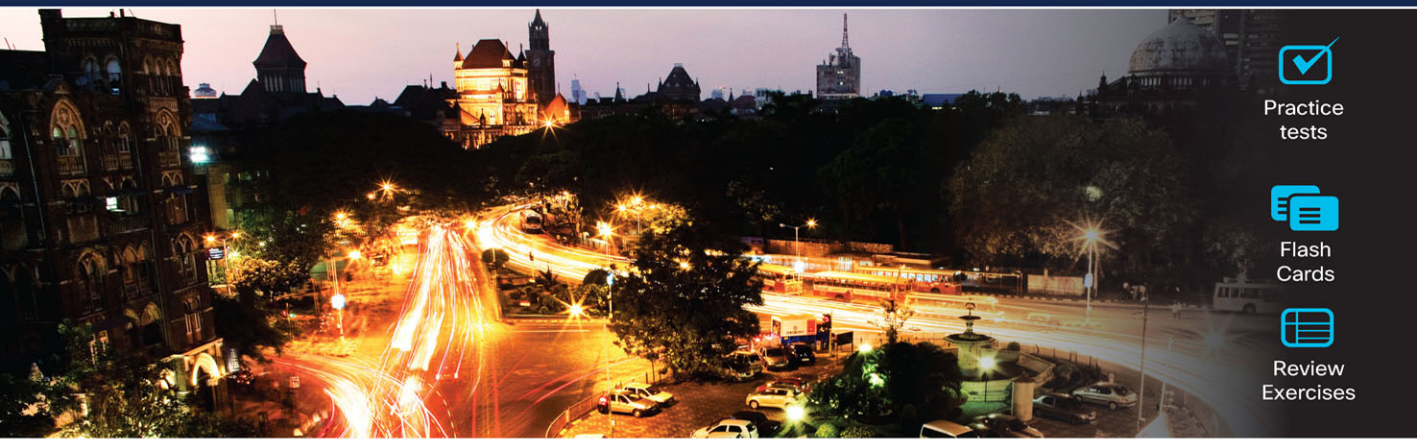
Official Cert Guide




Study Planner

# CCNP Enterprise Design

## Designing Cisco Enterprise Networks

## ENSLD 300-420

**2nd Edition**

**Anthony Bruno,** CCIE® No. 2738
**Steve Jordan,** CCIE® No. 11293

ciscopress.com

FREE SAMPLE CHAPTER

# CCNP Enterprise Design ENSLD 300-420 Official Cert Guide

**Second Edition**

## Companion Website and Pearson Test Prep Access Code

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

To access the companion website, simply follow these steps:

1. Go to www.ciscopress.com/register.
2. Enter the **print book ISBN:** 9780138247263.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

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

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

*This page intentionally left blank*

# CCNP Enterprise Design

## ENSLD 300-420

## **Official** Cert Guide

## Second Edition

**ANTHONY BRUNO, CCIE NO. 2738**
**STEVE JORDAN, CCIE NO. 11293**

**Cisco Press**

# CCNP Enterprise Design ENSLD 300-420 Official Cert Guide, Second Edition

Anthony Bruno
Steve Jordan



Published by:
Cisco Press
Hoboken, New Jersey



$PrintCode

Library of Congress Control Number: 2023949622

ISBN-13: 978-0-13-824726-3

ISBN-10: 0-13-824726-9

## Warning and Disclaimer

This book is designed to provide information about the CCNP Enterprise Design ENSLD 300-420 exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

## Trademark Acknowledgments

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

## Special Sales

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

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

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

## Feedback Information

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

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

We greatly appreciate your assistance.

**Vice President, IT Professional:** Mark Taub

**Alliance Manager:** Caroline Antonio

**Director, ITP Product Management:** Brett Bartow

**Executive Editor:** Nancy Davis

**Managing Editor:** Sandra Schroeder

**Development Editor:** Ellie Bru

**Senior Project Editor:** Tonya Simpson

**Copy Editor:** Chuck Hutchinson

**Technical Editor:** Kevin Yudong Wu

**Editorial Assistant:** Cindy Teeters

**Cover Designer:** Chuti Prasertsith

**Composition:** codeMantra

**Indexer:** Charlotte Kughen

**Proofreader:** Timothy Wright

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

## Pearson's Commitment to Diversity, Equity, and Inclusion

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

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

Our ambition is to purposefully contribute to a world where

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

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

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

# About the Authors

**Anthony Bruno**, CCIE No. 2738, is an enterprise architect with British Telecom (BT) with more than 30 years of experience in the internetworking field. Previously, he worked for International Network Services (INS) and Lucent Technologies, and he was a captain in the U.S. Air Force. He has consulted for many enterprise and service provider customers in the design, implementation, and optimization of large-scale networks. Anthony leads architecture and design teams in building next-generation networks for customers.

Anthony completed a master of science degree in electrical engineering at the University of Missouri–Rolla in 1994 and a bachelor of science in electrical engineering at the University of Puerto Rico–Mayaguez in 1990. For the past 23 years, he has coauthored *CCNP Enterprise Design ENSLD 300-420 Official Cert Guide: Designing Cisco Enterprise Networks* and five editions of the *CCDA Official Cert Guide* for Cisco Press.

Outside work, Anthony enjoys running marathons and Spartan obstacle races, and he has finished eight Ironman distance triathlons. He is also an avid genealogist and ancestry tree researcher. As an FAA certified remote pilot, Anthony also enjoys piloting his drone at home and when traveling.

**Steve Jordan**, CCIE No. 11293, is a principal architect with J. Network Architects and has 26 years of experience in the field of internetworking. For the last 16 years, Steve has specialized in data center and network security architectures involving compute, network, security, storage, and virtualization. Over the years, Steve has consulted with many enterprise and service provider customers in both pre-sales and post-sales engineering and architecture roles, along with working at several Cisco Gold Partners. He has extensive experience in data center and security architecture design and has implemented solutions in many energy, financial, gaming, healthcare, hospitality, and telecommunications industries. Steve is a 20-Year triple CCIE in the tracks of Enterprise Infrastructure, Storage Networking, and Data Center. His other certifications include CCNA, CCNP Enterprise, VMware VCIX6-NV, and VCP6-NV.

Steve lives in Houston, Texas, and when he is not working on technology, Steve can be found traveling to new places, enjoying sporting events, attending concerts, and trading stocks.

For the past 17 years, Steve has also coauthored *CCNP Enterprise Design ENSLD 300-420 Official Cert Guide: Designing Cisco Enterprise Networks* and three editions of the *CCDA Official Cert Guide*.

## About the Technical Reviewer

**Kevin Yudong Wu,** CCIE No. 10697 (Routing & Switching and Security), is a principal architect at AT&T Consulting. He has been engaged as a leading engineer in various network design projects, including LAN, WLAN, data center, and network security. Before joining AT&T, Kevin worked as a senior consultant at British Telecom (BT) and customer support engineer at Cisco High Touch Technical Support (HTTS), where he supported both Cisco LAN switching and security products. He holds master's degrees in both computer science (University of Texas at Arlington, 2003) and materials engineering (Beijing University of Aeronautics and Astronautics, 1995).

# Dedications

*Anthony Bruno:*

This book is dedicated to my wife of 32 years, Yvonne Bruno, Ph.D. Thank you for all your support during the development of this book.

*Steve Jordan:*

This book is dedicated to my love, Jelilian Jinang, for always supporting me during the development of this book. I also want to dedicate this book to my mother, Frances Brennan, and my dad, Steve Miller, for supporting me and providing encouragement during the writing of this book.

## Acknowledgments

This book would not have been possible without the efforts of many dedicated people.

I'd like to give special recognition to Ellie Bru, development editor, for providing her expert technical knowledge in editing the book. Thanks to Tonya Simpson, Nancy Davis, Brett Bartow, and Cindy Teeters for your support.

And thanks to my coauthor, Steve Jordan, for working with me again on developing this book. And a special thanks to the technical reviewer, Kevin Wu; your technical review, comments, and attention to detail made this book accurate.

—*Anthony Bruno*

This book would not have been possible without all the great people who have assisted me. I would first like to thank Anthony Bruno for inviting me to assist him in this endeavor once more. Thanks to Brett Bartow, Nancy Davis, and Tonya Simpson, for their guidance and support during the book's development. Thanks again to Ellie Bru, development editor, for supporting my schedule delays and keeping me on track.

Special thanks to the technical reviewer of this book, Kevin Wu, who provided wisdom and helped with keeping the book accurate.

Finally, thanks to all the managers and marketing people at Cisco Press who make all these books possible.

—*Steve Jordan*

# Contents at a Glance

## Reader Services

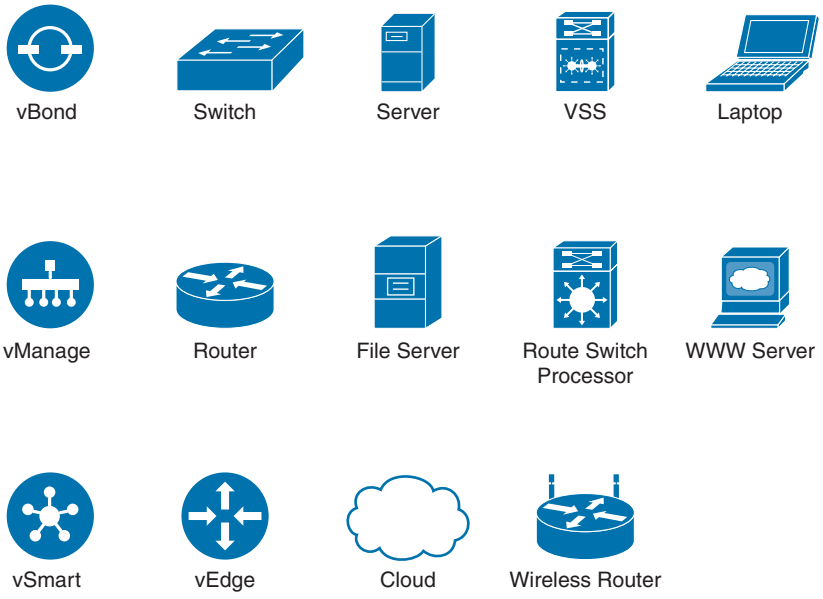
Register your copy at www.ciscopress.com/title/9780138247263 for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account.* Enter the product ISBN 9780138247263 and click **Submit**. When the process is complete, you will find any available bonus content under Registered Products.

