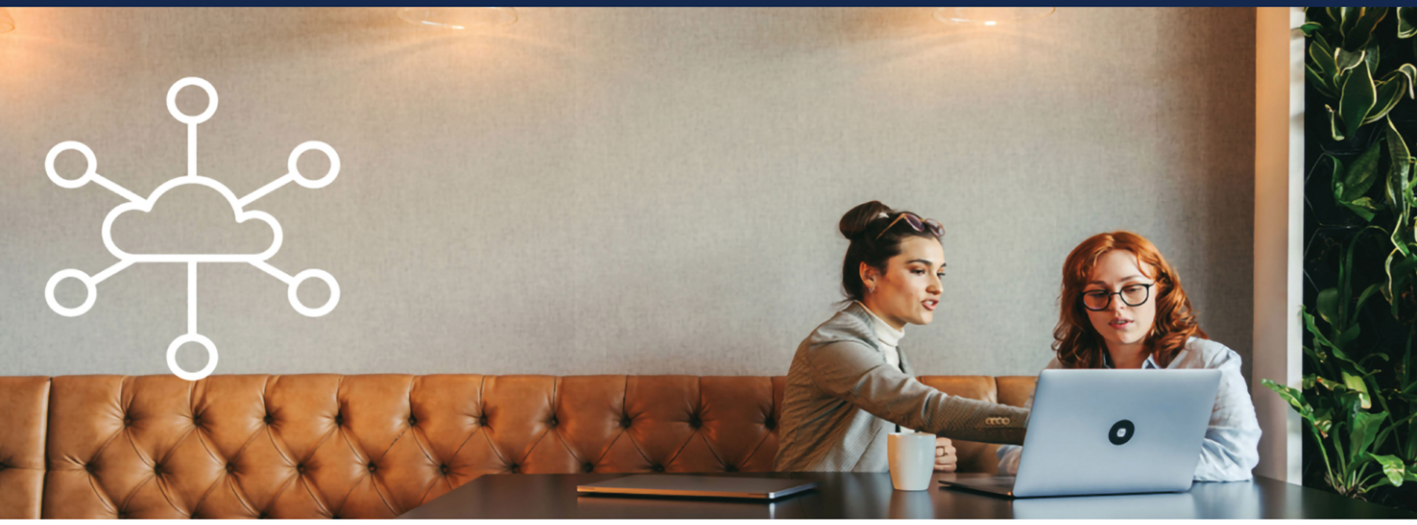
Cisco Catalyst SD-WAN

Design, Deploy, and Secure Your WAN

Second Edition



ANASTASIYA VOLKOVA
CCIE® X2 (ENT & SEC) NO. 54378
OSVALDO SALAZAR TOVAR
CONSTANTIN MOHOREA
CCIE® X2 (ENT, SEC) NO. 16223, CCDE® NO. 20170054
DUSTIN SCHUEMANN
CCIE® (ENT) NO. 59235

ciscopress.com

FREE SAMPLE CHAPTER

Cisco Catalyst SD-WAN: Design, Deploy, and Secure Your WAN

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, and more!

To access the companion website, simply follow these steps:

1. Go to **www.ciscopress.com/register**.
2. Enter the **print book ISBN:** 9780138313906.
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

Cisco Catalyst SD-WAN

Design, Deploy, and Secure Your WAN

ANASTASIYA VOLKOVA, CCIE No. 54378
OSVALDO SALAZAR TOVAR
CONSTANTIN MOHOREA, CCDE No. 20170054, CCIE No. 16623
DUSTIN SCHUEMANN, CCIE No. 59235

Cisco Press
221 River St.
Hoboken, NJ 07030 USA

Cisco Catalyst SD-WAN: Design, Deploy, and Secure Your WAN

Anastasiya Volkova, Osvaldo Salazar Tovar, Constantin Mohorea, and Dustin Schuemann

Published by:
Cisco Press

$PrintCode

Library of Congress Control Number: 2024941644

ISBN-13: 978-0-13-831390-6

ISBN-10: 0-13-831390-3

Warning and Disclaimer

This book is designed to provide information about Cisco Software-Defined Wide-Area Networks. 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 authors and are not necessarily those of Cisco Systems, Inc.

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

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.

GM K12, Early Career and Professional Learning: Soo Kang

Alliances Manager, Cisco Press: Caroline Antonio

Director, ITP Product Management: Brett Bartow

Senior Sponsoring Editor: Malobika Chakraborty

Managing Editor: Sandra Schroeder

Development Editor: Ellie C. Bru

Senior Project Editor: Mandie Frank

Technical Editors: Brad Edgeworth, Gina Cornett

Editorial Assistant: Cindy Teeters

Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Cheryl Ann Lenser

Proofreader: Donna E. Mulder

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

About the Authors

Anastasiya Volkova, CCIE No. 54378 (EN and Security), is a Solutions Architect on the Cisco Global Demo Engineering team, with a focus on Enterprise networking, Security and Cloud solutions, and multi-domain integrations. Anastasiya has more than 12 years of industry experience. Her background includes different areas of expertise, from hands-on experience in design, implementation, and support of network solutions to conducting trainings and technical presentations. She is very passionate about sharing her knowledge with others, hoping to help more people fall in love with the technology.

Osvaldo Salazar Tovar is a Technical Solutions Architect/Solutions Engineer in the Cisco Enterprise Routing and SD-WAN group. Throughout his career, he has supported the Global Service Provider and Enterprise Networking teams in LATAM through various technical sales engineering roles. He is currently working with different verticals in the United States, assisting customers and partners in designing and implementing next-generation WANs and emphasizing the importance of the WAN. He holds a bachelor of science degree in information and communication technologies from Instituto Tecnologico y de Estudios Superiores de Monterrey (ITESM).

Constantin Mohorea, CCIE No. 16223, CCDE No. 20170054, is a Customer Delivery Technical Leader at Cisco with more than 20 years of experience in the networking industry. He specializes in designing and delivering Cisco SD-WAN technologies to clients across various industries and has a strong history of helping clients achieve their business goals. He is passionate about the evolving trends in programmability and automation within the networking sector and has authored a Cisco Press DevNet certification book. Constantin resides in Toronto, Canada.

Dustin Schuemann, CCIE No. 59235 (R&S), is very passionate about giving back through mentoring and building communities in the IT industry. Dustin has 22 years of experience in the networking field, and before joining Cisco he worked in the manufacturing, retail, and finance industries. Dustin currently works in Cisco's Global Demo Engineering organization as a Solutions Architect, leading the demo strategic direction. Dustin speaks on SD-WAN at Cisco Live globally and has been inducted into the Cisco Live Hall of Fame by achieving Distinguished Speaker status at five different events.

About the Technical Reviewers

Brad Edgeworth, CCIE No. 31574 (R&S and SP), is an SD-WAN technical solutions architect at Cisco Systems. Brad is a distinguished speaker at Cisco Live, where he has presented on various topics. Before joining Cisco, Brad worked as a network architect and consultant for various Fortune 500 companies. Brad's expertise is based on enterprise and service provider environments, with an emphasis on architectural and operational simplicity. Brad holds a bachelor of arts degree in computer systems management from St. Edward's University in Austin, Texas. Brad can be found on Twitter as @BradEdgeworth.

Gina Cornett, CCIE Emeritus No. 3311 (R&S and Security), is a Technical Marketing Engineer in the Enterprise Business Unit, where she focuses on design and customer adoption of Cisco Catalyst SD-WAN technology. In addition to this customer-focused design work, Gina has also worked in Customer Support, Systems Test, and the Customer Proof of Concept Labs (CPOC) for a career at Cisco lasting more than 28 years. Her background is in campus switching, security, and SD-WAN.

Dedications

Anastasiya Volkova:

I dedicate this book to my husband, Vitaly, whose endless patience and wholehearted support made a huge contribution not only to this book but to many other ambitious projects as well. You believe in me more than I believe in myself!

I also dedicate it to my parents, who have always been a great example of unprecedented love and constant readiness to develop new skills and share knowledge. Now we have one more book author in our family!

Osvaldo Salazar Tovar:

I dedicate this book to my wife, Cinthia. Thanks for supporting and encouraging me to always do my best and thanks for your love and partnership. You (and the cats —Mia, Salem, and Dexter) are my engine to keep moving.

I also dedicate this project to my mom, Teresa, my dad, Fidencio, and my brother, Fidencio Jr., for putting so much of your dreams in my career. I will endlessly be in debt to you.

Tessa, as I write this, your mom and I can't wait to meet you. No matter what, always chase your dreams, don't be scared of new challenges, always try your best, and we will be here for you.

To the reader, if you are looking for an answer or simply trying to be a better engineer in this technology, keep up the good work; you will make it. Thanks for getting here.

Constantin Mohorea:

I dedicate this book to my family: my parents, my wife, and especially my children. Thank you for all your support!

I also dedicate this work to the Transplant Team at Toronto General Hospital. Your incredible work and daily miracles have profoundly impacted my life, and I am forever grateful.

In memory of Alexi Laiho, Tomas "Quorthon" Forsberg, and Darrell Lance Abbott, whose music provided the inspiring soundtrack to the creation of this book.

Finally, I dedicate this book to everyone committed to continuous study and self-improvement. Keep pushing forward; your dedication inspires me!

Dustin Schuemann:

I dedicate this book to my father. As I write this, it is Father's Day, and I can't help but remember all the good times I had with him. My father lost his battle with cancer two years ago, but without the life lessons my dad instilled in me, this book would have never come to fruition. My father taught me first and foremost that if you believe in something do it no matter what stands in the way and secondly to make sure you are always focused on the greater good. This book is a testament to both of those examples he set in his own life, and I hope to carry on.

I love you, Dad.

Acknowledgments

Anastasiya Volkova:

I want to thank my friend and colleague Dustin Schuemann. I wouldn't have been involved in so many interesting projects if it were not for you. Thank you for the inspiration, support, and for being a great example!

I also want to acknowledge our GDE leadership team, in particular Charlie Lewis and Jason Angelus. Thank you for all the opportunities you've given us, and for the incredible culture you've created in our organization. I am happy and proud to be a part of this team!

