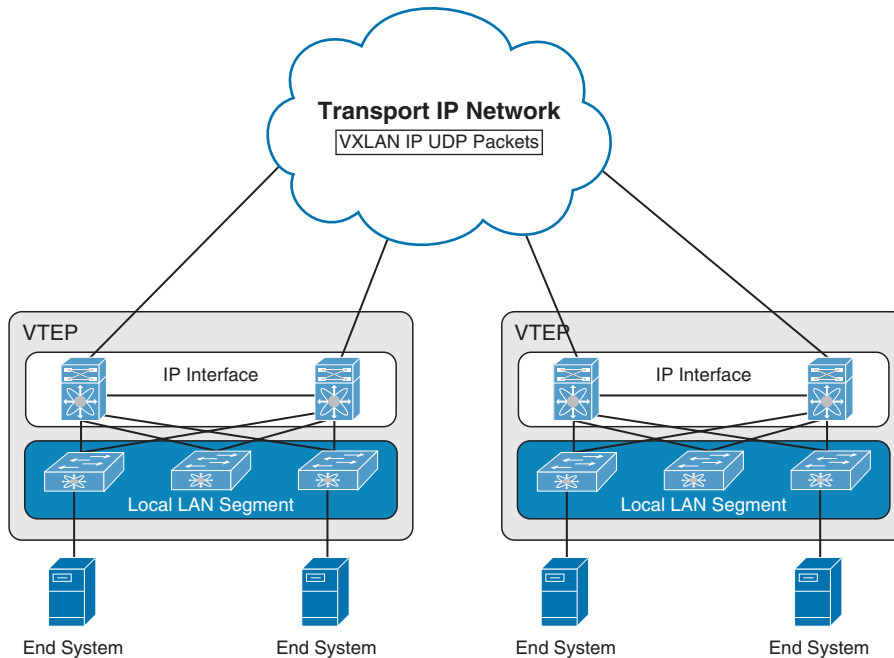
Key
Topic

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.

Key
Topic

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

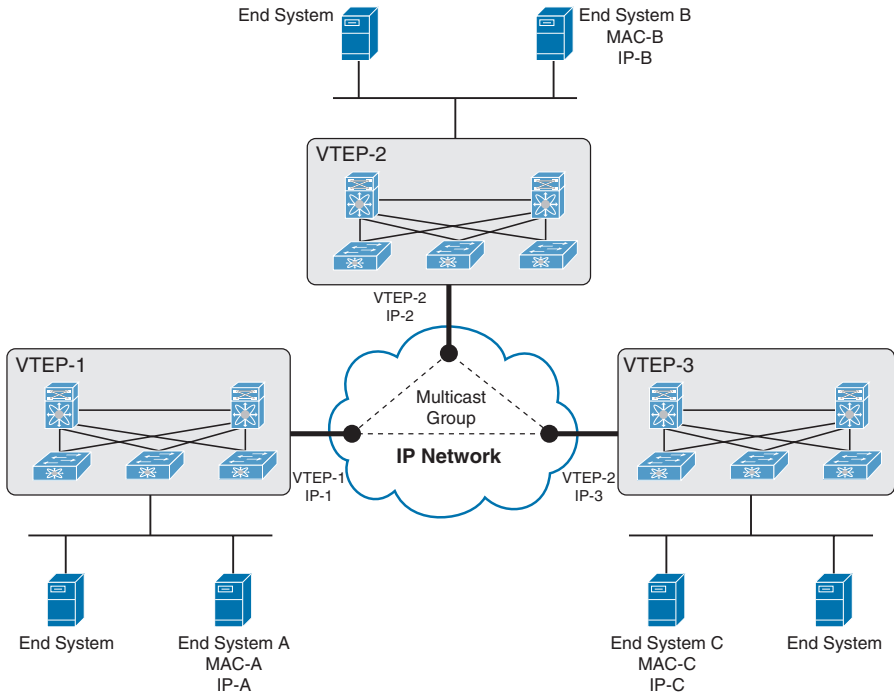


Figure 3-3 VXLAN Multicast Group in Transport Network

3

Key Topic

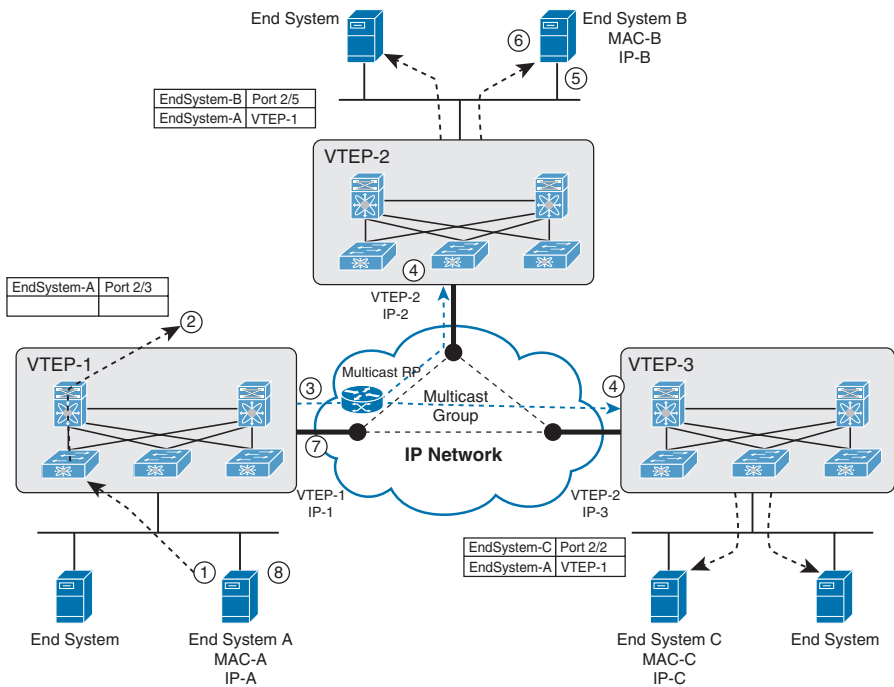


Figure 3-4 VXLAN Multicast Control Plane

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).

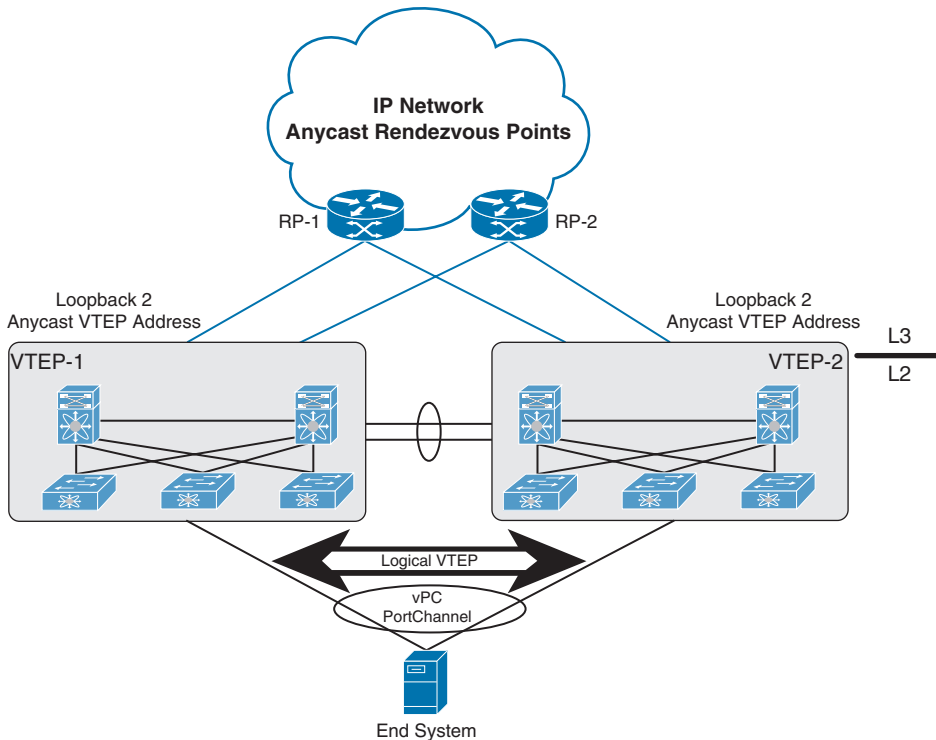


Figure 3-5 *VXLAN High Availability*

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.

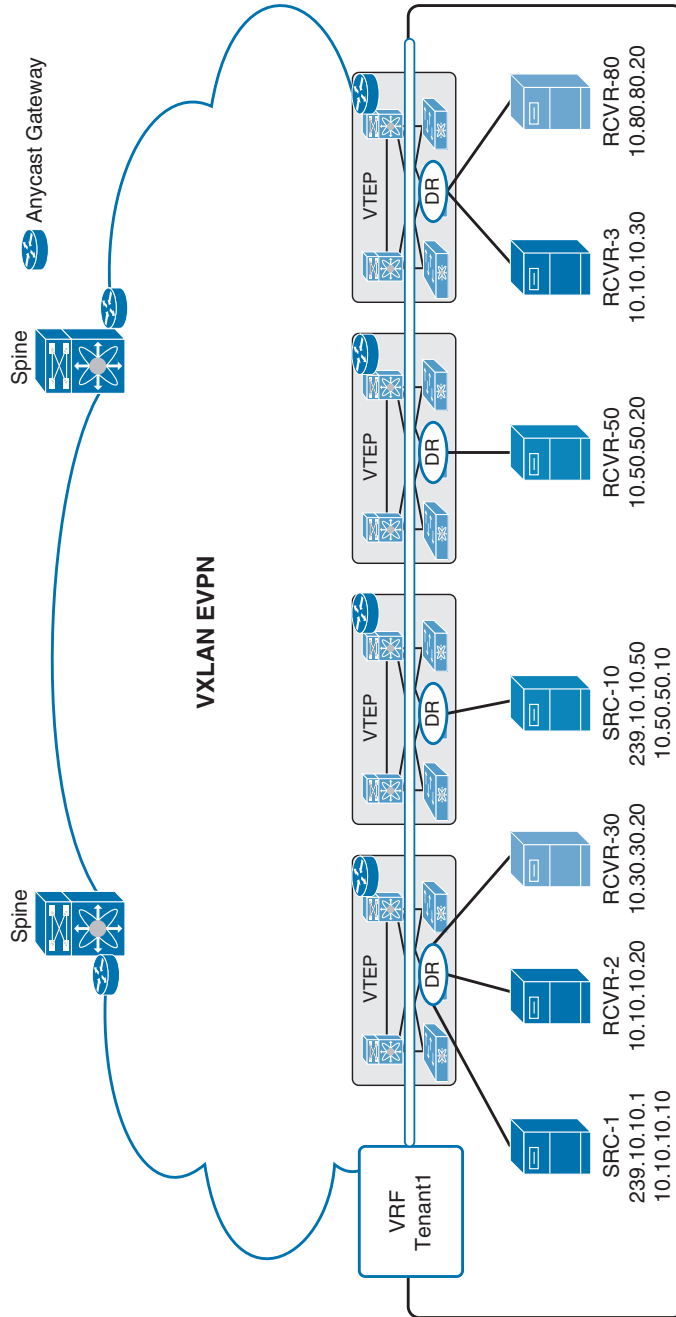


Figure 3-6 Tenant Routed Multicast (TRM)

Table 3-3 VXLAN Global-Level Commands

Command	Purpose
<code>feature nv overlay</code>	Enables the VXLAN feature.
<code>feature vn-segment-vlan-based</code>	Configures the global mode for all VXLAN bridge domains.
<code>vlan <i>vlan-id</i></code>	Specifies VLAN.
<code>vn-segment <i>vnid</i></code>	Specifies VXLAN virtual network identifier (VNID).
<code>bridge-domain <i>domain</i></code>	Enters the bridge domain configuration mode. It will create a bridge domain if it does not yet exist. Use from the global configuration mode.
<code>dot1q <i>vlan vni vni</i></code>	Creates mapping between VLAN and VNI. Use from the encapsulation profile configuration mode.
<code>encapsulation profile <i>name_of_profile</i> default</code>	Applies an encapsulation profile to a service profile. Use from the service instance configuration mode.
<code>encapsulation profile vni <i>name_of_profile</i></code>	Creates an encapsulation profile. Use from the global configuration mode.
<code>service instance <i>instance vni</i></code>	Creates a service instance. Use from the interface configuration mode.
<code>interface nve <i>x</i></code>	Creates a VXLAN overlay interface that terminates VXLAN tunnels.
<code>mac address-table static <i>mac-address vni vni-id</i></code> <code>interface nve <i>x</i> peer-ip <i>ip-address</i></code>	Specifies the MAC address pointing to the remote VTEP. NOTE: Only 1 NVE interface is allowed on the switch.
<code>ip igmp snooping vxlan</code>	Enables IGMP snooping for VXLAN VLANs. You have to explicitly configure this command to enable snooping for VXLAN VLANs.
<code>ip igmp snooping disable-nve-static-router-port</code>	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
<code>switchport vlan mapping enable</code>	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.
<code>switchport vlan mapping <i>vlan-id translated-vlan-id</i></code>	Translates a VLAN to another VLAN. The range for both the <i>vlan-id</i> and <i>translated-vlan-id</i> arguments is from 1 to 4094. <ul style="list-style-type: none">■ 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
	<ul style="list-style-type: none"> 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. <p>NOTE: Use the no form of this command to clear the mappings between a pair of VLANs.</p>
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 <i>src-if</i>	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 <i>vni</i>	Associates VXLAN virtual network identifiers (VNIs) with the NVE interface.
mcast-group <i>start-address</i> [<i>end-address</i>]	Assigns a multicast group to the VNIs. NOTE: Used only for BUM traffic.
ingress-replication protocol <i>bgp</i>	Enables BGP EVPN with ingress replication for the VNI.
ingress-replication protocol <i>static</i>	Enables static ingress replication for the VNI.
peer-ip <i>n.n.n.n</i>	Enables peer IP for static ingress-replication protocol.