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

# Contents

**Online Elements**

## Icons Used in This Book




## Command Syntax Conventions

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

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

# Introduction

Congratulations! If you are reading this Introduction, then you have probably decided to obtain a Cisco certification. Obtaining a Cisco certification will ensure that you have a solid understanding of common industry protocols along with Cisco's device architecture and configuration. Cisco has a high network infrastructure market share of routers, switches, and firewalls, and a global footprint.

Professional certifications have been an important part of the computing industry for many years and will continue to become more important. Many reasons exist for these certifications, but the most popularly cited reason is that they show the holder's credibility. All other factors being equal, a certified employee/consultant/job candidate is considered more valuable than one who is not certified.

Cisco provides three levels of certifications: Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP), and Cisco Certified Internetwork Expert (CCIE). The following are the most notable requirements:

- The CCNA certification is not a prerequisite for obtaining the CCNP certification.
- The exams test a candidate's ability to configure and troubleshoot network devices in addition to the candidate's ability to answer multiple-choice questions.
- The CCNP is obtained by taking and passing a Core exam and a Concentration exam.
- The CCIE certification requires candidates to pass the Core written exam before the CCIE lab can be scheduled.

CCNP Enterprise candidates need to take and pass the Implementing and Operating Cisco Enterprise Network Core Technologies ENCOR 350-401 examination. Then they need to take and pass one of the following Concentration exams to obtain their CCNP Enterprise certification:

- **300-410 ENARSI:** Implementing Cisco Enterprise Advanced Routing and Services
- **300-415 ENSDWI:** Implementing Cisco SD-WAN Solutions
- **300-420 ENSLD:** Designing Cisco Enterprise Networks
- **300-425 ENWLSD:** Designing Cisco Enterprise Wireless Networks
- **300-430 ENWLSI:** Implementing Cisco Enterprise Wireless Networks
- **300-435 ENAUTO:** Implementing Automation for Cisco Enterprise Solutions
- **300-440 ENCC:** Designing and Implementing Cloud Connectivity

This book helps you study for the Designing Cisco Enterprise Networks (ENSLD 300-420) exam. When you take the exam, you are allowed 90 minutes to complete about 60 questions. Testing is done at Pearson VUE testing centers or via Cisco online testing.

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

## Goals and Methods

The most important and somewhat obvious goal of this book is to help you pass the ENSLD 300-420 exam. In fact, if the primary objective of this book were different, then the book's title would be misleading; however, the methods used in this book to help you pass the ENSLD 300-420 exam are designed to also make you much more knowledgeable about how to do your job. While this book and the companion website together have more than enough questions to help you prepare for the actual exam, our goal is not simply to make you memorize as many questions and answers as you possibly can. One key methodology used in this book is to help you discover the exam topics that you need to review in more depth, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. So, this book does not try to help you pass by memorization but helps you truly learn and understand the topics. Designing Enterprise Networks is one of the concentration areas you can focus on to obtain the CCNP certification, and the knowledge tested in the ENSLD 300-420 exam is vitally important for a truly skilled enterprise network designer. This book would do you a disservice if it didn't attempt to help you learn the material.

This book will help you pass the ENSLD 300-420 exam by using the following methods:

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

## Who Should Read This Book?

This book is not designed to be a general networking topics book, although it can be used for that purpose. This book is intended to tremendously increase your chances of passing the ENSLD 300-420 CCNP exam. Although other objectives can be achieved by using this book, the book is written to help you pass the exam.

So why should you want to pass the ENSLD 300-420 CCNP exam? Because it's one of the milestones toward getting the CCNP certification. Getting this certification might translate to a raise, a promotion, and recognition. It would certainly enhance your resume. It would demonstrate that you are serious about continuing the learning process and that you're not content to rest on your laurels. It might also please your employer, which may need more certified employees.

## Strategies for Exam Preparation

The strategy you use to study for the ENSLD 300-420 exam might be slightly different than strategies used by other readers, depending on the skills, knowledge, and experience you already have obtained. For instance, if you have attended the ENSLD course, then you might take a different approach than someone who has learned enterprise design through on-the-job experience.

Regardless of the strategy you use or the background you have, this book is designed to help you get to the point where you can pass the exam in the least amount of time. For instance, there is no need to practice or read about IP addressing and subnetting if you fully understand it already. However, many people like to make sure that they truly know a topic and thus read over material that they already know. Some readers might want to jump into new technologies, such as SD-Access, SD-WAN, cloud-based services, and automation. Several book features will help you gain the confidence you need to be convinced that you know some material already and will help you know what topics you need to study more.

## The Companion Website for Online Content Review

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

To access the companion website, which gives you access to the electronic content provided with this book, start by establishing a login at www.ciscopress.com and registering your book. To do so, simply go to www.ciscopress.com/register and enter the ISBN of the print book: **9780138247263**. After you have registered your book, go to your account page and click the **Registered Products** tab. From there, click the **Access Bonus Content** link to get access to the book's companion website.

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

## How to Access the Pearson Test Prep (PTP) App

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

- **Print book:** You can get your access code by registering the print ISBN (9780138247263) on ciscopress.com/register. Make sure to use the print book ISBN regardless of whether you purchased an eBook or the print book. Once you register the book, your access code will be populated on your account page under the Registered Products tab. Instructions for how to redeem the code are available on the book's companion website by clicking the Access Bonus Content link.
- **Premium Edition:** If you purchase the Premium Edition eBook and Practice Test directly from the Cisco Press website, the code will be populated on your account page after purchase. Just log in at www.ciscopress.com, click **Account** to see details of your account, and click the **Digital Purchases** tab.

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

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

**Step 1.** Open this book's companion website, as just described.

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

**Step 3.** Follow the instructions provided 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 pearsontestprep.com, log in using the same credentials used to register your book or purchase the Premium Edition, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

## How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need to work with further. Chapters 1 through 5 cover IPv4, IPv6, EIGRP, OSPF, IS-IS, BGP, multicast, and network management. Chapters 6 and 7 cover enterprise LAN campus design. Chapters 8 and 9 cover WAN design. Chapters 10, 11, and 12 cover newer technologies, including SD-Access, SD-WAN, and automation. If you intend to read all the chapters, the order in the book is an excellent sequence to use.

The core chapters, Chapters 1 through 12, cover the following topics:

- **Chapter 1, "Internet Protocol Version 4 (IPv4) Design":** This chapter discusses the IPv4 header, addressing, subnet design, and protocols used by IPv4.
- **Chapter 2, "Internet Protocol Version 6 (IPv6) Design":** This chapter covers the IPv6 header, addressing, design best practices, and migration strategies.
- **Chapter 3, "Routing Protocol Characteristics, EIGRP, and IS-IS":** This chapter discusses metrics, design, and operation for EIGRP and IS-IS routing protocols.
- **Chapter 4, "OSPF, BGP, and Route Manipulation":** This chapter discusses OSPF and BGP routing protocols and summarization, redistribution, and manipulation of routing information.
- **Chapter 5, "IP Multicast and Network Management":** This chapter discusses multicast routing concepts, multicast services, and network management techniques.
- **Chapter 6, "Enterprise LAN Design and Technologies":** This chapter covers the design of Layer 2 infrastructures, hierarchical network models, LAN media, STP design considerations, and Layer 2 security technologies.
- **Chapter 7, "Advanced Enterprise Campus Design":** This chapter discusses campus LAN design and best practices, first-hop redundancy protocols, and high availability design.
- **Chapter 8, "WAN for the Enterprise":** This chapter discusses WANs, WAN transport technologies, cloud-based services, and site-to-site VPN design.

- **Chapter 9, "WAN Availability and QoS":** This chapter discusses WAN design methodologies, high availability, Internet connectivity, backup connectivity, and quality of service.
- **Chapter 10, "SD-Access Design":** This chapter discusses SD-Access architecture and SD-Access fabric design considerations for both wired and wireless access.
- **Chapter 11, "SD-WAN Design":** This chapter discusses SD-WAN architecture, the orchestration plane, the control plane and overlay design, scalability, security, and Cloud OnRamp design.
- **Chapter 12, "Automation":** This chapter discusses network APIs, NETCONF, RESTCONF, GRPC, GNMI, and model-driven telemetry.

## Certification Exam Topics and This Book

The questions for each certification exam are a closely guarded secret. However, we do know which topics you must know to *successfully* complete this exam. Cisco publishes them as an exam blueprint for the Designing Cisco Enterprise Networks ENSLD 300-420 exam. Table I-1 lists the exam topics listed in the blueprint and provides a reference to the book chapter that covers each topic. These are the topics you should be proficient in when designing Cisco enterprise networks in the real world.

