CCIE Routing and Switching Exam Preparation

CCIE Routing and Switching

Certification Guide

Fourth Edition

- ✔ Master **CCIE Routing and Switching 4.0 blueprint** exam topics
- ✔ Assess your knowledge with **chapter-opening quizzes**
- ✔ Review key concepts with **Exam Preparation Tasks**
- ✔ Practice with **realistic exam questions** on the CD-ROM

Wendell Odom, CCIE® No. 1624
Rus Healy, CCIE No. 15025
Denise Donohue, CCIE No. 9566

ciscopress.com

CCIE Routing and Switching Certification Guide, Fourth Edition

Wendell Odom, CCIE No. 1624

Rus Healy, CCIE No. 15025

Denise Donohue, CCIE No. 9566

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing November 2009

Library of Congress Cataloging-in-Publication Data

Odom, Wendell.

CCIE routing and switching exam certification guide / Wendell Odom, Rus Healy, Denise Donohue. -- 4th ed.

p. cm.

Includes index.

ISBN-13: 978-1-58705-980-3 (hardcover w/cd)

ISBN-10: 1-58705-980-0 (hardcover w/cd) 1. Telecommunications engineers—Certification—Study guides. 2. Routing (Computer network management)—Examinations—Study guides. 3. Telecommunication—Switching systems—Examinations—Study guides. 4. Computer networks—Examinations—Study guides. 5. Internetworking (Telecommunication)—Examinations—Study guides. I. Healy, Rus. II. Donohue, Denise. III. Title.

QA76.3.B78475 2010

004.6—dc22

2009041604

ISBN-13: 978-1-58705-980-3

ISBN-10: 1-58705-980-0

Warning and Disclaimer

This book is designed to provide information about Cisco CCIE Routing and Switching Written Exam, No. 350-001. 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.

Corporate and Government Sales

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact: **U.S. Corporate and Government Sales**
1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside of the U.S. please contact: **International Sales**
1-317-581-3793 international@pearsontechgroup.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.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Cisco Representative: Erik Ullanderson

Cisco Press Program Manager: Anand Sundaram

Executive Editor: Brett Bartow

Managing Editor: Patrick Kanouse

Development Editor: Dayna Isley

Project Editor: Seth Kerney

Copy Editor: Keith Cline

Technical Editor(s): Maurilio Gorito, Narbik Kocharians

Editorial Assistant: Vanessa Evans

Book Designer: Louisa Adair

Composition: Mark Shirar

Indexer: Tim Wright

Proofreader: Apostrophe Editing Services

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.**

Foreword

CCIE Routing and Switching Exam Certification Guide, Fourth Edition, is an excellent self-study resource for the CCIE Routing and Switching written exam. Passing this exam is the first step to attaining the valued CCIE Routing and Switching certification and qualifies candidates for the CCIE Routing and Switching lab exam.

Gaining certification in Cisco technology is key to the continuing educational development of today's networking professional. Through certification programs, Cisco validates the skills and expertise required to effectively manage the modern enterprise network.

Cisco Press Exam Certification Guides and preparation materials offer exceptional—and flexible—access to the knowledge and information required to stay current in your field of expertise or to gain new skills. Whether used as a supplement to more traditional training or as a primary source of learning, these materials offer users the information and knowledge validation required to gain new understanding and proficiencies.

Developed in conjunction with the Cisco certifications and training team, Cisco Press books are the only self-study books authorized by Cisco and offer students a series of exam practice tools and resource materials to help ensure that learners fully grasp the concepts and information presented.

Additional authorized Cisco instructor-led courses, e-learning, labs, and simulations are available exclusively from Cisco Learning Solutions Partners worldwide. To learn more, visit http://www.cisco.com/go/training.

I hope that you find these materials to be an enriching and useful part of your exam preparation.

Erik Ullanderson
Manager, Global Certifications
Learning@Cisco
October 2007

Introduction

The Cisco Certified Internetwork Expert (CCIE) certification may be the most challenging and prestigious of all networking certifications. It has received numerous awards and certainly has built a reputation as one of the most difficult certifications to earn in all of the technology world. Having a CCIE certification opens doors professionally typically results in higher pay and looks great on a resume.

Cisco currently offers several CCIE certifications. This book covers the version 4.0 exam blueprint topics of the written exam for the CCIE Routing and Switching certification. The following list details the currently available CCIE certifications at the time of this book's publication; check http://www.cisco.com/go/ccie for the latest information. The certifications are listed in the order in which they were made available to the public:

- CCIE Routing and Switching
- CCIE Security
- CCIE Service Provider
- CCIE Voice
- CCIE Storage Networking
- CCIE Wireless

Each of the CCIE certifications requires the candidate to pass both a written exam and a one-day, hands-on lab exam. The written exam is intended to test your knowledge of theory, protocols, and configuration concepts that follow good design practices. The lab exam proves that you can configure and troubleshoot actual gear.

Why Should I Take the CCIE Routing and Switching Written Exam?

The first and most obvious reason to take the CCIE Routing and Switching written exam is that it is the first step toward obtaining the CCIE Routing and Switching certification. Also, you cannot schedule a CCIE lab exam until you pass the corresponding written exam. In short, if you want all the professional benefits of a CCIE Routing and Switching certification, you start by passing the written exam.

The benefits of getting a CCIE certification are varied, among which are the following:

- Better pay
- Career-advancement opportunities
- Applies to certain minimum requirements for Cisco Silver and Gold Channel Partners, as well as those seeking Master Specialization, making you more valuable to Channel Partners
- Better movement through the problem-resolution process when calling the Cisco TAC
- Prestige
- Credibility for consultants and customer engineers, including the use of the Cisco CCIE logo

The other big reason to take the CCIE Routing and Switching written exam is that it recertifies an individual's associate-, professional-, and expert-level Cisco certifications. In other words, passing any CCIE written exam recertifies that person's CCNA, CCNP, CCIP, CCSP, CCDP, and so on. (Recertification requirements do change, so please verify the requirements at http://www.cisco.com/go/certifications.)

CCIE Routing and Switching Written Exam 350-001

The CCIE Routing and Switching written exam, at the time of this writing, consists of a two-hour exam administered at a proctored exam facility affiliated with Pearson VUE (http://www.vue.com/cisco). The exam typically includes approximately 100 multiple-choice questions. No simulation questions are currently part of the written exam.

As with most exams, everyone wants to know what is on the exam. Cisco provides general guidance as to topics on the exam in the CCIE Routing and Switching written exam blueprint, the most recent copy of which can be accessed from http://www.cisco.com/go/ccie.

Cisco changes both the CCIE written and lab blueprints over time, but Cisco seldom, if ever, changes the exam numbers. (In contrast, Cisco changes the exam numbers of the associate- and professional-level certifications when it makes major changes to what is covered on those exams.) Instead of changing the exam number when a CCIE exam changes significantly, Cisco publishes a new exam blueprint. Cisco assigns the new blueprint a version number, much like a software version.

The CCIE Routing and Switching written exam blueprint 4.0, as of the time of publication, is listed in Table I-1. Table I-1 also lists the chapters that cover each topic.