Finally, a very big appreciation goes to Prashant Tripathi. Your level of expertise and willingness to help significantly improved not only this book but my personal knowledge as well. Thank you for providing detailed explanations and answering a million questions about Catalyst SD-WAN in general and Cloud OnRamp in particular.

Osvaldo Salazar Tovar:

First, I would like to thank and recognize my coauthors, Anastasiya, Dustin, and Constantin. You are such hard workers and lead by example, and I'm glad we met and came to achieve this book as a result. Dustin, how can somebody invite you to be busier and still ask why are you working on a holiday or late night? I really appreciate your leadership on this amazing project. Thanks for considering me.

Second, to our technical reviewers, Brad Edgeworth and Gina Cornett. I have learned a lot from you.

Finally, to my friends and mentors Paquito, Dana, Prashant, Ali, Adam, Brendan, Lee, Luis, Adilson, Jason, and Jeffry: Thanks for your friendship, mentorship, encouragement, and trust in me. To the TME, PM, and Escalations teams that have always tolerated my questions and provided me light and knowledge: Thanks.

Greg, thanks a lot for all the support, brother. And thanks to all my other colleagues and management that has contributed to my growth. The best is yet to come!

Constantin Mohorea:

I would like to express my deepest gratitude to my coauthors, Anastasiya, Osvaldo, and Dustin. Working with you was a true pleasure, and your collaboration made this journey memorable.

Special thanks go to our technical reviewers, Gina Cornett and Brad Edgeworth. Your time, expertise, and patience have been greatly appreciated.

I am grateful to my immediate Cisco team for their direct and indirect support. Thank you, Doug, for your unwavering encouragement. Nikhail, your questions always sparked deeper thinking. Iftikhar, your exemplary thoroughness set a high standard for us all.

To the many wonderful people at Cisco who contributed to my growth by patiently addressing my questions and leading by example, I am sincerely grateful.

Finally, to you, my reader: Thank you for dedicating your time to this book. Your interest and engagement give meaning to my efforts.

Dustin Schuemann:

First off, I want to send a special thanks to my coauthors, Anastasiya, Osvaldo, and Constantin. Throughout this experience, you have shown just how dedicated you are to your craft and, more importantly, passing on your knowledge to help others grow. Your focus on the reader was apparent, and every choice you made was grounded in what is best for them. I know there were a lot of long hours, weekends, and time away from your families while writing this, and I'm grateful for everything you have done here. Each of you should be very happy with what you've accomplished. Thank you! When are we doing the third edition?

I would like to also thank our Cisco Press team for their support and for providing us with the opportunity. Ellie Bru, thank you for dealing with my endless questions, keeping us on track, and ensuring that this book was successfully delivered. From the entire team, I would like to thank Gina Cornett and Brad Edgeworth for technical editing. Your knowledge and expertise on all things SD-WAN were instrumental in the delivery of this book, even if we didn't completely agree on the IP addresses we used in the book.

Finally, I want to thank my leadership team at Cisco. Charlie Lewis and Jason Angelus, you've supported me in everything I have done personally and professionally. Over the past few years, it hasn't been easy for me, and your desire to make sure I had the time and freedom to deal with those things is greatly appreciated. The team you have created and the people you have surrounded me with are exceptional in everything they do, and this has made me a better person. Thank you!

Contents at a Glance

Reader Services

Register your copy of this book at www.ciscopress.com/title/9780138313906 for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account.* Enter the product ISBN 9780138313906 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

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

Contents

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.

Cover Credit

Cover Photo: Jacob Lund/Shutterstock

Introduction

The Implementing Cisco SD-WAN Solutions (ENSDWI 300-415) exam is a concentration exam for the CCNP Enterprise certification. If you pass the ENSDWI 300-415 exam, you also obtain the Cisco Certified Specialist—Enterprise SD-WAN Implementation certification. This exam covers core SD-WAN technologies, including SD-WAN architecture, controller deployment, edge router deployment, policies, security, quality of service, multicast, and management and operations.

TIP You can review the exam blueprint at https://learningnetwork.cisco.com/s/ensdwi-exam-topics.

This book gives you the foundation and covers the topics necessary to start the CCNP Enterprise certification, with a focus on the SD-WAN concentration exam or the Cisco Certified Specialist—Enterprise SD-WAN Implementation certification.

The CCNP Enterprise Certification

The CCNP Enterprise certification is one of the industry's most respected certifications. In order to earn the CCNP Enterprise certification, you must pass two exams—the ENCOR exam and one concentration exam of your choice—so you can customize your certification to your technical area of focus. This book focuses on the Implementing Cisco SD-WAN Solutions (ENSDWI 300-415) concentration exam.

TIP The ENCOR core exam is also the qualifying exam for the CCIE Enterprise Infrastructure and CCIE Enterprise Wireless certifications. Passing this exam is the first step toward earning both of these certifications.

The following are the CCNP Enterprise concentration exams:

- Implementing Cisco Enterprise Advanced Routing and Services (300-410 ENARSI)
- Implementing Cisco SD-WAN Solutions (300-415 ENSDWI)
- Designing Cisco Enterprise Networks (300-420 ENSLD)
- Designing Cisco Enterprise Wireless Networks (300-425 ENWLSD)
- Implementing Cisco Enterprise Wireless Networks (300-430 ENWLSI)
- Implementing Automation for Cisco Enterprise Solutions (300-435 ENAUTO)

TIP CCNP Enterprise now includes automation and programmability to help you scale your enterprise infrastructure. If you pass the Developing Applications Using Cisco Core Platforms and APIs v1.0 (DEVCOR 350-901) exam, the ENCOR exam, and the Implementing Automation for Cisco Enterprise Solutions (ENAUTO 300-435) exam, you will achieve the CCNP Enterprise and DevNet Professional certifications with only three exams. Every exam earns an individual Specialist certification, allowing you to get recognized for each of your accomplishments instead of waiting until you pass all the exams.

There are no formal prerequisites for CCNP Enterprise. In other words, you do not have to pass the CCNA or any other certifications in order to take CCNP-level exams. The same goes for the CCIE exams. On the other hand, CCNP candidates often have 3 to 5 years of experience in implementation enterprise networking solutions.

The Exam Objectives (Domains)

The Implementing Cisco SD-WAN Solutions (ENSDWI 300-415) exam is broken down into six major domains. This book covers each of the domains and the subtopics included in them, as illustrated here. The following table lists the breakdown of each of the domains represented in the exam.

Domain	Percentage of Representation in Exam
1: Architecture	20%
2: Controller Deployment	15%
3: Router Deployment	20%
4: Policies	20%
5: Security and Quality of Service	15%
6: Management and Operations	10%
	Total 100%

Here are the details of each domain:

Domain 1: Architecture: This domain is covered in Chapters 1, 2, and 3.

1.1 Describe Cisco SD-WAN Architecture and Components

1.1.a Orchestration plane (vBond, NAT)

1.1.b Management plane (vManage)

1.1.c Control plane (vSmart, OMP)

1.1.c.(i) TLOC

1.1.c.(ii) vRoute

1.1.d Data plane (WAN Edge)

1.1.d(i) IPsec and GRE

1.1.d(ii) BFD

1.1.e Multi-Region Fabric

1.2 Describe Cisco SD-WAN Edge platforms and capabilities

1.3 Describe Cisco SD-WAN Cloud OnRamp

1.3.a SaaS

1.3.b IaaS

1.3.c Colocation

1.3.d Multicloud (Cloud and Interconnect)

Domain 2: Controller Deployment: This domain is covered primarily in Chapters 2 and 5.

2.1 Describe controller cloud deployment

2.2 Describe controller on-premises deployment

2.2.a Hosting platforms (Public and Private)

2.2.b Installing controllers

2.2.c Scalability and redundancy

2.3 Configure certificates and device lists

2.4 Troubleshoot control plane connectivity

Domain 3: Router Deployment: This domain is covered primarily in Chapters 3 and 4.

3.1 Describe WAN Edge deployment

3.1.a On-boarding (ZTP and Bootstrap)

3.1.b Data center and regional hub deployments

3.2 Configure Cisco SD-WAN data plane

3.2.a Circuit termination and TLOC-extension

3.2.b Dynamic Tunnels

3.2.c Underlay–overlay connectivity

3.3 Configure OMP

3.4 Configure TLOCs

3.5 Configure CLI and vManage feature configuration templates

3.5.a VRRP

3.5.b OSPF

3.5.c BGP

3.5.d EIGRP

3.6 Describe multicast support in Cisco SD-WAN

3.7 Describe configuration groups, feature profiles, and workflows

Domain 4: Policies: This domain is covered primarily in Chapters 6, 7, 8, 9, and 10.

4.1 Configure control policies

4.2 Configure data policies

4.3 Configure end-to-end segmentation

4.3.a VPN segmentation

4.3.b Topologies

4.4 Configure Cisco SD-WAN application-aware routing

4.5 Configure direct Internet access

Domain 5: Security and Quality of Service: This domain is covered primarily in Chapters 10 and 11.

5.1 Configure service insertion

5.2 Describe Cisco SD-WAN security features

5.2.a Application-aware enterprise firewall

5.2.b IPS

5.2.c URL filtering

5.2.d AMP

5.2.e SSL and TLS proxy

5.2.f TrustSec

5.3 Describe Cloud security integration

5.3.a DNS security

5.3.b Secure Internet Gateway (SIG)

5.4 Configure QoS treatment on WAN Edge routers

5.4.a Scheduling

5.4.b Queuing

5.4.c Shaping

5.4.d Policing

5.4.e Marking

5.4.f Per-tunnel and adaptive QoS

5.5 Describe Application Quality of Experience (App-QoE)

5.5.a TCP optimization

5.5.b Data Redundancy elimination (DRE)

5.5.c Packet duplication

5.5.d Forward error correction (FEC)

5.5.e AppNav

Domain 6: Management and Operations: This domain is covered primarily in Chapters 4, 13, and 14.

6.1 Describe authentication, monitoring, and reporting from vManage

6.2 Configure authentication, monitoring, and reporting

6.3 Describe REST API monitoring

6.4 Describe software image management from vManage

Steps to Passing the Implementing Cisco SD-WAN Solutions (ENSDWI 300-415) Exam

There are no prerequisites for the ENSDWI exam; however, students must have an understanding of implementing networking solutions.