**Table I-1** ENSLD 300-420 1.1 Exam Topics and Chapter References

| ENSLD 300-420 Exam Topic | Chapter(s) in Which Topic Is Covered |
|---|---|
| **1.0 Advanced Addressing and Routing Solutions** | |
| 1.1 Create structured addressing plans for IPv4 and IPv6 | 1, 2 |
| 1.2 Create stable, secure, and scalable routing designs for IS-IS | 3 |
| 1.3 Create stable, secure, and scalable routing designs for EIGRP | 3 |
| 1.4 Create stable, secure, and scalable routing designs for OSPF | 4 |
| 1.5 Create stable, secure, and scalable routing designs for BGP | 4 |
| *1.5.a Address families* | 4 |
| *1.5.b Basic route filtering* | 4 |
| *1.5.c Attributes for path preference* | 4 |
| *1.5.d Route reflectors* | 4 |
| *1.5.e Load sharing* | 4 |
| 1.6 Determine IPv6 migration strategies | 2 |
| *1.6.a Overlay (tunneling)* | 2 |
| *1.6.b Native (dual-stacking)* | 2 |
| *1.6.c Boundaries (IPv4/IPv6 translations)* | 2 |
| **2.0 Advanced Enterprise Campus Networks** | |
| 2.1 Design campus networks for high availability | 7 |

| ENSLD 300-420 Exam Topic | Chapter(s) in Which Topic Is Covered |
|---|---|
| *2.1.a First Hop Redundancy Protocols* | 7 |
| *2.1.b Platform abstraction techniques* | 12 |
| *2.1.c Graceful restart* | 4 |
| *2.1.d BFD* | 4 |
| 2.2 Design campus Layer 2 infrastructures | 6 |
| *2.2a STP scalability* | 6 |
| *2.2.b Fast convergence* | 6 |
| *2.2.c Loop-free topologies* | 6 |
| *2.2.d PoE and WoL* | 6 |
| *2.2e Layer 2 security techniques such as STP security, port security, VACL* | 6 |
| 2.3 Design multicampus Layer 3 infrastructures | 7 |
| *2.3.a Convergence* | 7 |
| *2.3.b Load sharing* | 7 |
| *2.3.c Route summarization* | 7, 4 |
| *2.3.d Route filtering* | 7, 4 |
| *2.3.e VRFs* | 4 |
| *2.3.f Optimal topologies* | 7 |
| *2.3.g Redistribution* | 4 |
| 2.4 Describe SD-Access architecture (underlay, overlay, control and data plane, automation, wireless, and security) | 10 |
| 2.5 Describe SD-Access fabric design considerations for wired and wireless access (overlay fabric design, control plane design, border design, segmentation, virtual networks, scalability, over the top and fabric for wireless, multicast) | 10 |
| **3.0 WAN for Enterprise Networks** | |
| 3.1 Describe WAN connectivity options for on-premises, hybrid, and cloud solutions | 8, 9 |
| *3.1.a Layer 2 VPN* | 8 |
| *3.1.b MPLS Layer 3 VPN* | 8 |
| *3.1.c Metro Ethernet* | 8 |
| *3.1.d DWDM* | 8 |
| *3.1.e 4G/5G* | 8 |
| *3.1.f SD-WAN customer edge* | 8, 11 |
| 3.2 Design site-to-site VPN for on-premises, hybrid, and cloud solutions | 8 |
| *3.2.a Dynamic Multipoint VPN (DMVPN)* | 8 |

| ENSLD 300-420 Exam Topic | Chapter(s) in Which Topic Is Covered |
|---|---|
| *3.2.b Layer 2 VPN* | 8 |
| *3.2.c MPLS Layer 3 VPN* | 8 |
| *3.2.d IPsec* | 8 |
| *3.2.e Generic Routing Encapsulation (GRE)* | 8 |
| *3.2.f Group Encrypted Transport VPN (GET VPN)* | 8 |
| 3.3 Design high availability for enterprise WAN for on-premises, hybrid, and cloud solutions | 9 |
| *3.3.a Single-homed* | 9 |
| *3.3.b Multihomed* | 9 |
| *3.3.c Backup connectivity* | 9 |
| *3.3.d Failover* | 9 |
| 3.4 Describe Cisco SD-WAN architecture (orchestration plane, management plane, control plane, data plane, on-boarding, and provisioning, security) | 11 |
| 3.5 Describe Cisco SD-WAN design considerations (control plane design, overlay design, LAN design, high availability, redundancy, scalability, security design, QoS, and multicast over SD-WAN fabric) | 11 |
| **4.0 Network Services** | |
| 4.1 Select appropriate QoS strategies to meet customer requirements (DiffServ, IntServ) | 9 |
| 4.2 Design end-to-end QoS policies | 9 |
| *4.2.a Classification and marking* | 9 |
| *4.2.b Shaping* | 9 |
| *4.2.c Policing* | 9 |
| *4.2.d Queuing* | 9 |
| 4.3 Design network management techniques | 5 |
| *4.3.a In-band vs. out-of-band* | 5 |
| *4.3.b Segmented management networks* | 5 |
| *4.3.c Prioritizing network management traffic* | 5 |
| 4.4 Describe multicast routing concepts (source trees, shared trees, RPF, rendezvous points) | 5 |
| 4.5 Design multicast services (SSM, PIM directional, MSDP) | 5 |
| **5.0 Automation** | |
| 5.1 Differentiate between IETF, OpenConfig, and Cisco YANG models | 12 |
| 5.2 Differentiate between NETCONF and RESTCONF | 12 |

| ENSLD 300-420 Exam Topic | Chapter(s) in Which Topic Is Covered |
|---|---|
| 5.3 Describe the impact of model-driven telemetry on the network | 12 |
| *5.3.a Periodic publication* | 12 |
| *5.3.b On-change publication* | 12 |
| 5.4 Describe GRPC and GNMI | 12 |
| 5.5 Describe cloud connectivity options such as direct connect, cloud on ramp, MPLS direct connect, and WAN integration | 8, 11 |
| 5.6 Describe cloud-based service models in private, public, and hybrid deployments (SaaS, PaaS, IaaS) | 8, 11 |

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

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

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

Note that as CCNP enterprise network technologies continue to evolve, Cisco reserves the right to change the exam topics without notice. Although you can refer to the list of exam topics in Table I-1, always check Cisco.com to verify the actual list of topics to ensure that you are prepared before taking the exam. You can view the current exam topics on any current Cisco certification exam by visiting the Cisco.com website, choosing More, choosing Training & Events, choosing Certifications, and selecting the appropriate certification. Note also that, if needed, Cisco Press might post additional preparatory content on the web page associated with this book, at http://www.ciscopress.com/title/9780138247263. It's a good idea to check the website a couple weeks before taking your exam to be sure that you have up-to-date content.

*This page intentionally left blank*

CHAPTER 9

# WAN Availability and QoS

**This chapter covers the following subjects:**

**WAN Design Methodologies:** This section discusses the processes of identifying business and technology strategies, assessing the existing network, and creating a design that is scalable, flexible, and resilient.

**Design for High Availability:** This section covers removing the single points of failure from a network design by using software features or hardware-based resiliency.

**Internet Connectivity:** This section discusses public network access and securely connecting business locations.

**Backup Connectivity:** This section discusses providing an alternative WAN path between locations when primary paths are unavailable.

**QoS Strategies:** This section discusses design models for providing QoS service differentiation.

**Designing End-to-End QoS Policies:** This section discusses options for QoS mechanisms such as queuing, policing, and traffic shaping.

This chapter covers WAN design and QoS. Expect plenty of questions on the ENSLD 300-420 exam about the selection and use of WAN designs in enterprise networks. A CCNP enterprise designer must understand WAN availability and the QoS models that are available to protect traffic flows in the network. This chapter starts with WAN methodologies and then covers WAN availability with deployment models using MPLS, hybrid, and Internet designs. This chapter also explores backup connectivity and failover designs. Finally, it covers QoS strategies and designing end-to-end QoS policies.

## "Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz helps you identify your strengths and deficiencies in this chapter's topics. This quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you determine how to spend your limited study time. Table 9-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quiz Questions and Q&A Questions."

**Table 9-1** "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

| Foundation Topics Section | Questions Covered in This Section |
|---|---|
| WAN Design Methodologies | 1–2 |
| Design for High Availability | 3 |
| Internet Connectivity | 4–5 |
| Backup Connectivity | 6 |
| QoS Strategies | 7–8 |
| Designing End-to-End QoS Policies | 9–10 |

1. Which of the following is a measure of data transferred from one host to another in a given amount of time?
   a. Reliability
   b. Response time
   c. Throughput
   d. Jitter
2. Which of the following is a description of the key design principle scalability?
   a. Modularity with additional devices, services, and technologies
   b. Redundancy through hardware, software, and connectivity
   c. Ease of managing and maintaining the infrastructure
   d. Providing enough capacity and bandwidth for applications
3. What percentage of availability allows for four hours of downtime in a year?
   a. 99.5%
   b. 99.99%
   c. 99.999%
   d. 99.95%
4. What Internet connectivity option provides the highest level of resiliency for services?
   a. Single-router dual-homed
   b. Single-router single-homed
   c. Dual-router dual-homed
   d. Shared DMZ
5. Which of the following eliminates single points of failures with the router and the circuit?
   a. Dual-router dual-homed
   b. Single-router dual-homed
   c. Shared DMZ
   d. Single-router single-homed
6. What backup option allows for both a backup link and load-sharing capabilities using the available bandwidth?
   a. Dial backup
   b. Secondary WAN link

c. IPsec tunnel
d. GRE tunnel

7. Which of the following adds a strict priority queue to modular class-based QoS?
   a. FIFO
   b. CBWFQ
   c. WFQ
   d. LLQ
8. Which of the following is a mechanism to handle traffic overflow using a queuing algorithm with QoS?
   a. Congestion management
   b. Traffic shaping and policing
   c. Classification
   d. Link efficiency
9. Which QoS model uses Resource Reservation Protocol (RSVP) to explicitly request QoS for the application along the end-to-end path through devices in the network?
   a. DiffServ
   b. IntServ
   c. CBWFQ
   d. BE
10. What technique does traffic shaping use to release the packets into the output queue at a preconfigured rate?
   a. Token bucket
   b. Leaky bucket
   c. Tagging
   d. Interleaving

## Foundation Topics

This chapter describes the WAN design and QoS topics you need to master for the ENSLD 300-420 exam. These topics include WAN methodologies in the enterprise edge, WAN availability, and WAN designs including backup and failover options. In addition, this chapter describes quality of service (QoS) and how it can be used to prioritize network traffic and better utilize the available WAN bandwidth.