Table I-1 *CCIE Routing and Switching Written Exam Blueprint*

Topics	Book Chapters
1.00 Implement Layer 2 Technologies	
1.10 Implement Spanning Tree Protocol (STP)	3
(a) 802.1d	3
(b) 802.1w	3
(c) 801.1s	3
(d) Loop guard	3
(e) Root guard	3
(f) Bridge protocol data unit (BPDU) guard	3
(g) Storm control	3
(h) Unicast flooding	3
(i) Port roles, failure propagation, and Loop Guard operation	3
1.20 Implement VLAN and VLAN Trunking Protocol (VTP)	2
1.30 Implement trunk and trunk protocols, EtherChannel, and load-balance	2

Table I-1 *CCIE Routing and Switching Written Exam Blueprint (Continued)*

Topics	Book Chapters
1.40 Implement Ethernet technologies	1
(a) Speed and duplex	1
(b) Ethernet, Fast Ethernet, and Gigabit Ethernet	1
(c) PPP over Ethernet (PPPoE)	2
1.50 Implement Switched Port Analyzer (SPAN), Remote Switched Port Analyzer (RSPAN), and flow control	1
1.60 Implement Frame Relay	15
(a) Local Management Interface (LMI)	15
(b) Traffic shaping	15
(c) Full mesh	15
(d) Hub and spoke	15
(e) Discard eligible (DE)	15
1.70 Implement High-Level Data Link Control (HDLC) and PPP	15
2.00 Implement IPv4	
2.10 Implement IP version 4 (IPv4) addressing, subnetting, and variable-length subnet masking (VLSM)	4
2.20 Implement IPv4 tunneling and Generic Routing Encapsulation (GRE)	6
2.30 Implement IPv4 RIP version 2 (RIPv2)	E
2.40 Implement IPv4 Open Shortest Path First (OSPF)	8
(a) Standard OSPF areas	8
(b) Stub area	8
(c) Totally stubby area	8
(d) Not-so-stubby-area (NSSA)	8
(e) Totally NSSA	8
(f) Link-state advertisement (LSA) types	8
(g) Adjacency on a point-to-point and on a multi-access network	8
(h) OSPF graceful restart	8
2.50 Implement IPv4 Enhanced Interior Gateway Routing Protocol (EIGRP)	7
(a) Best path	7
(b) Loop-free paths	7
(c) EIGRP operations when alternate loop-free paths are available, and when they are not available	7

continues

Table I-1 *CCIE Routing and Switching Written Exam Blueprint (Continued)*

Topics	Book Chapters
(d) EIGRP queries	7
(e) Manual summarization and autosummarization	9
(f) EIGRP stubs	7
2.60 Implement IPv4 Border Gateway Protocol (BGP)	10
(a) Next hop	10
(b) Peering	10
(c) Internal Border Gateway Protocol (IBGP) and External Border Gateway Protocol (EBGP)	10, 11
2.70 Implement policy routing	6
2.80 Implement Performance Routing (PfR) and Cisco Optimized Edge Routing (OER)	6
2.90 Implement filtering, route redistribution, summarization, synchronization, attributes, and other advanced	9, 11
3.00 Implement IPv6	
3.10 Implement IP version 6 (IPv6) addressing and different addressing types	20
3.20 Implement IPv6 neighbor discovery	20
3.30 Implement basic IPv6 functionality protocols	20
3.40 Implement tunneling techniques	20
3.50 Implement OSPF version 3 (OSPFv3)	20
3.60 Implement EIGRP version 6 (EIGRPv6)	20
3.70 Implement filtering and route redistribution	20
4.00 Implement MPLS Layer 3 VPNs	19
4.10 Implement Multiprotocol Label Switching (MPLS)	19
4.20 Implement Layer 3 virtual private networks (VPNs) on provider edge (PE), provider (P), and customer edge (CE) routers	19
4.30 Implement virtual routing and forwarding (VRF) and Multi-VRF Customer Edge (VRF-Lite)	19
5.00 Implement IP Multicast	
5.10 Implement Protocol Independent Multicast (PIM) sparse mode	16, 17
5.20 Implement Multicast Source Discovery Protocol (MSDP)	17
5.30 Implement interdomain multicast routing	17
5.40 Implement PIM Auto-Rendezvous Point (Auto-RP), unicast rendezvous point (RP), and bootstrap router (BSR)	17

Table I-1 *CCIE Routing and Switching Written Exam Blueprint (Continued)*

Topics	Book Chapters
5.50 Implement multicast tools, features, and source-specific multicast	17
5.60 Implement IPv6 multicast, PIM, and related multicast protocols, such as Multicast Listener Discovery (MLD)	17
6.00 Implement Network Security	
6.01 Implement access lists	18
6.02 Implement Zone Based Firewall	18
6.03 Implement Unicast Reverse Path Forwarding (uRPF)	18
6.04 Implement IP Source Guard	18
6.05 Implement authentication, authorization, and accounting (AAA) (configuring the AAA server is not required, only the client side (IOS) is configured)	18
6.06 Implement Control Plane Policing (CoPP)	18
6.07 Implement Cisco IOS Firewall	18
6.08 Implement Cisco IOS Intrusion Prevention System (IPS)	18
6.09 Implement Secure Shell (SSH)	18
6.10 Implement 802.1x	18
6.11 Implement NAT	18
6.12 Implement routing protocol authentication	18
6.13 Implement device access control	18
6.14 Implement security features	18
7.00 Implement Network Services	
7.10 Implement Hot Standby Router Protocol (HSRP)	5
7.20 Implement Gateway Load Balancing Protocol (GLBP)	5
7.30 Implement Virtual Router Redundancy Protocol (VRRP)	5
7.40 Implement Network Time Protocol (NTP)	5
7.50 Implement DHCP	5
7.60 Implement Web Cache Communication Protocol (WCCP)	5
8.00 Implement Quality of Service (QoS)	
8.10 Implement Modular QoS CLI (MQC)	12
(a) Network-Based Application Recognition (NBAR)	12
(b) Class-based weighted fair queuing (CBWFQ), modified deficit round robin (MDRR), and low latency queuing (LLQ)	13
(c) Classification	12

continues

Table I-1 *CCIE Routing and Switching Written Exam Blueprint (Continued)*

Topics	Book Chapters
(d) Policing	14
(e) Shaping	14
(f) Marking	12
(g) Weighted random early detection (WRED) and random early detection (RED)	13
(h) Compression	15
8.20 Implement Layer 2 QoS: weighted round robin (WRR), shaped round robin (SRR), and policies	13
8.30 Implement link fragmentation and interleaving (LFI) for Frame Relay	15
8.40 Implement generic traffic shaping	14
8.50 Implement Resource Reservation Protocol (RSVP)	13
8.60 Implement Cisco AutoQoS	12
9.00 Troubleshoot a Network	
9.10 Troubleshoot complex Layer 2 network issues	3
9.20 Troubleshoot complex Layer 3 network issues	9
9.30 Troubleshoot a network in response to application problems	14
9.40 Troubleshoot network services	6
9.50 Troubleshoot network security	18
10.00 Optimize the Network	
10.01 Implement syslog and local logging	5
10.02 Implement IP Service Level Agreement SLA	5
10.03 Implement NetFlow	5
10.04 Implement SPAN, RSPAN, and router IP traffic export (RITE)	5
10.05 Implement Simple Network Management Protocol (SNMP)	5
10.06 Implement Cisco IOS Embedded Event Manager (EEM)	5
10.07 Implement Remote Monitoring (RMON)	5
10.08 Implement FTP	5
10.09 Implement TFTP	5
10.10 Implement TFTP server on router	5
10.11 Implement Secure Copy Protocol (SCP)	5
10.12 Implement HTTP and HTTPS	5
10.13 Implement Telnet	5