Table 3-6 VXLAN Global-Level Verification Commands

Command	Purpose
show tech-support vxlan [<i>platform</i>]	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 <i>peer_IP_address</i> <i>interface interface_ID counters</i>	Displays per-NVE peer statistics.
clear nve peer-ip <i>peer-ip-address</i>	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 <i>vni_number</i> <i>counters</i>	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.

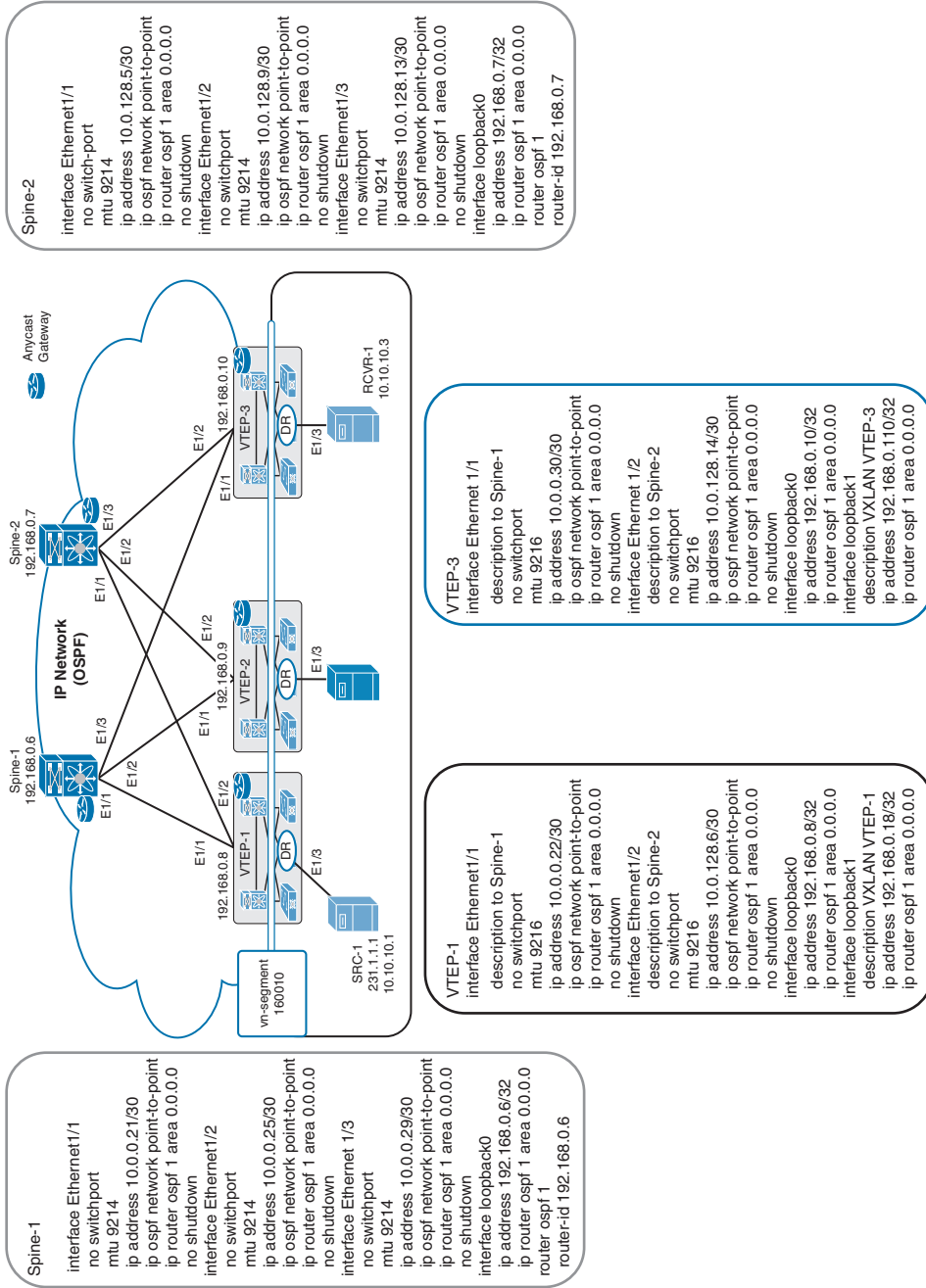


Figure 3-7 VXLAN Control Plane Topology

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 Priority	Bidir- Capable	BFD 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 Priority	Bidir- Capable	BFD 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 Priority	Bidir- Capable	BFD 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 Priority	Bidir- Capable	BFD 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 (VTEP-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 mrrib pim
  Incoming interface: Ethernet1/2, RPF nbr: 10.0.128.13
  Outgoing interface list: (count: 1)
    nve1, uptime: 00:02:34, mrrib
(*, 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.

**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

AAA model, 801

- accounting, 801, 900
- authentication, 801, 803–804, 899
- authorization, 801, 803–804, 899
- computer security, 875–876
- configuring AAA service options, 802–803
- default parameter settings, 804
- global commands, 804–806
- local AAA services, 911–912
- locking user accounts, 806
- NX-OS configurations, 804–807
- passphrase commands, 806
- RADIUS, 801–802
- remote AAA services, 802, 901
- servers
 - distribution, 913–914*
 - groups, 900*
 - monitoring, 900–901*
- storage security, 898
 - accounting, 900*
 - authentication, 899, 912–913*
 - authorization, 899, 912–913*
 - local AAA services, 911–912*
 - remote AAA services, 901*
 - server distribution, 913–914*
 - server groups, 900*
 - server monitoring, 900–901*
 - service configuration, 900*

TACACS+801–802

verification commands, 807

ABR, OSPF verification, 18–22

access

Cisco ACI

in-band management access, 214

out-of-band management access, 214–215

fabric access policies, Cisco ACI, 190–195

Guest Shell, 743–744

PTP, 933–934

RBAC, 807–809

Cisco NX-OS configurations, 811–815

user accounts, 914–919

accounting

AAA model, 801

storage security, 900

action statements, 733, 734–735

active zone sets, 407–409

addressing

FC, 371–372

FCoE, 447–448

adjacency, OSPF, 7

Admin Console page, ND GUI, 343–344

Administrative pages, ND GUI, 348

AEP, Cisco ACI, 207–208

AG (Application Gateways), 631

All-Flash configuration, Cisco HyperFlex, 714–715

All-NVMe, Cisco HyperFlex, 715–716

Ansible

authentication, 766

Cisco NX-OS example, 767–768

CLI

prompt, 766

tools, 767

components, 765–766

configuration files, 766

important concepts, 766

inventory files, 765

Jinja templates, 766

modules, 765

playbooks, 765–766

Cisco NX-OS example, 767–768

workflows using playbooks,
764–765

plays, 766

roles, 766

variable files, 766

variables, 766

workflows using playbooks, 764–765

Anywhere, Cisco HyperFlex, 713

API (Application Programming Interface)

CLI command API, Python, 771–772

NX-API

*Cisco NX-API Developer
Sandbox*, 759–760

error codes, 758–759

Requests/Responses elements,
757–759

Requests/Responses in JSON, 757

Requests/Responses in XML,
756–757

REST API, 752–753

authentication, 753–754

Responses, 754–755

APIC (Application Policy Infrastructure
Controllers), 176–179, 184–187

application profiles, Cisco ACI,
206–207

areas, OSPF, 10–12

ARP synchronization, vPC, 131

AS 65100, BGP configurations, 33

ASM (Any-Source Multicast), 51

attacks, man-in-the-middle, 817

authentication

AAA model, 801, 803–804, 875–876,
912–913

Ansible, 766

Cisco UCS Manager, multiple
authentication services
configuration, 892–894

keychain authentication, 868

Cisco NX-OS configurations,
868–870

commands, 869–870

key selection, 871–872

OSPF, 13

RADIUS, 888–892

REST API, 753–754

storage security, 899

TACACS+888–892

two-factor authentication, Cisco UCS
Manager, 879

VRRP, 77

authorization

AAA model, 801, 803–804, 876,
896–912

dev-ops role authority, displaying,
740–741

network-admin roles, displaying,
740–741

storage security, 899

Auto Install, firmware upgrades,
680–687

automation**Ansible**

- authentication*, 766
- Cisco NX-OS example*, 767–768
- CLI prompt*, 766
- CLI tools*, 767
- components*, 765–766
- configuration files*, 766
- important concepts*, 766
- inventory files*, 765
- Jinja templates*, 766
- modules*, 765
- playbooks*, 765–766, 767–768
- plays*, 766
- roles*, 766
- variable files*, 766
- variables*, 766
- workflows using playbooks*, 764–765

benefits, 730

Cisco HyperFlex, 708–709

EEM

- action statements*, 733, 734–735
- configuring*, 735–736
- event statements*, 733, 734
- monitoring module powerdowns*, 736
- overview*, 733
- policies*, 733–734
- verifying configurations*, 736

POAP, 777–778

- configuration scripts*, 778–779
- DHCP discovery phase*, 781–782
- limitations*, 778
- network requirements*, 778
- post-installation reload phase*, 782
- power-up phase*, 779
- processes (overview)*, 779–780

- script execution phase*, 782
- switch configurations*, 782–783
- USB discovery phase*, 779–780
- verification commands*, 783

PowerShell, 789

- installing*, 789–795
- listing UCS PowerShell cmdlets*, 793–795
- UCS PowerShell Library installations*, 790–791
- versions of*, 789–790, 791–793

Python, 768–769

- Cisco NX-OS, Python packages*, 769–771
- CLI command API*, 771–772
- interactive mode*, 772–773
- noninteractive mode*, 773–775
- UCS Manager Python SDK*, 775–777

Scheduler

- backups*, 739
- configuring*, 737–740
- displaying jobs/schedules*, 739–740
- job definitions*, 736
- overview*, 736–737
- prerequisites*, 737
- timetable definitions*, 736
- verifying configurations*, 739–740

Terraform, 783

- commands*, 786–789
- components*, 784–786
- concept*, 784
- workflows*, 784

Autozone, 410

availability, LAZ and Cisco HyperFlex data platforms, 726–727

B

backups

- Cisco UCS configuration management, 661–670
- configuring, 663–665
- creating, 661–663
- import backups, 668–670
- NX-OS, 272
- policies, 666–668
- Scheduler configurations, 739
- status, 665–666

bandwidth, port channels, 118

Bash Shell, 740

- displaying
 - dev-ops role authority*, 740–741
 - network-admin role authority*, 740–741
- enabling, 741–742
- feature RPM, 742
- patch RPM, 742–743
- running, 741–742

BB_credits, 372

BDR, OSPF, 12–13

BFD (Bidirectional Forwarding Detection), 37

- configuring, 38–42
- default parameter settings, 38–39
- failure detection, 38
- global commands, 39–40
- interface commands, 40
- neighbor relationships, 37–38
- network topologies, 40–41
- routing commands, 40
- verification commands, 40
- verifying configurations, 40–42