## WAN Design Methodologies

WAN design methodologies should be used when designing enterprise edge networks. Some keys to WAN design are the following processes:


- **Identifying the network requirements:** This includes reviewing the types of applications, the traffic volume, and the traffic patterns in the network.
- **Assessing the existing network:** This involves reviewing the technologies used and the locations of hosts, servers, network equipment, and other end nodes.

- **Designing the topology:** This is based on the availability of technology as well as the projected traffic patterns, technology performance, constraints, and reliability.

When designing the WAN topology, remember that the design should describe the functions that the enterprise modules should perform. The expected service levels provided by each WAN technology should be explained. WAN connections can be characterized by the cost of renting the transmission media from the service provider to connect two or more sites.

New network designs should be flexible and adaptable to future technologies and should not limit the customer's options going forward. For example, collaboration applications such as VoIP and video are common now, and most enterprise network designs should be able to support them. The customer should not have to undergo major hardware upgrades to implement these types of technologies. The ongoing support and management of the network are other important factors, and the design's cost-effectiveness is important as well.

Table 9-2 lists key design principles that can help serve as the basis for developing network designs.

Key Topic

**Table 9-2** Key Design Principles

| Design Principle | Description |
|---|---|
| High availability | Redundancy through hardware, software, and connectivity |
| Scalability | Modularity with additional devices, services, and technologies |
| Security | Measures to protect business data |
| Performance | Enough capacity and bandwidth for applications |
| Manageability | Ease of managing and maintaining the infrastructure |
| Standards and regulations | Compliance with applicable laws, regulations, and standards |
| Cost | Appropriate security and technologies given the budget |

High availability is what most businesses and organizations strive for in sound network designs. The key components of application availability are response time, throughput, and reliability. Real-time applications such as voice and video are not very tolerant of jitter and delay.

Table 9-3 identifies various application requirements for data, voice, and video traffic.

Key Topic

**Table 9-3** Application Requirements for Data, Voice, and Video Traffic

| Characteristic | Data File Transfer | Interactive Data Application | Real-Time Voice | Real-Time Video |
|---|---|---|---|---|
| **Response time** | Reasonable | Within a second | One-way delay less than 150 ms with low delay and jitter | Minimum delay and jitter |
| **Throughput and packet loss tolerance** | High/medium | Low/low | Low/low | High/medium |
| **Downtime (high reliability = low downtime)** | Reasonable | Low | Low | Minimum |

### Response Time

**Response time** is a measure of the time between a client user request and a response from the server host. An end user will be satisfied with a certain level of delay in response time. However, there is a limit to how long the user will wait. This amount of time can be measured and serves as a basis for future application response times. Users perceive the network communication in terms of how quickly the server returns the requested information and how fast the screen updates. Some applications, such as a request for an HTML web page, require short response times. On the other hand, a large FTP transfer might take awhile, but this is generally acceptable.

### Throughput

In network communications, **throughput** is a measure of data transferred from one host to another in a given amount of time. Bandwidth-intensive applications have a greater impact on a network's throughput than does interactive traffic such as a Telnet session. Most high-throughput applications involve some type of file-transfer activity. Because throughput-intensive applications have longer response times, you can usually schedule them when time-sensitive traffic volumes are lower, such as after hours.

### Reliability

**Reliability** is a measure of a given application's availability to its users. Some organizations require rock-solid application reliability, such as five nines (99.999%); this level of reliability has a higher price than most other applications. For example, financial and security exchange commissions require nearly 100% uptime for their applications. These types of networks are built with a large amount of physical and logical redundancy. It is important to ascertain the level of reliability needed for a network that you are designing. Reliability goes further than availability by measuring not only whether the service is there but whether it is performing as it should.

### Bandwidth Considerations

Table 9-4 compares several WAN technologies in terms of speeds and media types.

Key Topic

**Table 9-4** Physical Bandwidth Comparison

| WAN Connectivity | Bandwidth: Up to 100 Mbps | Bandwidth: 1 Gbps to 10 Gbps |
|---|---|---|
| Copper | Fast Ethernet | Gigabit Ethernet, 10 Gigabit Ethernet |
| Fiber | Fast Ethernet | Gigabit Ethernet, 10 Gigabit Ethernet, SONET/SDH, dark fiber |
| Wireless<br>LTE/5G | 802.11a/g<br>LTE/LTE Advanced | 802.11n/ac Wave1/Wave2<br>LTE Advance Pro/5G |

A WAN designer must engineer the network with enough bandwidth to support the needs of the users and applications that will use the network. How much bandwidth a network needs depends on the services and applications that will require network bandwidth. For example, VoIP requires more bandwidth than interactive Secure Shell (SSH) traffic. A large number of graphics or CAD drawings require an extensive amount of bandwidth compared to file or print sharing information being transferred on the network. A big driver in

increasing demand for bandwidth is the expanded use of collaboration applications that utilize video interactively.

When designing bandwidth for a WAN, remember that implementation and recurring costs are important factors. It is best to begin planning for WAN capacity early. When the link utilization reaches around 50% to 60%, you should consider increases and closely monitor the capacity. When the link utilization reaches around 75%, immediate attention is required to avoid congestion problems and packet loss that will occur when the utilization nears full capacity.

QoS techniques become increasingly important when delay-sensitive traffic such as VoIP is using the limited bandwidth available on the WAN. LAN bandwidth, on the other hand, is generally inexpensive and plentiful; in the age of robust real-time applications, however, QoS can be necessary. To provide connectivity on the LAN, you typically need to be concerned only with hardware and implementation costs.

## Design for High Availability

Most businesses need a high level of availability, especially for their critical applications. The goal of high availability is to remove the single points of failure in the network design by using software features or hardware-based resiliency. Redundancy is critical in providing high levels of availability for the enterprise. Some technologies have built-in techniques that enable them to be highly available. For technologies that do not have high availability, other techniques can be used, such as additional WAN circuits or backup power supplies.

### Defining Availability

System availability is a ratio of the expected uptime to the amount of downtime over the same period of time. Let's take an example of 4 hours of downtime per year. There are 365 days in a year, which equals 8760 hours (365 × 24 = 8760). Now, if we subtract 4 hours from the annual total of 8760 hours, we get 8756. Then, if we figure 8756 / 8760 × 100, we get the amount of availability percentage, which in this case is 99.95%.

Table 9-5 shows the availability percentages from 99% to 99.999999%, along with amounts of downtime per year.

Key Topic

**Table 9-5** Availability Percentages

| Availability | Downtime per Year | The Nines of Availability | Targets |
|---|---|---|---|
| 99.000000% | 3.65 days | Two nines | |
| 99.900000% | 8.76 hours | Three nines | |
| 99.990000% | 52.56 minutes | Four nines | Branch WAN high availability |
| 99.999000% | 5.256 minutes | Five nines | Branch WAN high availability |
| 99.999900% | 31.536 seconds | Six nines | Ultra high availability |
| 99.999990% | 3.1536 seconds | Seven nines | Ultra high availability |
| 99.999999% | .31536 seconds | Eight nines | Ultra high availability |

Figure 9-1 illustrates WAN router paths and the impacts to availability depending on the level of redundancy used.

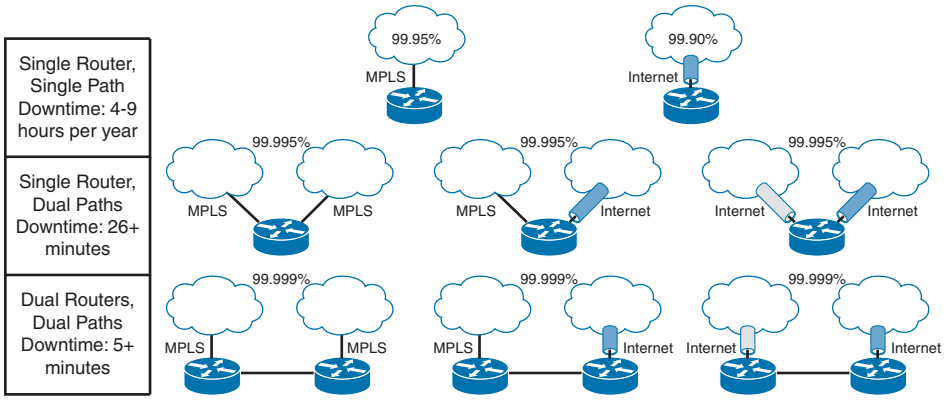



**Figure 9-1** *Router Paths and Availability Examples*

## Deployment Models

There are three common deployment models for WAN connectivity, each with pros and cons:

Key Topic

- **MPLS WAN:** Single- or dual-router MPLS VPN
- **Hybrid WAN:** MPLS VPN and Internet VPN
- **Internet WAN:** Single- or dual-router Internet VPN

An MPLS WAN involves single or dual routers for the MPLS VPN connections. It provides for the highest in SLA guarantees for both QoS capabilities and network availability. However, this option is the most expensive, and it ties the organization to the service provider. New cloud-based designs are using MPLS Direct Connect to provide connectivity to AWS, Azure, and Google Cloud.