Table I-1 *CCIE Routing and Switching Written Exam Blueprint (Continued)*

Topics	Book Chapters
11.00 Evaluate proposed changes to a Network	
11.01 Evaluate interoperability of proposed technologies against deployed technologies	N/A
(a) Changes to routing protocol parameters	N/A
(b) Migrate parts of a network to IPv6	N/A
(c) Routing Protocol migration	N/A
(d) Adding multicast support	N/A
(e) Migrate spanning tree protocol	N/A
(f) Evaluate impact of new traffic on existing QoS design	N/A
11.02 Determine operational impact of proposed changes to an existing network	N/A
(a) Downtime of network or portions of network	N/A
(b) Performance degradation	N/A
(c) Introducing security breaches	N/A
11.03 Suggest Alternative solutions when incompatible changes are proposed to an existing network	N/A
(a) Hardware/Software upgrades	N/A
(b) Topology shifts	N/A
(c) Reconfigurations	N/A

Version 4.0 of the blueprint provides more detail than the earlier versions of the blueprint. It is also helpful to know what topics Cisco has removed from earlier blueprints, because it is also useful to know what not to study as well as what to study. The more significant topics removed from the last few versions of the CCIE R/S Written blueprints include the following:

- **Version 2.0 (2005)**—Cisco announced the removal of ISDN/DDR, IS-IS, ATM, and SONET; they also added wireless LANs
- **Version 3.0 (2007)**—The Version 3.0 blueprint showed the removal of wireless LANs, and added IPv6 and MPLS concepts.
- **Version 4.0 (2009)**—The Version 4.0 blueprint shows that no significant topics were removed.

The Version 4.0 blueprint adds many new topics compared to the Version 3.0 blueprint. The blueprint mentions around 20 new small topics. In addition, the blueprint wording has been changed to be more aligned with the other Cisco certifications, with many of the topics listing the word *configuration*. Notably, MPLS configuration has been added since

Version 3.0, with several of the small topics, ranging in one to three pages of coverage in the book, also now including some configuration discussion.

The Version 4.0 blueprint also now includes five troubleshooting topics, as listed in section 9.0 of the blueprint, and paraphrased as follows:

- LANs
- IP routing
- Application performance (QoS)
- Network services
- Security

The existence of specific topics for troubleshooting may be a bit confusing at first, because the CCIE lab also now contains a specific troubleshooting component. However, the prior versions of the CCIE written exam already included questions asked in the context of a broken network or misconfigured device. These new blueprint items simply formalize the idea that you should not only understand proper configuration, but be able to predict what will happen when problems occur.

Finally, the other big change between the Version 3.0 and Version 4.0 blueprint relates to section 11.0 of the blueprint. This new section might be better termed “Dealing with issues that arise in real life when networks change.” Section 11.0, actually titled “Evaluate Proposed Changes to a Network,” diverges from the usual convention of a list of specific technologies. Instead, section 11.0 lists topics about how engineers do their jobs. Specifically, these topics relate to issues that arise when implementing network technologies in an existing network—topics that can be well learned by doing a network engineering job, and questions that can be answered by applying the vast amount of information covered through the whole book. From one perspective, the whole book already covers the topics in this section, but there is no specific section of the printed book that addresses these topics.

To give you practice on these topics, and pull the topics together, Edition 4 of the *CCIE Routing and Switching Exam Certification Guide* includes a large set of CD questions that mirror the types of questions expected for part 11 of the Version 4.0 blueprint. By their very nature, these topics require the application of the knowledge listed throughout the book. This special section of questions provides a means to learn and practice these skills with a proportionally larger set of questions added specifically for this purpose.

These questions will be available to you in the practice test engine database, whether you take full exams or choose questions by category.

About the CCIE Routing and Switching Official Exam Certification Guide, Fourth Edition

This section provides a brief insight into the contents of the book, the major goals, and some of the book features that you will encounter when using this book.

Book Organization

This book contains nine major parts. The book places the longer and the more long-lived topics earlier in the book. For example, the most familiar topics, LAN switching and IPv4 routing, occupy the first three parts, and consume more than 400 pages of the book. QoS, which has been a part of the blueprint for a long times, follows as part IV.

Beyond the chapters in the nine major parts of the book, you will find several useful appendixes gathered in Part X.

Following is a description of each part's coverage:

- Part I, "LAN Switching" (Chapters 1–3)

  This part focuses on LAN Layer 2 features, specifically Ethernet (Chapter 1), VLANs and trunking (Chapter 2), and Spanning Tree Protocol (Chapter 3).

- Part II, "IP" (Chapters 4–5)

  This part is titled "IP" to match the blueprint, but it might be better titled "TCP/IP" because it covers details across the spectrum of the TCP/IP protocol stack. It includes IP addressing (Chapter 4) and IP services such as DHCP and ARP (Chapter 5).

- Part III, "IP Routing" (Chapters 6–11)

  This part covers some of the more important topics on the exam and is easily the largest part of the book. It covers Layer 3 forwarding concepts (Chapter 6), followed by two routing protocol chapters, one each about EIGRP and OSPF (Chapters 7 and 8, respectively). (Note that while RIP Version 2 is listed in the blueprint, its role is waning; therefore, that material exists in this book as CD-only Appendix E.) Following that, Chapter 9 covers route redistribution between IGPs. At the end, Chapter 10 hits the details of BGP, with Chapter 11 looking at BGP path attributes and how to influence BGP's choice of best path.

- Part IV, "QoS" (Chapters 12–14)

  This part covers the more popular QoS tools, including some MQC-based tools, as well as several older tools, particularly FRTS. The chapters include coverage of classification and marking (Chapter 12), queuing and congestion avoidance (Chapter 13), plus shaping, policing, and link efficiency (Chapter 14).

- Part V, “Wide-Area Networks” (Chapter 15)

  The WAN coverage has been shrinking over the last few revisions to the CCIE R&S written exam. Chapter 15 includes some brief coverage of PPP and Frame Relay. Note that the previous version (V3.0) and current version (V4.0) of the blueprint includes another WAN topic, MPLS, which is covered in Part VIII, Chapter 19.

- Part VI, “IP Multicast” (Chapters 16–17)

  Chapter 16 covers multicast on LANs, including IGMP and how hosts join multicast groups. Chapter 17 covers multicast WAN topics.