Signing Up for the Exam

The steps required to sign up for the ENSDWI exam as follows:

Step 1. Create an account at https://home.pearsonvue.com/cisco.

Step 2. Complete the Examination Agreement, attesting to the truth of your assertions regarding professional experience and legally committing to adhering to the testing policies.

Step 3. Submit the examination fee.

Facts About the Exam

The ENSDWI 300-415 exam is a 90-minute exam. It is a computer-based test that consists of multiple-choice questions only. You must bring a government-issued identification card. No other forms of ID will be accepted.

TIP Refer to the Cisco Certification site at https://cisco.com/go/certifications for more information regarding this and other Cisco certifications.

About This Book

This book maps directly to the topic areas of the ENSDWI exam and uses a number of features to help you understand the topics and prepare for the exam.

Objectives and Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, 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. This book does not try to help you pass the exam only by memorization; it seeks to help you to truly learn and understand the topics. This book is designed to help you pass the Implementing Cisco SD-WAN Solutions (ENSDWI 300-415) exam by using the following methods:

- Helping you discover which exam topics you have not learned thoroughly enough
- Providing explanations and information to fill in your knowledge gaps
- Supplying review questions 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 on the companion website

Book Features

To help you customize your study time using this book, each chapter has several features that help you make the best use of your time:

- **Review All Key Topics:** The Key Topic icon appears next to the most important items in the chapter. The "Review All Key Topics" activity near the end of the chapter lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so you should review these.
- **Define Key Terms:** This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the glossary at the end of the book.
- **Review Questions:** Confirm that you understand the content you just covered by answering these questions and reading the answer explanations.

In addition, the companion website includes the Pearson Cert Practice Test engine, which allows you to answer practice exam questions. Use it to prepare with a sample exam and to pinpoint topics where you need more study.

How This Book Is Organized

This book contains 14 chapters, each of which covers a subset of the topics on the Implementing Cisco SD-WAN Solutions (ENSDWI 300-415) exam. The chapters map to the ENSDWI topic areas and cover the concepts and technologies that you will encounter on the exam.

Here's a brief summary of each chapter:

- **Chapter 1, "Introduction to Cisco Catalyst SD-WAN,"** provides an introduction to software-defined networking, controllers, and automation. This chapter also covers the benefits and value of automating management and operations.
- **Chapter 2, "Cisco Catalyst SD-WAN Components,"** provides an introduction to the SD-WAN components, including the various controllers, as well as the various types of deployment models. The chapter also introduces the control plane, data plane, and cloud integration.
- **Chapter 3, "Control Plane and Data Plane Operations,"** covers Overlay Management Protocol (OMP) and how it works to facilitate the orchestration of the control plane and ultimately influences the data plane. This chapter also covers how a secure data plane is constructed with IPsec. As with all routing protocols, there needs to be a loop-prevention mechanism, and this chapter discusses the various types of loop prevention within OMP.
- **Chapter 4, "Onboarding and Provisioning,"** covers how to provision data plane devices, either manually or via plug and play/zero-touch provisioning. It also discusses using templates as a means of gaining flexibility and scalability with configuration management.

- **Chapter 5, "Cisco Catalyst SD-WAN Design and Migration,"** covers the methodology behind SD-WAN design across the enterprise. This chapter also discusses preparation for SD-WAN migration, data center design, and branch design, as well as overlay and underlay routing integration.
- **Chapter 6, "Introduction to Cisco Catalyst SD-WAN Policies,"** covers the basics of Cisco SD-WAN policies, including the different types of policies, how policies are constructed, and how policies are applied to the Cisco SD-WAN fabric.
- **Chapter 7, "Centralized Control Policies,"** covers centralized control policies, which are used to manipulate or filter OMP updates in order to manipulate the structure and forwarding patterns in the Cisco SD-WAN fabric. This chapter also covers packet loss recovery techniques, including Forward Error Correction and packet duplication. It also provides a series of use cases that solve for different business requirements.
- **Chapter 8, "Centralized Data Policies,"** covers centralized data policies that are used to manipulate or filter flows in the data plane and override the natural forwarding behavior that is propagated through OMP. This chapter provides a series of use cases that solve for different business requirements.
- **Chapter 9, "Application-Aware Routing Policies,"** covers app-route policies and how they can be used to ensure that traffic is forwarded across the SD-WAN fabric using links that meet a required service-level agreement (SLA).
- **Chapter 10, "Localized Policies,"** covers localized policies, including local route policies, access control lists (ACLs), and quality of service (QoS).
- **Chapter 11, "Cisco Catalyst SD-WAN Security,"** covers what SD-WAN security is and why it is relevant to your organization. This chapter also covers how to deploy Enterprise Firewall with Application Awareness, intrusion detection and prevention, URL filtering, advanced malware protection (AMP) and Threat Grid, DNS web layer security, cloud security, and SD-WAN Manager authentication and authorization.
- **Chapter 12, "Cisco Catalyst SD-WAN Cloud OnRamp,"** covers what Cisco SD-WAN Cloud OnRamp is and how it can optimize your organization's application experience. This chapter also covers how to deploy OnRamp for SaaS, OnRamp for Multicloud, and SD-WAN Cloud Interconnect.
- **Chapter 13, "Cisco Catalyst SD-WAN Programmability,"** covers features and functionality of Cisco Catalyst SD-WAN APIs and using Python with Catalyst SD-WAN APIs such as REST. Finally, this chapter covers using infrastructure as code (IaC) tools such as Terraform and Ansible.
- **Chapter 14, "Cisco Catalyst SD-WAN Monitoring and Operations,"** covers SD-WAN Manager tools for monitoring the entire SD-WAN overlay and its individual components as well as troubleshooting tools to verify and troubleshoot SD-WAN operations in the SD-WAN fabric. It also discusses monitoring your SD-WAN fabric with ThousandEyes and provides an overview of SD-WAN Analytics.

- **Appendix A, "Answers to Chapter Review Questions,"** provides the answers to the review questions at the end of each chapter.
- The **Glossary of Key Terms** provides definitions for the key terms in each chapter.

The Companion Website for Online Content Review

All the electronic review elements, as well as other electronic components of the book, are available 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 www.ciscopress.com and register your book.

To do so, simply go to www.ciscopress.com/register and enter the ISBN of the print book: 9780138313906. 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.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title, please visit ciscopress.com/support. Our customer service representatives will assist you.

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:

- You can get your access code by registering the print ISBN (9780138313906) 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.
- 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 ciscopress.com click Account to see details of your account, and click the digital purchases tab.

NOTE After you register your book, your code can always be found in your account under the Registered Products tab.

Once 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 for both 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 pearsontestprep.com, log in using the same credentials used to register your book or purchase the Premium Edition, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

Customizing Your Exams

Once you are in the exam settings screen, you can choose to take exams in one of three modes:

- **Study mode:** This mode allows you to fully customize your exams and review answers as you are taking an exam. This is typically the mode you use to assess your knowledge and identify information gaps.
- **Practice Exam mode:** This mode locks certain customization options in order to present a realistic exam experience. Use this mode when you are preparing to test your exam readiness.
- **Flash Card mode:** This mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation, when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes do, so you should not use it if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters, or you can narrow your selection to just a single chapter or the chapters that make up a specific part of the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The two online exams that accompany this book are available to you, as are two additional exams of unique questions. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time you are allotted to take the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number

of correct answers for multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions for which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software while connected to the Internet, it checks whether there are any updates to your exam data and automatically downloads any changes made since the last time you used the software.

Sometimes, for many possible reasons, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams. To update a particular exam that you have already activated and downloaded, simply click the Tools tab and click the Update Products button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Windows desktop version of the Pearson Test Prep exam engine software and ensure that you are running the latest version of the software engine, simply click the Tools tab and click the Update Application button.

CHAPTER 2

Cisco Catalyst SD-WAN Components

This chapter covers the following topics:

- **Data Plane:** This section discusses the physical and virtual routers that actually carry data traffic.
- **Management Plane:** This section introduces the component that handles most of the day-to-day tasks in managing the Cisco Catalyst SD-WAN fabric.
- **Control Plane:** This section covers the component that handles all policies and routing.
- **Orchestration Plane:** This section introduces the component that facilitates discovery, authentication, and facilitation of the fabric.
- **Multi-tenancy Options:** This section introduces the various multi-tenancy options available in Cisco Catalyst SD-WAN.
- **Deployment Options:** This section covers the various deployment options, including Cisco cloud, private cloud, and on-premises deployments.

This chapter introduces the various components that make up the Cisco Catalyst SD-WAN architecture as well as the various deployment options. At a high level, these components can be grouped based on the purpose they play in Cisco Catalyst SD-WAN:

- Data plane
- Management plane
- Control plane
- Orchestration plane

In traditional networks, the management plane, data plane, and control plane are all on the same router, and together they facilitate communication within the network. A traditional router has network interfaces and line cards (which handle forwarding of data packets); this is a data plane. A CPU module, which handles calculating a routing table and advertising networks to the rest of the network, is a control plane, and the command-line interface (CLI) that is used to configure the router is a management plane. At the CLI, you type commands, and those commands program the CPU and line cards to act on your intent. Each router in a network has these three components.

A traditional network has a number of routers, each of which needs to be programmed independently to achieve the desired operational state of the network. As networks get larger, the

amount of human intervention required to configure the environment dramatically increases, potentially creating complexity. Each router must calculate its own routing table from its perspective of the network. For example, suppose you have a network with 6000 routes. Whenever there is a change in the network, each router may potentially have to process routing updates for each of these routes. This means the router must have the available CPU and memory required to process these updates, and this creates a lot of overhead. Tuning the routing table on a network with a large number of sites and routes—whether the network is full mesh, hub and spoke, partial mesh, and so on—can quickly become very complex. In addition, because each router is programmed individually, when you program the network on a router-by-router basis, you run the risk of undesired results due to improper design or human error on the CLI.

Cisco Catalyst SD-WAN is a distributed architecture that provides a clear separation between the management plane, control plane, and data plane. Figure 2-1 illustrates how the components fit into the architecture.

