



# Cisco Software-Defined Wide-Area Networks

Designing, Deploying and Securing  
Your Next Generation WAN with  
Cisco SD-WAN

**JASON GOOLEY**, CCIE® x2 (RS & SP) NO. 38759  
**DANA YANCH**, CCDE® NO. 20130071, CCIE (RS, DC) NO. 25567  
**DUSTIN SCHUEMANN**, CCIE® (RS) NO. 59235  
**JOHN CURRAN**

[ciscopress.com](http://ciscopress.com)

Foreword by **KHALID RAZA**, Founder/CTO Viptela

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



# Cisco Software-Defined Wide-Area Networks

## Special Offers

### **Save 70% on Complete Video Course**

Save 70% on Complete Video Course

The *CCNP and CCIE Enterprise Core ENCOR 350-401 Complete Video Course*, available for both streaming and download, provides you with hours of expert-level instruction mapped directly to exam objectives.

### **Save 80% on Premium Edition eBook and Practice Test**

*The Cisco Software-Defined Wide-Area Networks Premium Edition eBook and Practice Test* provides three eBook files (PDF, EPUB, and MOBI/Kindle) to read on your preferred device and an enhanced edition of the Pearson Test Prep practice test software. You also receive two additional practice exams with links for every question mapped to the PDF eBook.

**See the card insert in the back of the book for your Pearson Test Prep activation code and special offers.**

# Cisco Software-Defined Wide-Area Networks

---

## Designing, Deploying, and Securing Your Next Generation WAN with Cisco SD-WAN

Jason Gooley CCIE No. 38759

Dana Yanch, CCDE No. 20130071, CCIE No. 25567

Dustin Schuemann, CCIE No. 59235

John Curran

**Cisco Press**

221 River St.

Hoboken, NJ 07030 USA

# Cisco Software-Defined Wide-Area Networks

Jason Gooley  
Dana Yanch  
Dustin Schuemann  
John Curran

Copyright © 2021 Cisco Systems, Inc.

Published by:  
Cisco Press

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.

Library of Congress Control Number: 2020937215

ISBN-13: 978-0-13-653317-7

ISBN-10: 0-13-653317-5

## 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 author and are not necessarily those of Cisco Systems, Inc.

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose. All such documents and related graphics are provided “as is” without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services. The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screen shots may be viewed in full within the software version specified.

Microsoft® and Window® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. Screenshots and icons reprinted with permission from the Microsoft Corporation. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

## 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](mailto:corpsales@pearsoned.com) or (800) 382-3419.

For government sales inquiries, please contact [governmentsales@pearsoned.com](mailto:governmentsales@pearsoned.com).

For questions about sales outside the U.S., please contact [intlcs@pearson.com](mailto: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](mailto:feedback@ciscopress.com). Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

**Editor-in-Chief:** Mark Taub

**Alliances Manager, Cisco Press:**  
Makarand Chitale

**Director, Product Management:** Brett Bartow

**Managing Editor:** Sandra Schroeder

**Development Editor:** Christopher Cleveland

**Technical Editors:** Phil Davis, Aaron Rohyans

**Project Editor:** Lori Lyons

**Copy Editor:** Bart Reed

**Editorial Assistant:** Cindy Teeters

**Cover Designer:** Chuti Prasertsith

**Production Manager:** Aswini Kumar / codeMantra

**Composition:** codeMantra

**Indexer:** Tim Wright

**Proofreader:** Donna 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](http://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, CCFP, CCNA, CCNP, CCSP, CCOVP, 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, iQuickStudy, 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)

## About the Authors

**Jason Gooley, CCIE No. 38759 (RS and SP)**, is a very enthusiastic and spontaneous person who has more than 25 years of experience in the industry. Currently, Jason works as a Technical Evangelist for the Worldwide Enterprise Networking Sales team at Cisco Systems. Jason is very passionate about helping others in the industry succeed. In addition to being a Cisco Press author, Jason is a distinguished speaker at Cisco Live, contributes to the development of the Cisco CCIE and DevNet exams, provides training for Learning@Cisco, is an active CCIE mentor, is a committee member for the Cisco Continuing Education Program (CE), and is a program committee member of the Chicago Network Operators Group (CHI-NOG), [www.chinog.org](http://www.chinog.org). Jason also hosts a show called MetalDevOps. Jason can be found at [www.MetalDevOps.com](http://www.MetalDevOps.com), @MetalDevOps, and @Jason\_Gooley on all social media platforms.

**Dana Yanch, CCIE No. 25567 (RS,DC) CCDE No. 20130071**, at the time of writing content for this book was a Global Technical Solutions Architect at Cisco focused on designing and deploying SD-WAN solutions for large enterprises around the world. Prior to spending the last six years working with Viptela and other SD-WAN technologies, Dana had a focus on fabric-based data center technologies. Dana has presented at several Cisco Live Events worldwide and has a passion for public speaking and mentorship. Dana can now be found at Aviatrix, the multi-cloud networking platform, designing cloud connectivity architectures every single day. Dana can be found at [www.danayanch.com](http://www.danayanch.com) or @DanaYanch on Twitter.

**Dustin Schuemann, CCIE No. 59235 (R&S)**, is a Technical Solutions Architect at Cisco Systems. Within the Demo CoE organization, Dustin is a subject matter expert on all things SD-WAN, including development of SD-WAN demo offerings and CPOC labs for some of Cisco's largest customers. He has been a distinguished speaker at Cisco Live multiple times, where he has presented on multiple topics around Cisco SD-WAN. Dustin has more than 17 years of experience in the network engineering field, and before Cisco he was a network architect for multiple firms within the manufacturing and financial industries. He is very passionate about giving back to the IT community and helping to mentor other network engineers. Dustin currently resides in Raleigh, North Carolina. Dustin can be followed on Twitter as @dschuemann.

**John Curran** is a Technical Solutions Architect with Cisco's Global Virtual Engineering team, where he assists customers and partners with the design of their next-generation networks. John is a subject matter expert in routing and SD-WAN and is excited to spend time teaching and training on these topics. John presents regularly at Cisco Live events around the world and has been repeatedly recognized as a Distinguished Speaker. In his prior role at Cisco, John worked as a Network Consulting Engineer for Cisco's Advanced Services team, supporting government and education customers. John holds a Bachelor of Science degree in Computer Engineering Technology from the University of Cincinnati.

## About the Technical Reviewers

**Phil Davis, CCIE No. 2021**, is a Senior Systems Engineer with Aviatrix, specializing in cloud networking and security architecture. Phil has more than 25 years of experience in the industry and is a subject matter expert on SD-WAN. His background includes routing, switching, security, data center, and cloud networking, and he holds multiple certifications from Microsoft, VMware, Cisco, and Aviatrix. Phil has been instrumental in helping enterprise customers design and architect their networks while working for Cisco, VMware, and Viptela. Phil's current role at Aviatrix allows him to expand his work with enterprise customers and focus on their cloud and multi-cloud architectures. When Phil is not traveling all over the Midwest, he lives in Cincinnati, Ohio, with his beautiful wife, Karen, and their two wonderful children, Meredith and Max.

**Aaron Rohyans, CCIE No. 21945, CCNP**, is a Technical Marketing Engineer with Cisco Systems and has technical expertise in Cisco Security, Routing/Switching, as well as Unified Communications solutions. Aaron helps to drive the ~\$3B in annual routing revenue through various SD-WAN enablement activities such as competitive comparisons, technical evangelism (Cisco Live, roadshows), pre-sales deal support and sales acceleration (PoC/PoV, Customer Workshops, Training), and as a feedback liaison among field teams and product development.

## Dedications

### **Jason Gooley:**

This book is dedicated to my wife, Jamie, and my children, Kaleigh and Jaxon. I love you all more than anything! I also want to dedicate this book to my father and brother for always having my back. In addition, this book is dedicated to all the people who supported me over the years and all the candidates who are studying or trying to improve themselves through education.

### **Dana Yanch:**

This book is dedicated to James Winebrenner and Paul Ho, two of the best colleagues and mentors anyone could ask for. You have both championed me tirelessly and provided so many challenges for me to take on and succeed at over the past years. I look forward to building something new with you every single day. I also want to thank my friends and family for their patience and understanding for my being a complete ghost while working in this industry. It can be a bit addictive.

### **Dustin Schuemann:**

This book is dedicated to my lovely wife, Heather. Thanks for putting up with all my crazy projects such as this book. I promise I won't be taking on any more projects for at least a little while. I love you. I would also like to dedicate this book to my mother and father.

### **John Curran:**

This is dedicated to my wonderful wife, Rebecca, and my daughter, Grace. Thank you for your enduring support and unending encouragement throughout this process. I couldn't have done it without you. I love you both so very much.



## Acknowledgments

### Jason:

Thank you to Brett and Marianne Bartow as well as Chris Cleveland at Cisco Press! It's always a pleasure to work with such amazing and talented people!

Thank you to my team, Worldwide Enterprise Networking Sales, at Cisco for always supporting me through all the awesome projects I am fortunate enough to be a part of! #TeamGSD

Thank you to all the people who follow me on my journey, whether through social media or in person. You are much appreciated!

### Dana:

I would like to thank Ali Shaikh for being so patient with me during my early Viptela days. I am certain I asked hundreds of questions over the years and never once received an incomplete response from you. I would also like to thank Aaron Rohyans for providing such incredibly detailed information around Cloud onRamp for Colocation and both Aaron and Phil Davis for their incredible tech editing work.

### Dustin:

First off, I would like to thank my fellow authors, Jason, Dana, and John. We had a lot of laughs and a lot of stress throughout this project, but we got it done. Congratulations.

Secondly, I would also like to thank our tech editors, Aaron and Phil. I appreciate the feedback you provided, even if it was hard to swallow sometimes. Ultimately it made this a better book.

Thanks to the Demo CoE leadership team at Cisco. You've always supported me throughout all my endeavors. A special thank-you goes to my fellow teammates Steve Moore, Fish Fishburne, Paul Patrick, Christine Strom, and Gavin Wright. Now I can get back to work.

There are a few individuals who have helped with this book and various other projects throughout my career. I will always appreciate the support and willingness they've provided. A special thank-you to Brad Edgeworth, Mosaddaq Turabi, Ali Shaikh, Gina Cornett, Joe Astorino, Thomas Mckinnon, Tom Kunath, Fred Damstra, and Seth Lechlitner.

### John:

I would like to send a special thanks to Brent Colwell, Phil Davis, Dana Yanch, Ali Shaikh, and Larry Roberts for all of the help and training with Viptela across the years.

This project wouldn't have been possible without the support of the leadership of Cisco's Global Virtual Engineering team. In particular, special thanks to Henry Carmouche for saying "yes" to that first unreasonable request, Jeff Sweeney for helping this vision and many others become a reality, Femi Ajisafe for seeing this project through to completion, and John Ellis for all the support throughout these adventurous years.

A special thanks to Todd Osterberg, Jason Dumars, Shaker Nazer, and Brad Edgeworth. Each of you were always more than willing to take a chance on me, and I owe you each so much. I only hope that I will be able to pay it forward. Thank you.

## Contents at a Glance

	Introduction	xix
Chapter 1	Introduction to Cisco Software-Defined Wide Area Networking (SD-WAN)	1
Chapter 2	Cisco SD-WAN Components	25
Chapter 3	Control Plane and Data Plane Operations	43
Chapter 4	Onboarding and Provisioning	91
Chapter 5	Introduction to Cisco SD-WAN Policies	109
Chapter 6	Centralized Control Policies	133
Chapter 7	Centralized Data Policies	227
Chapter 8	Application-Aware Routing Policies	285
Chapter 9	Localized Policies	319
Chapter 10	Cisco SD-WAN Security	349
Chapter 11	Cisco SD-WAN Cloud onRamp	393
Chapter 12	Cisco SD-WAN Design and Migration	459
Chapter 13	Provisioning Cisco SD-WAN Controllers in a Private Cloud	493
	Appendix A: Answers to Chapter Review Questions	527
	Appendix B: Example 7-17	539
	Glossary of Key Terms	553
	Index	557

## Reader Services

Register your copy at [www.ciscopress.com/title/9780136533177](http://www.ciscopress.com/title/9780136533177) for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to [www.ciscopress.com/register](http://www.ciscopress.com/register) and log in or create an account.\* Enter the product ISBN 9780136533177 and click Submit. When 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.

# Contents

	Introduction	xix
<b>Chapter 1</b>	<b>Introduction to Cisco Software-Defined Wide Area Networking (SD-WAN)</b>	<b>1</b>
	Networks of Today	1
	Common Business and IT Trends	4
	Common Desired Benefits	5
	High-Level Design Considerations	7
	Introduction to Cisco Software-Defined WAN (SD-WAN)	9
	Transport Independence	10
	Rethinking the WAN	12
	Use Cases Demanding Changes in the WAN	13
	Bandwidth Aggregation and Application Load-Balancing	13
	Protecting Critical Applications with SLAs	14
	End-to-End Segmentation	15
	Direct Internet Access	15
	Fully Managed Network Solution	16
	Building an ROI to Identify Cost Savings	17
	Introduction to Multidomain	18
	Cloud Trends and Adoption	19
	Summary	21
	Review All Key Topics	22
	Key Terms	22
	Chapter Review Questions	22
<b>Chapter 2</b>	<b>Cisco SD-WAN Components</b>	<b>25</b>
	Data Plane	27
	Management Plane	32
	Control Plane	34
	Orchestration Plane	36
	Multi-Tenancy Options	38
	Deployment Options	38
	Summary	39
	Review All Key Topics	39
	Key Terms	40
	Chapter Review Questions	40
	References	42

**Chapter 3 Control Plane and Data Plane Operations 43**

- Control Plane Operations 44
  - Overlay Management Protocol 47
  - OMP Routes* 48
  - TLOC Routes* 52
  - Service Routes* 54
  - Path Selection 56
  - OMP Route Redistribution and Loop Prevention 58
- Data Plane Operations 65
  - TLOC Colors 66
  - Tunnel Groups 70
  - Network Address Translation 73
    - Full Cone NAT* 74
    - Symmetric NAT* 75
    - Address Restricted Cone NAT* 76
    - Port Restricted Cone NAT* 77
  - Network Segmentation 81
  - Data Plane Encryption 83
    - Data Plane Encryption with Pairwise 86
- Summary 88
- Review All Key Topics 88
- Key Terms 89
- Chapter Review Questions 89
- References 90