BGP (Border Gateway Protocol), 24–25

- AS 65100 configurations, 33

clear commands, 32–33

configuring, 30–37

default parameter settings, 30

feature-based licenses, 30

global commands, 31

interface configurations, 34

multiprotocol BGP, 29–30

network topologies, 33

path selection, 26–29

peering, 25–26

routing commands, 31–32

verification commands, 32–33

verifying configurations, 34–37

Bidir (Bidirectional shared trees), 51–52

blade chassis FEX, FI connections, 545–546

blade servers, Cisco UCS, 536–537

blocking duplicate frames, vPC, 129–131

boot sequences, NX-OS, 255–256

BPDU Filtering, 95, 96

BPDU Guard, 95, 96

Bridge Assurance, 95–96

bridge domains, Cisco ACI, 200–202

budgeting time, exam preparation, 932

C

Call Home

- Cisco UCS Manager system monitoring, 636–637
- infrastructure monitoring, 521–522

centralized management, Cisco HyperFlex, 709–710

CFS (Cisco Fabric Services), 380–381

CFSofC, 382–384

CFSofIP, 382–384

fabric lock, 382

features, 381–382

merges, 384

regions, 384–385

channel code matrix, port channels, 119

chapter-ending review tools, 935

checkpoints, NX-OS, 272–274

Cisco ACI (Application Centric Infrastructure)

access

in-band management access,
214

out-of-band management access,
214–215

AEP, 207–208

APIC, 176–179, 184–187

application profiles, 206–207

architectural building blocks, 176

benefits, 174–175

bridge domains, 200–202

components, 175–176

configuring

APIC, 184–187

initial setup, 182–187

LAB configurations, 221–223

contracts, 208–209

creating, 230–233

filters, 213, 230–233

taboo contracts, 209–210

vzAny rule, 210–212

design best practices, 221

endpoint groups, 201–203

fabric

access policies, 190–195

building, 224–227

building blocks, 195–196

discovery, 182, 187–189

loop detection, 220

overview, 179

traffic load balancing, 219–220

traffic storms, 219

upgrading, 189–190

filters, creating, 230–233

initial setup, 182–187

LAB configurations, 221–223

leaf switches, 179–182

management tenants, 213

microsegmentations, 207

multitier topologies, 179–180

overview, 174–176

policy identification/enforcement, 218

policy models, 197–198

SCVMM integration, 204–205

spine switches, 179–182

tenants, 198–200

creating, 227–230

intersubnet tenant traffic, 217–218

management tenants, 213

three-tier applications, 233–235

vCenter integration, 235–238

Virtual Edge, 206

VMM domains, 203–204

VMware overlays, 206

VMware vCenter integration, 205

VRF, 200

VXLAN, 215–216

vzAny rule, 210–212

Cisco ACI Contracts, 852–853

applying, 855–856

components, 851–852

configuring, 853–854

creating, 854–855

exporting between networks, 858–859

inter-private network contracts
communication, 858–859

Inter-Tenant Contracts, 857–858

microsegmentation, 860–867

modifying, 855

- multiple contracts unidirectional single filters, 860
- removing, 855
- single contract bidirectional reverse filters, 859
- single contract unidirectional with multiple filters, 859
- verifying, 855
- VRF Contracts, 856–857
- Cisco AVPair attribute, 878**
- Cisco Certification Exam Tutorial, types of questions, 935–939**
- Cisco, fiscal year and months example, 943**
- Cisco HyperFlex, 702, 704**
 - All-Flash configuration, 714–715
 - All-NVMe, 715–716
 - Anywhere, 713
 - automation, 708–709
 - benefits, 707–712
 - centralized management, 709–710
 - configuring, 705–706
 - data platforms, 716
 - cluster interfaces, 720*
 - cluster tolerated failures, 719*
 - datastores, 724–725*
 - disk management, 721–724*
 - HA, 718–719*
 - LAB clusters, 716–717*
 - LAZ, 726–727*
 - local encryption keys, 721*
 - Native Snapshots, 719–720*
 - Ready Clones, 719*
 - SED, 720–721*
 - server disk types, 722–723*
 - storage clusters, 717*
 - system clusters, 725–727*
- Dynamic Data Distribution, 711–712
- edges, 712–714
- flexibility, 715
- hardware, 715
- HCI, 704
- hybrid models, 714–715
- hyperconvergence, 704
- independent resource scaling, 710–711
- infrastructures, 705, 706–707
- interconnections, 705
- invisible cloud witness services, 713–714
- IO Visor, 707
- latency, 711–712
- multinode edges, 713
- resource optimization, 710–711
- SATA RAS, 715–716
- unified management, 709–710
- VAAI, 707
- VM density, 711–712
- Cisco Intersight, 648**
 - benefits, 648–649
 - dashboards, 650
 - features, 648–649
 - infrastructure, 647
 - invisible cloud witness services, 713–714
 - licensing, 652–656
 - management as a service, 648–649
 - supported software, 650–652
 - telemetry data collection, 650
- Cisco MDS 9100 series multilayer fabric switches, 362–365**
- Cisco MDS 9200 series multiservice switches, 361–362**
- Cisco MDS 9300 series multilayer fabric switches, 360–361**
- Cisco MDS 9700 series multilayer directors, 356–360**

Cisco MDS NX-OS Setup Utility,
490–498

Cisco NX-API Developer Sandbox,
759–760

Cisco NX-OS

Ansible, 767–768

Bash Shell, 740

*displaying dev-ops role
authority, 740–741*

*displaying network-admin role
authority, 740–741*

enabling, 741–742

feature RPM, 742

patch RPM, 742–743

running, 741–742

CoPP configurations, 844–851

DAI configurations, 819–827

DHCP snooping, 827–831

Guest Shell, 743

access, 743–744

capabilities, 744–746

*displaying Ethernet 1/47
interface counters, 745*

dohost command, 745

guestshell destroy command, 747

guestshell disable command, 747

guestshell enable command, 747

installing Python packages, 746

managing, 746–748

resource limits, 744

*running Python in Guest Shell,
745–746*

*show guestshell detail command,
747–748*

keychain authentication, 868–870

port security, 832–837

Python packages, 769–771

RBAC configurations, 811–815

rules, 809–810

user roles, 809–810

Cisco UCS (Unified Computing
System), 530

5108 Blade Server Chassis, 536

architecture, 532–534

blade servers, 536–537

chassis discovery, 577

Cisco UCS Mini, 539–540

Cisco X-Series system, 555–556

components, 534–535

configuration management, 660–661

backups, 661–670

system restore, 670–672

configuring, 557–564

FI, GUI configurations, 561–562

initial setup, 578–583

connectivity, 534–535

fabric failover for Ethernet, 569–570

fabric infrastructure, 539

*Cisco UCS 6300 Series fabric
interconnect, 543–544*

*Cisco UCS 6454 fabric
interconnect, 541–543*

*Cisco UCS 6536 fabric
interconnect, 540–541*

FEX, 544–550, 577

FI, 544–550

cluster verifications, 563–564

configuring, 565–567

connectivity, 565–567

*Ethernet switching mode,
570–577*

*fabric failover for Ethernet,
569–570*

GUI configurations, 561–562

IPv4 initialization, 559–560, 563

IPv6 initialization, 560–561, 563

- port modes*, 567–569
- vNIC*, 569–570
- firmware
 - infrastructure installations*, 688–691
 - server upgrades*, 691–699
 - updates*, 672–679
 - upgrades through Auto Install*, 680–687
 - version terminology*, 679
- flexibility, 533–534
- high availability, 533
- identity pools, 591–596
- initial setup, 557–564, 578–583
- IP pools, 593–595
- MAC pools, 593
- managing, 557–564
- network management, VLAN, 584–591
- QoS, 608–610
- rack servers, 537–538, 577
- SAN, connectivity, 611–616, 624–625
- scalability, 533
- servers
 - pools*, 596
 - profiles*, 599–602
- service profiles, 596–599, 602–607
- software updates, 672–679
- storage, 611
- storage servers, 537–539
- UUID pools, 591–593
- virtualization, 550–555
- vNIC*, 569–570
- VSAN, 616–621
- WWN pools, 621–624
- Cisco UCS Manager**
 - AAA model, 875–876
 - Cisco AVPair attribute example, 878
 - LDAP, 877
 - groups*, 879–888
 - nested LDAP*, 879
 - providers*, 879–888
 - user accounts*, 880
 - multiple authentication services
 - configuration, 894
 - RADIUS, 876, 877, 888–892
 - remote user role policies, 892–894
 - Session Timeout Period, 879
 - system monitoring, 630
 - AG*, 631
 - Call Home*, 636–637
 - database health*, 638
 - DME*, 631
 - events*, 632–634
 - hardware*, 638
 - logs*, 632–634
 - NetFlow*, 638–640
 - northbound interfaces*, 631–632
 - policies*, 634–640
 - Smart Call Home*, 636–637
 - SNMP*, 636
 - traffic monitoring*, 640–647
 - TACACS+, 877–878, 888–894
 - two-factor authentication, 879
 - Web Session Refresh Period, 879
- Cisco UCS S-Series storage servers**, 483–484
- clear commands**, BGP, 32–33
- clear-text passwords**, 809
- CLI (Command-Line Interface)**
 - Ansible
 - prompt*, 766
 - tools*, 767
 - modular QoS CLI, 842–844
 - Python command API, 771–772

clocks

- PTP, 281–282, 283–284
- watching, exam preparation, 932

cloud computing

- benefits, 243
- characteristics, 243–244
- community clouds, 250
- defined, 242–244
- hybrid clouds, 249–250
- IaaS, 246–248
- PaaS, 246
- private clouds, 248
- public clouds, 248–249
- SaaS, 245

clusters

- Cisco HyperFlex data platforms
 - cluster interfaces*, 720
 - LAB clusters*, 716–717
 - storage clusters*, 717
 - system clusters*, 725–727
 - tolerated failures*, 719
- Cisco UCS FI verification, 563–564
- ND cluster nodes, 339–341
- storage clusters
 - Cisco HyperFlex data platforms*, 717
 - compute nodes*, 717
 - converged nodes*, 717
 - datastores*, 717
 - drives*, 717
- system clusters, Cisco HyperFlex data platforms, 725–727
- tolerated failures, Cisco HyperFlex data platforms, 719

CNA (Converged Network Adapters), 436–437**collapsed-core topologies, FC, 365****commands****AAA model**

- global commands*, 804–806
- locking user accounts*, 806
- passphrase commands*, 806
- verification commands*, 807

BFD

- global commands*, 39–40
- interface commands*, 40
- routing commands*, 40
- verification commands*, 40

BGP

- clear commands*, 32–33
- global commands*, 31
- routing commands*, 31–32
- verification commands*, 32–33

FCoE, verification commands, 466**FHS, port security, 836–837****HSRP**

- global commands*, 80
- interface commands*, 80
- verification commands*, 82

keychain authentication, 869–870**multicast routing**

- global commands*, 58–59
- interface commands*, 59–61

NTP

- global commands*, 276–278
- verification commands*, 278

OSPF

- global commands*, 14
- interface commands*, 15
- process clear commands*, 15–16
- routing commands*, 14–15

port channels

- global commands*, 134–135
- interface commands*, 135
- verification commands*, 137

- PTP
 - global commands*, 282
 - interface commands*, 283
- SAN port channels, verification commands, 400–401
- SNMP
 - global commands*, 288–289
 - specific notation commands*, 291
 - verification commands*, 291–292
- STP
 - global commands*, 105
 - interface commands*, 106–107
 - verification commands*, 108
- Terraform, 786–789
- verification commands, PTP, 283
- vPC
 - domain commands*, 136
 - global commands*, 134–135
 - interface commands*, 135
 - verification commands*, 137
- VRRP
 - global commands*, 79–86
 - interface commands*, 80
 - verification commands*, 82
- VSAN, 392–393
- VXLAN
 - global commands*, 159–161
 - interface commands*, 161–162
 - NVE config commands*, 162
 - verification commands*, 162
- community clouds, 250
- compute nodes, storage clusters, 717
- computer security
 - AAA model, 875–876
 - Cisco AVPair attribute example, 878
 - LDAP, 877
 - groups*, 879–888
 - nested LDAP*, 879
 - providers*, 879–888
 - user accounts*, 880
 - multiple authentication services configuration, 892–894
 - RADIUS, 876, 877, 888–892
 - remote user role policies, 892–894
 - TACACS+877–878, 888–894
 - two-factor authentication, 879
- configuration consistency, vPC, 128–129
- configuration files, Ansible, 766
- configuration scripts, POAP, 778–779
- configuring
 - AAA model
 - NX-OS configurations*, 804–807
 - service options*, 802–803
 - AAA services, storage security, 900
 - ACI Contracts, 853–854
 - All-Flash configuration, Cisco HyperFlex, 714–715
 - backups, 663–665
 - BFD, 38–42
 - BGP, 30–37
 - Cisco ACI
 - APIC*, 184–187
 - initial setup*, 182–187
 - LAB configurations*, 221–223
 - Cisco HyperFlex, 705–706, 714–715
 - Cisco NX-OS
 - DAI configurations*, 819–827
 - keychain authentication*, 868–870
 - port security*, 832–837
 - RBAC configurations*, 811–815
 - Cisco UCS, 557–564, 660–661
 - backups*, 661–670
 - FI configurations*, 561–562, 565–567

- initial setup*, 578–583
 - system restore*, 670–672
 - device alias, 422–423
 - EEM, 735–736
 - FCoE, 469–474
 - Nexus 5000 switches*, 458–459
 - Nexus 7000 switches*, 456–458
 - Nexus 9000 switches*, 459–461
 - HSRP, 79–86
 - local encryption keys, 721
 - multicast routing, 56–69
 - named VLAN, 589–590
 - NTP, 279–280
 - NX-OS, 271
 - basic management*, 256–259
 - saves/backups*, 272
 - OSPF, 13–24
 - PIM, 164–167
 - port channels, 132–146
 - port security, 921–924
 - PTP, 283
 - RBAC, user accounts, 918–919
 - SAN port channels, 400–403
 - Scheduler, 737–740
 - SNMP, 292
 - STP, 102–117
 - switches, POAP configurations, 782–783
 - vPC, 132–146
 - VRRP, 79–86
 - VSAN, 391–394
 - VXLAN, 159–169
 - zoning, 414–417
 - consistency checks**, vPC, 129
 - contracts**, Cisco ACI, 208–209
 - creating, 230–233
 - filters, 213
 - taboo contracts, 209–210
 - vzAny rule, 210–212
 - control plane topologies**, VXLAN, 159–161
 - converged nodes**, storage clusters, 717
 - converting to UCS Manager Python SDK**, 777
 - CoPP (Control Plane Policing)**, 837–839
 - Cisco NX-OS configurations, 844–851
 - classification, 840–844
 - control plane packets, 839–840
 - creating, 850–851
 - modifying, 851
 - modular QoS CLI, 842–844
 - Nexus 5000, 844
 - Nexus 7000 comparisons, 843–844
 - Nexus 9000 comparisons, 842–843
 - rate control, 840–841
 - core-edge topologies**, FC, 366
 - CRUD operations**, UCS Manager Python SDK, 776
 - customizing exams**, 934–935
-
- ## D
-
- DAI (Dynamic ARP Inspection)**, 816, 817–819
 - Cisco NX-OS configurations, 819–827
 - DHCP snooping, 827–831
 - man-in-the-middle attacks, 817
 - data platforms**, Cisco HyperFlex, 716
 - clusters
 - interfaces*, 720
 - LAB clusters*, 716–717
 - storage clusters*, 717
 - system clusters*, 725–727
 - tolerated failures*, 719
 - datastores, 724–725