A hybrid WAN combines an MPLS VPN and an Internet VPN on a single router or on a pair of routers. This deployment model offers a balanced cost option between the higher-cost MPLS VPN connection and the lower-cost Internet VPN for backup. With a hybrid WAN, traffic can be split between the MPLS VPN for higher-priority-based traffic and Internet VPN for lower-priority-based traffic. Newer WAN designs are also using SDWAN with both MPLS and Internet-based transports.

An Internet WAN includes a single router or dual routers using Internet-based VPN only. These can also include cloud solutions for connectivity to AWS, Azure, and Google Cloud. This deployment model is the lowest-cost option but lacks the SLAs and QoS capabilities offered by carriers. The enterprise would be responsible for providing SLAs to the end users.

## Redundancy Options

Depending on the cost of downtime for an organization, different levels of redundancy can be implemented for a remote site. The more critical WAN sites will use higher levels of redundancy. With any of the deployment options—MPLS WAN, hybrid WAN, or Internet WAN—you can design redundant links with redundant routers, a single router with redundant links, or a single router with a single link.

For the most critical WAN sites, you typically want to eliminate single points of failure by designing with dual routers and dual WAN links along with dual power supplies. However, this highly available option comes with a higher price tag and is more complex to manage, but it offers failover capabilities. Another option available to reduce cost is to use a single router with dual power supplies and multiple WAN links providing power and link redundancy. Non-redundant, single-homed sites are the lowest cost, but they have multiple single points of failure inherent with the design, such as the WAN carrier or WAN link.

## Single-Homed Versus Multi-Homed WANs

The advantages of working with a single WAN carrier are that you have only one vendor to manage, and you can work out a common QoS model that can be used throughout your WAN. The major drawback with a single carrier is that if the carrier has an outage, it can be catastrophic to your overall WAN connectivity. This also makes it difficult to transition to a new carrier because all your WAN connectivity is with a single carrier.

On the other hand, if you have dual WAN carriers, the fault domains are segmented, and there are typically more WAN offerings to choose from because you are working with two different carriers. This design also allows for greater failover capabilities with routing and software redundancy features. The disadvantages with dual WAN carriers are that the overall design is more complex to manage, and there will be higher recurring WAN costs.

## Single-Homed MPLS WANs

Key Topic

In a single-MPLS-carrier design, each site is connected to a single MPLS VPN from one provider. For example, you might have some sites that are single-homed and some sites that are dual-homed to the MPLS VPN. Each site will consist of CE routers peering with the provider using eBGP, and iBGP will be used for any CE-to-CE peering. Each CE will advertise any local prefixes to the provider with BGP and redistribute any learned BGP routes from the provider into the IGP or use default routing. Common IGPs are standard-based OSPF and EIGRP.

Figure 9-2 illustrates a single-MPLS-carrier design with single- and dual-homed sites.

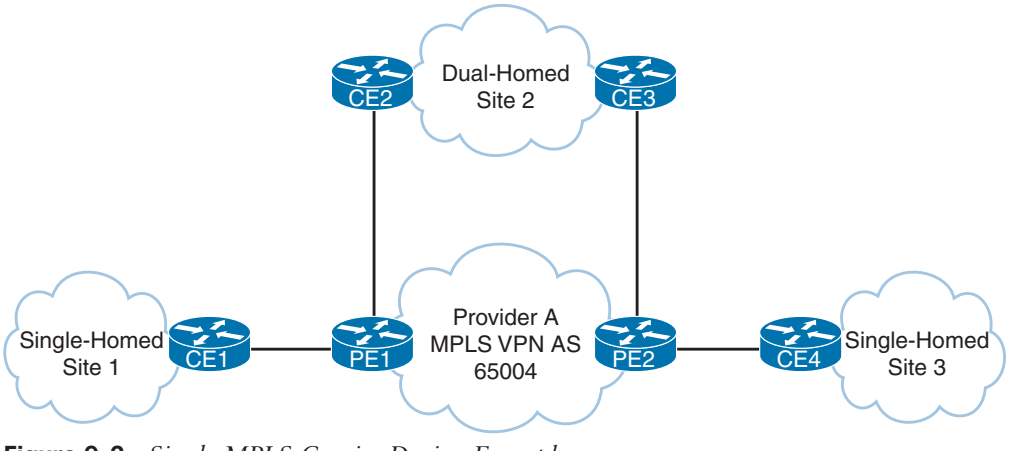



**Figure 9-2** *Single-MPLS-Carrier Design Example*

## Multi-Homed MPLS WANs

Key Topic

In a dual-MPLS-carrier design, each site is connected to both provider A and provider B. Some sites might have two routers for high availability, and others might have only a single router but with two links for link and provider redundancy. For example, each CE router would redistribute local routes from EIGRP into BGP. Routes from other sites would be redistributed from BGP into EIGRP as external routes. For sites that have two routers, filtering or tagging of the routes in and out of BGP would be needed to prevent routing loops.

Figure 9-3 illustrates a dual-MPLS-carrier design with single and dual routers.

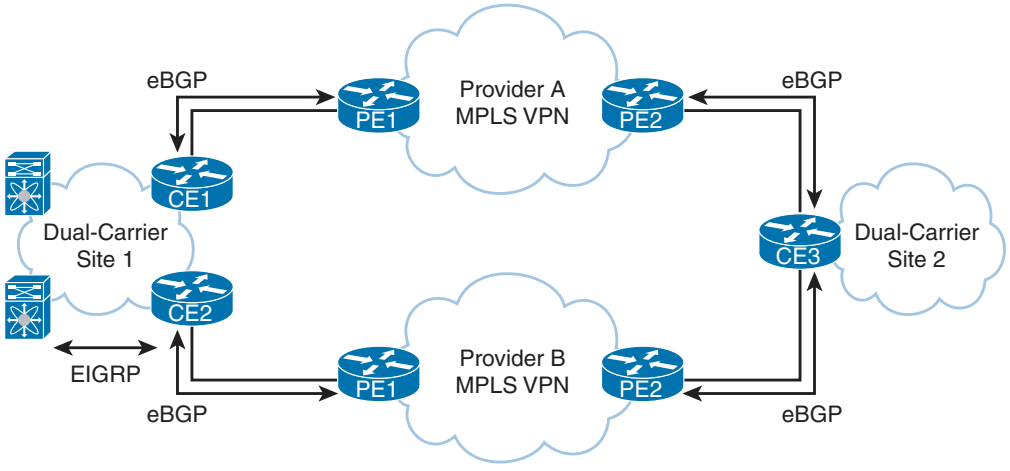



**Figure 9-3** *Dual-MPLS-Carrier Design Example*

## Hybrid WANs: Layer 3 VPN with Internet Tunnels

Key Topic

Hybrid WAN designs involve using an MPLS VPN for the primary connection and an Internet tunnel for the backup connection. In this design, eBGP would be used to peer with the MPLS VPN provider, and EIGRP would be used for routing for the IGP internally. At each site, the CE router would learn routes from the MPLS VPN via BGP and redistribute the routes from BGP into EIGRP. Then each site would redistribute EIGRP routes into BGP and use EIGRP to peer with other local routers at each site. The Internet tunnel routers would use EIGRP to exchange routes inside the VPN tunnels, and they would not need to redistribute routing information because they would run only EIGRP. On the MPLS VPN router, BGP-learned routes would be preferred because the BGP routes that would be redistributed into EIGRP routes would have a lower administrative distance. In this case, if you want the MPLS VPN router to be the primary path, you need to run an FHRP between the dual-homed routers, with the active router being the MPLS VPN-connected router. That way, it would choose the MPLS VPN path as the primary path and use the Internet tunnel path as the backup path for failover. Another option would be to modify the routing protocol metrics so that the MPLS VPN path is preferred. Another hybrid design approach is WAN integration that can be used to provide high availability for cloud connectivity with AWS, Azure, and Google Cloud.

WAN integration is a service that provides seamless connectivity between a customer's on-premises hosted data center and a cloud provider's data center. This service is delivered

through a hybrid WAN architecture that combines MPLS and Internet connections. WAN integration allows for improved application performance, optimized traffic routing, and reduced costs compared to dedicated MPLS connections.

Figure 9-4 illustrates a hybrid WAN design with an MPLS VPN and an Internet VPN.

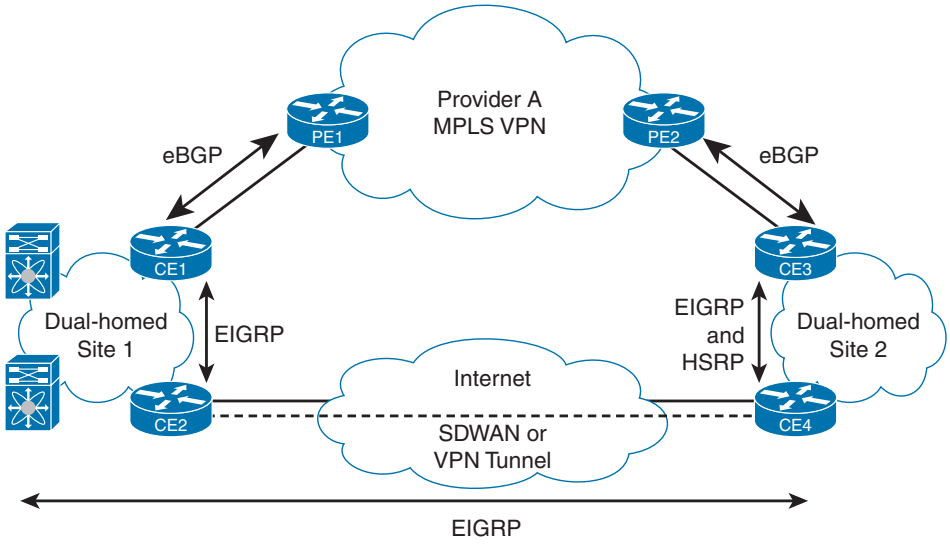



**Figure 9-4** *Hybrid WAN Design Example*

## Internet Connectivity

Most enterprises have multiple sites with different numbers of users at the sites, but they are usually grouped into two site types: larger central WAN sites and smaller branch WAN sites. The larger site types typically host more of the users and services. The smaller branch offices tend to have a low user count and a smaller number of hosted services. Both central and branch sites typically need Internet access, but there are high availability considerations to think about when selecting the Internet access design for a given site type. When choosing an Internet connectivity option, remember to consider the business requirements and the budget allocated for the design.