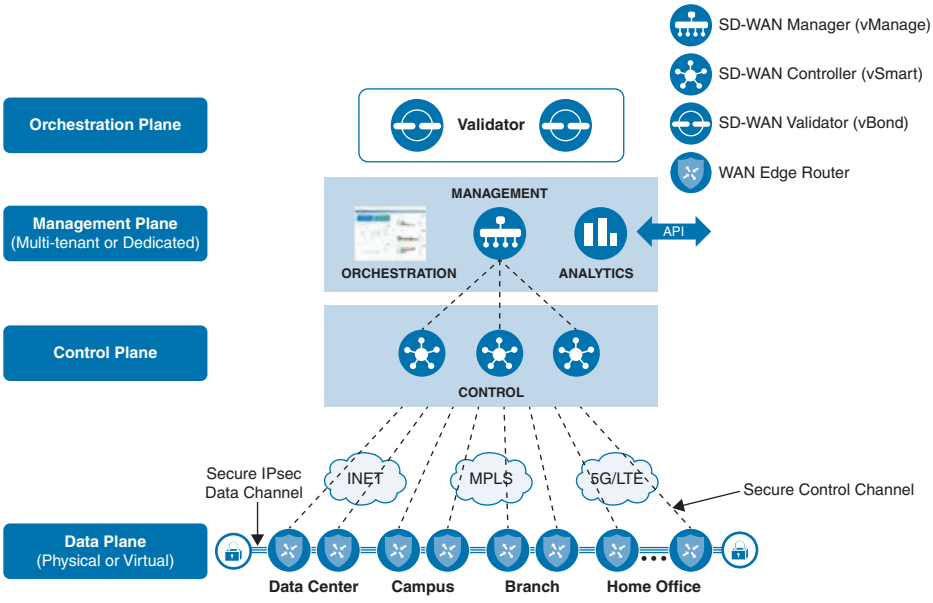


Figure 2-1 *Cisco Catalyst SD-WAN Distributed Architecture*

Key Topic

The Cisco Catalyst SD-WAN distributed architecture differs from traditional network architectures in that it allows you to support large-scale networks while reducing operational and computational overhead. Catalyst SD-WAN separates the data plane, the control plane, and the management plane from each other.

Because the control plane knows about all routes and nodes on the network, you have to calculate the routing table only once and can distribute the information to all the necessary nodes as a single routing update rather than have every router send routing updates to the others, with each determining its own Routing Information Base (RIB). This greatly reduces the overhead on the network and enables you to reduce required resources on the routers

so that you can bring additional features and capabilities to your edge devices. Because you have a complete view of the network, you can create a common network policy across the entire SD-WAN fabric—and the management plane needs to program it only once. As new devices are added to the network, they receive the same policy as well, ensuring that the network is operating as expected. This book shows how you can create various topologies and policies with ease while increasing scale and capability.

NOTE In 2023 Cisco SD-WAN was rebranded as Cisco Catalyst SD-WAN. In addition, starting with Cisco Catalyst SD-WAN Release 20.12, the following component changes apply:

- Cisco vManage is now Cisco Catalyst SD-WAN Manager.
- Cisco vAnalytics is now Cisco Catalyst SD-WAN Analytics.
- Cisco vBond is now Cisco Catalyst SD-WAN Validator.
- Cisco vSmart is now Cisco Catalyst SD-WAN Controller.
- Cisco SD-WAN Controllers (vManage, vSmart, and vBond together) are now Cisco Catalyst SD-WAN Control Components.

This change is reflected in the GUI and the official documentation. However, because the older names are more familiar to customers and are used in the ENSDWI certification exam, this book uses the new names but reminds you of the old names where appropriate.

Data Plane

Traditionally, the data plane has been composed of the physical interfaces that the physical layer plugs into (for example, Ethernet, fiber, serial). As mentioned previously, this is analogous to the line cards on routers and switches. In Cisco Catalyst SD-WAN, the data plane consists of WAN Edge devices, which could be Cisco IOS XE SD-WAN routers or legacy Cisco vEdge routers. Data plane devices may be deployed at branches, data centers, large campuses, colocation facilities, or in the cloud. At each site, you can have a single WAN Edge router or multiple WAN Edge routers, depending on your redundancy requirements.

The data plane is where the SD-WAN overlay resides and is the layer that forwards user, server, and other network traffic. Both IPv4 and IPv6 are supported for transport within the data plane. In addition, data policies (such as QoS and Application-Aware Routing) are enforced within the data plane.

Each WAN Edge router forms data plane connections to other WAN Edge routers within the SD-WAN overlay for the purposes of transporting user traffic. Data plane connections are only established between data plane devices. These tunnels are typically secured via Internet Protocol Security (IPsec). As described previously, the data plane has native segmentation. The segmentation information is encapsulated as defined in RFC 4023 and is carried across the SD-WAN overlay. Segmentation allows the network administrator to build separate instances of the data plane, depending on business requirements and regulations. The original data packets are typically encapsulated with IPsec, providing encryption and authentication.

Cisco Catalyst SD-WAN supports GRE as another method of data encapsulation. GRE provides less overhead but lacks all the security that IPsec provides, and it is used less often. Throughout this book, you can assume that IPsec encapsulation is being used unless noted otherwise.

Figure 2-2 illustrates the Cisco Catalyst SD-WAN packet structure.

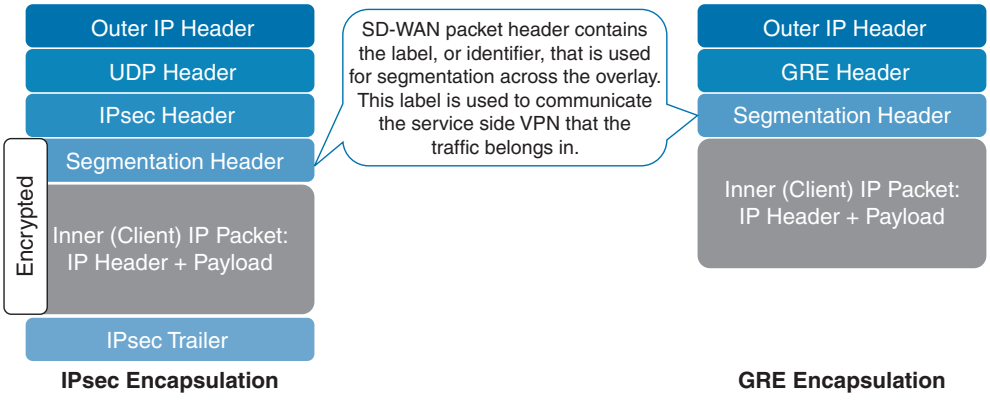


Figure 2-2 *Cisco Catalyst SD-WAN Packet Format*

Cisco Catalyst SD-WAN can support diverse topologies that are unique to each VPN segment or data plane instantiation. These VPN segments are completely isolated from communicating with each other unless policy explicitly allows communication. These VPNs are carried in a single IPsec tunnel. For example, corporate users could have a full-mesh topology, while PCI or HIPAA requirements could dictate the use of a hub-and-spoke topology for other devices. Figure 2-3 provides a graphical representation of this concept.

On the LAN, or service, side, the data plane supports OSPF, EIGRP, RIPv2, and BGP for routing protocols. For smaller locations that don't utilize a routing protocol, VRRP is supported to provide first-hop gateway redundancy.

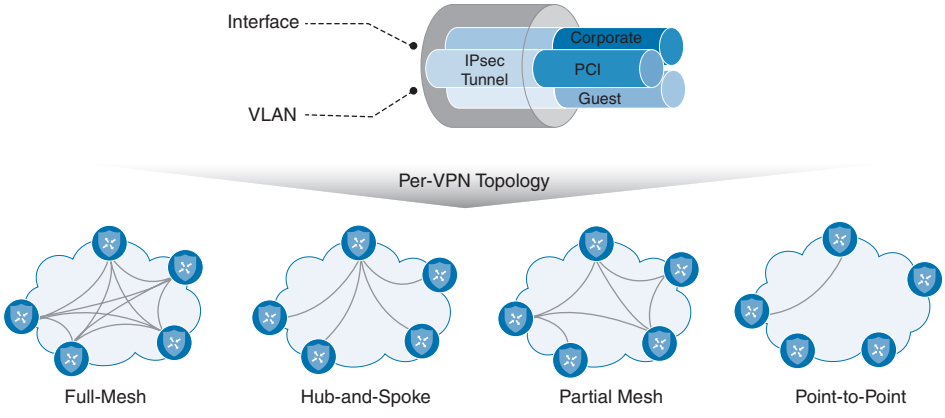


Figure 2-3 *Segmentation and Per-VPN Topologies*

NOTE In Cisco Catalyst SD-WAN, Virtual Private Networks (VPN) are synonymous with Virtual Routing and Forwarding (VRF) instances from a generic routing perspective. VRF instances and VPNs provide a method to separate the control and data planes into different logical parts. Segmentation in the data plane is accomplished by building multiple isolated routing table instances and binding specific interfaces to those instances.

WAN Edge routers have built-in security to prevent unauthorized access from the network. The WAN-facing interfaces only allow connections from authenticated SD-WAN fabric components, such as SD-WAN Manager (formerly vManage) and SD-WAN Controllers (formerly vSmarts) and from other WAN Edge devices in the fabric (as learned from SD-WAN Controllers). For the rest of the traffic, the WAN-facing interface firewall on the WAN Edge router, by default, will block everything coming in from the outside that isn't allowed explicitly; this is also called an "implicit ACL." By default, a WAN Edge router only allows inbound DHCP, DNS, ICMP, and HTTP services. Other inbound services that can be enabled are SSH, NETCONF, NTP, OSPF, BGP, SNMP, and STUN.

NOTE If a connection is initiated from a WAN Edge device and network address translation (NAT) is enabled on the WAN interface (for example, if Direct Internet Access is configured), return traffic is allowed by the NAT entry even if the implicit ACL has been configured as **no allow-service**. You can still block this traffic with an explicit ACL, as you will discover in later chapters.