- disk management, 721–724
 - HA, 718–719
 - LAZ, 726–727
 - local encryption keys, 721
 - Native Snapshots, 719–720
 - Ready Clones, 719
 - SED, 720–721
 - server disk types, 722–723
 - database health, Cisco UCS Manager system monitoring, 638
 - datastores**
 - Cisco HyperFlex data platforms, 724–725
 - storage clusters, 717
 - DCBX (Data Center Bridging Exchange), 440–442**
 - deleting**
 - LDAP providers, 885
 - named VLAN, 590–591
 - device alias, 418**
 - configuring, 422–423
 - distributions, 420–421
 - features, 419
 - modes, 419–420
 - verifying configurations, 422–423
 - zone alias comparisons, 421–422
 - device registration, switched fabric initialization and FC, 378–380**
 - dev-ops roles, displaying authority, 740–741**
 - DHCP (Dynamic Host Configuration Protocol)**
 - discovery phase, POAP, 781–782
 - snooping, 827–831
 - direct-attached topologies, FCoE, 452–453**
 - disk management, Cisco HyperFlex data platforms, 721–724**
 - displaying**
 - dev-ops role authority, 740–741
 - Ethernet 1/47 interface counters with Guest Shell, 745
 - jobs/schedules in Scheduler, 739–740
 - disruptive downgrades, MDS switches, 513–515**
 - disruptive upgrades, MDS switches, 505–507**
 - DITKA? questions, 940**
 - DME (Data Management Engine), 631**
 - dohost command, 745**
 - domains**
 - ID, principal switch selection and FC, 375–377
 - vPC, 124, 136
 - downgrading MDS switches**
 - disruptive downgrades, 513–515
 - nondisruptive downgrades, 508–512
 - software, 498–500
 - downlink connectivity, Cisco UCS FI, 567**
 - DPVM (Dynamic Port VSAN Membership), 388–389**
 - DR, OSPF, 12–13**
 - drag-and-drop questions, 937**
 - drives**
 - SED, Cisco HyperFlex data platforms, 720–721
 - storage clusters, 717
 - dual-control plane, vPC, 126**
 - duplicate frame prevention, vPC, 129–131**
 - Dynamic Data Distribution, Cisco HyperFlex, 711–712**
-
- E**
- ear plugs, exam preparation, 932**
 - edge ports, STP, 94**

- edge-core-edge topologies, FC, 367–368
- edges, Cisco HyperFlex, 712–714
- EEM (Embedded Event Manager), 522
 - action statements, 733, 734–735
 - configuring, 735–736
 - event statements, 733, 734
 - monitoring module powerdowns, 736
 - overview, 733
 - policies, 733–734
 - verifying configurations, 736
- enabling Bash Shell, 741–742
- encapsulation, VXLAN, 151–152
- encryption
 - local encryption keys, configuring, 721
 - SED, Cisco HyperFlex data platforms, 720–721
- endpoint groups, Cisco ACI, 201–203
- end-to-end automation, Cisco HyperFlex, 708–709
- enhanced zoning, 412–413
- ENodes, FCoE, 445–447
- EPLD (Electrical Programmable Logical Devices)
 - MDS 9000 series switches, upgrades, 515–521
 - upgrading, 269–271
- error codes, NX-API, 758–759
- Ethernet
 - 1/47 interface counters, displaying with Guest Shell, 745
 - Ethernet switching mode, Cisco UCS FI, 570–577
 - fabric failover for Ethernet, high availability vNIC, 569–570
 - FCoE, 434
 - addressing*, 447–448
 - benefits*, 451
 - CNA*, 436–437
 - configuring*, 469–474
 - DCBX*, 440–442
 - direct-attached topologies*, 452–453
 - ENodes*, 445–447
 - ETS*, 439–440
 - FCF*, 445–447
 - FEX topologies*, 453–454, 461–463
 - FIP*, 448–451
 - forwarding*, 447–448
 - FPMA*, 447
 - frame format*, 442–444
 - IEEE 802.1 standard*, 438
 - implementing*, 455
 - multi-hop topologies*, 454–455
 - Nexus 5000 switch configurations*, 458–459
 - Nexus 7000 switch configurations*, 456–458
 - Nexus 9000 switch configurations*, 459–461
 - NPV*, 463–465
 - overview*, 436–438
 - PFC*, 438–439
 - ports*, 445–447
 - remote-attached topologies*, 454
 - single-hop topologies*, 451–454
 - T11 standard*, 438
 - verification commands*, 466
 - verifying*, 466–474
 - VFC*, 444–445
 - traffic monitoring, 641–642
- ETS (Enhanced Transmission Selection), 439–440
- events
 - monitoring, Cisco UCS Manager, 632–634
 - statements, 733, 734

EVPN control plane, VXLAN,
156–157

exams

- Cisco fiscal year and months
example, 943
- customizing, 934–935
- news on releases, 944
- preparing for, 932
 - budgeting time*, 932
 - chapter-ending review*
tools, 935
 - Cisco Certification Exam*
Tutorial questions, 935–939
 - clock watching*, 932
 - customizing exams*, 934–935
 - DITKA? questions*, 940
 - drag-and-drop questions*, 937
 - ear plugs*, 932
 - fill-in-the-blank questions*, 937
 - final reviews*, 940
 - getting rest*, 932
 - multiple-choice, multiple-answer*
questions, 936
 - multiple-choice, single answer*
questions, 936
 - PTP*, 933–935
 - simlet questions*, 939
 - simulation questions*, 938
 - study plans*, 940
 - study trackers*, 932
 - taking notes*, 933
 - testlet questions*, 938–939
 - travel time*, 932
- study plans, 943–944
- updates, 942–943, 944
- exporting contracts between networks,
858–859
- extensions, STP, 94–95

F

fabric

- binding, 926–929
- CFS, 380–381
 - CFSofC*, 382–384
 - CFSofIP*, 382–384
 - fabric lock*, 382
 - features*, 381–382
 - merges*, 384
 - regions*, 384–385
- Cisco ACI
 - access policies*, 190–195
 - building*, 224–227
 - building blocks*, 195–196
 - fabric discovery*, 182, 187–189
 - loop detection*, 220
 - overview*, 179
 - traffic load balancing*, 219–220
 - traffic storms*, 219
 - upgrading*, 189–190
- Cisco MDS 9100 series multilayer
fabric switches, 362–365
- Cisco MDS 9300 series multilayer
fabric switches, 360–361
- Cisco UCS, 539
 - Cisco UCS 6300 Series fabric*
interconnect, 543–544
 - Cisco UCS 6454 fabric*
interconnect, 541–543
 - Cisco UCS 6536 fabric*
interconnect, 540–541
- fabric failover for Ethernet, high
availability vNIC, 569–570
- FLOGI, 378–380
- FPMA, 447
- MDS switches
 - Cisco MDS NX-OS Setup Utility*,
490–498

- disruptive downgrades*, 513–515
- disruptive upgrades*, 505–507
- nondisruptive downgrades*, 508–512
- nondisruptive upgrades*, 500–505
- upgrading/downgrading software*, 498–500
- NDFC, 325–326
 - features/benefits*, 326–331
 - GUI, 331–335
- switched fabric initialization, FC
 - device registration*, 378–380
 - domain ID*, 375–377
 - fabric reconfiguration*, 377
 - FCID, 377
 - FCNS databases, 378–380
 - FLOGI, 378–380
 - overview*, 373–374
 - PLOGI, 378
 - principal switch selection*, 374–377
 - PRLI, 378
- failure detection, BFD, 38
- fault-tolerant links, vPC, 124
- FC (Fibre Channel)
 - addressing, 371–372
 - basics, 365
 - BB_credits, 372
 - CFS, 380–381
 - CFSofC, 382–384
 - CFSofIP, 382–384
 - fabric lock*, 382
 - features*, 381–382
 - merges*, 384
 - regions*, 384–385
 - Cisco MDS 9100 series multilayer fabric switches, 362–365
 - Cisco MDS 9200 series multiservice switches, 361–362
 - Cisco MDS 9300 series multilayer fabric switches, 360–361
 - Cisco MDS 9700 series multilayer directors, 356–360
 - collapsed-core topologies, 365
 - core-edge topologies, 366
 - device alias, 418
 - configuring*, 422–423
 - distributions*, 420–421
 - features*, 419
 - modes*, 419–420
 - verifying configurations*, 422–423
 - zone alias comparisons*, 421–422
 - edge-core-edge topologies, 367–368
 - FCID, 371–372, 377
 - flow control, 372
 - NPIV, 424–431
 - NPV, 424–431
 - ports, 368–370
 - SAN port channels, 396
 - configuring*, 400–403
 - load balancing*, 398–399
 - modes*, 399–400
 - trunking*, 396–397
 - types of*, 396–398
 - verification commands*, 400–401
 - verifying configurations*, 400–403
 - switched fabric initialization
 - device registration*, 378–380
 - domain ID*, 375–377
 - fabric reconfiguration*, 377
 - FCID, 377
 - FCNS databases, 378–380
 - FLOGI, 378–380
 - overview*, 373–374
 - PLOGI, 378
 - principal switch selection*, 374–377
 - PRLI, 378

- topologies, 365–368
- traffic monitoring, 642–647
- VSAN, 386
 - advantages of*, 388
 - attributes*, 387–388
 - commands*, 392–393
 - configuring*, 391–394
 - DPVM, 388–389
 - features*, 386–387
 - ID, 387
 - names*, 388
 - states*, 387–388
 - switches*, 388
 - trunking*, 389–394
 - verifying configurations*, 391–394
 - zoning comparisons*, 406
- zone alias, device alias comparisons, 421–422
- zoning, 404
 - active zone sets*, 407–409
 - Autozone*, 410
 - configuring*, 414–417
 - enforcement*, 406–407
 - enhanced zoning*, 412–413
 - features*, 404–406
 - full zone sets*, 407–409
 - hard zoning*, 407
 - merges*, 410–411
 - smart zoning*, 411–412
 - verifying configurations*, 414–417
 - VSAN comparisons*, 406
- FCF (Fibre Channel Forwarders), 445–447
- FCID (Fibre Channel Identification), 371–372, 377
- FCNS databases, 378–380
- FCoE (Fibre Channel over Ethernet), 434
 - addressing, 447–448
 - benefits, 451
 - CNA, 436–437
 - configuring, 469–474
 - Nexus 5000 switches*, 458–459
 - Nexus 7000 switches*, 456–458
 - Nexus 9000 switches*, 459–461
 - DCBX, 440–442
 - direct-attached topologies, 452–453
 - ENodes, 445–447
 - ETS, 439–440
 - FCF, 445–447
 - FEX topologies, 453–454, 461–463
 - FIP, 448–451
 - forwarding, 447–448
 - FPMA, 447
 - frame format, 442–444
 - IEEE 802.1 standard, 438
 - implementing, 455
 - multi-hop topologies, 454–455
 - NPV, 463–465
 - overview, 436–438
 - PFC, 438–439
 - ports, 445–447
 - remote-attached topologies, 454
 - single-hop topologies, 451–454
 - T11 standard, 438
 - verification commands, 466
 - verifying, 466–474
 - VFC, 444–445
- feature RPM, managing with Bash Shell, 742
- feature-based licenses
 - BGP, 30
 - multicast routing, 57–58
 - OSPF, 14
 - VXLAN, 159

FEX (Fabric Extenders)

- blade chassis FEX, FI connections, 545–546
- Cisco UCS, 544–550, 577
- port channel mode, 547–548
- topologies, FCoE, 453–454, 461–463
- virtual links, 548

FHS (First-Hop Security)

- DAI, 816, 817–819
 - Cisco NX-OS configurations*, 819–827
 - DHCP snooping*, 827–831
 - man-in-the-middle attacks*, 817
- features, 815–816
- port security, 832–837

FI (Fabric Interconnects)

- blade chassis FEX connections, 545–546
- Cisco UCS, 544–550
 - cluster verifications*, 563–564
 - connectivity*, 565–567
 - Ethernet switching mode*, 570–577
 - fabric failover for Ethernet*, 569–570
 - FI configurations*, 565–567
 - GUI configurations*, 561–562
 - IPv4 initialization*, 559–560, 563
 - IPv6 initialization*, 560–561, 563
 - port modes*, 567–569
 - vNIC*, 569–570
- system restore, 671–672

files, NFS, 479–480

fill-in-the-blank questions, 937

filters, Cisco ACI contracts, 213, 230–233

final reviews, exam preparation, 940

FIP (FCoE Initialization Protocol), 448–451

firmware

- infrastructure installations, 688–691
- server upgrades, 691–699
- updates, Cisco UCS, 672–679
- upgrades
 - server upgrades*, 691–699
 - through Auto Install*, 680–687
- version terminology, 679

fiscal year and months example, Cisco, 943

flexibility

- Cisco HyperFlex, 715
- Cisco UCS, 533–534

FLOGI (Fabric Login), 378–380

Flood and Learn Multicast-based control plane, VXLAN, 154–156

flow control, FC, 372

FPMA (Fabric-Provided MAC Addresses), 447

full zone sets, 407–409

G

gateways

- AG, 631
- VXLAN, 157

global commands

- AAA model, 804–806
- BFD, 39–40
- BGP, 31
- FHS, port security, 836–837
- HSRP, 80
- multicast routing, 58–59
- NTP, 276–278
- OSPF, 14
- port channels, 134–135
- PTP, 282
- SNMP, 288–289