- Part VII, “Security” (Chapter 18)

  Given the CCIE tracks for both Security and Voice, Cisco has a small dilemma regarding whether to cover those topics on CCIE Routing and Switching, and if so, in how much detail. This part covers a variety of security topics appropriate for CCIE Routing and Switching, in a single chapter. This chapter focuses on switch and router security.

- Part VIII, “MPLS” (Chapter 19)

  As mentioned in the WAN section, the CCIE R&S exam’s coverage of MPLS has been growing over the last two versions of the blueprint. This chapter focuses on enterprise-related topics such as core MPLS concepts and MPLS VPNs, including basic configuration.

- Part IX, “IP Version 6” (Chapter 20)

  Chapter 20 examines a wide variety of IPv6 topics, including addressing, routing protocols, redistribution, and coexistence.

- Part X, “Appendixes”

  Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes”

  > This appendix lists answers and explanations for the questions at the beginning of each chapter.

  Appendix B, “Decimal to Binary Conversion Table”

  > This appendix lists the decimal values 0 through 255, with their binary equivalents.

  Appendix C, “CCIE Routing and Switching Exam Updates: Version 1.0”

  > As of the first printing of the book, this appendix contains only a few words that reference the web page for this book at http://www.ciscopress.com/title/9781587059803. As the blueprint

evolves over time, the authors will post new materials at the website. Any future printings of the book will include the latest newly added materials in printed form inside Appendix C. If Cisco releases a major exam update, changes to the book will be available only in a new edition of the book and not on this site.

NOTE Appendixes D through H and the Glossary are in printable, PDF format on the CD.

(CD-only) Appendix D, "IP Addressing Practice"

This appendix lists several practice problems for IP subnetting and finding summary routes. The explanations to the answers use the shortcuts described in the book.

(CD-only) Appendix E, "RIP Version 2"

This appendix lists a copy of the RIP Version 2 chapter from the previous edition of this book.

(CD-only) Appendix F, "IGMP"

This short appendix contains background information on Internet Group Management Protocol (IGMP) that was in the previous edition's first multicast chapter. It is included in case the background information might be useful to some readers.

(CD-only) Appendix G, "Key Tables for CCIE Study"

This appendix lists the most important tables from the core chapters of the book. The tables have much of the content removed so that you can use them as an exercise. You can print the PDF and then fill in the table from memory, checking your answers against the completed tables in Appendix H.

(CD-only) Glossary

The Glossary contains the key terms listed in the book.

Book Features

The core chapters of this book have several features that help you make the best use of your time:

- **"Do I Know This Already?" Quizzes**—Each chapter begins with a quiz that helps you to determine the amount of time you need to spend studying that chapter. If you score yourself strictly, and you miss only one question, you may want to skip the core of the chapter and move on to the "Foundation Summary" section at the end of the chapter, which lets you review facts and spend time on other topics. If you miss more than one, you may want to spend some time reading the chapter or at least reading sections that cover topics about which you know you are weaker.

- **Foundation Topics**—These are the core sections of each chapter. They explain the protocols, concepts, and configuration for the topics in that chapter.
- **Foundation Summary**—The "Foundation Summary" section of this book departs from the typical features of the "Foundation Summary" section of other Cisco Press Exam Certification Guides. This section does not repeat any details from the "Foundation Topics" section; instead, it simply summarizes and lists facts related to the chapter but for which a longer or more detailed explanation is not warranted.
- **Key topics—**Throughout the "Foundation Topics" section, a Key Topic icon has been placed beside the most important areas for review. After reading a chapter, when doing your final preparation for the exam, take the time to flip through the chapters, looking for the Key Topic icons, and review those paragraphs, tables, figures, and lists.
- **Fill In Key Tables from Memory**—The more important tables from the chapters have been copied to PDF files available on the CD as Appendix G. The tables have most of the information removed. After printing these mostly empty tables, you can use them to improve your memory of the facts in the table by trying to fill them out. This tool should be useful for memorizing key facts. That same CD-only appendix contains the completed tables so you can check your work.
- **CD-based practice exam—**The companion CD contains multiple-choice questions and a testing engine. The CD includes 200 questions unique to the CD. As part of your final preparation, you should practice with these questions to help you get used to the exam-taking process, as well as help refine and prove your knowledge of the exam topics.
- **Special question section for the "Implement Proposed Changes to a Network" section of the Blueprint**—To provide practice and perspectives on these exam topics, a special section of questions has been developed to help you both prepare for these new types of questions.

- **Key terms and Glossary**—The more important terms mentioned in each chapter are listed at the end of each chapter under the heading “Definitions.” The Glossary, found on the CD that comes with this book, lists all the terms from the chapters. When studying each chapter, you should review the key terms, and for those terms about which you are unsure of the definition, you can review the short definitions from the Glossary.
- **Further Reading**—Most chapters include a suggested set of books and websites for additional study on the same topics covered in that chapter. Often, these references will be useful tools for preparation for the CCIE Routing and Switching lab exam.

CHAPTER 2

Virtual LANs and VLAN Trunking

This chapter continues with the coverage of some of the most fundamental and important LAN topics with coverage of VLANs and VLAN trunking. As usual, for those of you current in your knowledge of the topics in this chapter, review the items next to the Key Topic icons spread throughout the chapter, plus the "Foundation Summary" and "Memory Builders" sections at the end of the chapter.

"Do I Know This Already?" Quiz

Table 2-1 outlines the major headings in this chapter and the corresponding "Do I Know This Already?" quiz questions.

Table 2-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section	Score
Virtual LANs	1–2	
VLAN Trunking Protocol	3–5	
VLAN Trunking: ISL and 802.1Q	6–9	
Configuring PPPoE	10	
Total Score		

In order to best use this pre-chapter assessment, remember to score yourself strictly. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

1. Assume that VLAN 28 does not yet exist on Switch1. Which of the following commands, issued from any part of global configuration mode (reached with the **configure terminal** exec command) would cause the VLAN to be created?

   a. **vlan 28**

   b. **vlan 28 name fred**

   c. **switchport vlan 28**

   d. **switchport access vlan 28**

   e. **switchport access 28**

2. Which of the following are the two primary motivations for using private VLANs?

   a. Better LAN security

   b. IP subnet conservation

   c. Better consistency in VLAN configuration details

   d. Reducing the impact of broadcasts on end-user devices

   e. Reducing the unnecessary flow of frames to switches that do not have any ports in the VLAN to which the frame belongs

3. Which of the following VLANs can be pruned by VTP on an 802.1Q trunk?

   a. 1–1023

   b. 1–1001

   c. 2–1001

   d. 1–1005

   e. 2–1005

4. An existing switched network has ten switches, with Switch1 and Switch2 being the only VTP servers in the network. The other switches are all VTP clients and have successfully learned about the VLANs from the VTP servers. The only configured VTP parameter on all switches is the VTP domain name (Larry). The VTP revision number is 201. What happens when a new, already-running VTP client switch, named Switch11, with domain name Larry and revision number 301, connects via a trunk to any of the other ten switches?

   a. No VLAN information changes; Switch11 ignores the VTP updates sent from the two existing VTP servers until the revision number reaches 302.

   b. The original ten switches replace their old VLAN configuration with the configuration in Switch11.

   c. Switch11 replaces its own VLAN configuration with the configuration sent to it by one of the original VTP servers.

   d. Switch11 merges its existing VLAN database with the database learned from the VTP servers, because Switch11 had a higher revision number.