Internet connectivity options include the following:

- **Dual-router dual-homed:** Provides the highest level of resiliency for Internet connectivity with full redundancy in hardware, links, and Internet service providers.
- **Single-router dual-homed:** Provides a good level of redundancy for Internet connectivity through the use of multiple links and multiple Internet service providers.
- **Single-router single-homed:** Provides the bare minimum for Internet connectivity, providing no levels of redundancy for the hardware, links, or Internet service providers.

Figure 9-5 shows Internet connectivity options with different levels of redundancy.

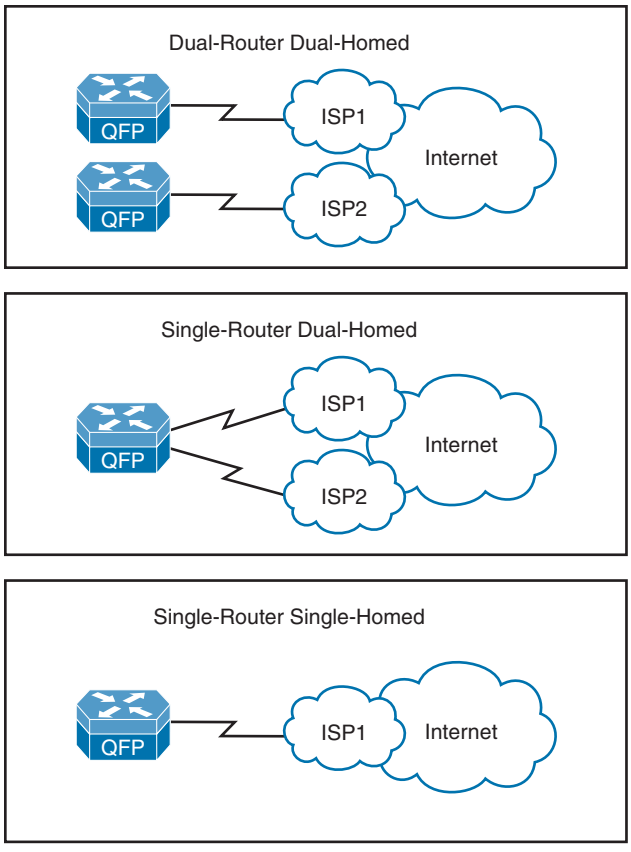



**Figure 9-5** *Internet Connectivity Options*

Because central sites have larger user populations, they normally have higher Internet bandwidth connectivity and centralized access control for the Internet traffic flows. Although most branch offices have Internet connections, many of them still have their Internet traffic backhauled over the WAN to the central site, where centralized access control can occur.

## Internet for Remote Sites

When designing the Internet traffic flows for remote site locations, you have two main options to consider. One option, referred to as centralized Internet access, involves tunneling all the Internet traffic back to the data center or main site. With this option, you have more control over the Internet traffic with centralized security services such as URL filtering, firewalling, and intrusion prevention. However, this approach has some drawbacks because the bandwidth requirements and cost will be higher for your WAN links to the branch locations, and it increases the delay for any Internet-based traffic. Another option is to allow Internet-destined traffic at each branch to use the dedicated local Internet connection or VPN split tunneling. There are some advantages with this approach; your bandwidth requirements and the cost for your MPLS VPN links will be lower for your branch locations because you do not need to transport Internet traffic on them. This approach does have some drawbacks, however, because the local Internet access may violate your security policy by exposing more Internet points within your organization that need protection with security services.

Here are some pros and cons of each of these options:

- **Centralized Internet for each remote site:** Higher bandwidth is available, and security policies are centralized, but traffic flows are suboptimal. This option might require additional redundancy at the Internet edge, which may or may not be present.
- **Direct Internet for remote site:** Traffic flows are optimal, but it is more difficult to manage distributed security policies. This option also has a higher risk of Internet attacks due to the greater number of attachment points.

### High Availability for the Internet Edge

When you have decided to have two Internet routers, each with a link to two different Internet service providers, you need to think about the logical design for the routers, including failover options. Logical Internet high availability design considerations include the following:

- Use a public BGP AS number for eBGP connections to the ISPs.
- Use provider-independent IP address space to allow for advertisement to both ISPs.
- Receive full or partial Internet routing tables to optimize forwarding outbound.
- Use HSRP/GLBP or an IGP such as EIGRP or OSPF internally.

## Backup Connectivity

Redundancy is a critical component of WAN design for the remote site because of the unreliable nature of WAN links compared to the LANs that they connect. Many enterprise edge solutions require high availability between the primary and remote sites. Because many remote site WAN links have lower reliability and lack bandwidth, they are good candidates for most WAN backup designs.

Remote site offices should have some type of backup strategy to deal with primary link failures. Backup links can either be permanent WAN or Internet-based connections.

WAN backup options are as follows:

- **Secondary WAN link:** Adding a secondary WAN link makes the network more fault tolerant. This solution offers two key advantages:
  - **Backup link:** The backup link provides for network connectivity if the primary link fails. Dynamic or static routing techniques can be used to provide routing consistency during backup events. Application availability can also be increased because of the additional backup link.
  - **Additional bandwidth:** Load sharing allows both links to be used at the same time, increasing the available bandwidth. Load balancing can be achieved over the parallel links using automatic routing protocol techniques.
- **IPsec tunnel across the Internet:** An IPsec VPN backup link can redirect traffic to the corporate headquarters when a network failure has been detected on the primary WAN link.

- **SDWAN with MPLS and Internet tunnel:** With SDWAN using two transports, an Internet link can carry traffic to the corporate headquarters by load balancing with the MPLS link or during a failover event when a network failure has occurred.

### Failover

Key Topic

An option for network connectivity failover is to use the Internet as the failover transport between sites. However, keep in mind that this type of connection does not support bandwidth guarantees. The enterprise also needs to set up the tunnels and advertise the company's networks internally so that remote offices have reachable IP destinations. IP SLA monitoring can be leveraged along with a floating static route to provide failover.

Security is of great importance when you rely on the Internet for network connectivity, so a secure tunnel using IPsec needs to be deployed to protect the data during transport.

Figure 9-6 illustrates connectivity between the headend or central site and a remote site using traditional MPLS Layer 3 VPN IP connections for the primary WAN link. The IPsec tunnel is a failover tunnel that provides redundancy for the site if the primary WAN link fails.

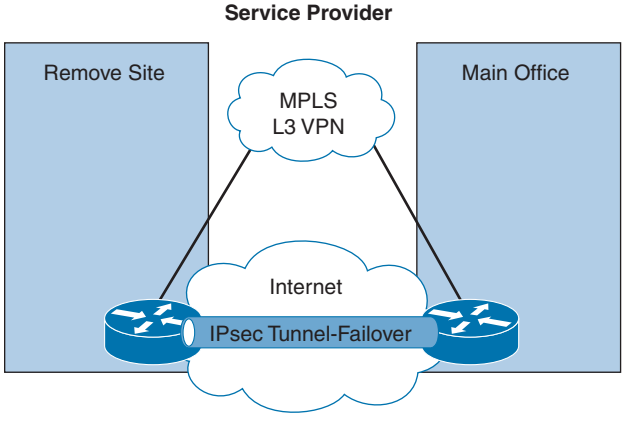



**Figure 9-6** *WAN Failover Using an IPsec Tunnel*

IPsec tunnels are configured between the source and destination routers using tunnel interfaces. Packets that are destined for the tunnel have the standard formatted IP header. IP packets that are forwarded across the tunnel also need an additional GRE/IPsec header placed on them. As soon as the packets have the required headers, they are placed in the tunnel with the tunnel endpoint as the destination address. After the packets cross the tunnel and arrive on the far end, the GRE/IPsec headers are removed. The packets are then forwarded normally, using the original IP packet headers. An important design consideration to keep in mind is that you might need to modify the MTU sizes between the source and destination of the tunnel endpoints to account for the larger header sizes of the additional GRE/IPsec headers.

## QoS Strategies

Quality of service (QoS) is a fundamental network technology that has been around for over 20 years and is still relevant in today's networks, even though bandwidth has been increasing rapidly over the years. QoS gives network operators techniques to help manage the contention for network resources and in turn provide better application experiences for end users. To help

us with this, Cisco supports three main models for providing QoS service differentiation: best-effort (BE), Differentiated Services (DiffServ), and Integrated Services (IntServ). These three models are different in how they enable applications to be prioritized throughout the network and how they handle the delivery of data packets with a specified level of service.

## Best-Effort QoS

The best-effort (BE) QoS model is typically the default QoS model and does not implement any QoS behaviors to prioritize traffic before other QoS traffic classes. This is the easiest of the three models because there is nothing you really need to do for it to work. You would not want to use best-effort QoS for any real-time applications such as voice or video traffic. It is a last-resort QoS model that you use after you have already prioritized all other important traffic classes that are sensitive to delay, jitter, and/or bandwidth within the network.