**Chapter 4 Onboarding and Provisioning 91**

- Configuration Templates 93
- Developing and Deploying Templates 97
- Onboarding Devices 101
  - Manual Bootstrapping of a WAN Edge 102
  - Automatic Provisioning with PNP or ZTP 103
- Summary 105
- Review All Key Topics 106
- Chapter Review Questions 106
- References 107

**Chapter 5 Introduction to Cisco SD-WAN Policies 109**

- Purpose of Cisco SD-WAN Policies 109
- Types of Cisco SD-WAN Policies 110

Centralized Policy	110
<i>Centralized Policies That Affect the Control Plane</i>	111
<i>Centralized Policies That Affect the Data Plane</i>	112
Localized Policy	112
Policy Domains	113
Cisco SD-WAN Policy Construction	115
Types of Lists	118
Policy Definition	119
Cisco SD-WAN Policy Administration, Activation, and Enforcement	122
Building a Centralized Policy	122
Activating a Centralized Policy	125
Packet Forwarding Order of Operations	127
Summary	128
Review All Key Topics	129
Define Key Terms	129
Chapter Review Questions	129
<b>Chapter 6 Centralized Control Policies</b>	<b>133</b>
Centralized Control Policy Overview	134
Use Case 1: Isolating Remote Branches from Each Other	136
Use Case 1 Review	149
Use Case 2: Enabling Branch-to-Branch Communication Through Data Centers	149
Enabling Branch-to-Branch Communication with Summarization	150
Enabling Branch-to-Branch Communication with TLOC Lists	152
Use Case 2 Review	168
Use Case 3: Traffic Engineering at Sites with Multiple Routers	169
Setting TLOC Preference with Centralized Policy	171
Setting TLOC Preference with Device Templates	177
Use Case 3 Review	179
Use Case 4: Preferring Regional Data Centers for Internet Access	180
Use Case 4 Review	188
Use Case 5: Regional Mesh Networks	188
Use Case 5 Review	195
Use Case 6: Enforcing Security Perimeters with Service Insertion	195
Use Case 6 Review	202

Use Case 7: Isolating Guest Users from the Corporate WAN	202
Use Case 7 Review	206
Use Case 8: Creating Different Network Topologies per Segment	206
Use Case 8 Review	210
Use Case 9: Creating Extranets and Access to Shared Services	211
Use Case 9 Review	222
Summary	223
Review All Key Topics	223
Define Key Terms	224
Chapter Review Questions	224
Reference	226

## **Chapter 7 Centralized Data Policies 227**

Centralized Data Policy Overview	228
Centralized Data Policy Use Cases	228
Use Case 10: Direct Internet Access for Guest Users	230
<i>Use Case 10 Review</i>	242
Use Case 11: Direct Cloud Access for Trusted Applications	243
<i>Use Case 11 Review</i>	253
Use Case 12: Application-Based Traffic Engineering	253
<i>Use Case 12 Review</i>	260
Use Case 13: Protecting Corporate Users with a Cloud-Delivered Firewall	261
<i>Use Case 13 Review</i>	269
Use Case 14: Protecting Applications from Packet Loss	269
<i>Forward Error Correction for Audio and Video</i>	270
<i>Packet Duplication for Credit Card Transactions</i>	274
<i>Use Case 14 Review</i>	280
Summary	280
Review All Key Topics	281
Define Key Terms	282
Chapter Review Questions	282
References	284

## **Chapter 8 Application-Aware Routing Policies 285**

The Business Imperative for Application-Aware Routing	286
The Mechanics of an App-Route Policy	286
Constructing an App-Route Policy	287

Monitoring Tunnel Performance	294
Liveliness Detection	295
<i>Hello Interval</i>	295
<i>Multiplier</i>	297
Path Quality Monitoring	298
<i>App-Route Poll Interval</i>	298
<i>App-Route Multiplier</i>	300
Mapping Traffic Flows to a Transport Tunnel	304
Packet Forwarding with Application-Aware Routing Policies	304
<i>Traditional Lookup in the Routing Table</i>	305
<i>SLA Class Action</i>	306
Summary	315
Review All Key Topics	316
Define Key Terms	316
Chapter Review Questions	316
<b>Chapter 9 Localized Policies</b>	<b>319</b>
Introduction to Localized Policies	319
Localized Control Policies	320
Localized Data Policies	334
Quality of Service Policies	338
Step 1: Assign Traffic to Forwarding Classes	339
Step 2: Map Forwarding Classes to Hardware Queues	341
Step 3: Configure the Scheduling Parameters for Each Queue	341
Step 4: Map All of the Schedulers Together into a Single QoS Map	342
Step 5: Configure the Interface with the QoS Map	343
Summary	346
Review All Key Topics	347
Chapter Review Questions	347
<b>Chapter 10 Cisco SD-WAN Security</b>	<b>349</b>
Cisco SD-WAN Security: Why and What	349
Application-Aware Enterprise Firewall	352
Intrusion Detection and Prevention	360
URL Filtering	367
Advanced Malware Protection and Threat Grid	372

DNS Web Layer Security	377
Cloud Security	381
vManage Authentication and Authorization	384
Local Authentication with Role-Based Access Control (RBAC)	384
Remote Authentication with Role-Based Access Control (RBAC)	387
Summary	389
Review All Key Topics	389
Define Key Terms	389
Chapter Review Questions	389

**Chapter 11 Cisco SD-WAN Cloud onRamp 393**

Cisco SD-WAN Cloud onRamp	393
Cloud onRamp for SaaS	394
Cloud onRamp for IaaS	412
Cloud onRamp for Colocation	429
Why Colocation?	432
How It Works	432
Service Chaining for a Single Service Node	434
Service Chaining for Multiple Service Nodes	436
Service Chaining and the Public Cloud	436
<i>Infrastructure as a Service</i>	438
<i>Software as a Service</i>	438
<i>Redundancy and High Availability</i>	440
<i>Service Chain Design Best Practices</i>	440
Configuration and Management	442
<i>Cluster Creation</i>	442
<i>Image Repository</i>	449
<i>Service Chain Creation</i>	449
Monitoring	454
Summary	455
Review All Key Topics	456
Define Key Terms	456
Chapter Review Questions	456

**Chapter 12 Cisco SD-WAN Design and Migration 459**

Cisco SD-WAN Design Methodology	459
Cisco SD-WAN Migration Preparation	460



Cisco SD-WAN Data Center Design	462
Transport-Side Connectivity	463
Loopback TLOC Design	465
Service-Side Connectivity	466
Cisco SD-WAN Branch Design	469
Complete CE Replacement—Single Cisco SD-WAN Edge	470
Complete CE Replacement—Dual Cisco SD-WAN Edge	471
Integration with Existing CE Router	475
Integration with a Branch Firewall	476
Integration with Voice Services	478
Cisco SD-WAN Overlay and Underlay Integration	480
Overlay Only	480
Overlay with Underlay Backup	481
Full Overlay and Underlay Integration	485
Summary	490
Review All Key Topics	490
Chapter Review Questions	490
<b>Chapter 13 Provisioning Cisco SD-WAN Controllers in a Private Cloud</b>	<b>493</b>
SD-WAN Controller Functionality Recap	493
Certificates	496
vManage Controller Deployment	501
Step 1: Deploy vManage Virtual Appliance on VMware ESXi or KVM	503
Step 2: Bootstrap and Configure vManage Controller	506
Step 3/4: Set Organization Name and vBond Address in vManage; Install Root CA Certificate	506
Step 5: Generate, Sign, and Install Certificate onto vManage Controller	511
vBond Controller Deployment	513
Step 1/2/3: Deploy vBond Virtual Machine on VMware ESXi; Bootstrap and Configure vBond Controller; Manually Install Root CA Certificate on vBond	514
Step 4/5: Add vBond Controller to vManage; Generate, Sign, and Install Certificate onto vBond Controller	516
vSmart Controller Deployment	518

Step 1/2/3: Deploy vSmart Virtual Machine from Downloaded OVA;  
Bootstrap and Configure vSmart Controller; Manually Install Root CA  
Certificate on vSmart 519

Step 4/5: Add vSmart Controller to vManage; Generate, Sign, and Install  
Certificate onto vSmart Controller 520

Summary 523

Review All Key Topics 524

Define Key Terms 524

Chapter Review Questions 524

References 526

**Appendix A: Answers to Chapter Review Questions 527**

**Appendix B: Example 7-17 539**

**Glossary of Key Terms 553**

**Index 557**

## 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.

## Figure Credits

Cover image	Cisco Brand Exchange, Cisco Systems, Inc.
UNFIG11-01	© 2020, Amazon Web Services, Inc.
UNFIG11-02	Microsoft Azure, © 2020 Microsoft
UNFIG11-03	© 2020, Amazon Web Services, Inc.
UNFIG11-04	Microsoft Azure, © 2020 Microsoft
FIG13-10	VMWare Settings Window screenshot, © Microsoft 2020
FIG13-11	Add Hardware Wizard screenshot, © Microsoft 2020
FIG13-12	Create new virtual disk, screenshot, © Microsoft 2020

## Foreword

It's a great pleasure for me to write the foreword for the first complete guide to SD-WAN. Being the founder of Viptela (Cisco SD-WAN), I am delighted to read a really comprehensive work on SD-WAN. SD-WAN is one of the major disruptions wide area networks have seen since MPLS was created in the 90s.

Since SD-WAN requires people to understand both technology and implementations of the new age WAN, I feel this book will provide a great reference guide for the reader. The topics covered will benefit both the novice and expert reader. Because this book is structured to walk you through from basic principles to advanced topics, it can be used as a reference guide.

This book is written by a team of individuals who have been instrumental in deploying and testing the largest SD-WAN networks.

I would strongly recommend reading this comprehensive book on the Cisco SD-WAN networking technology.

**Khalid Raza, Founder/CTO Viptela**

## 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.

Implementing Cisco SD-WAN Solutions (ENSDWI 300-415) is a 90-minute exam.

**Tip** You can review the exam blueprint from Cisco’s website 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 SD-WAN concentration exam or 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 for you 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 three to five years of experience in implementing enterprise networking solutions.

## The Exam Objectives (Domains)

The Implementing Cisco SD-WAN Solutions (ENSDWI 300-415) exam is broken down into six major domains. The contents of this book cover each of the domains and the subtopics included in them as illustrated in the following descriptions.

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.d Data plane (vEdge)

1.1.d [i] TLOC

1.1.d (ii) IPsec

1.1.d (iii) vRoute

1.1.d (iv) BFD

1.2 Describe WAN Edge platform types, capabilities (vEdges, cEdges)

**Domain 2: Controller Deployment:** This domain is covered primarily in Chapter 13.

2.1 Describe controller cloud deployment

2.2 Describe controller on-prem deployment

2.2.a Hosting platform (KVM/hypervisor)

2.2.b Installing controllers

2.2.c Scalability and redundancy

2.3 Configure and verify certificates and whitelisting

2.4 Troubleshoot control plane connectivity between controllers

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

3.1 Describe WAN Edge deployment

3.1.a Onboarding

3.1.b Orchestration with Zero Touch Provisioning/Plug and Play

3.1.c Single/multi data center/regional hub deployments

3.2 Configure and verify SD-WAN data plane

3.2.a Circuit termination/TLOC-extension

3.2.b Underlay–overlay connectivity

3.3 Configure and verify OMP

3.4 Configure and verify TLOCs

3.5 Configure and verify CLI and vManage feature configuration templates

3.5.a VRRP

3.5.b OSPF

3.5.c BGP

**Domain 4: Policies:** This domain is covered primarily in Chapters 5, 6, 7, and 8.

4.1 Configure and verify control policies

4.2 Configure and verify data policies

4.3 Configure and verify end-to-end segmentation

4.3.a VPN segmentation

4.3.b Topologies

4.4 Configure and verify SD-WAN Application-Aware Routing

4.5 Configure and verify Direct Internet Access

**Domain 5: Security and Quality of Service:** This domain is covered primarily in Chapters 9 and 10.

5.1 Configure and verify service insertion

5.2 Describe application-aware firewall

5.3 Configure and verify QoS treatment on WAN Edge routers

5.3.a Scheduling

5.3.b Queuing

5.3.c Shaping

5.3.d Policing

**Domain 6: Management and Operations:** This domain is covered primarily in Chapters 4, 6, and 7.

6.1 Describe monitoring and reporting from vManage

6.2 Configure and verify monitoring and reporting

6.3 Describe REST API monitoring

6.4 Describe software upgrade 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:

1. Create an account at <https://home.pearsonvue.com/cisco>.
2. Complete the Examination Agreement, attesting to the truth of your assertions regarding professional experience and legally committing to the adherence of the testing policies.
3. Submit the examination fee.



## Facts About the Exam

The exam is a computer-based test. The exam 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 *Cisco Software-Defined Wide-Area Networks: Designing, Deploying, and Securing Your Next-Generation WAN with Cisco SD-WAN*

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 mastered
- 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, the core chapters have 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.
- **Web-based Practice Exam:** 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 13 core chapters—Chapters 1 through 13. Each core chapter covers a subset of the topics on the Implementing Cisco SD-WAN Solutions (ENSDWI 300-415) exam. The core 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 Software-Defined Wide Area Networking (SD-WAN),”** covers 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 SD-WAN Components,”** covers an introduction to the SD-WAN components, including the various controllers. The various types of deployment models are introduced in this chapter as well. The chapter also introduces the control plane, data plane, and cloud integration.
- **Chapter 3, “Control Plane and Data Plane Operations,”** covers the 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. This chapter also discusses the various types of loop prevention within OMP.
- **Chapter 4, “Onboarding and Provisioning,”** covers how to provision the data plane devices, either manually or via Plug and Play/Zero Touch Provisioning. Templates are also discussed as a means to gain some flexibility and scale with configuration management.
- **Chapter 5, “Introduction to Cisco SD-WAN Policies,”** covers the basics of Cisco SD-WAN policies. This includes the different types of policies, how policies are constructed, and how they are applied to the Cisco SD-WAN fabric.
- **Chapter 6, “Centralized Control Policies,”** covers centralized control policies. These policies are used to manipulate or filter the 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. This chapter discusses a series of use cases that solve for different business requirements.