5. An existing switched network has ten switches, with Switch1 and Switch2 being the only VTP servers in the network. The other switches are all VTP clients, and have successfully learned about the VLANs from the VTP server. The only configured VTP parameter is the VTP domain name (Larry). The VTP revision number is 201. What happens when an already-running VTP server switch, named Switch11, with domain name Larry and revision number 301, connects via a trunk to any of the other ten switches?

- **a.** No VLAN information changes; all VTP updates between the original VTP domain and the new switch are ignored.
- **b.** The original ten switches replace their old VLAN configuration with the configuration in Switch11.
- **c.** Switch11 replaces its old VLAN configuration with the configuration sent to it by one of the original VTP servers.
- **d.** Switch11 merges its existing VLAN database with the database learned from the VTP servers, because Switch11 had a higher revision number.
- **e.** None of the other answers is correct.

6. Assume that two brand-new Cisco switches were removed from their cardboard boxes. PC1 was attached to one switch, PC2 was attached to the other, and the two switches were connected with a cross-over cable. The switch connection dynamically formed an 802.1Q trunk. When PC1 sends a frame to PC2, how many additional bytes of header are added to the frame before it passes over the trunk?

- **a.** 0
- **b.** 4
- **c.** 8
- **d.** 26

7. Assume that two brand-new Cisco Catalyst 3550 switches were connected with a cross-over cable. Before attaching the cable, one switch interface was configured with the **switchport trunk encapsulation dot1q**, **switchport mode trunk**, and **switchport nonegotiate** subcommands. Which of the following must be configured on the other switch before trunking will work between the switches?

- **a.** **switchport trunk encapsulation dot1q**
- **b.** **switchport mode trunk**
- **c.** **switchport nonegotiate**
- **d.** No configuration is required.

8. When configuring trunking on a Cisco router fa0/1 interface, under which configuration modes could the IP address associated with the native VLAN (VLAN 1 in this case) be configured?

   a. Interface fa 0/1 configuration mode
   b. Interface fa 0/1.1 configuration mode
   c. Interface fa 0/1.2 configuration mode
   d. None of the other answers is correct

9. Which of the following is false about 802.1Q?

   a. Encapsulates the entire frame inside an 802.1Q header and trailer
   b. Supports the use of a native VLAN
   c. Allows VTP to operate only on extended-range VLANs
   d. Is chosen over ISL by DTP

10. Which command enables PPPoE on the outside Ethernet interface on a Cisco router?

   a. **pppoe enable**
   b. **pppoe-client enable**
   c. **pppoe-client dialer-pool-number**
   d. **pppoe-client dialer-number**

Foundation Topics

Virtual LANs

In an Ethernet LAN, a set of devices that receive a broadcast sent by any one of the devices in the same set is called a *broadcast domain*. On switches that have no concept of virtual LANs (VLAN), a switch simply forwards all broadcasts out all interfaces, except the interface on which it received the frame. As a result, all the interfaces on an individual switch are in the same broadcast domain. Also, if the switch connects to other switches and hubs, the interfaces on those switches and hubs are also in the same broadcast domain.

A *VLAN* is simply an administratively defined subset of switch ports that are in the same broadcast domain. Ports can be grouped into different VLANs on a single switch, and on multiple interconnected switches as well. By creating multiple VLANs, the switches create multiple broadcast domains. By doing so, a broadcast sent by a device in one VLAN is forwarded to the other devices in that same VLAN; however, the broadcast is not forwarded to devices in the other VLANs.

Key Topic

With VLANs and IP, best practices dictate a one-to-one relationship between VLANs and IP subnets. Simply put, the devices in a single VLAN are typically also in the same single IP subnet. Alternately, it is possible to put multiple subnets in one VLAN, and use secondary IP addresses on routers to route between the VLANs and subnets. Also, although not typically done, you can design a network to use one subnet on multiple VLANs, and use routers with proxy ARP enabled to forward traffic between hosts in those VLANs. (Private VLANs might be considered to consist of one subnet over multiple VLANs as well, as covered later in this chapter.) Ultimately, the CCIE written exams tend to focus more on the best use of technologies, so this book will assume that one subnet sits on one VLAN, unless otherwise stated.

Layer 2 switches forward frames between devices in the same VLAN, but they do not forward frames between two devices in different VLANs. To forward data between two VLANs, a multilayer switch (MLS) or router is needed. Chapter 6, "IP Forwarding (Routing)," covers the details of MLS.

VLAN Configuration

Configuring VLANs in a network of Cisco switches requires just a few simple steps:

Step 1 Create the VLAN itself.

Step 2 Associate the correct ports with that VLAN.

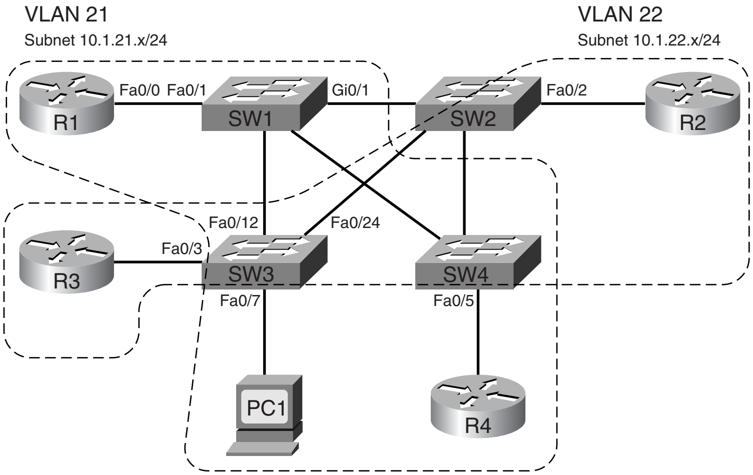
The challenge relates to how some background tasks differ depending on how the Cisco *VLAN Trunking Protocol (VTP)* is configured, and whether normal-range or extended-range VLANs are being used.

Using VLAN Database Mode to Create VLANs

To begin, consider Example 2-1, which shows some of the basic mechanics of VLAN creation in *VLAN database configuration mode*. VLAN database configuration mode allows the creation of VLANs, basic administrative settings for each VLAN, and verification of VTP configuration information. Only normal-range (VLANs 1–1005) VLANs can be configured in this mode, and the VLAN configuration is stored in a Flash file called vlan.dat.

Example 2-1 demonstrates VLAN database configuration mode, showing the configuration on Switch3 from Figure 2-1. The example shows VLANs 21 and 22 being created.