STP, 105
 vPC, 134–135
 VRRP, 79–86
 VXLAN, 159–161

Guest Shell, 743
 access, 743–744
 capabilities, 744–746
 displaying Ethernet 1/47 interface counters, 745
 dohost command, 745
 guestshell destroy command, 747
 guestshell disable command, 747
 guestshell enable command, 747
 managing, 746–748

Python
 installing packages, 746
 running in Guest Shell, 745–746

resource limits, 744
 show guestshell detail command, 747–748

GUI (Graphical User Interfaces)
 Cisco UCS FI configurations, 561–562

ND
 Admin Console page, 343–344
 Administrative pages, 348
 Infrastructure pages, 348
 One View page, 343
 Operations pages, 347–348
 overview, 342–348
 Overview page, 344
 Services page, 345–346
 Sites page, 345
 System Resources pages, 346–347

NDFC, 331–335
 NDI, 320–323

H

HA, Cisco HyperFlex data platforms, 718–719

hard zoning, 407

hardware
 Cisco HyperFlex, 715
 Cisco UCS Manager system monitoring, 638

HashiCorp Terraform, 783
 commands, 786–789
 components, 784–786
 concept, 784
 workflows, 784

HCI (HyperConverged Infrastructure), 704

hello packets, 7

high availability
 Cisco UCS, 533
 vNIC, 569–570
 VXLAN, 157–159

HSRP (Hot Standby Router Protocol), 69–72
 configuring, 79–86
 global commands, 79–86
 interface commands, 80
 load sharing, 72
 network topologies, 70–71, 82–83
 verification commands, 82
 verifying configurations, 79–86
 vPC gateways, 131

HX Data Platform, 716
 Clusters
 interfaces, 720
 tolerated failures, 719
 datastores, 724–725
 disk management, 721–724
 HA, 718–719

- LAB clusters, 716–717
 - LAZ, 726–727
 - local encryption keys, 721
 - Native Snapshots, 719–720
 - Ready Clones, 719
 - SED, 720–721
 - server disk types, 722–723
 - storage clusters, 717
 - system clusters, 725–727
 - hybrid clouds, 249–250**
-
- IaaS (Infrastructure as a Service), 246–248**
 - identity pools, Cisco UCS, 91–596
 - IEEE 802.1 FCoE standard, 438
 - IGMP (Internet Group Management Protocol), 43–46
 - default parameter settings, 56
 - interface commands, 59–61
 - switch IGMP snooping, 46
 - images, NX-OS, 254
 - import backups, 668–670
 - in-band management access, Cisco ACI, 214
 - independent resource scaling, Cisco HyperFlex, 710–711
 - infrastructure monitoring, 284, 521
 - Call Home, 521–522
 - EEM, 522
 - RMON, 523
 - SPAN, 523–528
 - system messages, 521
 - Infrastructure pages, ND GUI, 348**
 - installing**
 - PowerShell, 789–795
 - Python packages, 746
 - UCS PowerShell Library, 790–791
 - VIB
 - IO Visor*, 707
 - VAAI, 707
 - interactive mode, Python, 772–773**
 - interface commands**
 - BFD, 40
 - HSRP, 80–82
 - multicast routing, 59–61
 - OSPF, 15
 - port channels, 135
 - PTP, 283
 - STP, 106–107
 - vPC, 135
 - VRRP, 80
 - VXLAN, 161–162
 - interface configurations**
 - BGP, 34
 - OSPF, 17–18
 - inter-private network contracts communication, 858–859**
 - intersubnet tenant traffic, Cisco ACI, 217–218
 - Inter-Tenant Contracts, 857–858
 - inventory files, Ansible, 765
 - invisible cloud witness services, Cisco HyperFlex, 713–714
 - IO Visor, 707
 - IP pools, Cisco UCS, 593–595
 - IPv4, Cisco UCS FI initialization, 559–560, 563
 - IPv6 (Internet Protocol version 6)
 - Cisco UCS FI initialization, 560–561, 563
 - First Hop Redundancy, VRRP, 77–79
 - ISSU, NX-OS, 263–265

J

- Jinja templates, Ansible, 766
- Job, Scheduler
 - definitions, 736
 - displaying, 739–740
- JSON (JavaScript Object Notation), 751–752, 757

K

- keychain authentication, 868
 - Cisco NX-OS configurations, 868–870
 - commands, 869–870
 - key selection, 871–872

L

- LAB clusters, Cisco HyperFlex data platforms, 716–717
- latency, Cisco HyperFlex, 711–712
- LAZ, Cisco HyperFlex data platforms, 726–727
- LDAP (Lightweight Directory Access Protocol)
 - Cisco UCS Manager, 877
 - groups, 879–888
 - MDS switches, 909–911
 - nested LDAP, 879
 - providers, 879–888
 - storage security, 907–911
 - user accounts, 880
- leaf switches, Cisco ACI, 179–182
- licensing, Cisco Intersight, 652–656
- lifecycle management, NX-OS
 - software, 263
- link modes, port channels, 119
- listing UCS PowerShell cmdlets, 793–795

- load balancing
 - Cisco ACI fabric traffic, 219–220
 - port channels, 120–122
 - SAN port channels, 398–399
 - VSAN, 388

- load sharing
 - HSRP, 72
 - VRRP, 75–76

- local AAA services, 911–912

- local encryption keys, configuring, 721

- locking
 - up valuables, exam preparation, 932–933
 - user accounts, AAA model commands, 806

- logins
 - FLOGI, 378–380
 - PLOGI, 378
 - PRLI, 378

- logs
 - Cisco UCS Manager system monitoring, 632–634
 - system message logging, NX-OS, 284–285

- loop detection, Cisco ACI fabric, 220

- Loop Guard, 95, 96–97

- LSA (Link-State Advertisements), 7–10

M

- MAC (Media Access Control)
 - addresses, FPMA, 447
 - pools, Cisco UCS, 593
- management access, Cisco ACI, 214–215
- management tenants, 213
- managing
 - Cisco HyperFlex

- centralized management*, 709–710
- disk management*, 721–724
- flexibility*, 715
- unified management*, 709–710
- Cisco UCS, 557–564, 660–661
 - backups*, 661–670
 - networks, VLAN*, 584–591
 - system restore*, 670–672
- feature RPM with Bash Shell, 742
- Guest Shell, 746–748
- networks, SNMP, 286
- Nexus consoles, 254–255
- out-of-band management
 - access, Cisco ACI*, 214–215
 - Cisco MDS NX-OS Setup Utility*, 492–496
- patch RPM with Bash Shell, 742–743
- software
 - Cisco MDS NX-OS Setup Utility*, 490–498
 - lifecycles, NX-OS*, 263
 - MDS switch upgrades/downgrades*, 498–500
- time management, networks, 274–275
 - NTP*, 275–280
 - PTP*, 280–284
- man-in-the-middle attacks**, 817
- MDS switches**
 - 9000 series switches, EPLD upgrades, 515–521
- 9100 series multilayer fabric switches**, 362–365
- 9200 series multiservice switches**, 361–362
- 9300 series multilayer fabric switches**, 360–361
- 9700 series multilayer directors, 356–360
- Cisco MDS NX-OS Setup Utility, 490–498
- disruptive downgrades, 513–515
- disruptive upgrades, 505–507
- LDAP, 909–911
- nondisruptive downgrades, 508–512
- nondisruptive upgrades, 500–505
- NX-OS Setup Utility, 490–498
- RADIUS, 902–904
- RBAC, 918–919
- TACACS+, 905–907
- upgrading/downgrading software, 498–500
- verifying NX-OS version, 496–497
- MDT (Multicast Distribution Trees)**, 47–49
- member ports, vPC**, 124
- merges**
 - CFS, 384
 - zoning, 410–411
- MIB, SNMP**, 289–291
- microsegmentation, Cisco ACI**, 207, 860–867
- MLD (Multicast Listener Directory)**, 46–47
- modular QoS CLI, CoPP**, 842–844
- modules**
 - Ansible, 765
 - monitoring powerdowns, 736
- monitoring**
 - events, Cisco UCS Manager, 632–634
 - infrastructure monitoring, 284, 521
 - Call Home*, 521–522
 - EEM*, 522
 - RMON*, 523
 - SPAN*, 523–528
 - system messages*, 521
 - logs, Cisco UCS Manager, 632–634

- module powerdowns, 736
 - NetFlow, Cisco UCS Manager system monitoring, 638–640
 - network infrastructures, 284
 - RMON, 523
 - servers, AAA, 900–901
 - system monitoring, Cisco UCS Manager, 630
 - AG*, 631
 - Call Home*, 636–637
 - database health*, 638
 - DME*, 631, 638–640
 - events*, 632–634
 - hardware*, 638
 - logs*, 632–634
 - northbound interfaces*, 631–632
 - policies*, 634–640
 - Smart Call Home*, 636–637
 - SNMP*, 636
 - traffic monitoring*, 640–647
 - traffic monitoring, 640–641
 - Ethernet*, 641–642
 - FC*, 642–647
 - MPBGP EVPN control plane, VXLAN, 156–157
 - multicast forwarding, 55–56
 - multicast routing, 42–43
 - configuring, 56–69
 - default parameter settings, 56–57
 - feature-based licenses, 57–58
 - global commands, 58–59
 - IGMP, 43–46
 - default parameter settings*, 56
 - interface commands*, 59–61
 - interface commands, 59–61
 - MDT, 47–49
 - MLD, 46–47
 - network topologies, 61–62
 - PIM, 49–51
 - ASM*, 51
 - Bidir*, 51–52
 - configuring*, 164–167
 - default parameter settings*, 56–57
 - designated routers/forwarders*, 54–55
 - distribution modes*, 58
 - RP*, 53–54
 - SSM*, 52–53
 - verifying*, 164–167
 - RPF, 55–56
 - switch IGMP snooping, 46
 - TRM, 159
 - verifying configurations, 61–69
 - multi-hop topologies, FCoE, 454–455
 - multinode edges, Cisco HyperFlex, 713
 - multiple contracts unidirectional single filters, 860
 - multiple-choice, multiple-answer questions, 936
 - multiple-choice, single answer questions, 936
 - multiprotocol BGP, 29–30
 - multitier topologies, Cisco ACI, 179–180
- ## N
-
- named VLAN, 586–589
 - configuring, 589–590
 - deleting, 590–591
 - named VSAN, 616–618
 - NAS (Network-Attached Storage), 481–482
 - benefits, 483
 - Cisco UCS S-Series storage servers, 483–484
 - Native Snapshots, Cisco HyperFlex data platforms, 719–720

ND (Nexus Dashboard), 316–317

benefits, 317–318

cluster nodes, 339–341

external networks, 341–342

GUI

*Admin Console page, 343–344**Administrative pages, 348**Infrastructure pages, 348**One View page, 343**Operations pages, 347–348**overview, 342–348**Overview page, 344**Services page, 345–346**Sites page, 345**System Resources pages,
346–347*

NDDB, 335–337

NDFC, 325–326

*features/benefits, 326–331**GUI, 331–335*

NDI, 318–323

NDO, 323–324

platforms, 337–339

virtual form factors, 339

**NDDB (Nexus Dashboard Data Broker),
335–337****NDFC (Nexus Dashboard Fabric
Controller), 325–326**

features/benefits, 326–331

GUI, 331–335

**NDI (Nexus Dashboard Insights),
318–323****NDO (Nexus Dashboard Orchestrator),
323–324**

neighbor relationships, BFD, 37–38

nested LDAP, Cisco UCS Manager, 879

NetFlow, 293–298, 638–640

network-admin roles, displaying
authority, 740–741**Network Assurance Engine, 310–312****networks**ACI Contracts, exporting between
networks, 858–859

Cisco UCS, VLAN, 584–591

CNA, 436–437

infrastructure monitoring, 284, 521

*Call Home, 521–522**EEM, 522**RMON, 523**SPAN, 523–528**system messages, 521*inter-private network contracts
communication, 858–859

monitoring infrastructures, 284

ND external networks, 341–342

POAP, requirements, 778

ports, STP, 94

RMON, 523

SNMP, 286

*configuring, 292**global commands, 288–289**MIB, 289–291**security, 287–288**specific notation commands,
291**traps, 286–287**verification commands, 291–292*

time management, 274–275

*NTP, 275–280**PTP, 280–284*

topologies

*BFD, 40–41**BGP, 33**HSRP, 82–83**multicast routing, 61–62**OSPF, 16**port channels, 137–138*