- **Chapter 7, “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 the OMP. This chapter discusses a series of use cases that solve for different business requirements.
- **Chapter 8, “Application-Aware Routing Policies,”** covers App-Route policies and how these policies 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 9, “Localized Policies,”** covers localized policies, including local route policies, access control lists (ACLs), and quality of service (QoS).
- **Chapter 10, “Cisco SD-WAN Security,”** covers what SD-WAN security is and why it is relevant to your organization. This chapter also covers how to deploy Application-Aware Enterprise Firewall, intrusion detection and prevention, URL filtering, Advanced Malware Protection (AMP) and Threat Grid, DNS web layer security, cloud security, and vManage authentication and authorization.
- **Chapter 11, “Cisco 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 IaaS, and onRamp for Colocation.
- **Chapter 12, “Cisco SD-WAN Design and Migration,”** covers the methodology behind SD-WAN design across the enterprise. This chapter also covers preparation for SD-WAN migration, data center design, and branch design, as well as overlay and underlay routing integration.
- **Chapter 13, “Provisioning Cisco SD-WAN Controllers in a Private Cloud,”** covers how to deploy the controllers in a private cloud, on premises, or in a lab environment. This chapter also discusses the various methods to handle certificates. Certificates play a critical piece in encrypting and authenticating the control plane.
- **Appendix A, “Answers to Chapter Review Questions,”** provides the answers to the review questions at the end of each chapter.
- **Appendix B, “Example 7-17,”** shows the full and complete policy for all of the configuration that was performed in Chapters 6 and 7.
- 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, 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 [www.ciscopress.com](http://www.ciscopress.com) and register your book.

To do so, simply go to [www.ciscopress.com/register](http://www.ciscopress.com/register) and enter the ISBN of the print book: 9780136533177. 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 [www.pearsonITcertification.com/contact](http://www.pearsonITcertification.com/contact) and select the **Site Problems/Comments** option. 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:

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

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

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

- Step 1.** Open this book's companion website, as was 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.pearsonstestprep.com](http://www.pearsonstestprep.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.

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

**Note** Other eBook customers: As of the time of publication, only the publisher and Amazon supply PTP access codes when you purchase their eBook editions of this book.

## Customizing Your Exams

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

- **Study mode:** Allows you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Locks certain customization options, as it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness.
- **Flash Card 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 in 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 well as 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 of 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 on 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 if there are any updates to your exam data and automatically downloads any changes that were made since the last time you used the software.

Sometimes, due to many factors, 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 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 Pearson Test Prep exam engine software, Windows desktop version, simply click the **Tools** tab and click the **Update Application** button. This ensures that you are running the latest version of the software engine.

## Introduction to Cisco Software-Defined Wide Area Networking (SD-WAN)

This chapter covers the following topics:

- **Networks of Today:** This section covers the technologies and challenges of today's networks.
- **Common Business and IT Trends:** This section of the chapter covers the most common trends having a considerable impact on the WAN.
- **Common Desired Benefits:** This section examines the benefits and desired outcomes of what businesses are looking for.
- **High-Level Design Considerations:** This section covers various aspects of WAN design and things that impact the deployment and operations of WANs today.
- **Introduction to Cisco Software-Defined WAN (SD-WAN):** This section examines, from a high level, the benefits and drivers of Cisco SD-WAN.
- **Use Cases Demanding Changes in the WAN:** This section covers a variety of use cases businesses are adopting that are putting pressure on the WAN environment.
- **Building an ROI to Identify Cost Savings:** This section examines the potential cost savings of deploying Cisco SD-WAN and the value of a well-prepared return on investment (ROI).
- **Introduction to Multidomain:** This section examines the purpose of Multidomain and the value associated with having a Multidomain environment.

### Networks of Today

The IT industry is constantly changing and evolving. As time goes on, there is an ever-increasing amount of technologies putting a strain on the network. New paradigms are formed as others are being shifted away from. New advances are being developed and adopted within the networking realm. These advances are being created to provide faster

innovation and the ability to adopt relevant technologies in a simplified way. This requires the need for more intelligence and the capability to leverage the data from connected and distributed environments such as the campus, branch, data center, and wide area network (WAN). Doing so allows for the use of data in interesting and more powerful ways than ever seen in the past. Some of the advances driving these outcomes are the following:

- Artificial intelligence (AI)
- Machine learning (ML)
- Cloud services
- Virtualization
- Internet of Things (IoT)

The influx of these technologies is putting strain on the IT operations staff. This strain comes in the form of more robust planning, agreed-upon relevant use cases, and having detailed adoption journey materials for easy consumption. All these requirements are becoming critical to success. Another area of importance is the deployment and day-to-day operations of these technologies as well as how they fit within the network environment. Disruption to typical operations is more imminent with regards to some of these technologies and how they will be consumed by the business. Other advances in technology are being adopted to reduce cost of operations as well as reduce complexity. It can be said that every network, to some degree, has inherent complexity. However, having tools that can help manage this burden is becoming a necessity these days.

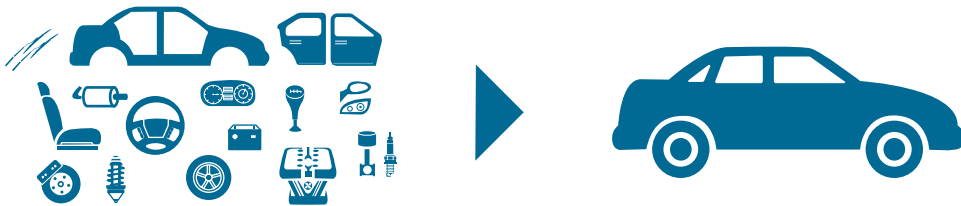
Automation is something that many in the industry are striving for. This is because the networks of today are becoming more and more complicated. Oftentimes businesses are operating with a lean IT staff, a flat or reduced budget, and are struggling to find ways to increase the output of what the network can do for the business. Another driver for the adoption of these technologies is improving the overall user experience within the environment. This includes users being able to have the flexibility and capability to access any business-critical application from anywhere in the network and have an exceptional experience. In addition to improving user experience, IT operations is searching for ways to simplify the operations of the network.

There are many inherent risks associated with manually configuring networks. There is risk in the form of not being able to move fast enough when deploying new applications or services to the network. Risk could also be seen as misconfigurations that could cause an outage or suboptimal network performance, resulting in impacted business operations and potentially causing financial repercussions. Finally, there is risk that the business itself, relying on the network for some business-critical services, might not be available due to the IT operations staff not being able to keep up with the scalability demand. According to a Cisco Technical Assistance Center (TAC) survey taken in 2016, 95% of Cisco customers are performing configuration and deployment tasks manually in their networks. The survey also stated that 70% of TAC cases created are related to misconfigurations. This means that typos or incorrectly used commands are the culprit for a majority of issues seen in the network environment. This is where automation shines: being able to have the



capability to signify the intent of the change that needs to be made, such as deploying quality of service (QoS) across the network, and then having the network configure it properly and automatically. Consistently and correctly configuring services or features with great speed is a tremendous value to the business. Simplifying operations and reducing human error ultimately reduces risk.

A simple analogy for this would be to think of an automobile. As consumers of automobiles, most people use them to meet a specific desired outcome (in this case, it would be to get from point A to point B). An automobile is operated as a holistic system, not a collection of parts that make up that system. For example, there is a dashboard that provides the user all the necessary information of how the vehicle is operating and the current state of the vehicle. When the user wants to use the vehicle, there are certain operational steps required to do so. Drivers simply signify the intent to drive the car by putting it in gear and using the system to get from point A to point B. Figure 1-1 illustrates this analogy.



**Figure 1-1** *Automobile as a System*

Why can't networks be thought of in the same way? Thinking of a network as a collection of devices such as routers, switches, and wireless components is how the industry has been doing it for over 30 years. The shift in mindset to look at the network as a holistic system is a more recent concept that stems from the advent of network controllers. The splitting of role and functionality from one another can be described as separating the control plane from the data plane. Having a controller that sits on top of a collection of network devices gives the advantage of taking a step back and operating the network as a whole from a centralized management point—similar to operating an automobile from the driver's seat versus trying to manage the automobile via individual pieces and components. To put this in more familiar terms, think of the command line interface (CLI). The CLI was not designed to make massive scale configuration changes to multiple devices at the same time. Traditional methods of managing and maintaining the network aren't sufficient to keep up with the pace and demands of the networks of today. The IT operations staff needs to be able to move faster and simplify all the operations and configurations that have traditionally gone into networking. Cisco Software-Defined Networking (SDN) and controller capabilities are becoming areas of focus in the industry, and they are evolving to a point where they can address the challenges faced by IT operations teams. Controllers offer the ability to manage the network as a system, which means that policy management can be automated and abstracted. This provides the capability of supporting dynamic, scalable, and consistent policy changes throughout the network.

## Common Business and IT Trends

Traditional networking infrastructure was deployed when the security perimeter was well defined. Most applications were low bandwidth, and most content and applications resided in centralized corporate data centers. Today, enterprises have very different requirements. High-bandwidth, real-time, and big-data applications are pushing the capacity limits of the network. In some cases, the majority of traffic is destined for the Internet or public cloud, and the security perimeter, as it existed in the past, is quickly disappearing. This is due to a surge in bring-your-own-device (BYOD), cloud, and dynamic business-to-business (B2B) ecosystems. The downside and risks of staying status quo are significant, and technological innovation has failed to comprehensively address the problem. There has been a huge increase in the use of Software as a Service (SaaS) and Infrastructure as a Service (IaaS) offerings. It seems as if more applications are moving to the cloud each day. The adoption of solutions like Microsoft Office 365, Google Apps, Salesforce.com (SFDC), and other SaaS-based productivity and business applications is not effectively addressed by traditional designs that utilize Internet capabilities out of one or more centralized data centers. The following list contains some of the most common trends being seen in the industry:

- Applications are moving to the cloud (private and public)
- Internet edge is moving to the remote branch sites
- Mobile devices (BYOD and guest access)
- High-bandwidth applications
- IoT devices

The number of mobile devices at the remote sites accessing these applications and accessing the Internet as a result of BYOD and guest services is increasing. The additional load of traffic resulting from all of these devices as well as trends such as IoT are putting an additional strain on the network. In addition to everything mentioned, interactive video has finally become the new voice-over IP. Converging voice and data services was an important transition. When it comes to video, however, today's networks not only have to account for optimized QoS handling for video applications, but also need to address the high-bandwidth, latency-sensitive applications that users are demanding. This is going to require rethinking capacity planning to include looking for ways to maximize on current investments. Offloading certain types of traffic and moving to active/active WAN deployment models are some of the ways to accomplish this; however, traditionally these tasks are not easy to implement and require many manual configurations to deploy. Manual intervention when failover or redundancy was required was almost a must. This also led to additional complexity in the network environment.

With everything that was covered from a business and IT trend perspective still in mind, it is important to translate these trends into real challenges that businesses are facing and put them into IT vernacular. As mentioned previously, the WAN is seeing pressure like never before. This is forcing IT teams to look for ways to alleviate that pressure.

Businesses are also looking for ways to improve the user and application experience with what they currently own as well as to drive cost down. Lack of control over visibility, application performance, and keeping up with the ever-growing security attack surface is also contributing to businesses looking for a better way forward. However, organizational silos have also caused many businesses to not be able to achieve the benefits from some of these newer technologies. Breaking down silos to work toward a common goal for the business as a whole is required for businesses to take full advantage of what some of these software-defined advancements have to offer.

## Common Desired Benefits

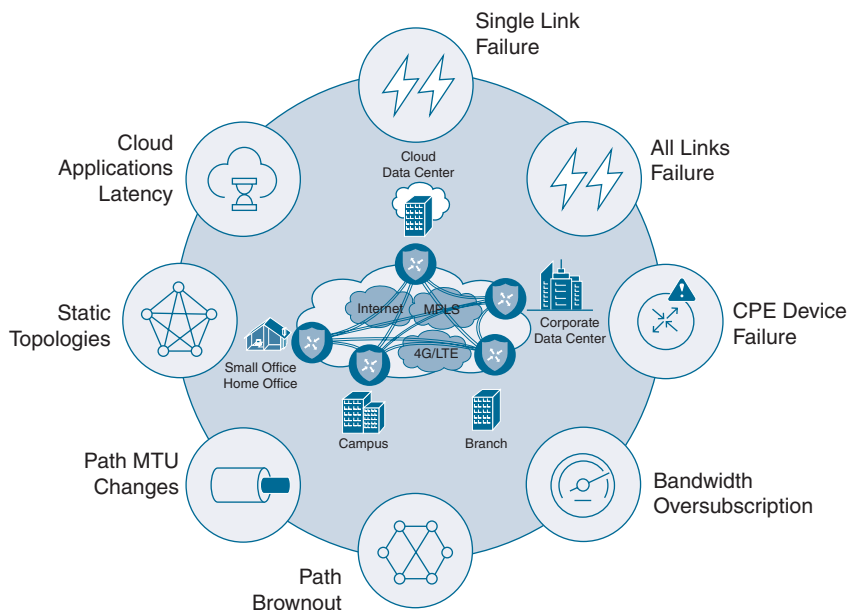
This section of this chapter will cover some of the most common benefits that businesses are looking for from their network and WAN. Designing and deploying the next-generation WAN is about taking advantage of some very useful benefits and the impact they have on the network environment and overall user experience. Here is each of the benefits we will discuss:

- Prioritize and secure traffic with granular control
- Reduce costs and lower operational complexity
- Augment or replace premium WAN bandwidth
- Provide a consistent, high-quality user experience
- Offload guest and public cloud traffic
- Ensure remote site uptime

Oftentimes businesses want to augment or replace premium bandwidth services and move from active/standby WAN transport models to active/active models. This alone will help them to reduce costs. However, the challenge becomes that augmentation of services can increase operational complexity. Complexity is something that must be avoided as businesses look to simplify IT and create a consistent operational model. Ensuring remote site uptime to support business continuity is about more than simply protecting against blackout situations. Critical applications that are impacted by conditions such as latency, jitter, and loss can ultimately render the applications unusable. This is analogous to the applications being completely unavailable. These are called brownouts. Providing a consistent high-quality application experience is top of mind for most businesses today. Because not all applications are created equal, each organization or department might have its own applications that are critical to it and are required to support its business. Voice and video, for example, may be the most critical applications for one business, such as a contact center. However, in the retail vertical, the point of sales (PoS) system or online marketplace may be more critical. It comes down to the level of importance each application plays within a specific organization. Businesses demand the flexibility and power to prioritize applications with granular control. There is a shift to take back control and not have to rely on the service provider for making changes and for ensuring connectivity. This goes beyond typical routing or QoS and extends into application experience

and availability. Many businesses are still not comfortable with the Internet edge moving into their remote site edge. This is necessary to more effectively support the rollout of public cloud applications such as Software as a Service (SaaS) and productivity applications. This is also needed for more optimized access to Infrastructure as a Service (IaaS). However, many businesses are interested in offloading guest traffic to directly attached Internet connectivity in remote branches. This is because it is better to offload this traffic locally rather than consume WAN bandwidth by routing it through a centralized data center for Internet services. This is not efficient and wastes expensive WAN bandwidth.