Figure 2-1 *Simple Access and Distribution*



Example 2-1 *VLAN Creation in VLAN Database Mode–Switch3*

```
! Below, note that FA 0/12 and FA0/24 missing from the list, because they have
! dynamically become trunks, supporting multiple VLANs.
Switch3# show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23
```

Example 2-1 *VLAN Creation in VLAN Database Mode–Switch3 (Continued)*

```
! Below, "unsup" means that this 2950 switch does not support FDDI and TR
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
! Below, vlan database moves user to VLAN database configuration mode.
! The vlan 21 command defines the VLAN, as seen in the next command output
! (show current), VLAN 21 is not in the "current" VLAN list.
Switch3# vlan database
Switch3(vlan)# vlan 21
VLAN 21 added:
    Name: VLAN0021
! The show current command lists the VLANs available to the IOS when the switch
! is in VTP Server mode. The command lists the VLANs in numeric order, with
! VLAN 21 missing.
Switch3(vlan)# show current
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Backup CRF Mode: Disabled
    Remote SPAN VLAN: No

  VLAN ISL Id: 1002
    Name: fddi-default
    Media Type: FDDI
    VLAN 802.10 Id: 101002
    State: Operational
    MTU: 1500
    Backup CRF Mode: Disabled
    Remote SPAN VLAN: No
! Lines omitted for brevity
! Next, note that show proposed lists VLAN 21. The vlan 21 command
! creates the definition, but it must be "applied" before it is "current".
Switch3(vlan)# show proposed
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Backup CRF Mode: Disabled
    Remote SPAN VLAN: No
```

continues

Example 2-1 *VLAN Creation in VLAN Database Mode–Switch3 (Continued)*

Key Topic

```
  VLAN ISL Id: 21
    Name: VLAN0021
    Media Type: Ethernet
    VLAN 802.10 Id: 100021
    State: Operational
    MTU: 1500
    Backup CRF Mode: Disabled
    Remote SPAN VLAN: No
! Lines omitted for brevity
! Next, you could apply to complete the addition of VLAN 21,
! abort to not make the changes and exit VLAN database mode, or
! reset to not make the changes but stay in VLAN database mode.
Switch3(vlan)# ?
VLAN database editing buffer manipulation commands:
  abort  Exit mode without applying the changes
  apply  Apply current changes and bump revision number
  exit   Apply changes, bump revision number, and exit mode
  no     Negate a command or set its defaults
  reset  Abandon current changes and reread current database
  show   Show database information
  vlan   Add, delete, or modify values associated with a single VLAN
  vtp    Perform VTP administrative functions.
! The apply command was used, making the addition of VLAN 21 complete.
Switch3(vlan)# apply
APPLY completed.
! A show current now would list VLAN 21.
Switch3(vlan)# vlan 22 name ccie-vlan-22
VLAN 22 added:
    Name: ccie-vlan-22
! Above and below, some variations on commands are shown, along with the
! creation of VLAN 22, with name ccie-vlan-22.
! Below, the vlan 22 option is used on show current and show proposed
! detailing the fact that the apply has not been done yet.
Switch3(vlan)# show current 22
VLAN 22 does not exist in current database
Switch3(vlan)# show proposed 22
  VLAN ISL Id: 22
! Lines omitted for brevity
! Finally, the user exits VLAN database mode using CTRL-Z, which does
! not inherently apply the change. CTRL-Z actually executes an abort.
Switch3(vlan)# ^Z
```

Using Configuration Mode to Put Interfaces into VLANs

To make a VLAN operational, the VLAN must be created, and then switch ports must be assigned to the VLAN. Example 2-2 shows how to associate the interfaces with the correct VLANs, once again on Switch3.

NOTE At the end of Example 2-1, VLAN 22 had not been successfully created. The assumption for Example 2-2 is that VLAN 22 has been successfully created.

Example 2-2 *Assigning Interfaces to VLANs–Switch3*

```
! First, the switchport access command assigns the VLAN numbers to the
! respective interfaces.

Switch3# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch3(config)# int fa 0/3
Switch3(config-if)# switchport access vlan 22
Switch3(config-if)# int fa 0/7
Switch3(config-if)# switchport access vlan 21
Switch3(config-if)# ^Z
! Below, show vlan brief lists these same two interfaces as now being in
! VLANs 21 and 22, respectively.
Switch3# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
21   VLAN0021                         active    Fa0/7
22   ccie-vlan-22                     active    Fa0/3
! Lines omitted for brevity
! While the VLAN configuration is not shown in the running-config at this point,
! the switchport access command that assigns the VLAN for the interface is in the
! configuration, as seen with the show run int fa 0/3 command.
Switch3# show run int fa 0/3
interface FastEthernet0/3
switchport access vlan 22
```

Using Configuration Mode to Create VLANs

At this point, the two new VLANs (21 and 22) have been created on Switch3, and the two interfaces are now in the correct VLANs. However, Cisco IOS switches support a different way to create VLANs, using configuration mode, as shown in Example 2-3.

Example 2-3 *Creating VLANs in Configuration Mode–Switch3*

Key Topic

```
! First, VLAN 31 did not exist when the switchport access vlan 31 command was
! issued. As a result, the switch both created the VLAN and put interface fa0/8
! into that VLAN. Then, the vlan 32 global command was used to create a
```

continues

Example 2-3 *Creating VLANs in Configuration Mode–Switch3 (Continued)*

```
! VLAN from configuration mode, and the name subcommand was used to assign a
! non-default name.
Switch3# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch3(config)# int fa 0/8
Switch3(config-if)# switchport access vlan 31
% Access VLAN does not exist. Creating vlan 31
Switch3(config-if)# exit
Switch3(config)# vlan 32
Switch3(config-vlan)# name ccie-vlan-32
Switch3(config-vlan)# ^Z
Switch3# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23
21   VLAN0021                         active    Fa0/7
22   ccie-vlan-22                     active    Fa0/3
31   VLAN0031                         active    Fa0/8
32   ccie-vlan-32                     active
! Portions omitted for brevity
```

Example 2-3 shows how the **switchport access vlan** subcommand creates the VLAN, as needed, and assigns the interface to that VLAN. Note that in Example 2-3, the **show vlan brief** output lists fa0/8 as being in VLAN 31. Because no ports have been assigned to VLAN 32 as of yet, the final line in Example 2-3 simply does not list any interfaces.

The VLAN creation process is simple but laborious in a large network. If many VLANs exist, and they exist on multiple switches, instead of manually configuring the VLANs on each switch, you can use VTP to distribute the VLAN configuration of a VLAN to the rest of the switches. VTP will be discussed after a brief discussion of private VLANs.

Private VLANs

Engineers may design VLANs with many goals in mind. In many cases today, devices end up in the same VLAN just based on the physical locations of the wiring drops. Security is another motivating factor in VLAN design: devices in different VLANs do not overhear each other's broadcasts. Additionally, the separation of hosts into different VLANs and subnets requires an intervening router or multilayer switch between the subnets, and these types of devices typically provide more robust security features.

Regardless of the design motivations behind grouping devices into VLANs, good design practices typically call for the use of a single IP subnet per VLAN. In some cases, however, the need to increase security by separating devices into many small VLANs conflicts with the design goal of conserving the use of the available IP subnets. The Cisco private VLAN feature addresses this issue. Private VLANs allow a switch to separate ports as if they were on different VLANs, while consuming only a single subnet.