- STP, 108
- VRRP, 74, 82–83
- VSAN, 386
 - advantages of*, 388
 - attributes*, 387–388
 - commands*, 392–393
 - configuring*, 391–394
 - DPVM, 388–389
 - features*, 386–387
 - ID, 387
 - names*, 388
 - states*, 387–388
 - switches*, 388
 - trunking*, 389–394
 - verifying configurations*, 391–394
 - zoning comparisons*, 406
- networks, security**
 - AAA model, 801
 - accounting*, 801
 - authentication*, 801, 803–804
 - authorization*, 801, 803–804
 - configuring AAA service options*, 802–803
 - default parameter settings*, 804
 - global commands*, 804–806
 - locking user accounts*, 806
 - passphrase commands*, 806
 - RADIUS, 801–802
 - remote AAA services*, 802
 - TACACS+801–802
 - verification commands*, 807
 - ACI Contracts, 852–853
 - applying*, 855–856
 - components*, 851–852
 - configuring*, 853–854
 - creating*, 854–855
 - exporting between networks*, 858–859
 - inter-private network contracts communication*, 858–859
 - Inter-Tenant Contracts*, 857–858
 - microsegmentation*, 860–867
 - modifying*, 855
 - multiple contracts unidirectional single filters*, 860
 - removing*, 855
 - single contract bidirectional reverse filters*, 859
 - single contract unidirectional with multiple filters*, 859
 - verifying*, 855
 - VRF Contracts, 856–857
 - CoPP, 837–839
 - Cisco NX-OS configurations*, 844–851
 - classification*, 840–844
 - control plane packets*, 839–840
 - creating*, 850–851
 - modifying*, 851
 - modular QoS CLI*, 842–844
 - Nexus 5000, 844
 - Nexus 7000 comparisons*, 843–844
 - Nexus 9000 comparisons*, 842–843
 - rate control*, 840–841
 - FHS
 - DAI, 816–827
 - features*, 815–816
 - keychain authentication, 868
 - Cisco NX-OS configurations*, 868–870
 - commands*, 869–870
 - key selection*, 871–872
 - NX-OS configurations, 804–807
 - RBAC, 807–809, 811–815

news on exam releases, 944**Nexus**

console management, 254–255

ND, 316–317

*benefits, 317–318**cluster nodes, 339–341**external networks, 341–342*

GUI, 342–348

NDDB, 335–337

NDFC, 325–335

NDI, 318–323

NDO, 323–324

*platforms, 337–339**virtual form factors, 339*

NDDB, 335–337

NDFC, 325–326

features/benefits, 326–331

GUI, 331–335

NDI, 318–323

NDO, 323–324

NX-OS*boot sequences, 255–256**checkpoints, 272–274**configuring, 271–274**configuring basic management,
256–259**images, 254*

ISSU, 263–265

NetFlow, 293–298

NTP, 275–280

PLD upgrades, 269–271

PTP, 280–284

*rollbacks, 272–274**saves/backups, 272*

Smart Call Home, 292–293

SNMP, 286–292

software lifecycle management, 263

SPAN, 298–306

*streaming telemetry, 306–309**system message logging, 284–285**time management, 274–284**upgrade/downgrade procedures,
265–269*

routing support, 5–6

switches, POAP configurations,
259–263**Nexus 5000 switches**

CoPP comparisons, 844

FCoE configurations, 458–459

Nexus 7000 switches

CoPP comparisons, 843–844

FCoE configurations, 456–458

Nexus 9000 switches

CoPP comparisons, 842–843

FCoE configurations, 459–461

leaf switches, 179–182

spine switches, Cisco ACI, 179–182

Nexus 9300 series, 181–182**Nexus 9500 series, 181, 264****Nexus CoPP (Control Plane Policing),
837–839**

Cisco NX-OS configurations, 844–851

classification, 840–844

control plane packets, 839–840

creating, 850–851

modifying, 851

modular QoS CLI, 842–844

Nexus 5000, 844

Nexus 7000 comparisons, 843–844

Nexus 9000 comparisons, 842–843

rate control, 840–841

**Nexus DAI (Dynamic ARP Inspection),
816, 817–819**

Cisco NX-OS configurations, 819–827

DHCP snooping, 827–831

man-in-the-middle attacks, 817

Nexus FHS (First-Hop Security)

DAI, 816, 817–819

Cisco NX-OS configurations,
819–827

DHCP snooping, 827–831
man-in-the-middle attacks, 817

features, 815–816

port security, 832–837

NFS (Network File Systems), 479–480

**NIC (Network Interface Cards), vNIC
and high availability, 569–570**

**nondisruptive downgrades, MDS
switches, 508–512**

**nondisruptive upgrades, MDS switches,
500–505**

noninteractive mode, Python, 773–775

non-vPC ports, 124

normal ports, STP, 94

northbound interfaces, 631–632

note taking, exam preparation, 933

**NPIV (N Port Identifier Virtualization),
424–431**

NPV (N Port Virtualization), 424–431

NTP (Network Time Protocol), 275

configuring, 279–280

default parameter settings, 275–276

global commands, 276–278

verification commands, 278

numeric usernames, 808

NVE config commands, VXLAN, 162

NX-API

Cisco NX-API Developer Sandbox,
759–760

error codes, 758–759

Requests/Responses

elements, 757–759

in JSON, 757

in XML, 756–757

NX-OS

AAA model configurations, 804–807

boot sequences, 255–256

checkpoints, 272–274

configuring, 271

basic management, 256–259

saves/backups, 272

images, 254

NetFlow, 293–298

PLD, upgrading, 269–271

rollbacks, 272–274

Smart Call Home, 292–293

SNMP, 286

configuring, 292

global commands, 288–289

MIB, 289–291

security, 287–288

specific notation commands, 291

traps, 286–287

verification commands, 291–292

software

ISSU, 263–265

lifecycle management, 263

upgrade/downgrade procedures,
265–269

SPAN, 298–306

streaming telemetry, 306–309

system message logging, 284–285

time management, 274–275

NTP, 275–280

PTP, 280–284



One View page, ND GUI, 343

Operations pages, ND GUI, 347–348

optimizing Cisco HyperFlex resources,
710–711

orchestration**Ansible**

- authentication*, 766
- Cisco NX-OS example*, 767–768
- CLI prompt*, 766
- CLI tools*, 767
- components*, 765–766
- configuration files*, 766
- important concepts*, 766
- inventory files*, 765
- Jinja templates*, 766
- modules*, 765
- playbooks*, 765–766, 767–768
- plays*, 766
- roles*, 766
- variable files*, 766
- variables*, 766
- workflows using playbooks*, 764–765

POAP, 777–778

- configuration scripts*, 778–779
- DHCP discovery phase*, 781–782
- limitations*, 778
- network requirements*, 778
- post-installation reload phase*, 782
- power-up phase*, 779
- processes (overview)*, 779–780
- script execution phase*, 782
- switch configurations*, 782–783
- USB discovery phase*, 779–780
- verification commands*, 783

PowerShell, 789

- installing*, 789–795
- listing UCS PowerShell cmdlets*, 793–795
- UCS PowerShell Library installations*, 790–791
- versions of*, 789–790, 791–793

Python, 768–769

- Cisco NX-OS, Python packages*, 769–771
- CLI command API*, 771–772
- interactive mode*, 772–773
- noninteractive mode*, 773–775
- UCS Manager Python SDK*, 775–777

Terraform, 783

- commands*, 786–789
- components*, 784–786
- concept*, 784
- workflows*, 784

orphaned ports, vPC, 124**OSPF (Open Shortest Path First)**, 6–7

- ABR verification*, 18–22
- adjacency*, 7
- areas*, 10–12
- authentication*, 13
- BDR*, 12–13
- configuring*, 13–24
- DR*, 12–13
- feature-based licenses*, 14
- global commands*, 14
- hello packets*, 7
- interface commands*, 15
- interface configurations*, 17–18
- LSA*, 7–10
- network topology*, 16
- OSPFv2 and OSPF3 comparisons*, 7
- process clear commands*, 15–16
- router configuration*, 22–24
- routing commands*, 14–15
- verifying configurations*, 15–16
- virtual links*, 12

out-of-band management

- access*, Cisco ACI, 214–215

- Cisco MDS NX-OS Setup Utility, 492–496
 - overlay protocols, VXLAN**
 - configuring, 159–169
 - control plane topologies, 159–161
 - encapsulation, 151–152
 - EVPN control plane, 156–157
 - feature-based licenses, 159
 - Flood and Learn Multicast-based control plane, 154–156
 - gateways, 157
 - global commands, 159–161
 - high availability, 157–159
 - interface commands, 161–162
 - MPBGP EVPN control plane, 156–157
 - NVE config commands, 162
 - overview, 151–152
 - packet formats, 151–152
 - TRM, 159
 - verification commands, 162
 - verifying configurations, 164–169
 - VNI, 153–154
 - VTEP, 152–153
 - Overview page, ND GUI, 344**
-
- P**
- PaaS (Platform as a Service), 246**
 - packet formats, VXLAN, 151–152**
 - passphrase commands, AAA model, 806**
 - passwords**
 - clear-text passwords, 809
 - strong passwords, 808–809
 - patch RPM, managing with Bash Shell, 742–743**
 - peer gateways, vPC, 131–132**
 - peer links, vPC, 124**
 - peer switches, vPC, 124**
 - peering, BGP, 25–26**
 - peer-keepalives, vPC, 124**
 - PFC (Priority-based Flow Control), 438–439**
 - PIM (Protocol Independent Multicast), 49–51**
 - ASM, 51
 - Bidir, 51–52
 - configuring, 164–167
 - default parameter settings, 56–57
 - designated routers/forwarders, 54–55
 - distribution modes, 58
 - RP, 53–54
 - SSM, 52–53
 - verifying, 164–167
 - Pip Python Package Manager, installing Python packages with Guest Shell, 746**
 - playbooks, Ansible, 765–766**
 - Cisco NX-OS example, 767–768
 - workflows using playbooks, 764–765
 - plays, Ansible, 766**
 - PLD (Programmable Logical Devices), 269–271**
 - PLOGI (Port Login), 378**
 - POAP (PowerOn Auto Provisioning), 777–778**
 - configuration scripts, 778–779
 - DHCP discovery phase, 781–782
 - limitations, 778
 - network requirements, 778
 - Nexus switches, 259–263
 - post-installation reload phase, 782
 - power-up phase, 779
 - processes (overview), 779–780
 - script execution phase, 782
 - switch configurations, 782–783
 - USB discovery phase, 779–780
 - verification commands, 783

policies

backups, 666–668

Cisco ACI

*policy identification/
enforcement, 218**policy models, 197–198*Cisco UCS Manager system
monitoring, 634–640

EEM, 733–734

port channels, 117–118, 119–120

bandwidth, 118

benefits, 118

channel code matrix, 119

configuring, 132–146

default parameter settings, 132–133

FEX, 547–548

global commands, 134–135

interface commands, 135

link modes, 119

load balancing, 120–122

network topologies, 137–138

redundancy, 118

SAN port channels, 396

*configuring, 400–403**load balancing, 398–399**modes, 399–400**trunking, 396–397**types of, 396–398**verification commands, 400–401**verifying configurations,
400–403*

STP, 118

verification commands, 137

ports

Cisco UCS FI port modes, 567–569

DPVM, 388–389

FC ports, 368–370

FCoE, 445–447

member ports, vPC, 124

NPIV, 424–431

NPV, 424–431

PLOGI, 378

security, 832–837, 919–921

*configuring, 921–924**fabric binding comparison,
928–929**verifying, 924–926*

SPAN, 298–306, 523–526

*configuring, 526**remote SPAN, 526–528*

STP ports

*edge ports, 94**network ports, 94**normal ports, 94*

vPC

*non-vPC ports, 124**orphaned ports, 124***post-installation reload phase, POAP,
782****PowerShell, 789**

installing, 789–795

listing UCS PowerShell cmdlets,
793–795UCS PowerShell Library installations,
790–791

versions of, 789–790, 791–793

power-up phase, POAP, 779**preparing for exams, 932**

chapter-ending review tools, 935

customizing exams, 934–935

DITKA? questions, 940

drag-and-drop questions, 937

ear plugs, 932

fill-in-the-blank questions, 937

final reviews, 940

getting rest, 932

- multiple-choice, multiple-answer questions, 936
- multiple-choice, single answer questions, 936
- PTP
 - access*, 933–934
 - Cisco Certification Exam Tutorial questions*, 935–939
 - customizing exams*, 934–935
 - Premium Edition*, 935
 - updating exams*, 935
- simlet questions, 939
- simulation questions, 938
- study plans, 940
- study trackers, 932
- taking notes, 933
- testlet questions, 938–939
- time
 - budgeting*, 932
 - clock watching*, 932
 - travel time*, 932
- primary roles, vPC, 127–128**
- private clouds, 248**
- PRLI (Process Login), 378**
- process clear commands, OSPF, 15–16**
- PTP (Pearson Test Prep)**
 - access, 933–934
 - customizing exams, 934–935
 - Premium Edition, 935
 - updating exams, 935
- PTP (Precision Time Protocol), 280**
 - clocks, 281–282, 283–284
 - configuring, 283
 - default parameter settings, 282
 - global commands, 282
 - interface commands, 283
 - verification commands, 283
- public clouds, 248–249**
- Python, 768–769**
 - Cisco NX-OS, Python packages, 769–771
 - CLI command API, 771–772
 - Guest Shell, running Python in, 745–746
 - installing packages with Guest Shell, 746
 - interactive mode, 772–773
 - noninteractive mode, 773–775
 - Pip Python Package Manager, installing Python packages with Guest Shell, 746
 - UCS Manager Python SDK, 775–777
 - converting to*, 777
 - CRUD operations*, 776

Q

QoS (Quality of Service)

- Cisco UCS, 608–610
- modular QoS CLI, CoPP, 842–844

questions

- Cisco Certification Exam Tutorial, 935–939
- DITKA? questions, 940
- drag-and-drop questions, 937
- fill-in-the-blank questions, 937
- multiple-choice, multiple-answer questions, 936
- multiple-choice, single answer questions, 936
- simlet questions, 939
- simulation questions, 938
- testlet questions, 938–939