Networks of today cannot scale at the speed necessary to address the changing needs that the businesses require. Hardware-centric networks are traditionally more expensive and have fixed capacity. They are also more difficult to support due to the box-by-box configurations approach, siloed management tools, and lack of automated provisioning. Conflicting policies between domains and different configurations between services make them inflexible, static, expensive, and cumbersome to maintain. This leads to the network being more prone to misconfigurations and security vulnerabilities. It is important to shift from a connectivity-centric architecture to an application- or service-centric infrastructure that focuses on user experience and simplicity. Figure 1-2 shows the key factors affecting critical service level agreements (SLAs) that can disrupt business continuity.



**Figure 1-2** Issues That Impact Critical SLAs

The solution required to support today's cloud-enabled enterprise needs to be complete and comprehensive. It should be based on the software-defined approach mentioned earlier by leveraging the controller concept. The solution must also include a robust set of capabilities that reduce cost and complexity as well as promote business continuity

and rapid innovation. These capabilities should include the separation of the management plane, control plane, and data plane. This will provide more horizontal scaling capabilities and the security of knowing where the data is at all times.

It should provide various consumption models, such as being hosted in the cloud or being managed on-premises, with complete redundancy between the two. The solution must also provide a complete set of network visibility and troubleshooting tools that are all accessible from a single place. Having this type of solution would assist in providing the following business outcomes and use cases:

- Faster branch deployment with no operational interaction
- Complete end-to-end network segmentation for enhanced security and privacy
- Increased WAN performance
- Topology independence
- Better user experience

All of the things mentioned thus far are critical in terms of what businesses are demanding to drive their network into becoming an asset that truly sets them apart from their industry peers. Many organizations rely on the network to function at its best to provide value and competitive differentiation so their businesses can excel. This is what is driving the industry to these types of technologies. This is also why the industry has increased the speed of adoption and deployment of these solutions.

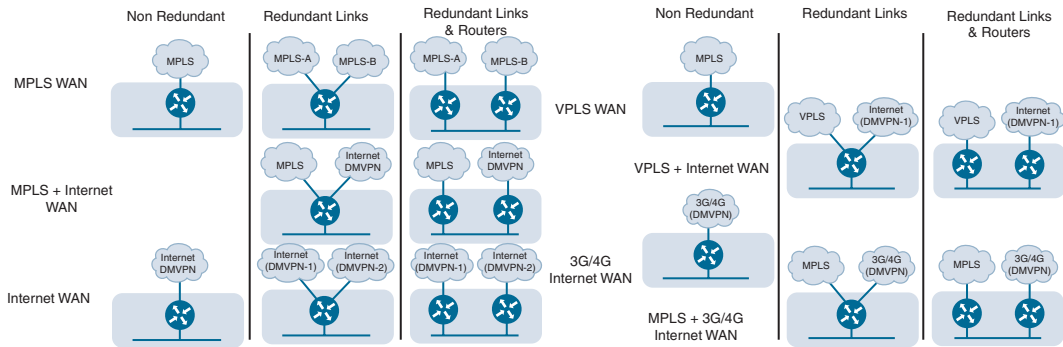
## High-Level Design Considerations

Considering the complexity of a majority of the networks out there today, they can be classified in a couple of categories, such as redundant and non-redundant. Typically, redundancy leads to increased complexity. Oftentimes, the simplest of networks do not plan for failures or outages and are commonly single-homed designs with multiple “single points of failure.” Networks can contain different aspects of redundancy. There can be redundant links, routers, and service providers when speaking strictly of the WAN portion of the environment. Table 1-1 lists some of the common techniques introduced when dealing with redundancy.

**Table 1-1** *Common Redundancy Techniques*

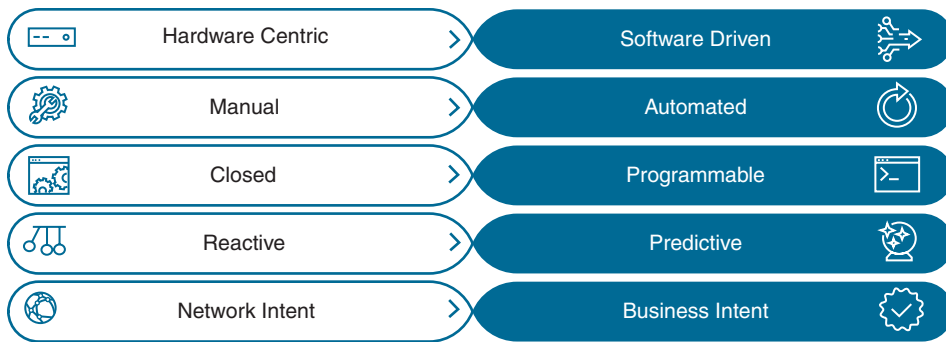
<b>Redundant Links</b>	<b>Redundant Devices</b>
Administrative distance	Redistribution
Traffic engineering	Loop prevention
Preferred path selection	Preferred path selection
Prefix summarization	Advanced filtering
Filtering	

Having a visual of what some of these topologies look like is often helpful. Figure 1-3 showcases some of these various topologies and their associated redundancy types, putting into context how the network will need to be configured and managed to support these types of redundancy options.



**Figure 1-3** *Topology-Based and Link Redundancy Options*

Outside of the complexity associated with redundancy, there are many other aspects of the network that cause complexity within a network environment. Some of these aspects can include things such as securing the network, to shield it from malicious behavior; leveraging network segmentation, to keep traffic types separate for compliance or governance reasons; and even implementing quality of service (QoS), to ensure application performance and increase users' quality of experience. What further complicates the network is having to manually configure these options. The networks of today are too rigid, and things need to evolve. The industry is moving from the era of connectivity-centric network delivery models to an era of digital transformation. A shift is required to transition to a digital transformation model. The shift is from hardware and device-centric options to open, extensible, software-driven, programmable and cloud-enabled solutions. Figure 1-4 depicts the transition in a simple summary. Intent-based networking (IBN) is taking the industry by storm. The concept revolves around signifying the intent of the business and automatically translating that intent into the appropriate corresponding networking tasks—relying more on automation to handle the day-to-day operational tasks and getting back time to focus on how to make the network provide value to the business. This is delivered through policy-driven, automated, and self-optimizing capabilities. This provides closed-loop, automated service assurance that will empower network operations staff to transition from a reactive nature to a more proactive and predictive approach. Freeing up more of the operations staff's time will hopefully allow them to focus on more strategic initiatives within the business.



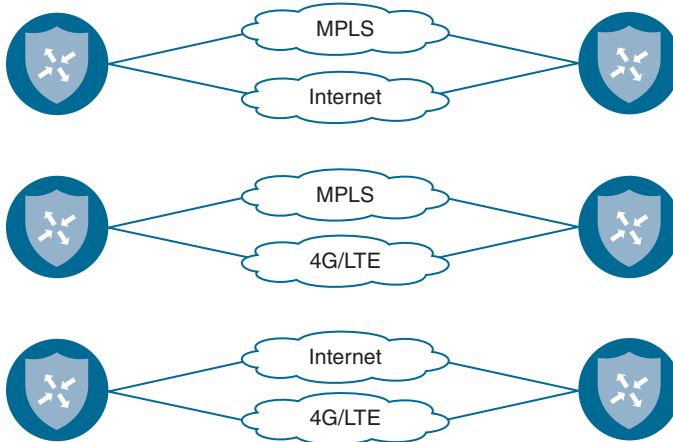
**Figure 1-4** *Digital Transformation Transition*

## Introduction to Cisco Software-Defined WAN (SD-WAN)

Shifting focus from a network-centric model to a business intent-based WAN network is a very powerful change. The WAN architecture can provide simplicity in terms of application deployment and management. However, the mindset must shift from a network topology focus to an application services topology. A common challenge for network operations staff is to support new and existing applications on the WAN. As mentioned previously in this chapter, these applications consume tremendous amounts of bandwidth and are very sensitive to variations in the quality of bandwidth that's available. Things such as jitter, loss, and delay impact most applications, which makes it more important to improve the WAN environment for these applications. Furthermore, cloud-based applications such as Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM) are placing bandwidth demands on the WAN. Non-flexible connectivity options to keep up with the growing amount of cloud applications requiring bandwidth make it costly and difficult to provision new applications and services. Most businesses today have to rely on service providers for MPLS L3VPN to control their WAN routing and network SLAs. This impacts their ability to change and adapt to application delivery methods such as cloud and SaaS. Service providers could take months to implement the necessary changes to their environment in order to support these applications. In addition, some service providers will charge their customers a large amount of money to make these changes, and some may not make the changes at all. Because service providers currently have control of the WAN core, there's no way to instantiate VPNs independent of the underlying transport. Because of this, implementing differentiated service levels for individual applications becomes extremely difficult, if not impossible.

This is why the concept of hybrid WAN was originated. Hybrid WAN is where additional non-MPLS links are acquired by businesses and added to the WAN to provide alternate paths that the applications can take across the WAN environment. These are circuits that businesses have complete control over—from routing control to application performance.

Typically, VPN tunnels are created over the top of these circuits to provide secure transport over any type of link. Examples of these types of links are commodity broadband Internet, L2VPN, wireless, and 4G/LTE. This provides what is called *transport independence*. This allows for the capability to use any type of transport underneath the VPN and get deterministic routing and application performance. This means that some applications can be sent over these commodity links versus the traditional service provider–controlled L3VPN MPLS links. This provides unique granularity of traffic control, redundancy, and resiliency. Figure 1-5 illustrates some common hybrid WAN topologies.



**Figure 1-5** Common Hybrid WAN Topologies

Hybrid WANs need connectivity that is based on a service topology and can be centrally managed using policies. Currently, WAN connectivity is based on the network topology and managed using a peer-to-peer model. This means routing relationships are established by multiple control planes that operate independently of each other. Routing protocols such as Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) are used to establish site VPN routes, and IPsec is commonly used to secure the transport. These routing and security control planes run independently of each other and have their own scaling limitations, convergence requirements, and policy enforcement. This means each control plane is required to have its own independent policy and configuration. As a result, when a configuration change is required in the network, it has to be provisioned and propagated across all the control plane peers, for all transports, which creates operational pitfalls. This also creates the potential risk of misconfigurations or missing configuration that might cause applications to suffer.

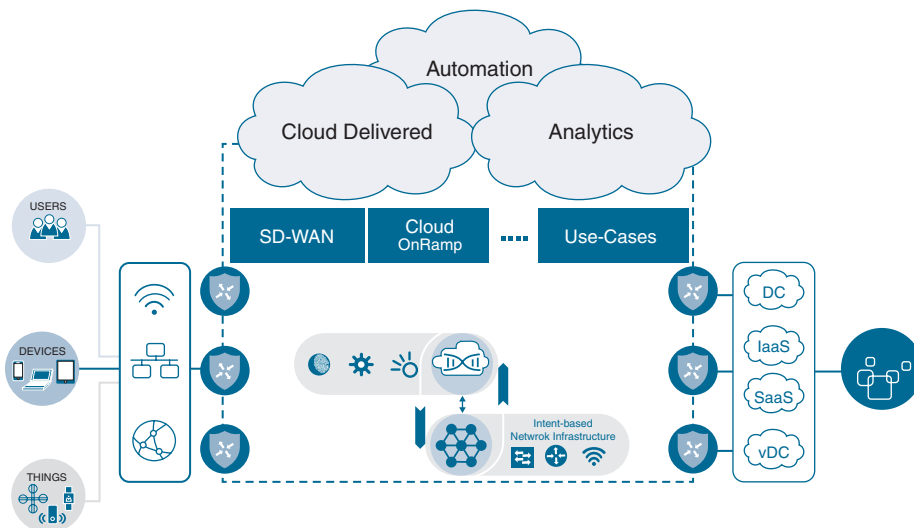


### Transport Independence

Cisco Software-Defined WAN (SD-WAN) leverages a transport-independent fabric technology that is used to connect remote locations together. This is accomplished by using an overlay technology. The overlay works by tunneling traffic over any kind of transport between any destination within the WAN environment. This is the VPN concept that was mentioned

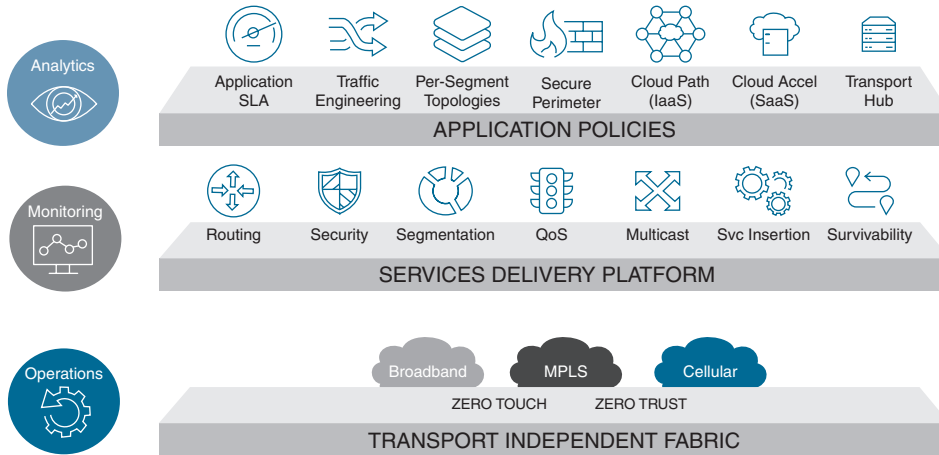


earlier in this chapter—for example, being able to connect remote branches that use MPLS to remote branches that use broadband Internet circuits. This gives true flexibility to routing applications across any portion of the network regardless of what type of circuit or transport is in use. This is the definition of transport independence. By having a fabric overlay network, it means that every remote site, regardless of physical or logical separation, is always a single hop away from another. This is of great benefit in terms of application latency and dynamic communication scenarios such as voice or interactive video. This not only provides increased simplicity in terms of network operations, but also provides seamless mobility from a user experience perspective. Transport independence is also one of the primary aspects of Cisco SD-WAN that allows for the use of flexible, lower-cost commodity circuits versus high-cost, inflexible static bandwidth. Although service providers can upgrade the bandwidth of a circuit, cost is usually a barrier. In addition, there are many times that, based on the type of circuit the bandwidth is riding on, an entire physical circuit upgrade or swap may be more likely. An example of this is having a 100Mbps MPLS handoff wherein the physical circuit it is delivered on is also only 100Mbps. In cases like this, another higher-speed port on the provider side is required, such as gigabit or 10-gigabit Ethernet ports. Many times, the circuit may ride over a different type of medium, and the entire circuit and delivery mechanism must be changed—for example, trying to go from a 45Mbps DS3 to a 1-gigabit Ethernet link. All of this takes time, and that is one of the things SD-WAN was created to address. Businesses can typically order a high-speed commodity Internet circuit and have it delivered within weeks. This new Internet circuit can be immediately added to the environment and taken advantage of by using SD-WAN. There are situations where multiple branch locations need to act as a single large branch across the WAN. This means having a virtual fabric over disparate transports such as MPLS and Internet. Given everything that has been covered thus far, it is important to show what an example of a Cisco SD-WAN diagram would look like. Figure 1-6 illustrates the high-level overview of a Cisco SD-WAN environment and how users, devices, and applications fit into the overall design.