Bidirectional Forwarding Detection (BFD) is used inside IPsec tunnels between all WAN Edge routers. BFD sends Hello packets to measure link liveness as well as packet loss, jitter, and delay. Each WAN Edge router makes its own determination about how to react to this BFD information. Depending on the policy defined by the management plane, routing across the data plane could be adjusted, such as having applications prefer one transport over the other, depending on the transport performance. BFD operates in echo mode, which means the neighbor doesn't actually participate in the processing of the BFD packet; instead, the BFD packet is simply echoed back to the original sender. This greatly reduces the impact on the CPU, as the neighbor doesn't need to process the packets. However, if the neighbor was involved in the processing of the BFD packets, and the remote neighbor's CPU were busy with some other processing, there could be potential delay in responding to the BFD packet. By eliminating this, you can reduce outage detection time and improve user experience. BFD cannot be turned off, but timers can be tuned in the SD-WAN fabric to identify and illicit a response to potential issues more quickly. Another advantage of using echo mode is that the original packet is echoed back to the original sender, and from this information, the WAN Edge router has a complete round-trip view of the transport.

When the WAN Edge router initially gets connected to the network and has no configuration present, it first tries to reach out to a Plug and Play (PNP) or Zero-Touch Provisioning (ZTP) server. Figure 2-4 provides a high-level overview of the PNP/ZTP process. This process will be discussed further in Chapter 4, "Onboarding and Provisioning," but for now, you just need to know that this is the process in which the router connects to the orchestration plane, learns about all of the various components in the network, and receives its configuration. Once the control plane is established, the last step is to build data plane connections to all other WAN Edge routers. By default, a full-mesh topology will be built, though policy

can be built to limit data plane connections and influence the routing topology. It should be noted, as well, that if PNP or ZTP isn't available, there are other options available to manually bootstrap the configuration using the CLI or a USB thumb drive.

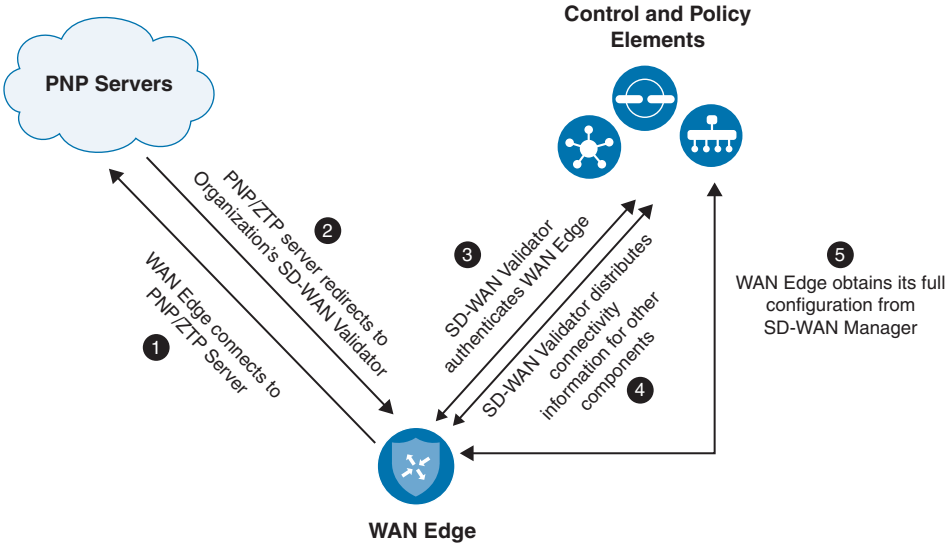


Figure 2-4 *High-Level Overview of the PNP/ZTP Process*

NOTE There are two auto-provisioning methods for WAN Edge devices: PNP for Cisco IOS-XE Catalyst SD-WAN routers and ZTP, originally developed for Cisco vEdge routers. While the processes are quite similar, they rely on two different services. Both services are cloud based, but there's also an on-premises deployment option for ZTP that supports both device types. On-premises deployment can help in scenarios where Internet access is not available or local hosting of the PNP functionality is desirable.

SD-WAN Supported Platforms

Key Topic

Cisco offers the wide selection of platforms and appliances so that you can deploy SD-WAN anywhere, as illustrated in Figure 2-5. With Cisco Catalyst SD-WAN, you can create a comprehensive fabric and scale your entire network into hybrid and multicloud environments with ease.

In the ever-evolving landscape of networking, keeping up with product offerings can be challenging. At this writing, the leading Cisco Catalyst SD-WAN hardware platforms include Cisco Catalyst 8500, 8300, and 8200 Series Edge platforms, along with Cisco 1100 Series Integrated Services Routers (ISRs). Cisco Catalyst SD-WAN can also be deployed on SD-Branch solutions such as the Catalyst 8200 Series Edge uCPE and Cisco 5000 Enterprise Network Compute System (ENCS) using Network Functions Virtualization (NFV).

While Cisco Catalyst SD-WAN remains compatible with earlier hardware generations, like Cisco 4000 Series ISRs, Cisco Advanced Services Routers (ASRs), and original vEdge routers, it is important to note that these platforms are at different stages of their end-of-life lifecycle. Consequently, they are not recommended for new deployments.

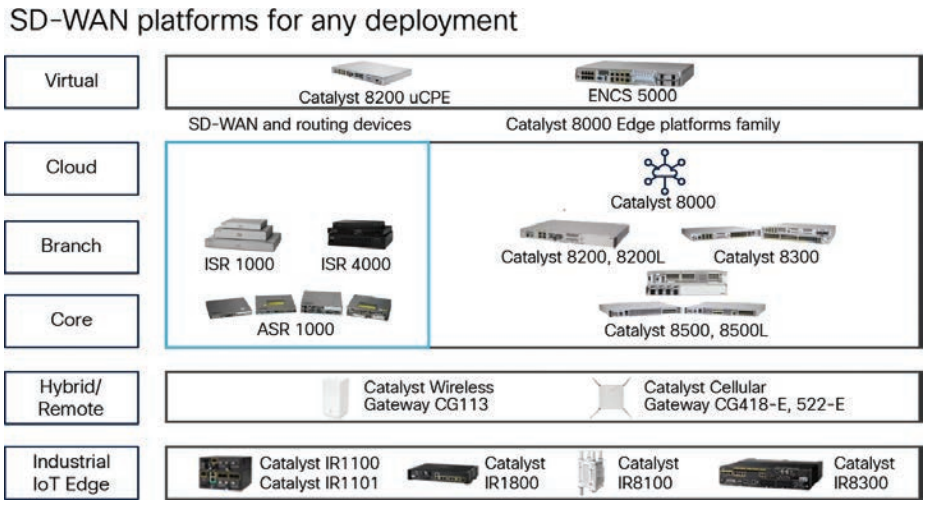


Figure 2-5 *Cisco Catalyst SD-WAN Supported Platforms*

A noteworthy feature of Cisco Catalyst SD-WAN is its seamless integration with public cloud environments, made possible through the Cisco Catalyst 8000V Edge Software and the legacy Cloud Services Router 1000V Series virtual platforms. Deployments in Amazon Web Services, Google Cloud, and Microsoft Azure are supported, offering flexibility and scalability. Virtual platforms can also be deployed in private clouds, running on either VMware ESXi or KVM hypervisors.

When deciding on WAN Edge platform, it's crucial to assess your specific requirements, including deployment type (physical or virtual), throughput needs, data plane tunnel scalability (such as the number of branches the router will communicate with), and the required interface types.

NOTE Information about the Cisco Catalyst SD-WAN platform is accurate as of this writing. For the most current details, please consult the Cisco Catalyst SD-WAN home page or refer to the "SD-WAN Platforms" section in the Cisco Catalyst SD-WAN Solution Overview document on the Cisco documentation site.

NOTE While Cisco Catalyst SD-WAN continues to support the original Cisco Viptela vEdge hardware models, including vEdge 100, vEdge 1000, vEdge 2000, and vEdge 5000, it is imperative to acknowledge the announced end of life for these devices. (For specific milestones and dates, please consult the product end-of-sale and end-of-life announcements.) Consequently, software development for this platform is concluding, with Version 20.6 marking the final release of Cisco Catalyst SD-WAN that includes support for Cisco vEdge 100 and vEdge 1000 devices. Version 20.9 is the last release for Cisco vEdge 2000 and vEdge 5000 routers.

Given these changes, this book focuses on the Cisco IOS XE SD-WAN platforms. All functionalities and features are described as they are implemented on Cisco IOS XE devices. Throughout the book, examples exclusively use Cisco IOS XE commands and configuration syntax, unless explicitly stated otherwise.

Some of the most important features supported on Cisco Catalyst SD-WAN routers are for advanced security use cases. While accessing the Internet directly via a local Internet circuit might pose security risks at the branch, overlaying security on top of Cisco Catalyst SD-WAN enables safe implementation of new use cases such as Direct Internet Access (DIA) and Direct Cloud Access (DCA).

Direct Internet Access allows certain Internet-bound traffic (for example, Facebook traffic, YouTube traffic) to be forwarded from the branch directly to the Internet instead of being backhauled to data center via SD-WAN fabric. Direct Cloud Access enables cloud traffic (for example, Office365 traffic, Salesforce traffic, Box traffic, Google traffic) to be sent from the branch directly to the Internet or, optionally, backhauled to data centers based on path performance. Figure 2-6 illustrates these concepts.