## DiffServ

The **DiffServ** QoS model separates traffic into multiple classes that can be used to satisfy varying QoS requirements. A packet's class can be marked directly inside the packet that classifies packets into different treatment categories.

Key Topic

With the DiffServ model, packets are classified and marked to receive a per-hop behavior (PHB) at the edge of the network. Then the rest of the network along the path to the destination uses the DSCP value to provide proper treatment. Each network device then treats the packets according to the defined PHB. The PHB can be specified in different ways, such as by using the 6-bit Differentiated Services Code Point (DSCP) setting in IP packets or by using ACLs with source and destination addresses.

Priorities are marked in each packet using DSCP values to classify the traffic according to the specified QoS policy for the traffic class. Typically, the marking is performed per packet at the QoS domain boundaries within the network. Additional policing and shaping operations can be implemented to enable greater scalability.

Table 9-6 maps applications to DSCP and decimal values.

Key Topic

**Table 9-6** DSCP Mapping Table

| Application | DSCP | Decimal Value |
|---|---|---|
| Network control | CS7 | 56 |
| Internetwork control | CS6 | 48 |
| VoIP | EF | 46 |
| Broadcast video | CS5 | 40 |
| Multimedia conferencing | AF4 | 34–38 |
| Real-time interaction | CS4 | 32 |
| Multimedia streaming | AF3 | 26–30 |
| Signaling | CS3 | 24 |
| Transactional data | AF2 | 18–22 |
| Network management | CS2 | 16 |
| Bulk data | AF1 | 10–14 |
| Scavenger | CS1 | 8 |
| Best-effort | Default | 0 |

### IntServ

The **IntServ** QoS model was designed for the needs of real-time applications such as video, multimedia conferencing, and virtual reality. It provides end-to-end QoS treatment that real-time applications require by explicitly reserving network resources and giving QoS treatment to user packet flows. The IntServ model applications ask the network for an explicit resource reservation per flow and use admission control mechanisms as key building blocks to establish end-to-end QoS throughout the network.

Key Topic

IntServ uses Resource Reservation Protocol (RSVP) to explicitly request QoS for the application along the end-to-end path through devices in the network. Before an application begins transmitting, it requests that each network device reserve the necessary bandwidth along the path. The network, in turn, accepts or rejects the reservation per flow based on available network resources.

IntServ requires several functions on each of the routers and switches between the source and destination of the packet flow:

- **Admission control:** Determines whether the requested flows can be accepted without impacting existing reservations
- **Classification:** Identifies traffic that requires different levels of QoS
- **Policing:** Allows or drops packets when traffic does not conform to the QoS policy
- **Queuing and Scheduling:** Forwards traffic for permitted QoS reservations

## Designing End-to-End QoS Policies

Cisco has developed many different QoS mechanisms, such as queuing, policing, and traffic shaping, to enable network operators to manage and prioritize the traffic flowing on a network. Applications that are delay sensitive, such as VoIP, require special treatment to ensure proper application functionality.

### Classification and Marking

For a flow to have priority, it must be classified and marked. **Classification** is the process of identifying the type of traffic. Marking is the process of setting a value in the IP header based on the classification. The following are examples of technologies that support classification:

Key Topic

- **Network-based application recognition (NBAR):** This technology uses deep packet content inspection to identify network applications. An advantage of NBAR is that it can recognize applications even when they do not use standard network ports. Furthermore, it matches fields at the application layer. Before NBAR, classification was limited to Layer 4 TCP and User Datagram Protocol (UDP) port numbers.
- **Committed access rate (CAR):** CAR uses a rate limit to set precedence and allows customization of the precedence assignment by user, source or destination IP address, and application type.

### Shaping

**Traffic shaping and policing** are mechanisms that inspect traffic and take action based on the traffic's characteristics, such as DSCP or IP precedence bits set in the IP header.

Key Topic

Traffic shaping involves slowing down the rate at which packets are sent out an interface (egress) by matching certain criteria. Traffic shaping uses a token bucket technique to release the packets into the output queue at a preconfigured rate. Traffic shaping helps eliminate potential bottlenecks by throttling back the traffic rate at the source. In enterprise environments, traffic shaping is used to smooth the flow of traffic going out to the provider. Smoothing the flow is desirable for several reasons. For example, in provider networks, it prevents the provider from dropping traffic that exceeds the contracted rate.

### Policing

Policing involves tagging or dropping traffic, depending on the match criteria. Generally, policing is used to set the limit of traffic coming into an interface (ingress) and uses a "leaky bucket mechanism." Policing can be used to forward traffic based on conforming traffic and to drop traffic that violates the policy. Policing is also referred to as *committed access rate* (*CAR*). One example of using policing is giving preferential treatment to critical application traffic by elevating to a higher class and reducing best-effort traffic to a lower-priority class.

Key Topic

When you contrast traffic shaping with policing, remember that traffic shaping buffers packets, while policing can be configured to drop packets. In addition, policing propagates bursts, but traffic shaping does not.

### Queuing

Key Topic

Queuing refers to the buffering process used by routers and switches when they receive traffic faster than it can be transmitted. Different queuing mechanisms can be implemented to influence the order in which the different queues are serviced (that is, how different types of traffic are emptied from the queues).

QoS is an effective tool for managing a WAN's available bandwidth. Keep in mind that QoS does not add bandwidth; it only helps you make better use of the existing bandwidth. For chronic congestion problems, QoS is not the answer; in such situations, you need to add more bandwidth. However, by prioritizing traffic, you can make sure that your most critical traffic gets the best treatment and available bandwidth in times of congestion. One popular QoS technique is to classify your traffic based on a protocol type or a matching access control list (ACL) and then give policy treatment to the class. You can define many classes to match or identify your most important traffic classes. The remaining unmatched traffic then uses a default class in which the traffic can be treated as best-effort.

Table 9-7 describes QoS options for optimizing bandwidth.

Key Topic

**Table 9-7** QoS Options

| QoS Category | Description |
|---|---|
| Classification | Identifies and marks flows |
| **Congestion management** | Handles traffic overflow using a queuing algorithm |
| Link-efficiency mechanisms | Reduce latency and jitter for network traffic on low-speed links |
| Traffic shaping and policing | Prevent congestion by policing ingress and egress flows |

#### Congestion Management

Two types of output queues are available on routers: the hardware queue and the software queue. The hardware queue uses the first-in, first-out (FIFO) strategy. The software queue schedules packets first and then places them in the hardware queue. Keep in mind that the

software queue is used only during periods of congestion. The software queue uses QoS techniques such as priority queuing, custom queuing, weighted fair queuing, class-based weighted fair queuing, low-latency queuing, and traffic shaping and policing.

### Priority Queuing

Priority queuing (PQ) is a queuing method that establishes four interface output queues that serve different priority levels: high, medium, default, and low. Unfortunately, PQ can starve other queues if too much data is in one queue because higher-priority queues must be emptied before lower-priority queues.

### Custom Queuing

Custom queuing (CQ) uses up to 16 individual output queues. Byte size limits are assigned to each queue so that when the limit is reached, CQ proceeds to the next queue. The network operator can customize these byte size limits. CQ is fairer than PQ because it allows some level of service to all traffic. This queuing method is considered legacy due to improvements in the other queuing methods.

### Weighted Fair Queuing

Weighted fair queuing (WFQ) ensures that traffic is separated into individual flows or sessions without requiring that you define ACLs. WFQ uses two categories to group sessions: high bandwidth and low bandwidth. Low-bandwidth traffic has priority over high-bandwidth traffic. High-bandwidth traffic shares the service according to assigned weight values. WFQ is the default QoS mechanism on interfaces below 2.0 Mbps.

### Class-Based Weighted Fair Queuing

**Class-based weighted fair queuing (CBWFQ)** extends WFQ capabilities by providing support for modular user-defined traffic classes. CBWFQ lets you define traffic classes that correspond to match criteria, including ACLs, protocols, and input interfaces. Traffic that matches the class criteria belongs to that specific class. Each class has a defined queue that corresponds to an output interface.

After traffic has been matched and belongs to a specific class, you can modify its characteristics, such as by assigning bandwidth and specifying the maximum queue limit and weight. During periods of congestion, the bandwidth assigned to the class is the guaranteed bandwidth that is delivered to the class.

One of the key advantages of CBWFQ is its modular nature, which makes it extremely flexible for most situations. It is often referred to as Modular QoS CLI (MQC), which is the framework for building QoS policies. Many classes can be defined to separate network traffic as needed in the MQC.

### Low-Latency Queuing

**Low-latency queuing (LLQ)** adds a strict priority queue to CBWFQ. The strict priority queue allows delay-sensitive traffic such as voice to be sent first, before other queues are serviced. That gives voice preferential treatment over the other traffic types. Unlike PQ, LLQ provides for a maximum threshold on the priority queue to prevent lower-priority traffic from being starved by the priority queue.

Without LLQ, CBWFQ would not have a priority queue for real-time traffic. The additional classification of other traffic classes is done using the same CBWFQ techniques. LLQ is the standard QoS method for many VoIP networks.

### Link Efficiency

With Cisco IOS, several link-efficiency mechanisms are available. Link fragmentation and interleaving (LFI), Multilink PPP (MLP), and Real-Time Transport Protocol (RTP) header compression can provide for more efficient use of bandwidth.

Table 9-8 describes Cisco IOS link-efficiency mechanisms.