**Figure 1-6** High-Level SD-WAN Overview

Moving from a network-centric WAN to an application- and services-focused WAN requires a different view of the wide area network. Figure 1-7 illustrates the new view of a business intent-based network, its components, and how they fit within the new model.



**Figure 1-7** *Business Intent-Based Network Components*

## Rethinking the WAN

If the current WAN technology and approach were to be redefined, it would have to include some fundamental changes to how WANs are constructed and managed today. These changes would involve the following key areas:

- Secure elastic connectivity
- Cloud-first approach
- Application quality of experience
- Agile operations

From a security perspective, end-to-end segmentation and policy are critical. The control, data, and management planes must be separated across the entire environment. The environment should be able to support native encryption that is robust and scalable, offer lightweight key management, and leverage a zero-trust model, meaning every aspect of the onboarding process must be authenticated and verified.

Rethinking the WAN from a connectivity perspective, these elements would be built on top of security functionality by integrating routing, security, and policy for optimal use of connectivity. The solution must allow for multiple types of transport connectivity options simultaneously and ultimately create a transport-independent operation model. Scale, both horizontally and vertically, is necessary at any layer. Additionally, advanced VPN capabilities and topologies to address any business intent or requirements are critical.

In terms of application support, the solution should support full application awareness across all elements in the system and offer built-in optimization techniques for the networks and applications. The network has evolved to be application aware, and it must be capable of choosing the most optimal path to connect to on-premises or cloud-based applications. The application experience must be optimal in terms of both access and security.

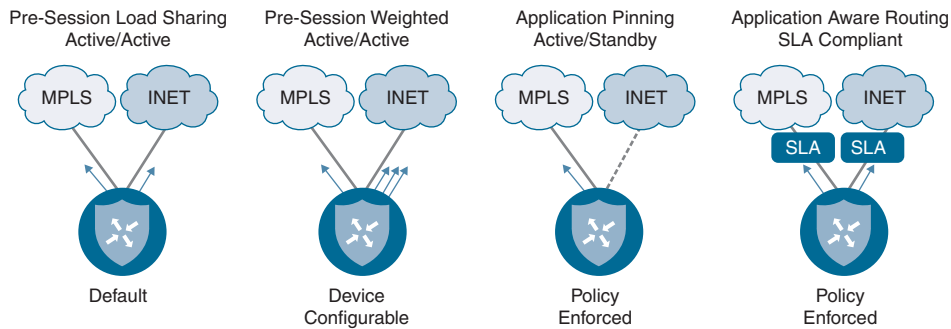
When it comes to the operation of this new application- and services-oriented WAN, network operations staff must be able to define network-wide policies that leverage templates, rather than just a device- or node-level policy. The controller must have the ability to coordinate the paths between the WAN Edge routers, based on centralized policy orchestration. As organizations' network requirements change and evolve over time, the policy should be able to be changed in one single place. This not only reduces the amount of time spent on configuration, but it also lowers the risk associated with misconfiguration errors as well. Programmable, open application programming interfaces (APIs) should be available to provide northbound access for automation and orchestration capabilities. Support of southbound APIs for integration with other solutions should also be included.

## Use Cases Demanding Changes in the WAN

In this day and age, there are many reasons to look at enhancing the WAN environment—from load-balancing traffic to ensuring applications have the best performance possible. The following sections cover some of the use cases causing changes to the WAN.

### Bandwidth Aggregation and Application Load-Balancing

There are many different use cases that demand changes to the way WANs are handled today. Some are as simple as businesses wanting bandwidth aggregation. This is the ability to use both public and private transports together at the same time. This is what is considered using  $A + B$  versus  $A$  or  $B$ , meaning the secondary transport link (Link B) usually sits idle without any traffic using it until Link A fails. However, in a hybrid WAN approach, being able to leverage multiple links at the same time provides an ability to use bandwidth from both links. This is considered an  $A + A$  or an Active/Active scenario. Application load-balancing is achieved using these types of designs as well. This type of hybrid environment allows for greater application performance at a fraction of the cost of two premium transport links. This also increases scale and flexibility without any security compromise. Figure 1-8 illustrates the various options of application load-balancing over multiple links in a hybrid environment. You can see that, by default, per-session Active/Active load-sharing is achieved. Weighted per-session round-robin is also configurable on a device basis. Application pinning, or forcing an application to take a specific transport, is also something that can be enforced via policy. Similarly, Application-Aware Routing or SLA-compliant routing is achieved by enforcing a policy that looks for specific traffic characteristics such as jitter, loss, and delay to determine the path the application should take over the available transports.

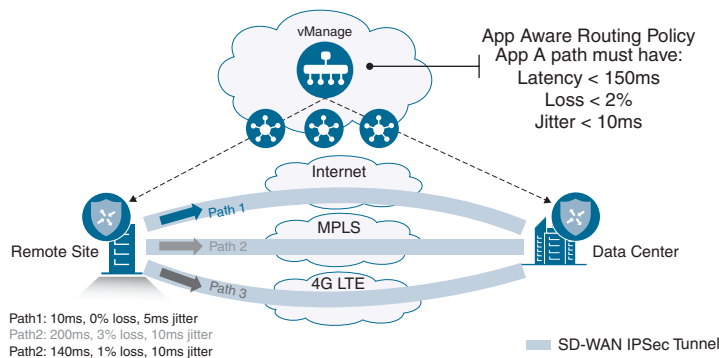


**Figure 1-8** *Application Load-Balancing Options*

**Key Topic**

**Protecting Critical Applications with SLAs**

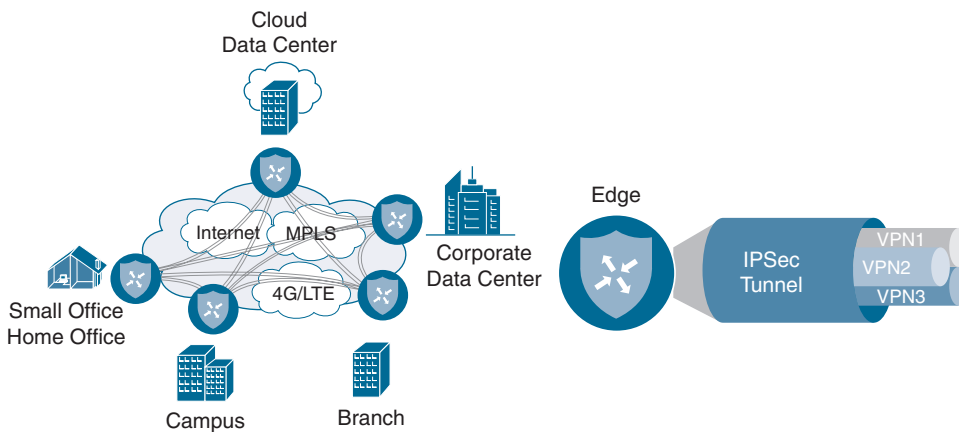
Another use case that drives changes in the WAN is the capability to provide an SLA for critical applications. This is accomplished by being able to route traffic based on the application requirements, as mentioned briefly earlier. This also provides statistics on how the applications are performing. Based on the policy that can be created, an SLA determines if the application is adhering to that policy, and performing properly, or if it is experiencing some sort of detriment such as jitter, loss, or delay. If this is the case, the application can be routed to another transport that will ensure the application is within policy and able to perform to the SLA that is expected of it. Figure 1-9 illustrates this particular scenario. A good example of this in a hybrid WAN environment would be an MPLS link and an Internet link. If the MPLS link is experiencing 5% packet loss and the Internet link is not, it might be appropriate to route the application over the Internet link to ensure that the application is functioning properly and users are having the best experience interacting with the application.



**Figure 1-9** *Routing Based on Application Performance*

## End-to-End Segmentation

Segmentation is another use case that drives these changes in the WAN. Oftentimes, businesses have different departments that require separation. For example, Research and Development may need to be segmented from the Production environment. There may be extranets that connect to partners, or the business may be merging or acquiring another business in which the networks need to be able to communicate but segmentation may still be required between the two. This may require multiple topologies that can be managed as one. Figure 1-10 depicts an end-to-end segmentation topology, along with how different VPNs are carried over the tunnels. Each of these tunnels terminates at an edge router within the environment.

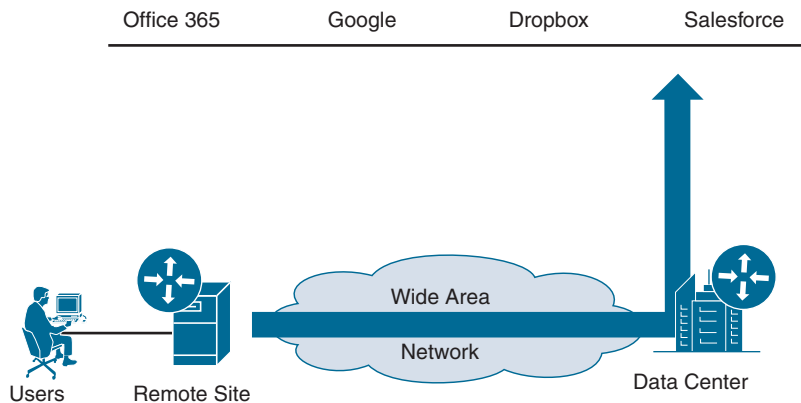


**Figure 1-10** *End-to-End Segmentation*



## Direct Internet Access

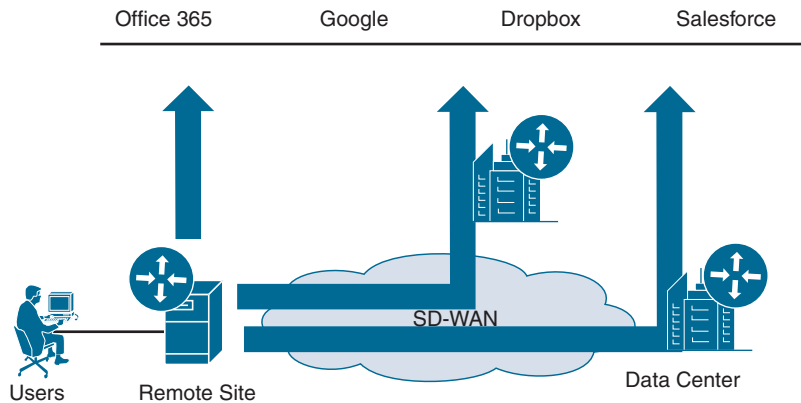
One of the most common use cases is something called Direct Internet Access (DIA). DIA gives branches the capability to send traffic directly out of the local Internet transport instead of carrying it all the way back to a centralized data center to be inspected. This allows for cloud-based applications to go directly to the Internet and cloud service providers without having to use unnecessary WAN bandwidth. This is increasingly becoming the method that is being adopted. Figure 1-11 depicts the traditional way that cloud applications are accessed. This causes suboptimal performance for users trying to access these applications. This also, as mentioned earlier, puts a strain on the WAN infrastructure, as the expensive and limited WAN bandwidth is being consumed by applications that could be sent directly to the Internet from the remote site. This also introduces increased application latency, as the traffic has to cross the entire network to get to the data center to reach the Internet.



**Figure 1-11** *Traditional Cloud Application Access via WAN*

Looking at changing and rethinking the WAN allows for different mechanisms that will allow for better performance and scale. A great example of this is using the Direct Internet Access design to offload the latency-sensitive cloud applications directly to the Internet. This method also gives the flexibility to have a local firewall or inspection device in the branch to ensure the branch is protected from any malicious threats coming into the local branch Internet link.

Figure 1-12 shows an example of what this would look like in a new WAN environment.



**Figure 1-12** *Direct Internet Access and Cloud Access Topologies*

### Fully Managed Network Solution

Finally, there is a use case that allows for the business to simply let someone else, such as Cisco or a Cisco Partner, manage the network as a fully managed solution. This provides the flexibility to not only have the network managed as a whole for the business,

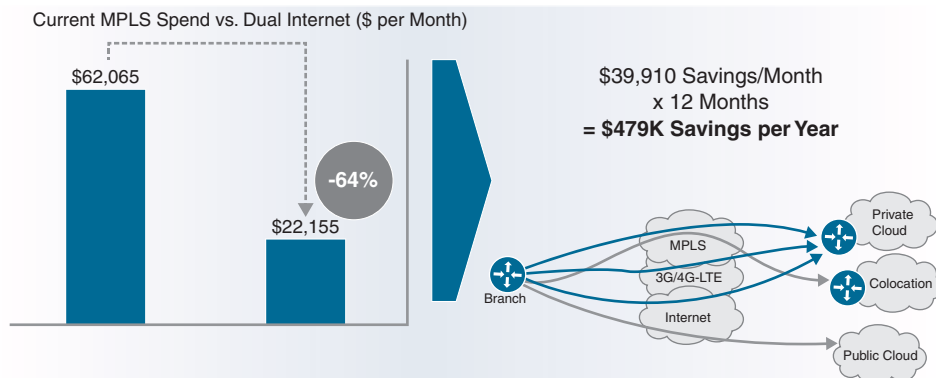
but also to allow the business to have control over the policy and reporting portion of the managed service. This is becoming a more attractive option for customers who want to move to an OpEx model. This allows them to pay for their network on a subscription basis versus the traditional CapEx model and is analogous to paying an electric or cell phone bill. The consumption models available today are really opening up new options for customers.

**Note** All of these use cases and technologies will be covered in detail in the coming chapters of this book.

## Building an ROI to Identify Cost Savings

A really important exercise when looking at Cisco SD-WAN is to build a quantifiable return on investment (ROI). Oftentimes businesses investigating Cisco SD-WAN find that removing certain expensive links and leveraging high-speed commodity Internet links for transport not only lowers the overall cost of the WAN but also adds redundancy and resiliency. Typically, these benefits weren't realized in the environment prior to moving to Cisco SD-WAN.