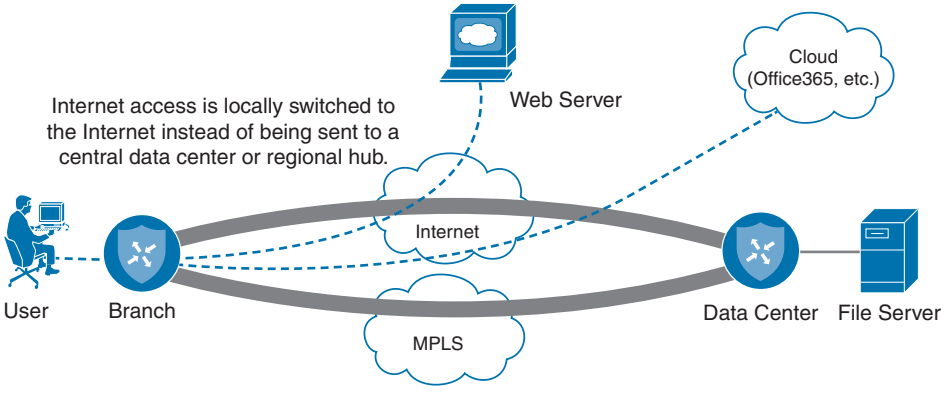


Figure 2-6 *Direct Internet Access/Direct Cloud Access Overview*

Security use cases are discussed in more detail in Chapter 11, "Cisco Catalyst SD-WAN Security," but here is a list of some of the currently supported security features:

- DNS security (Cisco Umbrella)
- Secure Internet Gateways (SIGs) and Cisco Secure Access integration
- Cisco Enterprise Firewall with Application Awareness
- Intrusion Prevention Systems (IPSs)
- URL Filtering
- Cisco Advanced Malware Protection
- SSL/TLS Proxy for Decryption of TLS Traffic

Traditionally, security requirements dictated centralization of the Internet access where all Internet traffic is backhauled to data centers, colocation, or regional sites. It was cost-effective to implement security at a central location rather than deal with the management and costs of disparate security components across many sites. With Cisco Catalyst SD-WAN security, businesses can now decentralize security functions, moving them to the branch

level. This movement allows organizations to offload Internet access at remote sites. Here are some other areas where a business might see benefits from DIA:

- Reduced bandwidth requirements and latency on costly WAN circuits
- Guest access
- Improved user experience to cloud SaaS and IaaS applications

Chapter 8, "Centralized Data Policies," discusses DIA in more detail.

When a WAN Edge router joins the fabric, it attempts to build control connections to SD-WAN Control Components across each transport deployed at that site. By default, if a transport doesn't have control connectivity to any of the SD-WAN Control Components, then it won't build a data plane connection across that transport either. This may be the case with cloud deployments where the controllers are in a public cloud and MPLS transport has no connectivity to the Internet.

NOTE There are a few options to still activate the data plane for a transport with no control connectivity. One option is to disable control connections on that transport via the **max-control-connections 0** command. Be aware that when control connections aren't established on an interface, there will be no control plane monitoring over that transport. You still have monitoring from a data plane perspective, however.

Management Plane

As mentioned previously, network devices of the past were managed individually via the CLI. Cisco Catalyst SD-WAN, however, introduces SD-WAN Manager (formerly vManage), which is a network management system (NMS) that provides a single pane of glass to manage Catalyst SD-WAN. SD-WAN Manager can be used for device onboarding, provisioning, policy creation, software management, troubleshooting, and monitoring.

While SD-WAN Manager offers a rich feature set, if the preference is to interface with it programmatically, SD-WAN Manager also supports communication via REST APIs. In fact, the SD-WAN Manager GUI is fully API driven, meaning that actions performed in it are executed using REST API calls. With full access to SD-WAN APIs, users can automate tasks, build scripts, and interface with SD-WAN Manager programmatically.

As you can see in Figure 2-7, SD-WAN Manager provides an intuitive and easy-to-consume dashboard. When you first log in to SD-WAN Manager, you are presented with an overview of the current state of the network.

vManage deployment options range from standalone nodes to three- or six-node clustered setups, offering enhanced scale and redundancy. A single SD-WAN Manager can potentially handle up to 1000 to 1500 devices, and a six-node SD-WAN Manager cluster may support more than 10,000 devices. It's important to note that these numbers may vary based on a number of factors, such as SD-WAN Manager resources (instances/CPU/RAM/storage), the statistics load, and the version of SD-WAN software in use. (Numbers mentioned in this chapter are specific to Version 20.12.) For more accurate specifications, please consult the "Recommended Computing Resources for Cisco Catalyst SD-WAN Control Components"

document for the SD-WAN software version you are using or are planning to use, available on the Cisco website.

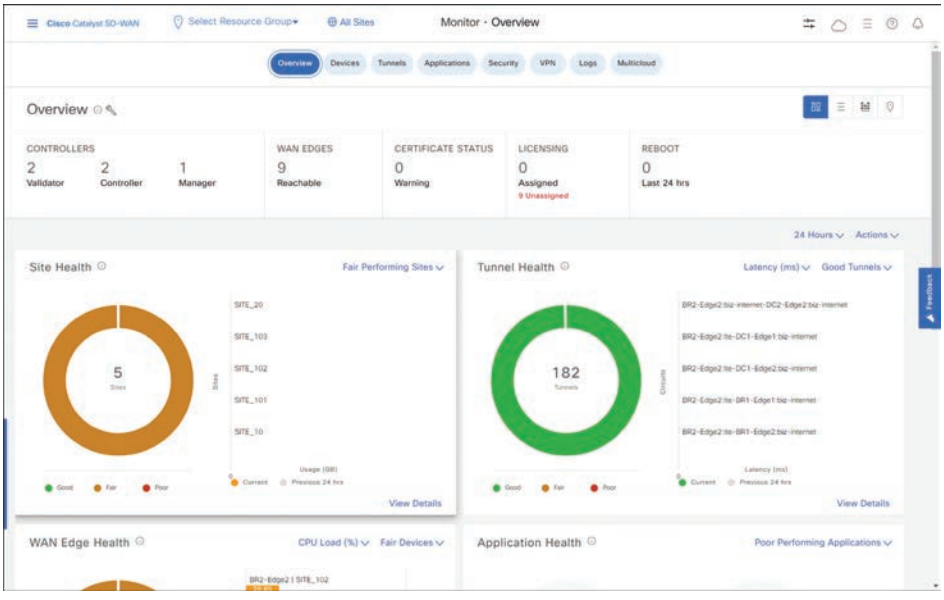


Figure 2-7 *Cisco SD-WAN Manager*

An SD-WAN Manager cluster is designed to tolerate the failure of a single server, but for high availability, a standby cluster should be implemented to handle a complete cluster failure. Typically, it is deployed in a geographically redundant location, such as a secondary data center in another region.

SD-WAN Manager can use multiple authentication sources, including RADIUS, TACACS, and SAML 2.0, for external user connectivity. By default, SD-WAN Manager is deployed in a single-tenant mode; however, if the requirements call for support of a service provider model, multi-tenancy may be used.

All configuration for the SD-WAN fabric should be performed via SD-WAN Manager in order to maintain consistency and scalability. As discussed further in Chapter 4, you can build device configurations in SD-WAN Manager via configuration groups, feature templates, or CLI templates. You can also configure policies to control things such as network topology, routing, QoS, and security in SD-WAN Manager. SD-WAN Manager is also where you perform troubleshooting and monitoring of the network. Network administrators can simulate traffic flows to show data paths, troubleshoot WAN impairment, analyze traffic flows in the network with Network-Wide Path Insights (NWPI), and access real-time operational information (such as routing tables) for all network devices. This greatly simplifies operations as there is no longer a need to log in to each WAN Edge router individually. Instead, troubleshooting can be accomplished via a single dashboard.

Each WAN Edge router forms a single management plane connection to SD-WAN Manager. If a device has multiple transports available, only one will be used for management plane connectivity to SD-WAN Manager. If a cluster is in place, the control connection will be load balanced across cluster nodes. If a transport hosting the management plane connection

experiences an outage, the WAN Edge router will briefly lose connectivity to SD-WAN Manager, and any changes made will be pushed when the device reconnects.

The last component in the management plane is SD-WAN Analytics (formerly vAnalytics). As shown in Figure 2-8, SD-WAN Analytics gives the network administrator predictive analytics to provide actionable insight into the WAN. With SD-WAN Analytics, the business can perform trending and capacity planning of circuits, and it can review how application performance is trending globally. With capacity planning, you can see how new applications may interact on your WAN before actually deploying them, allowing your business to right-size connectivity. SD-WAN Analytics ingests data from the network and uses machine learning to predict capacity trends. SD-WAN Analytics is cloud based, it requires additional licensing, and it is not enabled by default.

NOTE It is important to note that SD-WAN Manager should be used for a real-time, raw data view of the network, while SD-WAN Analytics should be used as a tool to review the historical performance of the network and get forward-looking insight into network adjustments.

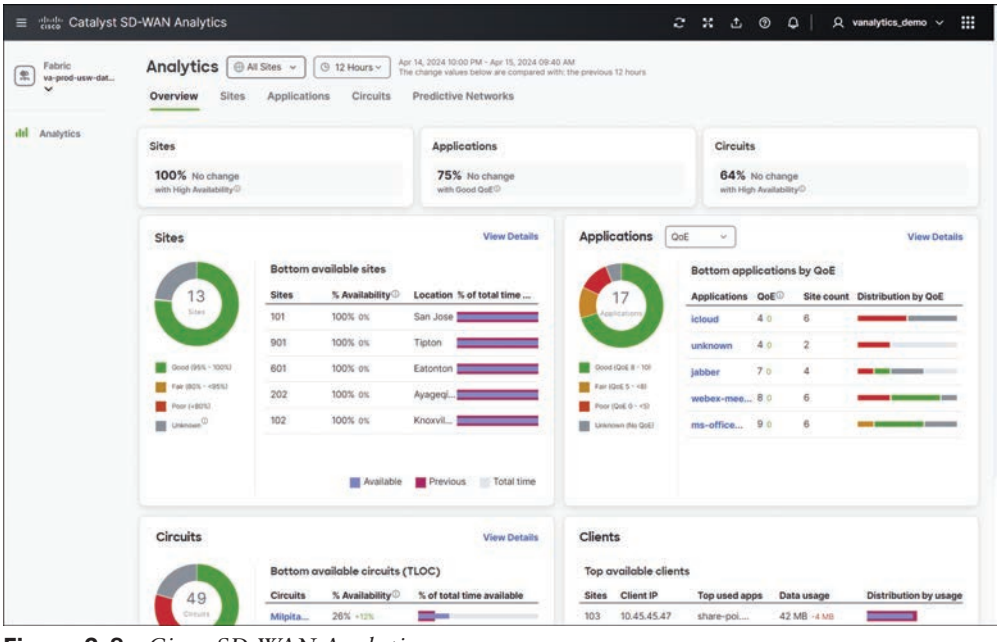


Figure 2-8 *Cisco SD-WAN Analytics*

Key Topic

Control Plane

Previously, you learned how the control plane has traditionally been separated from the data plane. SD-WAN Controller (vSmart) is the component that provides control plane functionality and is the brain of the SD-WAN fabric. It is highly scalable and can handle up to 5000 control connections per instance, with up to 12 SD-WAN Controllers in a single production deployment (as of SD-WAN Version 20.12). With these numbers, a deployment can support very large SD-WAN networks.