A common place to implement private VLANs is in the multitenant offerings of a service provider (SP). The SP can install a single router and a single switch. Then, the SP attaches devices from multiple customers to the switch. Private VLANs then allow the SP to use only a single subnet for the whole building, separating different customers' switch ports so that they cannot communicate directly, while supporting all customers with a single router and switch.

Conceptually, a private VLAN includes the following general characterizations of how ports communicate:

- Ports that need to communicate with all devices
- Ports that need to communicate with each other, and with shared devices, typically routers
- Ports that need to communicate only with shared devices

To support each category of allowed communications, a single private VLAN features a *primary VLAN* and one or more *secondary VLANs*. The ports in the primary VLAN are *promiscuous* in that they can send and receive frames with any other port, including ports assigned to secondary VLANs. Commonly accessed devices, such as routers and servers, are placed into the primary VLAN. Other ports, such as customer ports in the SP multitenant model, attach to one of the secondary VLANs.

Secondary VLANs are either *community VLANs* or *isolated VLANs*. The engineer picks the type based on whether the device is part of a set of ports that should be allowed to send frames back and forth (community VLAN ports), or whether the device port should not be allowed to talk to any other ports besides those on the primary VLAN (isolated VLAN). Table 2-2 summarizes the behavior of private VLAN communications between ports.

Table 2-2 *Private VLAN Communications Between Ports*

Description of Who Can Talk to Whom	Primary VLAN Ports	Community VLAN Ports[1]	Isolated VLAN Ports[1]
Talk to ports in primary VLAN (promiscuous ports)	Yes	Yes	Yes
Talk to ports in the same secondary VLAN (host ports)	N/A[2]	Yes	No
Talks to ports in another secondary VLAN	N/A[2]	No	No

[1] Community and isolated VLANs are secondary VLANs.

[2] Promiscuous ports, by definition in the primary VLAN, can talk to all other ports.

VLAN Trunking Protocol

VTP advertises VLAN configuration information to neighboring switches so that the VLAN configuration can be made on one switch, with all the other switches in the network learning the VLAN information dynamically. VTP advertises the VLAN ID, VLAN name, and VLAN type for each VLAN. However, VTP does not advertise any information about which ports (interfaces) should be in each VLAN, so the configuration to associate a switch interface with a particular VLAN (using the **switchport access vlan** command) must still be configured on each individual switch. Also, the existence of the VLAN IDs used for private VLANs is advertised, but the rest of the detailed private VLAN configuration is not advertised by VTP.

Each Cisco switch uses one of three VTP modes, as outlined in Table 2-3.

Table 2-3 *VTP Modes and Features**

Function	Server Mode	Client Mode	Transparent Mode
Originates VTP advertisements	Yes	Yes	No
Processes received advertisements to update its VLAN configuration	Yes	Yes	No
Forwards received VTP advertisements	Yes	Yes	Yes
Saves VLAN configuration in NVRAM or vlan.dat	Yes	Yes	Yes
Can create, modify, or delete VLANs using configuration commands	Yes	No	Yes

*CatOS switches support a fourth VTP mode (off), meaning that the switch does not create, listen to, or forward VTP updates.

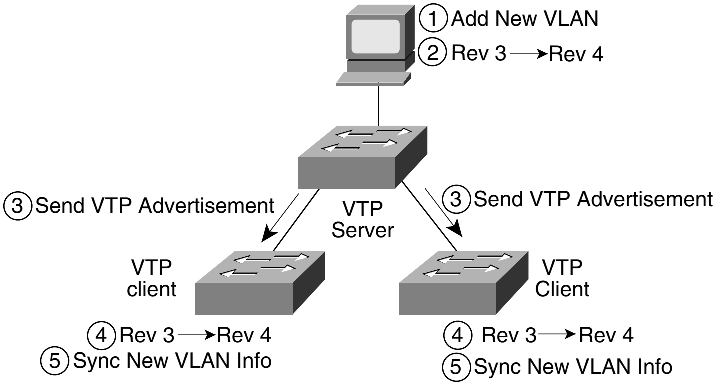
VTP Process and Revision Numbers

The VTP update process begins when a switch administrator, from a VTP server switch, adds, deletes, or updates the configuration for a VLAN. When the new configuration occurs, the VTP server increments the old VTP *revision number* by 1, and advertises the entire VLAN configuration database along with the new revision number.

The VTP revision number concept allows switches to know when VLAN database changes have occurred. Upon receiving a VTP update, if the revision number in a received VTP update is larger than a switch's current revision number, it believes that there is a new version of the VLAN database. Figure 2-2 shows an example in which the old VTP revision number was 3, the server adds a new VLAN, incrementing the revision number to 4, and then propagates the VTP database to the other switches.

Figure 2-2 *VTP Revision Number Basic Operation*

Key Topic



Cisco switches default to use VTP server mode, but they do not start sending VTP updates until the switch has been configured with a VTP domain name. At that point, the server begins to send its VTP updates, with a different database and revision number each time its VLAN configuration changes. However, the VTP clients in Figure 2-2 actually do not have to have the VTP domain name configured. If not configured, the client will assume it should use the VTP domain name in the first received VTP update. However, the client does need one small bit of configuration, namely, the VTP mode, as configured with the **vtp mode** global configuration command.

VTP clients and servers alike will accept VTP updates from other VTP server switches. When using VTP, for better availability, a switched network using VTP needs at least two VTP server switches. Under normal operations, a VLAN change could be made on one server switch, and the other VTP server (plus all the clients) would learn about the changes to the VLAN database. Once learned, both VTP servers and clients store the VLAN configuration in their respective vlan.dat files in flash memory; they do not store the VLAN configuration in NVRAM.

With multiple VTP servers installed in a LAN, it is possible to accidentally overwrite the VTP configuration in the network. If trunks fail and then changes are made on more than one VTP server, the VTP configuration databases could differ, with different configuration revision numbers. When the formerly-separated parts of the LAN reconnect using trunks, the VTP database with a higher revision number is propagated throughout the VTP domain, replacing some switches' VTP databases. Note also that because VTP clients can actually originate VTP updates, under the right circumstances, a VTP client can update the VTP database on another VTP client or server. See http://www.ciscopress.com/1587201968 and look for downloads, to download a document that describes how a client could update the VLAN database on another VTP client or server. In summary, for a newly-connected VTP server or client to change another switch's VTP database, the following must be true:

- The new link connecting the new switch is trunking.
- The new switch has the same VTP domain name as the other switches.
- The new switch's revision number is larger than that of the existing switches.
- The new switch must have the same password, if configured on the existing switches.

Key Topic

The revision number and VTP domain name can be easily seen with a Sniffer trace; to prevent DoS attacks with VTP, set VTP passwords, which are encoded as message digests (MD5) in the VTP updates. Also, some installations simply use VTP transparent mode on all switches, which prevents switches from ever listening to other switch VTP updates and erroneously deleting their VLAN configuration databases.

VTP Configuration

VTP sends updates out all active trunk interfaces (ISL or 802.1Q). However, with all default settings from Cisco, switches are in server mode, with no VTP domain name configured, and they do not send any VTP updates. Before any switches can learn VLAN information from another switch, at least one switch must have a bare-minimum VTP server configuration—specifically, a domain name.