There are many companies that provide these ROI models at no cost to the customer and have proven to be an almost mandatory step in the Cisco SD-WAN journey. Some customers have seen enough cost savings and increases in overall bandwidth that the project was completed without any additional costs to the business. Figure 1-13 shows an example of an ROI calculation. Note the staggering details of a 64% cost savings from moving from a dual MPLS link design to a dual commodity Internet link design. At the very least, this proves the exercise is worthwhile to complete prior to getting started with implementation and deployment.



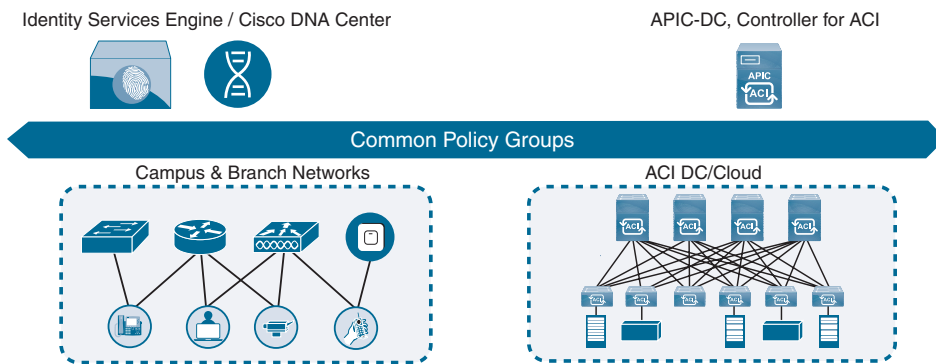
**Figure 1-13** Simple ROI Calculation Example

**Note** These numbers were taken from a real customer example. However, every business will have different ROI calculations based on cost of circuits, type of circuits, and location. These numbers are examples only and will be different for anyone reading this book or having ROI calculations performed on their own environment.

## Key Topic

## Introduction to Multidomain

A common trend arising in the industry is data being generated and stored in many areas of the network. Traditionally, a majority of the data for a business was stored in a centralized data center. With the influx of guest users, mobile devices, bring your own device (BYOD), and Internet of Things (IoT), data is now being generated remotely in a distributed manner. This means the industry is shifting from data centers to multiple centers of data. That being said, simple, secure, and highly available connectivity is a must to allow for enhanced user and application experience. The other big piece to this is having a seamless policy that can go across these multiple centers of data. An example of this is policy that extends from the campus environment across the WAN and into the data center and back down to the campus. This provides consistency and deterministic behavior across multiple domains. Figure 1-14 illustrates a high-level example of sharing policy between a campus branch location and a data center running Cisco Application Centric Infrastructure (ACI).

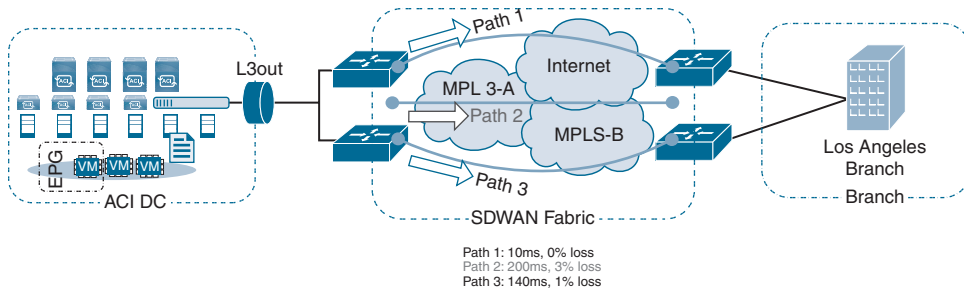


**Figure 1-14** *High-Level Multidomain Example*

In future evolutions of Multidomain, the common policy will consequently provide end-to-end policy management across all three domains. This gives the capability of leveraging things like application SLAs from the data center to the WAN and back. This ensures the applications are performing to the best of their ability across the entire network, relieving strain on the WAN and providing a better user experience when using the



applications. Figure 1-15 shows a high-level example of what this could look like from a topology perspective.

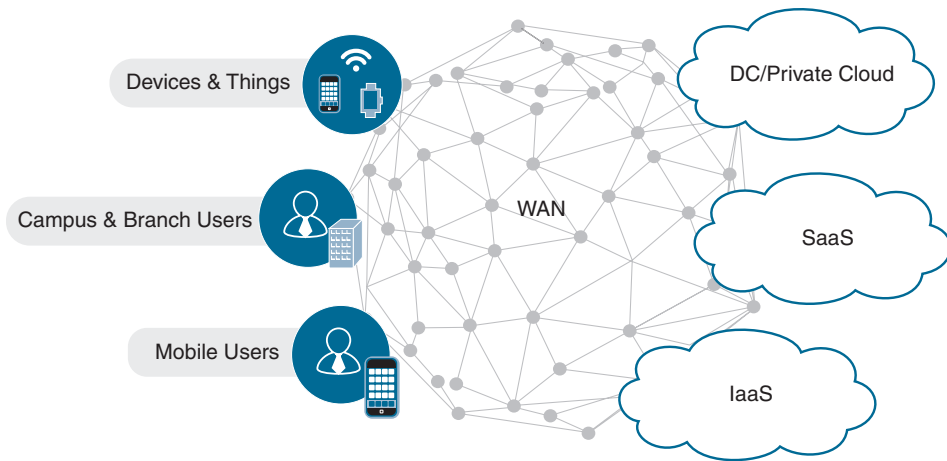


**Figure 1-15** *High-Level Multidomain and SD-WAN Example*

Multidomain offers the capability to have the network operate as a holistic system, as mentioned previously in this chapter. This takes intent-based networks to the next level by taking policy across all domains for a seamless application experience. This also implements security everywhere and provides complete granularity in terms of control and operations.

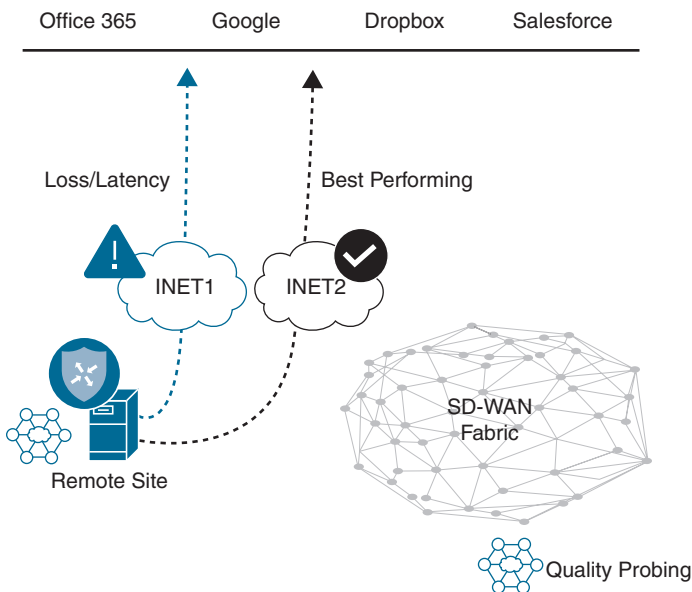
## Cloud Trends and Adoption

Cloud adoption has been taking the industry by storm. Over the years the reliance on the cloud has grown significantly, starting with music, movies, and storage and moving into Software as a Service (SaaS) and Infrastructure as a Service (IaaS). Today, there are many aspects of businesses such as application development, quality assurance, and production that are running in the cloud. To make things even more complicated, companies are relying on multiple cloud vendors to operate their business. This requires unique sets of policies, storage capacity requirements, and overall operational skills on a per-vendor basis. Companies are also struggling with things such as shadow IT and backdoor applications in their environment. This means that lines of business are going to cloud providers on their own without any knowledge or guidance from IT departments and spinning up applications on demand in the cloud. This causes major concerns from a security and privacy perspective. In addition, the potential loss of confidential information or intellectual property could damage the brand and reputation of the business. The risks are significant. Furthermore, the applications in the cloud, whether legitimate production or development, still require certain levels of priority and treatment to ensure the applications are being delivered properly to the users who consume them. This is where some of the capabilities of Cisco SD-WAN can help to ensure the applications are being treated appropriately and the experience for the users is adequate. Figure 1-16 illustrates the demand on the WAN and how the Internet is becoming critical to the operations of the business.



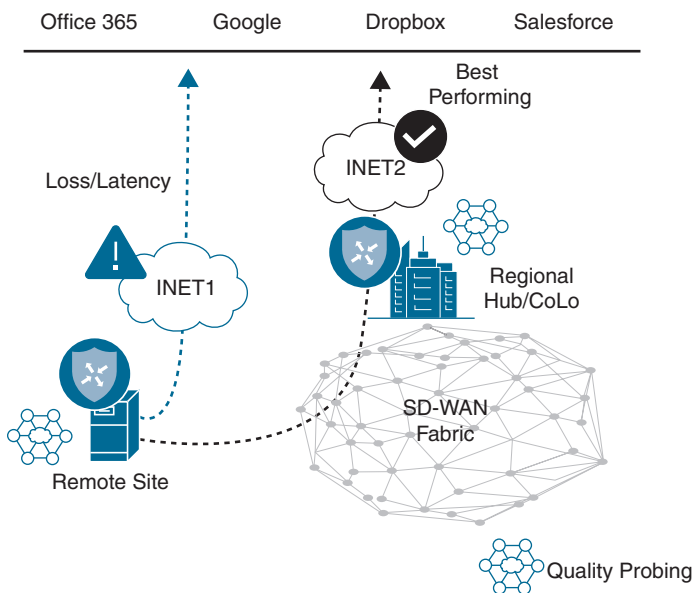
**Figure 1-16** Demand on WAN for Internet-Based Applications

Having Direct Internet Access can assist with this, as mentioned earlier. By being able to detect application performance through one or more Direct Internet Access circuits, the edge routers are able to choose the best-performing path based on the application-specific parameters. If one of the links to the cloud application fails or has degradation in performance, the application can automatically fail over to another direct Internet link. This process is fully automated and requires no interaction from the network operations staff. Figure 1-17 shows this scenario with multiple Direct Internet Access links.



**Figure 1-17** Multiple Direct Internet Access Links to Cloud Applications

This concept also works in environments that have a remote branch site that has a local direct Internet link as well as an Internet link within a centralized data center. The same process takes place in that the application performance is measured and the path that provides the best performance will be the path chosen for the application. Similarly, blackout or link failures will also be protected against because of redundancy built into the solution by having multiple available paths. Figure 1-18 depicts this scenario of having a local directly attached Internet link and an Internet link available in a centralized data center. Again, this leaves the router to make the decision based on the policy and application parameters that were configured. Not only are these decisions fully automated and made on a per-application and per-VPN basis, but ultimately an amazing amount of flexibility and control over the application performance within the environment is provided.



**Figure 1-18** *Direct Internet Access and Centralized Internet Link to Cloud Applications*

## Summary

This chapter covered a high-level overview of how the networks of today are causing challenges for businesses and their operations staff. The common business and IT trends the industry is seeing and how they impact the networks of today were also covered. The overall benefits desired by organizations and their IT staff lead to the need to rethink the WAN environment. Cloud applications and the influx of the amount of data within the network are causing strain on the WAN. This is causing businesses to look at ways to alleviate the pressure being put on the WAN and the organization as a whole. The use cases covered in this chapter will each be covered in depth in the upcoming chapters in this book. Cost is not the only driver for organizations to look at SD-WAN. Application

performance, security, segmentation, improved user experience, redundancy, and resiliency are also key drivers that point to SD-WAN.



## Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 1-2 lists these key topics and the page numbers on which each is found.

**Table 1-2** *Key Topics for Chapter 1*

Key Topic Element	Description	Page Number
Section	Transport Independence	10
Section	Protecting Critical Applications with SLAs	14
Paragraph	Direct Internet Access	15
Section	Introduction to Multidomain	18

## Key Terms

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

Multidomain, artificial intelligence (AI), machine learning, cloud, virtualization, Internet of Things (IoT), quality of service (QoS), command line interface (CLI), Software-Defined Networking (SDN), bring your own device (BYOD), Software as a Service (SaaS), Infrastructure as a Service (IaaS), application programming interface (API), Cisco Software-Defined WAN (Cisco SD-WAN), Cisco Application Centric Infrastructure (Cisco ACI), service level agreement (SLA)

## Chapter Review Questions

1. What are some of the common IT trends putting pressure on the WAN? (Choose three.)
  - a. IoT
  - b. Cloud
  - c. Fog computing
  - d. BYOD
  - e. Low-bandwidth applications
2. What are some benefits businesses are looking for from their WAN? (Choose three.)
  - a. Lower operational complexity
  - b. Increased usable bandwidth
  - c. Reduced uptime in branch locations
  - d. Topology dependence
  - e. Improved overall user experience

3. What are some of the tools or technologies that may be necessary to implement when redundant links are used in branch locations? (Choose three.)
  - a. Administrative distance
  - b. Traffic engineering
  - c. Redistribution
  - d. Loop prevention
  - e. Preferred path selection
4. Part of having an intent-based network is to move to a hardware-centric approach.
  - a. True
  - b. False
5. Which of the following are part of the digital transformation journey? (Choose two.)
  - a. Automated
  - b. Manual
  - c. Proactive
  - d. Reactive
  - e. Predictive
6. Organizations are looking to deploy SD-WAN for what reasons? (Choose two.)
  - a. To take all routing control from the service provider
  - b. To create end-to-end SLAs for the organization's traffic
  - c. To offload all routing control to the service provider
  - d. To leverage the service provider's SLA for end-to-end traffic
7. What are some of the benefits of SD-WAN? (Choose four.)
  - a. Lower cost
  - b. Improved user experience
  - c. Transport independence
  - d. Increased cloud consumption
  - e. IoT devices
  - f. Increased bandwidth
8. What are some of the transport options for SD-WAN? (Choose three.)
  - a. Dual MPLS
  - b. Hybrid WAN
  - c. Dual route processor
  - d. Hybrid single link
  - e. Dual Internet
9. Direct Internet Access is used to offload applications directly to the data center.
  - a. True
  - b. False

- 10.** What is one of the benefits of Cisco Multidomain?
- a. Single policy across multiple environments
  - b. Multiple policies across single domain
  - c. Simplified reporting for IoT devices
  - d. Enhanced service provider support