SD-WAN Controller is responsible for the implementation of control plane policies, centralized data polices, service chaining, and VPN topologies. It also handles key management, which is an important part in the security and encryption of the fabric.

Separating the control plane from the data and management planes allows a solution to achieve greater scale while simplifying network operations. With Cisco Catalyst SD-WAN, all SD-WAN Controllers learn all the routing information. Then they calculate the routing table and distribute it to the WAN Edge routers, taking into consideration applicable centralized control policies.

A WAN Edge router can connect to multiple SD-WAN Controllers at a time but needs connectivity to only one to get its routing and policy information.

The protocol that SD-WAN Controllers use to communicate all this information is called *Overlay Management Protocol (OMP)*. Although OMP handles routing, it would be a disservice to consider it simply a routing protocol. OMP is used to manage and control the overlay beyond just routing (key management, configuration updates, and so on). As illustrated in Figure 2-9, OMP runs between SD-WAN Controller and WAN Edge routers inside a secured tunnel. When a policy is built via the management plane, it is distributed to SD-WAN Controller via NETCONF, and SD-WAN Controller then distributes this policy via an OMP update to WAN Edge routers.

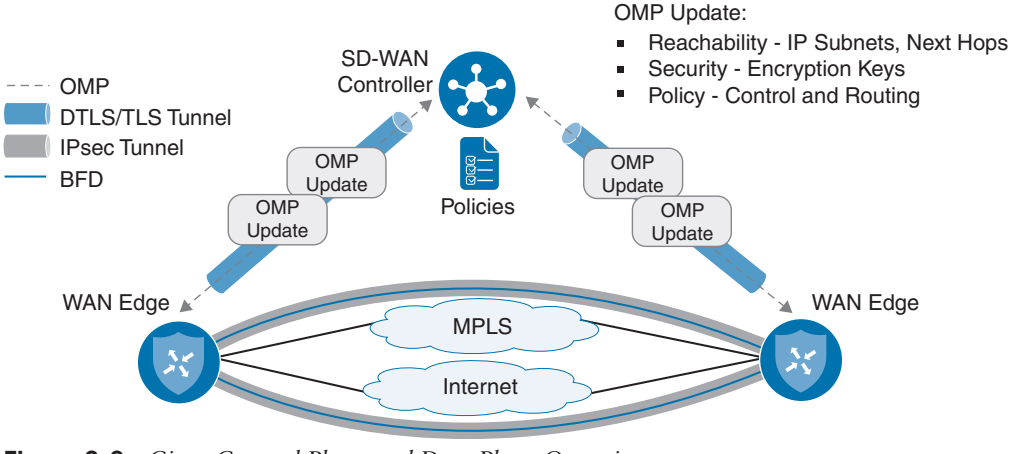


Figure 2-9 *Cisco Control Plane and Data Plane Overview*

SD-WAN Controller operates similarly to a BGP route reflector in iBGP. It receives routing information from each WAN Edge router and can apply policies before advertising this information back out to other WAN Edge routers. One example of these policies is the creation of distinct per-VPN topologies. To achieve it, the control policy is defined in SD-WAN Manager, which then distributes the policy through the management plane. Then, SD-WAN Controller applies the policy to the fabric. In this example, topology modification is achieved by manipulating what routes get distributed and how the data plane is built between WAN Edge routers.

NOTE Note that SD-WAN Controllers are only involved in control plane communication. SD-WAN Controllers help WAN Edge routers build the data plane but are never a part of the data plane and never forward data packets.

The control plane also plays an important role in the encryption of the fabric. In legacy WAN technologies, securing the network required a considerable amount of processing power, as each device would compute its own encryption keys per peer and distribute those keys to peers by using a protocol such as ISAKMP/IKE. For more efficient scaling in Cisco SD-WAN networks, key exchange and distribution have been moved to the SD-WAN Controller, and no IKE is implemented since identity has already been established between the WAN Edge routers and SD-WAN Control Components. Each WAN Edge router computes its own set of keys per transport and sends them to SD-WAN Controllers. SD-WAN Controllers then distribute them to each WAN Edge router, according to the defined policy. This process repeats when IPsec security associations (SAs) expire and new keys are generated. By moving the key exchange to a centralized location, you achieve greater scale as each WAN Edge router doesn't need to handle key negotiation or distribution. (Refer to Figure 2-9 for an overview of how the control and data planes are built.) Chapter 3, "Control Plane and Data Plane Operations," covers this in more detail.

If control connectivity has been established but has been lost due to an outage, data plane connectivity continues to work. By default, WAN Edge routers continue forwarding data plane traffic in the absence of control plane connectivity for up to 12 hours, utilizing the last-known state of the routing table, although this is configurable, depending on your requirements. When control plane connectivity is reestablished, WAN Edge routers are updated with any policy changes that were made during the outage. When the control connection is restored, the routing table is refreshed, and any stale routes are flushed.

For redundancy, it is the best practice to deploy at least two geographically dispersed SD-WAN Controllers. They should have identical policy configuration to ensure network stability. If these configurations differ, there's a risk of suboptimal routing and potential blackholing of traffic. SD-WAN Controllers maintain a full mesh of OMP sessions among themselves and exchange control and routing information, although each operates autonomously (that is, there is no database synchronized between them).

Figure 2-10 shows how OMP is established between multiple SD-WAN Controllers and WAN Edge routers. SD-WAN Controllers form a full mesh among themselves, which ensures that they stay synchronized. WAN Edge routers establish one OMP session to each of two (by default) SD-WAN Controllers, but they do not create OMP sessions with each other. When there are more than two SD-WAN Controllers in the network, their selection is based on an algorithm to ensure that load balancing occurs. In the event of the total failure of an SD-WAN Controller, the sessions are redistributed between the remaining SD-WAN Controllers to maintain network continuity and stability.

By default, each WAN Edge router establishes multiple secure control connections, one over each available transport, to each selected SD-WAN Controller. However, only one OMP session is established between the WAN Edge device and each SD-WAN Controller, using one of those control connections as a transport.

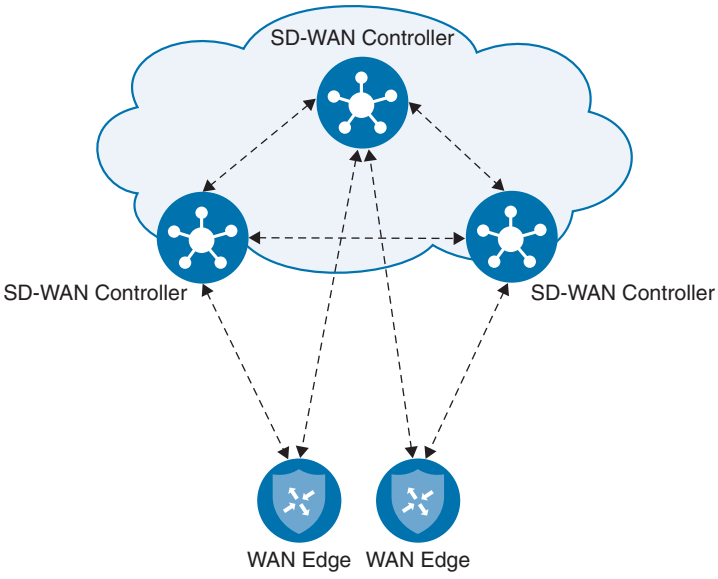


Figure 2-10 *OMP Session Establishment*

Key Topic

Orchestration Plane

The final, and probably the most important, component in Cisco Catalyst SD-WAN is SD-WAN Validator (formerly vBond). This component is very important because it provides initial authentication for participation in the fabric and acts as the glue that discovers and brings together all other components. Multiple SD-WAN Validator instances can be deployed to achieve high availability. Since a WAN Edge router can point to only a single SD-WAN Validator, it is recommended to configure WAN Edge routers to use a DNS name that has a single A record pointing to the IP addresses of all SD-WAN Validators. When the WAN Edge router tries to resolve the DNS record for the SD-WAN Validator, the DNS server provides multiple IP addresses for the hostname, and the WAN Edge router tries to connect to each of them sequentially until a successful control connection is made.

When a WAN Edge router first joins the overlay, the only thing it knows about the SD-WAN network is the IP address or DNS name of the SD-WAN Validator. It receives this information via one of these methods:

- PNP/ZTP
- Bootstrap configuration
- Manual configuration

The WAN Edge router attempts to build a temporary connection to the SD-WAN Validator over each transport. Once the control plane connectivity is up to SD-WAN Controller and SD-WAN Manager, the connection to the SD-WAN Validator is torn down. When the WAN Edge router connects to the SD-WAN Validator, they both go through an authentication process in which each component authenticates the other and, if successful, a Datagram Transport Layer Security (DTLS) tunnel is established. The SD-WAN Validator then distributes the connectivity information for the SD-WAN Controller and SD-WAN Manager to the WAN

Edge router. You can see why the SD-WAN Validator is referred to as the glue of the network: It tells all the components about each other. (This process is discussed in more detail in Chapters 3 and 4.)

One remaining functionality that the SD-WAN Validator provides is NAT traversal. By default, the SD-WAN Validator operates as a STUN server (RFC 5389). A WAN Edge router operates as a STUN client. What this means is that the SD-WAN Validator can detect when WAN Edge routers are behind a NAT device such as a firewall. When a WAN Edge router goes to establish its DTLS tunnel, the interface IP address it knows about is written into the outer IP header and noted within a payload of the message. When SD-WAN Validator receives this information, it compares the two values. If they are different, it can be inferred that NAT is in the transit path of the WAN Edge router (since the outer IP header was changed to a NAT IP address and no longer matches the IP address noted in the payload of the packet). The SD-WAN Validator communicates this back to the WAN Edge router, and the WAN Edge router can communicate this information to the rest of the overlay components—ultimately allowing data plane connectivity to be established through a NAT device. There are, however, some scenarios where this won't work, such as with symmetric NAT (as discussed in more detail in Chapters 3 and 4). Figure 2-11 explains how STUN is used to detect when a WAN Edge router or another SD-WAN Control Component is subject to NAT.