R

- rack servers, Cisco UCS, 537–538, 577
- RADIUS, 801–802**
 - authentication, 888–892
 - Cisco UCS Manager, 876, 877, 888–892
 - MDS switches, 902–904
 - storage security, 902–904
 - TACACS+ mergers, 914
- Rapid PVST+98–105**
- rate control, CoPP, 840–841
- RBAC (Role-Based Access Control), 807–809**
 - Cisco NX-OS configurations, 811–815
 - MDS switches, 918–919
 - user accounts, 914
 - roles, 915, 917*
 - rules, 915–917*
 - sample configuration, 918–919*
- Ready Clones, Cisco HyperFlex data platforms, 719**
- redundancy, port channels, 118
- regions, CFS, 384–385
- registering devices, switched fabric
 - initialization and FC, 378–380
- remote AAA services, 802, 901
- remote-attached topologies, FCoE, 454
- remote SPAN, 526–528
- remote users, Cisco UCS Manager role policies, 892–894
- removing ACI Contracts, 855
- Requests, NX-API**
 - elements, 757–759
 - in JSON, 757
 - in XML, 756–757
- reserved FDIC, 372
- resources
 - limits, Guest Shell, 744
 - optimization, Cisco HyperFlex, 710–711
 - scaling, Cisco HyperFlex, 710–711
- Responses**
 - NX-API**
 - elements, 757–759*
 - in JSON, 757*
 - in XML, 756–757*
 - REST API, 754–755
- rest, exam preparation, 932**
- REST API, 752–753**
 - authentication, 753–754
 - Responses, 754–755
- RMON (Remote Network Monitoring), 523**
- roles**
 - Ansible, 766
 - Cisco NX-OS, user roles, 809–810
 - RBAC, 807–809, 915, 917
- rollbacks, NX-OS, 272–274
- Root Guard, 95, 97**
- routing**
 - BFD, 37
 - configuring, 38–42*
 - default parameter settings, 38–39*
 - failure detection, 38*
 - global commands, 39–40*
 - interface commands, 40*
 - neighbor relationships, 37–38*
 - network topologies, 40–41*
 - routing commands, 40*
 - verification commands, 40*
 - verifying configurations, 40–42*
 - BGP, 24–25
 - AS 65100 configurations, 33*
 - clear commands, 32–33*
 - configuring, 30–37*
 - default parameter settings, 30*

- feature-based licenses*, 30
- global commands*, 31
- interface configurations*, 34
- multiprotocol BGP*, 29–30
- network topologies*, 33
- path selection*, 26–29
- peering*, 25–26
- routing commands*, 31–32
- verification commands*, 32–33
- verifying configurations*, 34–37
- HSRP, 69–72
 - configuring*, 79–86
 - global commands*, 79–86
 - interface commands*, 80
 - load sharing*, 72
 - network topologies*, 70–71, 82–83
 - verification commands*, 82
 - verifying configurations*, 79–86
- multicast routing, 42–43
 - configuring*, 56–69
 - default parameter settings*, 56–57
 - feature-based licenses*, 57–58
 - global commands*, 58–59
 - IGMP*, 43–46, 56, 59–61
 - interface commands*, 59–61
 - MDT*, 47–49
 - MLD*, 46–47
 - network topologies*, 61–62
 - PIM*, 49–55, 56–61, 164–167
 - RPF*, 55–56
 - switch IGMP snooping*, 46
 - TRM*, 159
 - verifying*, 62–69
 - verifying configurations*, 61–69
- Nexus support, 5–6
- OSPF, 6–7
 - ABR verification*, 18–22
 - adjacency*, 7
 - areas*, 10–12
 - authentication*, 13
 - BDR*, 12–13
 - configuring*, 13–24
 - DR*, 12–13
 - feature-based licenses*, 14
 - global commands*, 14
 - hello packets*, 7
 - interface commands*, 15
 - interface configurations*, 17–18
 - LSA*, 7–10
 - network topology*, 16
 - OSPFv2 and OSPF3 comparisons*, 7
 - process clear commands*, 15–16
 - router configuration*, 22–24
 - routing commands*, 14–15
 - verifying configurations*, 15–16
 - virtual links*, 12
- VRRP, 73, 74
 - authentication*, 77
 - benefits*, 75
 - configuring*, 79–86
 - global commands*, 79–86
 - groups*, 75
 - interface commands*, 80
 - IPv6 First Hop Redundancy*, 77–79
 - load sharing*, 75–76
 - network topologies*, 74, 82–83
 - operation*, 73–75
 - router priority/preemption*, 76–77
 - tracking*, 77
 - verification commands*, 82
 - verifying configurations*, 79–86

RP, PIM, 53–54

RPF (Reverse Path Forwarding), 55–56

RPM, managing with Bash Shell

feature RPM, 742

patch RPM, 742–743

rules

Cisco NX-OS, 809–810

RBAC, user accounts, 915–917

running

Bash Shell, 741–742

Python in Guest Shell, 745–746

S

SaaS (Software as a Service), 245

SAN (Storage Area Networks)

Cisco UCS, connectivity, 611–616,
624–625

port channels, 396

configuring, 400–403

load balancing, 398–399

modes, 399–400

trunking, 396–397

types of, 396–398

verification commands, 400–401

verifying configurations, 400–403

SATA RAS, Cisco HyperFlex, 715–716

saves/backups, NX-OS, 272

scalability, Cisco UCS, 533

Scheduler

backups, 739

configuring, 737–740

displaying jobs/schedules, 739–740

job definitions, 736

overview, 736–737

prerequisites, 737

timetable definitions, 736

verifying configurations, 739–740

scripting

Bash Shell, enabling, 741–742

EEM, monitoring module
powerdowns, 736

execution phase, POAP, 782

Guest Shell

*displaying Ethernet 1/47
interface counters, 745*

dobost command, 745

guestshell destroy command, 747

guestshell disable command, 747

guestshell enable command, 747

installing Python packages, 746

*show guestshell detail command,
747–748*

JSON, 751–752, 757

NX-API

*Cisco NX-API Developer
Sandbox, 759–760*

error codes, 758–759

*Requests/Responses elements,
757–759*

*Requests/Responses in JSON,
757*

*Requests/Responses in XML,
756–757*

POAP, 777–778

configuration scripts, 778–779

DHCP discovery phase, 781–782

limitations, 778

network requirements, 778

*post-installation reload phase,
782*

power-up phase, 779

processes (overview), 779–780

script execution phase, 782

switch configurations, 782–783

USB discovery phase, 779–780

verification commands, 783

- Python, 768–769
 - Cisco NX-OS, Python packages,* 769–771
 - CLI command API,* 771–772
 - interactive mode,* 772–773
 - noninteractive mode,* 773–775
 - UCS Manager Python SDK,* 775–777
- REST API, 752–753
 - authentication,* 753–754
 - Responses,* 754–755
- Scheduler
 - backups,* 739
 - displaying jobs/schedules,* 739–740
- setup scripts, Cisco MDS NX-OS Setup Utility, 490–491
- XML, 748–749
 - Requests/Responses and REST API,* 756–757
 - structure example,* 749–750
 - syntax,* 750–751
- SCVMM, Cisco ACI integration, 204–205
- secondary roles, vPC, 127–128
- security
 - Cisco UCS Manager
 - AAA model,* 875–876
 - Cisco AVPair attribute example,* 878
 - LDAP,* 877
 - LDAP providers/groups,* 879–888
 - multiple authentication services configuration,* 892–894
 - RADIUS,* 876, 877, 888–892
 - remote user role policies,* 892–894
 - Session Timeout Period,* 879
 - TACACS+877–878, 888–894*
 - two-factor authentication,* 879
 - Web Session Refresh Period,* 879
 - clear-text passwords, 809
 - computer security
 - AAA model,* 875–876
 - Cisco AVPair attribute example,* 878
 - LDAP,* 877
 - LDAP providers/groups,* 879–888
 - multiple authentication services configuration,* 892–894
 - RADIUS,* 876, 877, 888–892
 - remote user role policies,* 892–894
 - TACACS+877–878, 888–894*
 - two-factor authentication,* 879
 - encryption
 - local encryption keys,* 721
 - SED,* 720–721
 - FHS
 - DAI,* 816–827
 - features,* 815–816
 - locking up valuables, exam preparation, 932–933
 - network security
 - AAA model,* 801–807
 - ACI Contracts,* 851–867
 - CoPP,* 837–851
 - FHS,* 815–837
 - Keychain Authentication,* 868–872
 - RBAC,* 807–815
 - passwords
 - clear-text passwords,* 809
 - strong passwords,* 808–809
 - ports, 832–837
 - ports, security, 919–921

- configuring*, 921–924
- fabric binding comparison*, 928–929
- verifying*, 924–926
- SED, Cisco HyperFlex data platforms, 720–721
- SNMP, 287–288
- storage security
 - AAA model*, 898–901
 - fabric binding*, 926–929
 - LDAP*, 907–911
 - port security*, 919–926
 - RADIUS*, 902–904, 914
 - RBAC*, 914–919
 - TACACS+* 904–907, 914
- strong passwords, 808–809
- SED, Cisco HyperFlex data platforms, 720–721
- servers**
 - Cisco HyperFlex disk types, 722–723
 - Cisco UCS
 - 5108 Blade Server Chassis*, 536
 - blade servers*, 536–537
 - Cisco UCS Mini*, 539–540
 - pools*, 596
 - profiles*, 599–602
 - rack servers*, 537–538, 577
 - storage servers*, 537–539
 - firmware upgrades, 691–699
 - monitoring, AAA, 900–901
- services**
 - CFS, 380–381
 - CFSofC*, 382–384
 - CFSofIP*, 382–384
 - fabric lock*, 382
 - features*, 381–382
 - merges*, 384
 - regions*, 384–385
 - Cisco Intersight management as a service, 648–649
 - IaaS, 246–248
 - PaaS, 246
 - profiles, Cisco UCS, 596–599, 602–607
 - SaaS, 245
 - Services page**, ND GUI, 345–346
 - Session Timeout Period**, Cisco UCS Manager, 879
 - setup scripts**, Cisco MDS NX-OS Setup Utility, 490–491
 - shells**
 - Bash Shell, 740
 - displaying dev-ops role authority*, 740–741
 - displaying network-admin role authority*, 740–741
 - enabling*, 741–742
 - feature RPM*, 742
 - patch RPM*, 742–743
 - running*, 741–742
 - Guest Shell, 743
 - access*, 743–744
 - capabilities*, 744–746
 - displaying Ethernet 1/47 interface counters*, 745
 - dohost command*, 745
 - guestshell destroy command*, 747
 - guestshell disable command*, 747
 - guestshell enable command*, 747
 - installing Python packages*, 746
 - managing*, 746–748
 - resource limits*, 744
 - running Python in Guest Shell*, 745–746
 - show guestshell detail command*, 747–748
 - show guestshell detail command**, 747–748

- simlet questions, 939
- simulation questions, 938
- single contract bidirectional reverse filters, 859
- single contract unidirectional with multiple filters, 859
- single-hop topologies, FCoE, 451–454
- Sites page, ND GUI, 345
- Smart Call Home, 292–293, 636–637
- smart zoning, 411–412
- snapshots, Cisco HyperFlex data platforms, 719–720
- SNMP (Simple Network Management Protocol), 286
 - Cisco UCS Manager system monitoring, 636
 - configuring, 292
 - global commands, 288–289
 - MIB, 289–291
 - security, 287–288
 - specific notation commands, 291
 - traps, 286–287
 - verification commands, 291–292
- software
 - Cisco Intersight supported software, 650–652
 - EPLD, upgrading, 269–271
 - managing
 - Cisco MDS NX-OS Setup Utility*, 490–498
 - MDS switch upgrades/downgrades*, 496–497
 - MDS switches, upgrading/downgrading software, 498–500
 - NX-OS
 - ISSU, 263–265
 - lifecycle management*, 263
 - upgrade/downgrade procedures*, 265–269
 - PLD, upgrading, 269–271
 - updates, Cisco UCS, 672–679
- SPAN (Switched Port Analyzers), 298–306, 523–526
 - configuring, 526
 - remote SPAN, 526–528
- special characters in usernames, 808
- specific notation commands, SNMP, 291
- spine switches, Cisco ACI, 179–182
- SSM (Source-Specific Multicast), 52–53
- storage
 - Cisco UCS, 611
 - S-Series storage servers*, 483–484
 - storage servers*, 537–539
 - datastores, Cisco HyperFlex data platforms, 724–725
 - NAS, 481–482
 - benefits*, 483
 - Cisco UCS S-Series storage servers*, 483–484
 - VSAN, 386
 - advantages of*, 388
 - attributes*, 387–388
 - commands*, 392–393
 - configuring*, 391–394
 - DPVM, 388–389
 - features*, 386–387
 - ID, 387
 - names*, 388
 - states*, 387–388
 - switches*, 388
 - trunking*, 389–394
 - verifying configurations*, 391–394
 - zoning comparisons*, 406

storage clusters

- Cisco HyperFlex data platforms, 717
- compute nodes, 717
- converged nodes, 717
- datastores, 717
- drives, 717

storage security

- AAA model, 898
 - accounting*, 900
 - authentication*, 899, 912–913
 - authorization*, 899, 912–913
 - local AAA services*, 911–912
 - remote AAA services*, 901
 - server distribution*, 913–914
 - server groups*, 900
 - server monitoring*, 900–901
 - service configuration*, 900

- fabric binding, 926–929

- LDAP, 907–911

- port security, 919–921

- configuring*, 921–924
 - fabric binding comparison*, 928–929
 - verifying*, 924–926