# Index

## A

---

- ACLs (access control lists), 112, 319–320, 338
  - creating, 334–335
  - effects of applying to localized policy, 338
  - referencing, 337
- activating, centralized policies, 125–127
- address restricted cone NAT, 76–77
- administrative distances, WAN Edges, 60
- AMP (Advanced Malware Protection), 349, 350–351, 372–377
  - dashboard, 376–377
  - monitoring statistics, 375
  - policy configuration, 373–374
- APIs (application programming interfaces), 13
- application lists, 118
- application service containers, 360–361
- Application-Aware Enterprise Firewall, 349
  - actions, 355
    - dashboard, 359
    - destination zone, 353
    - firewall policies, 354
    - firewall policy, 353
    - inter-zone security, 356
    - intra-zone security, 355
    - monitoring statistics, 359
    - self-zone policy, 353
    - source zone, 353
    - zone pair, 353
    - zones, 352–353
- Application-Aware Routing, 350–351
  - business imperative for, 286
- application-based traffic engineering, 253–254
  - application forwarding behavior without policy changes, 254
  - policy, 255–257
  - steady and failed state, 258–260
- applications, protecting from packet loss, 269–270
  - FEC (Forward Error Correction), 270–274
  - packet duplication, 274–280

applying changes to localized data policies, 337

### App-Route policies

applying, 292

backup-sla-preferred color action, 314–315

BFD (Bidirectional Forwarding Detection)

*App-Route Multiplier*, 300–304

*App-Route Poll Interval*, 298–300

*liveliness detection*, 295–297

*path quality monitoring*, 298

*settings*, 303–304

construction, 287–294

mapping traffic flows to a transport tunnel, 304

mechanics, 286–287

monitoring tunnel performance, 294

packet forwarding, 304

*SLA class action*, 306–315

*traditional lookup in the routing table*, 305–306

preferred color, 312

sample, 293–294

sequence rules, 289

sequences, 309–311

SLA class lists, 287

traffic forwarding configurations, 309–315

App-Route Poll Interval, 298–300

automatic provisioning, 102

automatic rollback, 91

automation, 2

## B

---

B2B (business-to-business), 4

bandwidth, WANs, 9

best path selection, OMP, 56–58

BFD (Bidirectional Forwarding Detection), 28–29, 138, 294

liveliness detection, 295–297

*Hello Interval*, 295–297

*Multiplier value*, 297

path quality monitoring

*App-Route Multiplier*, 300–304

*App-Route Poll Interval*, 298–300

settings, 303–304

BGP (Border Gateway Protocol), 466–467

routing loop prevention, 62–63

branch-to-branch communication, enabling

with summarization, 150–152

with TLOC lists, 152–168

brownouts, 5–6

BYOD (bring-your-own-device), 4, 18

## C

---

C,I,R (chosen, installed, resolved), 51

calculating, ROI, 17–18

CAs (certificate authorities), 494

CDFW (cloud-delivered firewall), 261

connectivity, 261–263

SIG policy, 263–267

validating service insertion, 266–269

centralized control policies. *See* control policies

centralized data policies. *See* data policies

centralized policies, 110–112, 117, 134–136. *See also* control policies; data policies; localized policies

activation, 125–127

application-aware routing, 112



- cflowd, 112
- construction, 118, 122–125
- control, 111
- creating, 117–118, 122–125
  - and localized policies, 328
  - VPN membership, 111
- certificates, 496–501
  - automatic enrollment, 498–501
  - generating, 511–512
- Cisco ACI (Application Centric Infrastructure), 18
- Cisco ASR (Advanced Services Router), 30
- Cisco Cloud, 38
- Cisco IOS-XE, upgrading, 31
- Cisco ISR (Integrated Services Router), 30
- Cisco SD-WAN (Software-Defined WAN), 9–10, 387–389. *See also* Application-Aware Enterprise Firewall; Cloud onRamp; control plane; data plane; management plane
  - automatic rollback, 91
  - Cloud onRamp, 394
  - configuration management, 91
  - control plane, 44
    - BFD*, 28–29
    - DTLS/TLS tunnels*, 45–46
    - encryption*, 35
    - OMP*, 44, 47–48
    - OMP routes*, 48–51
    - path selection*, 56–58
    - security*, 45
    - service routes*, 54–56
    - TLOC routes*, 52–54
    - vSmart*, 34–35
    - WAN Edges*, 27, 28, 29, 32
  - controllers, 493–494
  - data plane, 27–32, 44, 65
    - address restricted cone NAT*, 76–77
    - encryption*, 83–84
    - full cone NAT*, 74
    - key exchange process*, 84–86
    - NAT*, 73–74, 81
    - network segmentation*, 81–82
    - pairwise encryption keys*, 86–87
    - port restricted cone NAT*, 77–80
    - security*, 65–66
    - segmentation*, 66
    - symmetric NAT*, 75–76
    - TLOC colors*, 66–70
    - tunnel groups*, 70–73
  - deployment options, 38–39
  - design methodology, 459–460
  - DIA, 31–32
  - distributed architecture, 26–27
  - DPI (Deep Packet Inspection), 400–402
  - firewall policy, configuration, 356–359
  - management plane, 44
    - vAnalytics*, 32–33
    - vManage*, 32–33
  - migrating to
    - branch design*, 469
    - complete CE replacement*, 470–475
    - data center design*, 462–463
    - integration with branch firewall*, 476–478
    - integration with existing CE router*, 475

- integration with voice services,*  
478–479
- loopback TLOC design,*  
465–466
- overlay and underlay*  
*integration, 480–489*
- preparation, 460–462*
- service-side connectivity,*  
466–469
- transport-side connectivity,*  
463–465
- multi-tenancy options, 38
- onboarding devices, 101–102
  - automatic provisioning,*  
103–105
  - manual bootstrapping of a*  
*WAN Edge, 102*
- orchestration plane, 36–37, 44
- physical platforms, 30
- policies, 109. *See also* policies
  - centralized, 110–112, 117–118*
  - construction, 115–118*
  - definition, 119–122*
  - domains, 113–114*
  - lists, 118–119*
  - localized, 112–113*
  - matching criteria, 120–121*
  - monitoring, 147*
  - packet forwarding order of*  
*operations, 127–128*
  - purpose, 109–110*
  - saving, 147*
- on-premises deployment, 494
- ROI, 17–18
- security suite, 349–351, 361
  - AMP (Advanced Malware*  
*Protection), 372–377*
  - Application-Aware Enterprise*  
*Firewall, 352–360*
  - benefits, 351–352*
  - cloud security, 381–383*
  - DNS Web Layer security,*  
377–381
  - IDS/IPS (intrusion detection*  
*and prevention), 360–367*
  - Threat Grid, 372–377*
  - URL filtering, 367–372*
  - vManage authentication and*  
*authorization, 384–389*
- supported platforms, 30–31
- templates, 91, 93–94
  - creating, 97–101*
  - device, 94, 96–97*
  - feature, 94–95*
  - options, 96–97*
  - values, 95–96*
- transport independence, 10–12
- virtual platforms, 30
- VPNs, 27
- Cisco Umbrella, 377**
  - DNS Web Layer security  
configuration, 378–381
- Cisco vEdges, 30**
- Cisco Webex, corporate direct cloud**  
access, 243–252
- CLI (command line interface), 3,**  
25–26
- Cloud onRamp, 394**
  - for Colocation, 429–431, 432
  - cluster creation, 442–448*
  - IaaS integration, 438*
  - image repository, 449*
  - monitoring, 454–455*
  - network services, 432–434*
  - redundancy and high*  
*availability, 440*
  - SaaS integration, 438–440*

- service chain creation*, 449–454
- service chain design best practices*, 440–441
- service chaining for a single service node*, 434–436
- service chaining for multiple service nodes*, 436
- for IaaS, 412–418
  - configuration*, 415–426
  - transit VPCs*, 413–415
  - viewing VPC statistics*, 426–428
- for SaaS, 394–403
  - benefits*, 395
  - configuration*, 404–412
  - DIA (Direct Internet Access)*, 395
  - hybrid deployment*, 397
  - monitoring statistics*, 398
  - prerequisites for all site types*, 403
  - prerequisites for DIA or gateway sites*, 404–412
  - through a gateway*, 397
  - vQoE score*, 398–399
- cloud services**, 4, 5–6
  - adoption, 19
  - challenges of, 393–394
  - DIA (Direct Internet Access), 15–16
  - private clouds, 38
  - security, 349, 381–383
  - trends, 19–21
  - VPC (virtual private cloud), 413
- colocation**, 432
- color lists**, 118
- colors**, 312
- commands**, 25–26
  - encapsulation, 177
  - export-to, 211–212, 220
  - local-tloc, 255
  - max-control-connections 0, 495–496
  - preferred-color, 312
  - service, 263
  - service local, 266–267
  - show app-route stats, 310
  - show bfd sessions, 73
  - show bfd summary, 151–152
  - show ip bgp, 174
  - show omp routes, 175, 201–202, 204–206
  - show omp services, 56
  - show omp tlocs detail, 53–54
  - show policy data-policy-filter, 241, 269
  - show policy from-vsmart, 241
  - show policy service-path, 250–252, 269
  - show policy tunnel-path, 250–252
  - show run omp, 59
  - show run vpn 10, 59
  - show running-config policy, 306, 313–315, 344–346
  - show tunnel statistics fec, 274
  - sla-class, 313
  - strict, 315
  - tloc-list, 255
  - traceroute, 138, 148–149, 151–152, 168, 190, 194–195, 197–198, 207
  - vpn, 507–508
- common desired benefits, WANs**, 5–7
- configuration management**, 91
- connectivity**
  - CDFW (cloud-delivered firewall), 261–263
  - WANs, 12

**control plane, 3, 6–7, 25–27, 44**

DTLS/TLS tunnels, 45–46

OMP, 44, 47–48

*attributes, 49–50**graceful restart, 47**origin types, 59–60**redistribution, 58–60**routes, 48–51**routing loop prevention, 60–65**service routes, 54–56**TLOC routes, 52–54*

path selection, 56–58

security, 45

**control policies, 111, 134–136. See also localized policies**

isolating remote branches from each other, 136–149

monitoring, 147

multi-topology, 206–210

saving, 147

use cases

*creating different network topologies per segment, 206–210**creating extranets and access to shared services, 211–222**enabling branch-to-branch communication through data centers, 149–152, 152–168**enforcing security perimeters with service insertion, 195–200**isolating guest users from the corporate WAN, 202–206**isolating remote branches from each other, 136–149**preferring regional data centers for Internet access, 180–188**regional mesh networks, 188–195**traffic engineering at sites with multiple routers, 169–176, 177–178***controllers. See also vBond; vManage; vSmart**

authentication, 497

automatic enrollment for certificates, 498–501

deployment

*vBond, 513–518**vManage, 501–512**vSmart, 518–522*

obtaining a certificate, 498

on-premises deployment, 495–496

whitelist files, 497–498

**counters, 241****creating**

ACLs, 334–335

App-Route policies, 287–294

extranets, 211–222

localized control policies, 325–327

policies, 115–118

*centralized, 118, 122–125*

templates, 97–101

**credit card transactions, packet duplication, 274–280****CRM (Customer Relationship Management), 9****CVVS (Common Vulnerability Scoring System), 363****D**

---

**dashboard**

AMP (Advanced Malware Protection), 376–377

- Application-Aware Enterprise Firewall, 359
- IDS/IPS, 366–367
- URL filtering, 371–372
- data centers, 4**
- data plane, 3, 6–7, 25–32, 44, 65**
  - encryption, 83–84
    - key exchange process, 84–86*
    - pairwise encryption keys, 86–87*
  - NAT, 73–74, 81
    - address restricted cone NAT, 76–77*
    - full cone, 74*
    - port restricted cone, 77–80*
    - symmetric, 75–76*
  - security, 65–66
  - segmentation, 66, 81–82
  - TLOC colors, 66–68
    - restrict keyword, 68–70*
    - tunnel groups, 70–73*
- data policies, 114, 227, 228. See also App-Route policies; localized policies**
- App-Route, 285
  - backup-sla-preferred color action, 314–315*
  - BFD, 294–304
  - construction, 287–294*
  - mapping traffic flows to a transport tunnel, 304*
  - mechanics, 286–287*
  - monitoring tunnel performance, 294*
  - packet forwarding, 304, 305–315*
  - preferred color, 312*
  - sequences, 309–311*
  - traffic forwarding configurations, 309–315*
- data prefix lists, 232–233
- editing, 235–236
- effects on users in the guest VPN, 239–242
- naming, 238
- sequence types, 233–235
- use cases, 228–229
  - application-based traffic engineering, 253–260*
  - direct cloud access for trusted applications, 243–252*
  - direct Internet access for guest users, 230–242*
  - protecting applications from packet loss, 269–280*
  - protecting corporate users with a cloud-delivered firewall, 261–269*
- data prefix lists, 232–233
- decryption, pairwise keys, 86–87
- defining, policies, 119–122
- destination zone, 353
- device templates, 94, 96–97
  - adding localized control policy, 327–330
  - setting TLOC preference, 177–178
- devices**
  - provisioning
    - automatic, 103–105*
    - manual bootstrapping of a WAN Edge, 102*
  - Viptela, 102
    - minimal configuration, 102–103*

DIA (Direct Internet Access), 15–16, 31–32, 349–350, 395

direct cloud access for trusted applications, 243–252

distributed architecture, 26–27

DNS Web Layer security, 349, 377–378

configuration, 378

security policy configuration, 378–381

DTLS (Datagram Transport Layer Security), 36–37, 45–46

## E

---

echo mode, BFD (Bidirectional Forwarding Detection), 28–29

editing, data policies, 235–236

EIGRP (Enhanced Interior Gateway Routing Protocol), routing loop prevention, 63–65

encapsulation command, 177

encryption

- data plane, 83–84
  - key exchange process*, 84–86
  - pairwise encryption keys*, 86–87
- vSmart, 35

end-to-end segmentation, 15

ERP (Enterprise Resource Planning), 9

export-to command, 211–212, 220

extranets, creating, 211–222

## F

---

feature templates, 94–95

FEC (Forward Error Correction), protecting applications from packet loss, 270–274

FEC blocks, 271

firewall(s), 381. *See also* Application-Aware Enterprise Firewall

Application-Aware Enterprise Firewall

- destination zone*, 353
- firewall policy*, 353
- self-zone policy*, 353
- source zone*, 353
- zone pair*, 353
- zones*, 352–353

cloud-delivered, 261

- connectivity*, 261–263
- SIG policy*, 263–267
- validating service insertion*, 266–269

policies, 353, 354–355, 356–359

service insertion, 195–200

full cone NAT, 74

## G-H

---

graceful restart, 47

guest users, direct Internet access, 230–242

Hello Interval, BFD (Bidirectional Forwarding Detection), 295–297

hybrid WANs, 9–10

- Active/Active, 13

## I

---

IaaS (Infrastructure as a Service), 4, 5–6, 19

Cloud onRamp, 412–418

- configuration*, 415–426
- transit VPCs*, 413–415
- viewing VPC statistics*, 426–428