Key Topic

**Table 9-8** Link-Efficiency Mechanisms

| Mechanisms | Description |
|---|---|
| Link fragmentation and interleaving (LFI) | Reduces delay and jitter on slower-speed links by breaking up large packet flows and inserting smaller data packets (Telnet, VoIP) between them. |
| Multilink PPP (MLP) | Bonds multiple links between two nodes, which increases the available bandwidth. MLP can be used on analog or digital links and is based on RFC 1990. |
| Real-Time Transport Protocol (RTP) header compression | Provides increased efficiency for applications that take advantage of RTP on slow links. Compresses RTP/UDP/IP headers from 40 bytes down to 2–5 bytes. |

### Window Size

The **window size** defines the upper limit of frames that can be transmitted without getting a return acknowledgment. Transport protocols such as TCP rely on acknowledgments to provide connection-oriented reliable transport of data segments. For example, if the TCP window size is set to 8192, the source stops sending data after 8192 bytes if no acknowledgment has been received from the destination host. In some cases, the window size might need to be modified because of unacceptable delay for larger WAN links. If the window size is not adjusted to coincide with the delay factor, retransmissions can occur, which affects throughput significantly. It is recommended that you adjust the window size to achieve better connectivity conditions.

## References and Recommended Readings

RFC 1990: *The PPP Multilink Protocol*, https://tools.ietf.org/html/rfc1990

Cisco, "Campus QoS Design Simplified," https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2018/pdf/BRKCRS-2501.pdf

Cisco, "Cisco IOS Quality of Service Solutions Configuration Guide Library, Cisco IOS Release 15M&T," http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/config_library/15-mt/qos-15-mt-library.html

Cisco, "DSCP and Precedence Values," https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/sw/4_0/qos/configuration/guide/nexus1000v_qos/qos_6dscp_val.pdf

Cisco, "Highly Available Wide Area Network Design," https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/BRKRST-2042.pdf

Cisco, "Module 4: Enterprise Network Design," Designing for Cisco Internetwork Solution Course (DESGN) v3.0

Wikipedia, "LTE: LTE (telecommunications)," en.wikipedia.org/wiki/LTE_(telecommunication)

# Exam Preparation Tasks

You have a couple of choices for exam preparation: the following review sections, Chapter 13, "Final Preparation," and the exam practice questions on the companion website.

## Review All Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. Table 9-9 lists these key topics and the page number on which each is found.

Key Topic

**Table 9-9** Key Topics for Chapter 9

| Key Topic Element | Description | Page |
|---|---|---|
| List | WAN design methodologies | 312 |
| Table 9-2 | Key Design Principles | 313 |
| Table 9-3 | Application Requirements for Data, Voice, and Video Traffic | 313 |
| Table 9-4 | Physical Bandwidth Comparison | 314 |
| Table 9-5 | Availability Percentages | 315 |
| List | Deployment models | 316 |
| Paragraph | Single-homed MPLS WANs | 317 |
| Paragraph | Dual-homed MPLS WANs | 318 |
| Paragraph | Hybrid WANs: Layer 3 VPN with Internet tunnels | 318 |
| List | Internet for remote sites | 321 |
| List | WAN backup options | 321 |
| Paragraph | Failover | 322 |
| Paragraph | DiffServ | 323 |
| Table 9-6 | DSCP Mapping Table | 323 |
| Paragraph | IntServ | 324 |
| List | Classification technologies | 324 |
| Paragraph | Shaping | 325 |
| Paragraph | Policing | 325 |
| Paragraph | Queuing | 325 |
| Table 9-7 | QoS Options | 325 |
| Table 9-8 | Link-Efficiency Mechanisms | 327 |

## Complete Tables and Lists from Memory

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

## Define Key Terms

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

class-based weighted fair queuing (CBWFQ), classification, congestion management, DiffServ, IntServ, low-latency queuing (LLQ), reliability, response time, throughput, traffic shaping and policing, window size

## Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the exam engine on the companion website.

1. Which of the following is based on the availability of technology as well as the projected traffic patterns, technology performance, constraints, and reliability?
   - **a.** Designing the topology
   - **b.** Assessing the existing network
   - **c.** Identifying the network requirements
   - **d.** Characterizing the existing network
2. Which design principle involves redundancy through hardware, software, and connectivity?
   - **a.** Performance
   - **b.** Security
   - **c.** Scalability
   - **d.** High availability
3. Which application requires round-trip times of less than 400 ms with low delay and jitter?
   - **a.** Data file transfer
   - **b.** Real-time voice
   - **c.** Real-time video
   - **d.** Interactive data
4. Which of the following is a measure of a given application's availability to its users?
   - **a.** Response time
   - **b.** Throughput
   - **c.** Reliability
   - **d.** Performance
5. Which of the following defines the upper limit of frames that can be transmitted without a return acknowledgment?
   - **a.** Throughput
   - **b.** Link efficiency
   - **c.** Window size
   - **d.** Low-latency queuing

6. Which of the following is the availability target range for branch WAN high availability?
   a. 99.9900%
   b. 99.9000%
   c. 99.0000%
   d. 99.9999%
7. Which WAN deployment model provides for the best SLA guarantees?
   a. MPLS WAN with dual routers
   b. Hybrid WAN with MPLS and Internet routers
   c. Internet WAN with dual routers
   d. Internet WAN with a single router
8. Which Internet connectivity option provides for the highest level of resiliency?
   a. Single-router single-homed
   b. Single-router dual-homed
   c. Dual-router dual-homed
   d. GRE tunnels
9. When you are designing Internet for remote sites, which option provides control for security services such as URL filtering, firewalling, and intrusion prevention?
   a. Centralized Internet
   b. Direct Internet
   c. Direct Internet with split tunnel
   d. IPsec with split tunnel
10. Which design considerations are most important for Internet high availability design? (Choose two.)
    a. Using a public BGP AS number for eBGP connections to ISPs
    b. Using provider-independent IP address space for advertisements to ISPs
    c. Using BGP communities
    d. Using extended ACLs
11. Which WAN backup option provides for redundancy and additional bandwidth?
    a. Backup link
    b. IPsec tunnel
    c. GRE tunnel
    d. NAT-T
12. Which failover option can be used to back up the primary MPLS WAN connection?
    a. BGP
    b. GLBP
    c. HSRP
    d. IPsec tunnel

13. Which of the following is not a model for providing QoS?
    a. Best-effort
    b. DiffServ
    c. IntServ
    d. NSF
14. In QoS markings, what DSCP value is used for VoIP traffic?
    a. AF4
    b. CS2
    c. EF
    d. CS5
15. Which QoS method uses a strict priority queue in addition to modular traffic classes?
    a. CBWFQ
    b. Policing
    c. WFQ
    d. LLQ
16. Within RSVP, what function is used to determine whether the requested flows can be accepted?
    a. Admission control
    b. Classification
    c. Policing
    d. Queuing and scheduling
17. Which of the following slows down the rate at which packets are sent out an interface (egress) by matching certain criteria?
    a. Policing
    b. CAR
    c. Shaping
    d. NBAR
18. What is the buffering process that routers and switches use when they receive traffic faster than it can be transmitted?
    a. Policing
    b. Queuing
    c. NBAR
    d. Shaping
19. What do service providers use to define their service offerings at different levels?
    a. SWAN
    b. WAN tiers
    c. WWAN
    d. SLA

**20.** Which of the following has mechanisms to handle traffic overflow using a queuing algorithm?

- **a.** Link-efficiency mechanisms
- **b.** Classification
- **c.** Congestion management
- **d.** Traffic shaping and policing

**21.** Which QoS category identifies and marks flows?

- **a.** Congestion management
- **b.** Traffic shaping and policing
- **c.** Link-efficiency mechanisms
- **d.** Classification and marking

**22.** Which design principle balances the amount of security and technologies with the budget?

- **a.** Performance
- **b.** Standards and regulations
- **c.** Cost
- **d.** Security

**23.** Which application type has requirements for low throughput and response time within a second?

- **a.** Real-time video
- **b.** Interactive data
- **c.** Real-time voice
- **d.** Interactive video

**24.** Which of the following WAN connectivity options has bandwidth capabilities of 1 Gbps to 10 Gbps?

- **a.** 802.11a
- **b.** LTE
- **c.** LTE Advance Pro
- **d.** LTE Advanced

**25.** How many days of downtime per year occur with 99.00000% availability?

- **a.** 8.76 days
- **b.** 5.2 days
- **c.** 3.65 days
- **d.** 1.2 days

**26.** With dual-router and dual-path availability models, how much downtime is expected per year?

- **a.** 4 to 9 hours per year
- **b.** 26 hours per year

**c.** 5 hours per year

**d.** 5 minutes per year

**27.** Which deployment model for WAN connectivity has a single router or dual routers and uses both MPLS and an Internet VPN?

**a.** Hybrid WAN

**b.** Internet WAN

**c.** MPLS WAN

**d.** VPLS WAN

**28.** When you are designing the Internet with high availability, which of the following is a design consideration?

**a.** Use public address space for internal addressing

**b.** Use private address space for route advertising to the ISPs

**c.** Block all Internet routes

**d.** Use HSRP/GLBP or an IGP internally

**29.** Which of the following is an important design consideration when using IPsec over GRE tunnels?

**a.** QoS classification

**b.** MTU size

**c.** Header type

**d.** Payload length

**30.** When you are using DSCP to classify traffic, which of the following is prioritized the most?

**a.** Signaling

**b.** Transactional data

**c.** Real-time interaction

**d.** VoIP

*This page intentionally left blank*

# Index

## Numerics



## A

## B

## C

## D

## E

# F

## G



## H

## J-K



## L

# M

# N

## O

# P

## Q



## R

# S

## T



## U

# V

## W

# X-Y-Z