- RADIUS, 902–904, 914

- RBAC, 914–919

- TACACS+904–907, 914

STP (Spanning Tree Protocol), 93

- BPDU Filtering, 95, 96
- BPDU Guard, 95, 96
- Bridge Assurance, 95–96
- configuring, 102–117
- edge ports, 94
- extension default settings, 102
- extensions (overview), 94–95
- global commands, 105
- interface commands, 106–107
- Loop Guard, 95, 96–97

- network ports, 94

- network topologies, 108

- normal ports, 94

- port channels, 118

- Rapid PVST+98–105

- Root Guard, 95, 97

- topologies, 93–94, 108

- UDLD, 97–98, 102–105

- verification commands, 108

- verifying configurations, 109–117

streaming telemetry, NX-OS, 306–309**strong passwords, 808–809****structure example, XML, 749–750****study plans, exams, 940, 943–944****study trackers, 932****switched fabric initialization, FC**

- device registration, 378–380

- domain ID, 375–377

- fabric reconfiguration, 377

- FCID, 377

- FCNS databases, 378–380

- FLOGI, 378–380

- overview, 373–374

- PLOGI, 378

- principal switch selection, 374–377

- PRLI, 378

switches

- Cisco MDS

- FCoE configurations

- Nexus 5000 switches*, 458–459

- Nexus 7000 switches*, 456–458

- Nexus 9000 switches*, 459–461

- IGMP snooping, 46

- leaf switches, Cisco ACI, 179–182

- MDS switches

- 9000 series switches, EPLD upgrades*, 515–521

- 9100 series multilayer fabric switches, 362–365
- 9200 series multiservice switches, 361–362
- 9300 series multilayer fabric switches, 360–361
- disruptive downgrades, 513–515
- disruptive upgrades, 505–507
- nondisruptive downgrades, 508–512
- nondisruptive upgrades, 500–505
- NX-OS Setup Utility, 490–498
- upgrading/downgrading software, 498–500
- verifying NX-OS version, 496–497
- peer switches, vPC, 124
- POAP configurations, 259–263, 782–783
- port security, 919–921
 - configuring, 921–924
 - fabric binding comparison, 928–929
 - verifying, 924–926
- spine switches, Cisco ACI, 179–182
- VSAN, 388
- switching protocols**
 - port channels, 117–118, 119–120
 - bandwidth, 118
 - benefits, 118
 - channel code matrix, 119
 - configuring, 132–146
 - default parameter settings, 132–133
 - global commands, 134–135
 - interface commands, 135
 - link modes, 119
 - load balancing, 120–122
 - network topologies, 137–138
 - redundancy, 118
 - STP, 118
 - verification commands, 137
 - vPC, 134–135
 - STP, 93
 - BPDU Filtering, 95, 96
 - BPDU Guard, 95, 96
 - Bridge Assurance, 95–96
 - configuring, 102–117
 - edge ports, 94
 - extension default settings, 102
 - extensions (overview), 94–95
 - global commands, 105
 - interface commands, 106–107
 - Loop Guard, 95, 96–97
 - network ports, 94
 - network topologies, 108
 - normal ports, 94
 - port channels, 118
 - Rapid PVST+98–102
 - Root Guard, 95, 97
 - topologies, 93–94, 108
 - UDLD, 97–98, 102–105
 - verification commands, 108
 - verifying configurations, 109–117
 - vPC, 122
 - ARP synchronization, 131
 - components, 124–125
 - configuration consistency, 128–129
 - configuring, 132–146
 - consistency checks, 129
 - domain commands, 136
 - domains, 124
 - dual-control plane, 126
 - duplicate frame prevention, 129–131

- fault-tolerant links*, 124
- HSRP gateways*, 131
- implementing*, 133–134
- interface commands*, 135
- member ports*, 124
- non-vPC ports*, 124
- orphaned ports*, 124
- peer gateways*, 131–132
- peer links*, 124
- peer switches*, 124
- peer-keepalives*, 124
- primary roles*, 127–128
- secondary roles*, 127–128
- topologies*, 122–123
- traffic flows*, 125–126
- verification commands*, 137

syntax, XML, 750–751

system clusters, Cisco HyperFlex data platforms, 725–727

system messages

- infrastructure monitoring, 521
- logging, NX-OS, 284–285

system monitoring, Cisco UCS Manager, 630

- AG, 631
- Call Home, 636–637
- database health, 638
- DME, 631
- events, 632–634
- hardware, 638
- logs, 632–634
- NetFlow, 638–640
- northbound interfaces, 631–632
- policies, 634–640
- Smart Call Home, 636–637
- SNMP, 636
- traffic monitoring, 640–647

System Resources pages, ND GUI, 346–347

system restore, Cisco UCS configuration management, 670–672

T

T11 FCoE standard, 438

taboo contracts, 209–210

TACACS+801–802

- authentication, 888–892
- Cisco UCS Manager, 876, 888–892
- MDS switches, 905–907
- RADIUS mergers, 914
- remote user role policies, 892–894
- storage security, 904–907, 914

telemetry data collection, Cisco Intersight, 650

tenants

- ACI Contracts, 857–858
- Cisco ACI, 198–200
 - creating*, 227–230
 - intersubnet tenant traffic*, 217–218
 - management tenants*, 213
- intersubnet tenant traffic, 217–218
- management tenants, 213

Terraform, 783

- commands, 786–789
- components, 784–786
- concept, 784
- workflows, 784

testlet questions, 938–939

three-tier Cisco ACI applications, 233–235

time

- exam preparation
 - budgeting time*, 932

- clock watching*, 932
 - travel time*, 932
 - management, networks, 274–275
 - NTP*, 275–280
 - PTP*, 280–284
 - timetable definitions, Scheduler, 736
 - topologies
 - FC, 365–368
 - FCoE
 - direct-attached topologies*, 452–453
 - FEX topologies*, 453–454, 461–463
 - multi-hop topologies*, 454–455
 - remote-attached topologies*, 454
 - single-hop topologies*, 451–454
 - multitier topologies, Cisco ACI, 179–180
 - network topologies
 - BFD*, 40–41
 - BGP*, 33
 - HSRP*, 70–71, 82–83
 - multicast routing*, 61–62
 - OSPF*, 16
 - port channels*, 137–138
 - STP*, 108
 - VRRP*, 74, 82–83
 - STP, 93–94, 108
 - vPC, 122–123
 - VXLAN control plane, 163
 - tracking, VRRP, 77
 - traffic flows, vPC, 125–126
 - traffic load balancing, Cisco ACI fabric, 219–220
 - traffic monitoring
 - Cisco UCS Manager system monitoring, 640–641
 - Ethernet, 641–642
 - FC, 642–647
 - traffic storms, Cisco ACI fabric, 219
 - traps, SNMP, 286–287
 - travel time, exam preparation, 932
 - TRM (Tenant Routed Multicast), 159
 - trunking
 - SAN port channels, 396–397
 - VSAN, 389–394
 - two-factor authentication, Cisco UCS Manager, 879
-
- ## U
-
- UCS Manager Python SDK, 775–777
 - converting to, 777
 - CRUD operations, 776
 - UCS PowerShell cmdlets, listing, 793–795
 - UCS PowerShell Library, installing, 790–791
 - UDLD (Unidirectional Link Detection), 97–98, 102–105
 - unified management, Cisco HyperFlex, 709–710
 - updates
 - exams, 935, 942–943, 944
 - firmware, Cisco UCS, 672–679
 - software, Cisco UCS, 672–679
 - upgrading
 - EPLD, 269–271
 - fabric, Cisco ACI, 189–190
 - firmware, through Auto Install, 680–687
 - MDS 9000 series switches, EPLD upgrades, 515–521
 - MDS switches
 - disruptive upgrades*, 505–507
 - nondisruptive upgrades*, 500–505
 - software*, 498–500
 - Nexus 9500 series, 264

NX-OS, 265–269

PLD, upgrading, 269–271

uplink connectivity, Cisco UCS FI, 567

USB discovery phase, POAP,
779–780

user accounts

LDAP, 880

locking commands, AAA model, 806

numeric usernames, 808

RBAC, 914

roles, 915, 917

rules, 915–917

sample configuration, 918–919

special characters in usernames, 808

usernames

numeric usernames, 808

special characters in usernames, 808

UUID pools, Cisco UCS, 591–593

V

**VAAI (vStorage API for Array
Installation), 707**

**valuables (exam preparation), locking
up, 932–933**

variables, Ansible, 766

vCenter, Cisco ACI integration,
235–238

verification commands

FCoE, 466

HSRP, 82

NTP, 278

port channels, 137

PTP, 283

SAN port channels, 400–401

SNMP, 291–292

STP, 108

vPC, 137

VRRP, 82

VXLAN, 162

verifying

AAA verification commands, 807

ACI Contracts, 855

BFD, 40–42

BGP configurations, 34–37

Cisco UCS FI, cluster verifications,
563–564

device alias configurations, 422–423

EEM configurations, 736

FCoE, 466–474

HSRP, 79–86

multicast routing, 62–69

multicast routing configurations,
61–69

NX-OS version, MDS switches, 496–497

OSPF configurations, 15–16

PIM, 164–167

POAP verification commands, 783

port security, 924–926

SAN port channel configurations,
400–403

Scheduler configurations, 739–740

STP configurations, 109–117

VRRP configurations, 79–86

VSAN configurations, 391–394

VXLAN configurations, 164–169

zoning configurations, 414–417

VFC (Virtual Fibre Channel), 444–445

VIB (vSphere Installation Bundles)

IO Visor, 707

VAAI, 707

VIC (Virtual Interface Cards), 552–555

Virtual Edge, Cisco ACI, 206

virtual links

FEX, 548

OSPF, 12

virtualization

- Cisco UCS, 550–555

- NPIV, 424–431

- NPV, 424–431

VLAN (Virtual LAN)

- Cisco UCS network management, 584–591

- named VLAN, 586–589

- configuring*, 589–590

- deleting*, 590–591

- VM, Cisco HyperFlex, VM density**, 711–712

- VMM, Cisco ACI VMM domains**, 203–204

- VMware overlays, Cisco ACI integration**, 206

- VMware vCenter, Cisco ACI integration**, 205

- VNI (Virtual Network Identifiers)**, 153–154

- vNIC, high availability**, 569–570

- vPC (Virtual Port Channels)**, 122

- ARP synchronization, 131

- components, 124–125

- configuration consistency, 128–129

- configuring, 132–146

- consistency checks, 129

- domain commands, 136

- domains, 124

- dual-control plane, 126

- duplicate frame prevention, 129–131

- fault-tolerant links, 124

- global commands, 134–135

- HSRP gateways, 131

- implementing, 133–134

- interface commands, 135

- non-vPC ports, 124

- orphaned ports, 124

- peer gateways, 131–132

- peer links, 124

- peer switches, 124

- peer-keepalives, 124

- primary roles, 127–128

- secondary roles, 127–128

- topologies, 122–123

- traffic flows, 125–126

- verification commands, 137

- vPC ports, member ports, 124

VRF (Virtual Routing and Forwarding)

- Cisco ACI, 200

- Contracts, 856–857

VRRP (Virtual Router Redundancy Protocol), 73, 74

- authentication, 77

- benefits, 75

- configuring, 79–86

- global commands, 79–86

- groups, 75

- interface commands, 80

- IPv6 First Hop Redundancy, 77–79

- load sharing, 75–76

- network topologies, 74, 82–83

- operation, 73–75

- router priority/preemption, 76–77

- tracking, 77

- verification commands, 82

- verifying configurations, 79–86

VSAN (Virtual Storage-Area Networks), 386

- advantages of, 388

- attributes, 387–388

- Cisco UCS, 616–621

- commands, 392–393

- configuring, 391–394

- DPVM, 388–389

- features, 386–387
- ID, 387
- named VSAN, 616–618
- names, 388
- states, 387–388
- switches, 388
- trunking, 389–394
- verifying configurations, 391–394
- zone sets, 618–621
- zones, 618–621
- zoning comparisons, 406
- VTEP (VXLAN Tunnel Endpoints), 152–153**
- VXLAN (Virtual Extensible LAN)**
 - Cisco ACI, 215–216
 - configuring, 159–169
 - control plane topologies, 159–161
 - encapsulation, 151–152
 - EVPN control plane, 156–157
 - feature-based licenses, 159
 - Flood and Learn Multicast-based control plane, 154–156
 - gateways, 157
 - global commands, 159–161
 - high availability, 157–159
 - interface commands, 161–162
 - MPBGP EVPN control plane, 156–157
 - NVE config commands, 162
 - overview, 151–152
 - packet formats, 151–152
 - TRM, 159
 - verification commands, 162
 - verifying configurations, 164–169
 - VNI, 153–154
 - VTEP, 152–153
- vzAny rule, 210–212**

W

Web Session Refresh Period, Cisco UCS Manager, 879

workflows

- Ansible, 764–765
- Terraform, 784

WWN pools, Cisco UCS, 621–624

X

XML (Extensible Markup Language), 748–749

- Requests/Responses and REST API, 756–757
- structure example, 749–750
- syntax, 750–751

Y - Z

zone alias, device alias comparisons, 421–422

zone sets, VSAN, 618–621

zones, VSAN, 618–621

zoning, 404

- active zone sets, 407–409
- Autozone, 410
- configuring, 414–417
- enforcement, 406–407
- enhanced zoning, 412–413
- features, 404–406
- full zone sets, 407–409
- hard zoning, 407
- merges, 410–411
- smart zoning, 411–412
- verifying configurations, 414–417
- VSAN comparisons, 406