**IBN (intent-based networking), 8**  
**IDS/IPS (intrusion detection and prevention)**  
 application service containers, 360–361  
 configuration, 362–363  
 dashboard, 366–367  
 policy configuration, 365–366  
 security virtual image upload, 364–365  
 signature sets, 363–364  
 Snort, 361  
**interactive video, 4**  
**Internet access**  
 for guest users, 230–242  
 regionalizing, 180–188  
**inter-zone security, 356**  
**intra-zone security, 355**  
**intrusion detection and prevention, 349**  
**IoT (Internet of Things), 4, 18**  
**IPsec (Internet Protocol Security), 27**  
**IT industry**  
 advances in, 1–2  
 automation, 2  
 trends, 4–5  
  
**K-L**  


---

**KVM (Kernel Virtual Machines), 361**  
**lists, 118–119**  
 SLA class, 287  
**liveliness detection, BFD (Bidirectional Forwarding Detection), 295–297**  
 Hello Interval, 295–297  
 Multiplier value, 297  
**localized policies, 112–113, 319–320**

and centralized policies, 328  
 control, 320–322, 324  
*adding to the device template, 327–330*  
*creating, 325–327*  
*naming, 326–327*  
*route policy configuration, 322–324, 325*  
*viewing effects of route policies on neighboring routers, 333–334*  
*viewing route policies, 330–332*  
 data, 334  
*ACL, creating, 334–335*  
*ACL, referencing, 337*  
*applying changes, 337*  
*effects of applying an ACL, 338*  
*previewing, 335–336*  
**QoS policy configuration, 338–339**  
*assign traffic to forwarding class, 339–341*  
*configure scheduling parameters for each queue, 341–342*  
*configure the transport interface with the QoS map, 343–346*  
*map forwarding classes to hardware queues, 341*  
*map schedulers into a single QoS map, 342–343*  
**local-tloc command, 255**  
**LxC (Linux Virtual Containers), 361**  
  
**M**  


---

**management plane, 6–7, 25–27, 44**  
**manually configured networks, risks, 2–3**

**max-control-connections 0 command, 495–496**

**migrating to Cisco SD-WAN**

- branch design, 469
- complete CE replacement, 470–475
- data center, 462–463
- integration with branch firewall, 476–478
- integration with existing CE router, 475
- integration with voice services, 478–479
- loopback TLOC design, 465–466
- overlay and underlay integration
  - full overlay and underlay integration, 485–489*
  - overlay only, 480–481*
  - overlay with underlay backup, 481–485*
- preparation, 460–462
- service-side connectivity, 466–469
- transport-side connectivity, 463–465

**mobile devices, 4**

**monitoring**

- centralized policies, 147
- tunnel performance, 294

**MPLS (Multiprotocol Label Switching), 10–11**

**Multidomain, 18–19**

**multi-tenancy, Cisco SD-WAN (Software-Defined WAN), 38**

**multi-topology policies, 206–210**

## N

---

**naming**

- data policies, 238
- localized control policies, 326–327

**NAT (network address translation), 73–74, 81**

- address restricted cone, 76–77
- full cone, 74
- port restricted cone, 77–80
- symmetric, 75–76

**NAT fallback, 249–250, 253**

**nat use-vpn 0 action, 249–250, 253**

**network controllers, 3**

**networks. *See also* IBN (intent-based networking)**

- complexity, 8
- redundancy, 7, 7–8

## O

---

**OMP (Overlay Management Protocol), 34, 44, 47–48**

- graceful restart, 47
- origin types, 59–60
- redistribution, 58–60
- route attributes, 49–50
- routing loop prevention
  - BGP, 62–63*
  - EIGRP, 63–65*
  - OSPF, 60–62*
- service routes, 54–56
- status codes, 175
- TLOC routes, 52–54

**onboarding devices, 101–102**

- automatic provisioning, 103–105
- manual bootstrapping of a WAN Edge, 102

**orchestration plane, 44**

**OSPF (Open Shortest Path First), routing loop prevention, 60–62**

**overlay networks, 10–11**



## P

---

packet duplication, 274–280

packet forwarding, App-Route policies, 304

- SLA class action, 306–315
- traditional lookup in the routing table, 305–306

packet loss, protecting applications from, 269–270

- FEC (Forward Error Correction), 270–274
- packet duplication, 274–280

pairwise encryption keys, 86–87

parity packets, 271, 274

path quality monitoring, App-Route policies, 298

path selection, OMP, 56–58

PnP (Plug and Play), 101–102

policers, 119

policies. *See also* App-Route policies; centralized policies; control policies; data policies; localized policies

- centralized, 110–112, 117, 134–136
  - activation*, 125–127
  - application-aware routing*, 112
  - cflowd*, 112
  - construction*, 118, 122–125
  - control*, 111
  - isolating remote branches from each other*, 136–149
  - monitoring*, 147
  - multi-topology*, 206–210
  - VPN membership*, 111
- construction, 115–118
- definition, 119–122
- domains, 113–114

- firewall, 354
- lists, 118–119
- localized, 112–113
- matching criteria, 120–121
- packet forwarding order of operations, 127–128
- saving, 147

port restricted cone NAT, 77–80

PoS (point of sales) systems, 5–6

preferred-color command, 312

prefix lists, 118–119

on-premises deployment, 494

- Cisco SD-WAN (Software-Defined WAN), 38
- installation process, 495

previewing, localized data policies, 335–336

private cloud deployment, Cisco SD-WAN (Software-Defined WAN), 38

## Q

---

QoS (quality of service), 2–3, 5–6, 8, 112, 319–320, 339

policies, configuration

- assign traffic to forwarding class*, 339–341
- configure scheduling parameters for each queue*, 341–342
- configure the transport interface with the QoS map*, 343–346
- map forwarding classes to hardware queues*, 341
- map schedulers into a single QoS map*, 342–343

## R

---

redundancy, 7, 7–8

vSmart, 35

regional mesh networks, use case for centralized policies, 188–195

regionalizing Internet access, 180–188

RFC 4023, 27

RIB (Routing Information Base), 26–27

risks, of manually configured networks, 2–3

ROI models, 17–18

routers, 25–26

routing loop prevention

BGP, 62–63

EIGRP, 63–65

OSPF (Open Shortest Path First), 60–62

routing policies. *See also* policies, construction, 115–118

## S

---

SaaS (Software as a Service), 4, 5–6, 9, 19

Cloud onRamp

*benefits*, 395

*configuration*, 404–412

*DIA (Direct Internet Access)*, 395

*hybrid deployment*, 397

*monitoring statistics*, 398

*prerequisites for all site types*, 403

*prerequisites for DIA or gateway sites*, 404–412

*through a gateway*, 397

*vQoE score*, 398–399

saving, policies, 147

security

AMP (Advanced Malware Protection), 372–377

*dashboard*, 376–377

*monitoring statistics*, 375

*policy configuration*, 373–374

Application-Aware Enterprise Firewall

*actions*, 355

*dashboard*, 359

*firewall policy*, 353

*firewall policy configuration*, 356–359

*inter-zone security*, 356

*intra-zone security*, 355

*monitoring statistics*, 359

*self-zone policy*, 353

*zone pair*, 353

*zones*, 352–353

benefits, 351–352

cloud, 381–383

control plane, 45

data plane, 65–66

destination zone, 353

DIA (Direct Internet Access), 349–350, 350

DNS Web Layer security, 377–378  
*security policy configuration*, 378–381

IDS/IPS (intrusion detection and prevention), 360–361

application service containers, 360–361

*configuration*, 362–363

CVVS, 363

- dashboard*, 366–367
- policy configuration*, 365–366
- security virtual image upload*, 364–365
- signature sets*, 363–364
- policies, 112
- Snort, 361
- source zone, 353
- Threat Grid, 372–377
- threat surface, 350
- URL filtering, 350–351, 367–369
  - dashboard*, 371–372
  - policy configuration*, 369–371
- vManage authentication and authorization
  - local authentication with RBAC*, 384–387
  - remote authentication with RBAC*, 387–389
- WANs, 12
- segmentation**
  - data plane, 66, 81–82
  - end-to-end, 15
- self-zone policy**, 353
- sequences**
  - App-Route policies, 309–311
  - rules, App-Route policies, 289
  - types, data policies, 233–235
- service chaining**, 54–56
  - and the public cloud, 436
- service command**, 263
- service insertion**
  - CDFW (cloud-delivered firewall), 266–269
  - firewall, 195–200
- service local command**, 266–267
- service providers**, 9
- service routes**, 54–56
- show app-route stats command**, 310
- show bfd sessions command**, 73
- show bfd summary command**, 151–152
- show ip bgp command**, 174
- show omp routes command**, 175, 201–202, 204–206
- show omp services command**, 56
- show omp tlocs detail command**, 53–54
- show policy data-policy-filter command**, 241, 269
- show policy from-vsmart command**, 241
- show policy service-path command**, 250–252, 269
- show policy tunnel-path command**, 250–252
- show run omp command**, 59
- show run vpn 10 command**, 59
- show running-config policy command**, 306, 313–315, 344–346
- show tunnel statistics fec command**, 274
- Simulate Flows tool, 182, 241, 243, 244, 248, 310
- single points of failure, 7
- sla-class command**, 313
- SLAs (service-level agreements), 6–7, 9, 14, 253
  - class action, 306–308
  - class lists, 119, 287
  - App-Route policies*, 308–309
- Snort, 361, 372
- source zone, 353
- strict command**, 315

summarization, enabling branch-to-branch communication, 150–152  
 symmetric NAT, 75–76

## T

---

TCP-Opt, 280

templates, 91, 93–94

creating, 97–101

device, 94, 96–97

*adding localized control policy,*  
 327–330

feature, 94–95

options, 96–97

values, 95–96

Threat Grid, 349, 372–377

policy configuration, 373–374

TLOC lists, 119, 169

enabling branch-to-branch  
 communication, 152–168

tloc-list command, 166, 255

TLOCs (Transport Location  
 Identifiers), 52–54, 137–138,  
 139–140

colors, 66–68

*restrict keyword, 68–70*

loopback design, 465–466

sequence rules, 142–145

setting preferences

*with centralized policy, 171–*  
*176*

*with device templates, 177–178*

tloc-list, 166

TLS (Transport Layer Security),  
 45–46

traceroute command, 138, 148–149,  
 151–152, 168, 190, 194–195,  
 197–198, 207

transit VPCs, 413–415

transport independence, 9–12

trends

in cloud computing, 19–21

in the IT industry, 4–5

trusted applications, direct cloud  
 access, 243–252

tunnel groups, 70–73

## U

---

upgrading, Cisco IOS-XE, 31

URL filtering, 349, 350–351,  
 367–369

dashboard, 371–372

policy configuration, 369–371

use cases

control policies

*creating different network*  
*topologies per segment,*  
*206–210*

*creating extranets and access to*  
*shared services, 211–222*

*enabling branch-to-branch*  
*communication through data*  
*centers, 149–152, 152–168*

*enforcing security perimeters*  
*with service insertion,*  
*195–200*

*isolating guest users from the*  
*corporate WAN, 202–206*

*isolating remote branches from*  
*each other, 136–149*

*preferring regional data centers*  
*for Internet access, 180–188*

*regional mesh networks,*  
*188–195*

*traffic engineering at sites with*  
*multiple routers, 169–176,*  
*177–178*

- data policies, 228–229
  - application-based traffic engineering*, 253–260
  - direct cloud access for trusted applications*, 243–252
  - direct Internet access for guest users*, 230–242
  - protecting applications from packet loss*, 269–280
  - protecting corporate users with a cloud-delivered firewall*, 261–269

## V

---

- validating, CDFW service insertion, 266–269
- vAnalytics, 32–33
- vBond, 36–37
  - deployment
    - add controller to vManage*, 516–518
    - initial bootstrap configuration*, 514–515
  - initial system configuration, 514
  - root certificate chain install, 515
  - VPN 0 and VPN 512 configuration, 515
- version control, 91
- video, 4, 5–6
- Viptela devices, 508
  - minimal configuration, 102–103
- vManage, 32, 45, 353
  - authentication and authorization
    - local authentication with RBAC*, 384–387
    - remote authentication with RBAC*, 387–389
  - configuring Cloud onRamp for SaaS, 404–412
  - deployment, 503–505
    - apply initial bootstrap configuration*, 506–510
    - bootstrap and configure controller*, 506
    - generate certificates*, 511–512
  - GUI, 142
  - initial system configuration, 507
  - New Policy Wizard, 140–141
  - Real Time option, 137
  - VPN 0 and VPN 512 configuration, 508
  - whitelist files, 497
- VPC (virtual private cloud), 413
- vpn command, 507–508
- VPN lists, 119
- VPNs, 10–11, 27, 82
  - and VRFs, 28
  - zones, 352–353
- VRF (Virtual Routing and Forwarding), and VPNs, 28
- vSmart, 34–35, 44, 45, 57, 147
  - deployment
    - add controller to vManage*, 520–522
    - initial bootstrap configuration*, 519–520
  - displaying App-Route policy, 306–308
  - encryption, 35
  - initial system configuration, 519
  - OMP, 34
  - redundancy, 35
  - root certificate chain install, 520
  - VPN 0 and VPN 512 configuration, 519–520

## W

---

WAN Edges, 27, 28, 29, 32, 35, 44, 70, 350–351

administrative distances, 60

firewall, configuration, 197–198

manual bootstrapping, 102

QoS policy configuration, 339

*assign traffic to forwarding class, 339–341*

*configure scheduling parameters for each queue, 341–342*

*configure the transport interface with the QoS map, 343–346*

*map forwarding classes to hardware queues, 341*

*map schedulers into a single QoS map, 342–343*

vBond, 36–37

WANs, 4–5. *See also* Cisco SD-WAN (Software-Defined WAN); hybrid WANs

application support, 13

bandwidth, 9

common desired benefits, 5–7

connectivity, 12

redefining, 12–13

security, 12

use cases demanding changes in

*bandwidth aggregation and application load balancing, 13–14*

*DIA (Direct Internet Access), 15–16*

*end-to-end segmentation, 15*

*fully managed network solution, 16–17*

*protecting critical applications with SLAs, 14*

whitelist files, 497–498

## Z

---

zone pair, 353

zones, 352–353

ZTP (Zero Touch Provisioning), 101–102