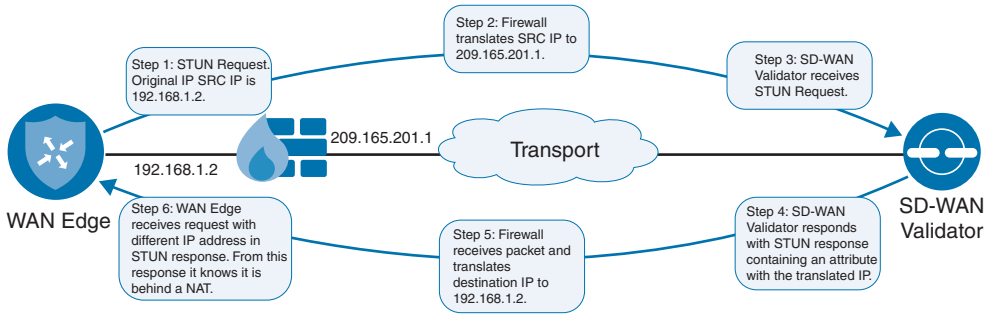


Figure 2-11 *STUN NAT Detection Method*

When deploying an SD-WAN Validator, one special consideration is that it must be reachable directly from all transports with enabled control connectivity. This implies that SD-WAN Validator needs a public IP address (or a private IP address with 1:1 static NAT) when Internet transports are used in SD-WAN fabric.

Other SD-WAN Control Components (including SD-WAN Managers and SD-WAN Controllers) can use private IP addresses as long as they have connectivity to SD-WAN Validator since they use the same NAT discovery method (STUN) as the WAN Edge routers.

Multi-tenancy Options

Cisco Catalyst SD-WAN supports multiple modes of segmentation in the control, data, management, and orchestration planes, as shown in Figure 2-12. One mode is dedicated tenancy. In this mode, each tenant has dedicated components, and the data plane is segmented as well. The second option is VPN tenancy. This mode segments only the data plane of the VPN topology and allows you to define read-only users who can view and monitor their VPN within SD-WAN Manager. VPN tenancy still shares the same SD-WAN components, however. The third option is multi-tenancy. With Cisco Catalyst SD-WAN multi-tenancy, a service provider can manage multiple customers, called tenants, from SD-WAN Manager.

The tenants share the same set of underlying SD-WAN Control Components: SD-WAN Manager, SD-WAN Validators, and SD-WAN Controllers. The tenant data is logically isolated on these shared SD-WAN Control Components. WAN Edge devices are typically tenant specific (that is, not shared), but service providers managing a multi-tenant SD-WAN deployment may deploy a multi-tenant WAN Edge device to serve as a shared gateway for traffic belonging to multiple tenants.

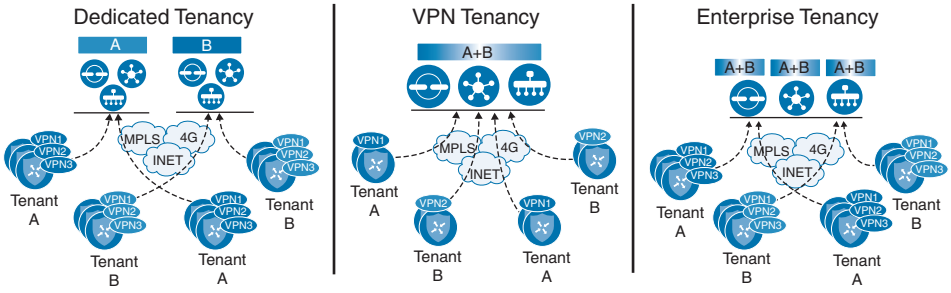


Figure 2-12 *Cisco Catalyst SD-WAN Multi-Tenancy Options*

Deployment Options

Cisco Catalyst SD-WAN supports multiple deployment options for SD-WAN Control Components:

- **Cisco cloud hosted:** This is the recommended and the most common deployment option, where Cisco builds, operates, and monitors all the SD-WAN Control Components introduced in this chapter. This greatly simplifies the deployment, allowing the network administrator to focus on the configuration and policy administration of the Cisco Catalyst SD-WAN fabric. Customers can manage their deployments through the Cisco Catalyst SD-WAN portal (https://ssp.sdwan.cisco.com), a cloud-infrastructure automation tool tailored for Cisco Catalyst SD-WAN. Using this portal, they can submit fabric provision requests, indicating the preferred cloud provider (AWS or Azure) and regions for hosting SD-WAN Control Components and data. The SD-WAN portal also offers additional functions, such as controller monitoring and fabric maintenance.
- **Managed service provider (MSP) or partner hosted:** SD-WAN Control Components are hosted in a private or public (AWS or Azure) cloud of an MSP or partner. The provider is responsible for provisioning of the SD-WAN Control Components and backups/disaster recovery.
- **On premises:** This option is suitable when business requirements dictate hosting SD-WAN Control Components in a traditional data center. With this approach, customers assume full responsibility for deploying, managing, and monitoring the SD-WAN Control Components. While it offers full control, customers must also manage the operations and maintenance of servers hosting these components. Another challenge is resource scaling, which is not as easy as with cloud-hosted solutions. On-premises deployment is particularly important for companies that are subject to strict regulations, such as those in the government, financial, healthcare, and utilities sectors.

- **Customer cloud hosted:** In this mix of previous options, SD-WAN Control Components are deployed in a public cloud (AWS or Azure), but customers are fully responsible for their deployment, management, and monitoring. Compared to on-premises hosting, customer cloud deployments have a low initial setup cost, as there is no need to purchase additional data center infrastructure. This option brings in traditional cloud benefits: ease of provisioning, stability, security, and scaling.

Summary

This chapter introduces the components that make up Cisco Catalyst SD-WAN. It discusses the data plane, wherein user traffic is routed and forwarded across the WAN. The data plane is similar to routers that would be deployed in a traditional WAN; in Cisco Catalyst SD-WAN, they are referred to as WAN Edge routers.

This chapter also introduces SD-WAN Manager, which is part of the management plane, where all Day 0, Day 1, and Day N functions are performed, including WAN Edge configuration, routing and control policies, troubleshooting, and monitoring.

You have seen that SD-WAN Controller, the brain of the Cisco Catalyst SD-WAN fabric, is responsible for calculating and deploying all control and data policies as well as handling the distribution of encryption keys for data plane connectivity.

You have also seen that SD-WAN Validator makes up the orchestration plane and is responsible for authenticating components on the fabric in addition to distributing control and management plane information to the WAN Edge routers. SD-WAN Validator is the component that aids in discovery of the fabric for all other components (such as when devices are behind NAT).

Finally, this chapter discusses deployment options. The most common deployment method is Cisco cloud hosted, but there are three other options to consider: on-premises, public cloud, and customer cloud hosted. By supporting all four deployment options, Cisco Catalyst SD-WAN can support all business requirements.

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 2-1 lists these key topics and the page number on which each is found.

Key Topic

Table 2-1 Key Topics

Key Topic Element	Description	Page
Figure 2-1	Cisco Catalyst SD-WAN distributed architecture	15
Section	Data plane	16
Section	Cisco Catalyst SD-WAN supported platforms	19
Section	Management plane	22
Section	Control plane	24
Section	Orchestration plane	27

Key Terms

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

control plane, data plane, management plane, orchestration plane, Overlay Management Protocol (OMP), SD-WAN Controller, SD-WAN Manager, SD-WAN Validator, WAN Edge

Chapter Review Questions

1. What are the three Cisco Catalyst SD-WAN Control Components? (Choose three.)
   - **a.** SD-WAN Controller
   - **b.** SD-WAN Validator
   - **c.** WAN Edge
   - **d.** SD-WAN Manager
   - **e.** SD-WAN Orchestrator
2. How does the Cisco Catalyst SD-WAN architecture differ from traditional WAN technologies? (Choose three.)
   - **a.** Single pane of glass
   - **b.** Increased scale with centralized control plane
   - **c.** Reduced uptime in branch locations
   - **d.** Topology dependence
   - **e.** Distributed architecture
3. What are the three functions of SD-WAN Manager in Cisco Catalyst SD-WAN?
   - **a.** Troubleshooting
   - **b.** Configuration
   - **c.** Redistribution
   - **d.** Loop prevention
   - **e.** Monitoring
4. True or false: WAN Edge routers provide data plane encryption via IPsec.
   - **a.** True
   - **b.** False
5. What traditional networking concept does SD-WAN Controller closely relate to?
   - **a.** OSPF designated router
   - **b.** DHCP helper
   - **c.** BGP route reflector
   - **d.** PIM designated router
6. What functions does SD-WAN Validator provide in the SD-WAN environment? (Choose two.)
   - **a.** Authentication and authorization of the SD-WAN components
   - **b.** NAT detection and traversal
   - **c.** Pushing configuration to WAN Edge routers
   - **d.** Software upgrades

7. True or false: Cisco Catalyst SD-WAN supports multi-tenancy.
   a. True
   b. False
8. Which routing protocols are not supported on the service side of Cisco Catalyst SD-WAN? (Choose two.)
   a. EIGRP
   b. OSPF
   c. RIPv1
   d. OMP
   e. BGP
9. What attributes are measured with BFD? (Choose three.)
   a. Delay
   b. Loss
   c. Jitter
   d. Out-of-order packets
10. True or false: Cisco Catalyst SD-WAN is able to provide segmentation and different topologies per VPN.
    a. True
    b. False
11. Which is not a valid option for the deployment of SD-WAN Control Components?
    a. Cisco cloud hosted
    b. Customer on premises
    c. Partner cloud hosted
    d. Cisco on premises

References

RFC 4023, "Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)," https://tools.ietf.org/html/rfc4023, March 2005.

RFC 5389, "Session Traversal Utilities for NAT (STUN)," https://tools.ietf.org/html/rfc5389, October 2008.

"Cisco Catalyst SD-WAN," https://www.cisco.com/site/us/en/solutions/networking/sdwan/index.html.

"SD-WAN Platforms," https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-sol-overview-cte-en.html#SDWANplatforms.

This page intentionally left blank

This page intentionally left blank

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z