Example 2-4 shows Switch3 configuring a VTP domain name to become a VTP server and advertise the VLANs it has configured. The example also lists several key VTP **show** commands. (Note that the example begins with VLANs 21 and 22 configured on Switch3, and all default settings for VTP on all four switches.)

Example 2-4 *VTP Configuration and* **show** *Command Example*

```
! First, Switch3 is configured with a VTP domain ID of CCIE-domain.
Switch3# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch3(config)# vtp domain CCIE-domain
Changing VTP domain name from NULL to CCIE-domain
Switch3(config)# ^Z
! Next, on Switch1, the VTP status shows the same revision as Switch3, and it
! learned the VTP domain name CCIE-domain. Note that Switch1 has no VTP-related
```

Example 2-4 *VTP Configuration and* **show** *Command Example (Continued)*

```
! configuration, so it is a VTP server; it learned the VTP domain name from.
! Switch3.
Switch1# sh vtp status
VTP Version                     : 2
Configuration Revision          : 2
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 7
VTP Operating Mode              : Server
VTP Domain Name                 : CCIE-domain
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x0E 0x07 0x9D 0x9A 0x27 0x10 0x6C 0x0B
Configuration last modified by 10.1.1.3 at 3-1-93 00:02:55
Local updater ID is 10.1.1.1 on interface Vl1 (lowest numbered VLAN interface found)
! The show vlan brief command lists the VLANs learned from Switch3.
Switch1# show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/10
                                                Fa0/11, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Gi0/2
21   VLAN0021                         active
22   ccie-vlan-22                     active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Example 2-4 shows examples of a few VTP configuration options. Table 2-4 provides a complete list, along with explanations.

Table 2-4 *VTP Configuration Options*

Key Topic

Option	Meaning
domain	Sends domain name in VTP updates. Received VTP update is ignored if it does not match a switch's domain name. One VTP domain name per switch is allowed.
password	Used to generate an MD5 hash that is included in VTP updates. Received VTP updates are ignored if the passwords on the sending and receiving switch do not match.
mode	Sets server, client, or transparent mode on the switch.

continues

Table 2-4 *VTP Configuration Options (Continued)*

Option	Meaning
version	Sets version 1 or 2. Servers and clients must match version to exchange VLAN configuration data. Transparent mode switches at version 2 forward version 1 or version 2 VTP updates.
pruning	Enables VTP pruning, which prevents flooding on a per-VLAN basis to switches that do not have any ports configured as members of that VLAN.
interface	Specifies the interface whose IP address is used to identify this switch in VTP updates.

Normal-Range and Extended-Range VLANs

Some VLAN numbers are considered to be *normal*, whereas some others are considered to be *extended*. Normal-range VLANs are VLANs 1–1005, and can be advertised via VTP versions 1 and 2. These VLANs can be configured in VLAN database mode, with the details being stored in the vlan.dat file in Flash.

Extended-range VLANs range from 1006–4094, inclusive. However, these additional VLANs cannot be configured in VLAN database mode, nor stored in the vlan.dat file, nor advertised via VTP. In fact, to configure them, the switch must be in VTP transparent mode. (Also, you should take care to avoid using VLANs 1006–1024 for compatibility with CatOS-based switches.)

Both ISL and 802.1Q support extended-range VLANs today. Originally, ISL began life only supporting normal-range VLANs, using only 10 of the 15 bits reserved in the ISL header to identify the VLAN ID. The later-defined 802.1Q used a 12-bit VLAN ID field, thereby allowing support of the extended range. Following that, Cisco changed ISL to use 12 of its reserved 15 bits in the VLAN ID field, thereby supporting the extended range.

Table 2-5 summarizes VLAN numbers and provides some additional notes.

Table 2-5 *Valid VLAN Numbers, Normal and Extended*

Key Topic

VLAN Number	Normal or Extended?	Can Be Advertised and Pruned by VTP Versions 1 and 2?	Comments
0	Reserved	—	Not available for use
1	Normal	No	On Cisco switches, the default VLAN for all access ports; cannot be deleted or changed
2–1001	Normal	Yes	

Table 2-5 *Valid VLAN Numbers, Normal and Extended (Continued)*

VLAN Number	Normal or Extended?	Can Be Advertised and Pruned by VTP Versions 1 and 2?	Comments
1002–1005	Normal	No	Defined specifically for use with FDDI and TR translational bridging
1006–4094	Extended	No	

Storing VLAN Configuration

Catalyst IOS stores VLAN and VTP configuration in one of two places—either in a Flash file called vlan.dat or in the running configuration. (Remember that the term "Catalyst IOS" refers to a switch that uses IOS, not the Catalyst OS, which is often called CatOS.) IOS chooses the storage location in part based on the VTP mode, and in part based on whether the VLANs are normal-range VLANs or extended-range VLANs. Table 2-6 describes what happens based on what configuration mode is used to configure the VLANs, the VTP mode, and the VLAN range. (Note that VTP clients also store the VLAN configuration in vlan.dat, and they do not understand extended range VLANs.)

Table 2-6 *VLAN Configuration and Storage*

Key Topic

Function	When in VTP Server Mode	When in VTP Transparent Mode
Normal-range VLANs can be configured from	Both VLAN database and configuration modes	Both VLAN database and configuration modes
Extended-range VLANs can be configured from	Nowhere—cannot be configured	Configuration mode only
VTP and normal-range VLAN configuration commands are stored in	vlan.dat in Flash	Both vlan.dat in Flash and running configuration[1]
Extended-range VLAN configuration commands stored in	Nowhere—extended range not allowed in VTP server mode	Running configuration only

[1] When a switch reloads, if the VTP mode or domain name in the vlan.dat file and the startup-config file differ, the switch uses only the vlan.dat file's contents for VLAN configuration.

> **NOTE** The configuration characteristics referenced in Table 2-6 do not include the interface configuration command **switchport access vlan**; it includes the commands that create a VLAN (**vlan** command) and VTP configuration commands.

Of particular interest for those of you stronger with CatOS configuration skills is that when you erase the startup-config file, and reload the Cisco IOS switch, you do not actually erase the normal-range VLAN and VTP configuration information. To erase the VLAN and VTP configuration, you must use the **delete flash:vlan.dat** exec command. Also note that if multiple switches are in VTP server mode, if you delete vlan.dat on one switch and then reload it, as soon as the switch comes back up and brings up a trunk, it learns the old VLAN database via a VTP update from the other VTP server.

VLAN Trunking: ISL and 802.1Q

VLAN trunking allows switches, routers, and even PCs with the appropriate NICs to send traffic for multiple VLANs across a single link. In order to know to which VLAN a frame belongs, the sending switch, router, or PC adds a header to the original Ethernet frame, with that header having a field in which to place the VLAN ID of the associated VLAN. This section describes the protocol details for the two trunking protocols, followed by the details of how to configure trunking.

ISL and 802.1Q Concepts

If two devices are to perform trunking, they must agree to use either ISL or 802.1Q, because there are several differences between the two, as summarized in Table 2-7.

Table 2-7 *Comparing ISL and 802.1Q*

Key Topic

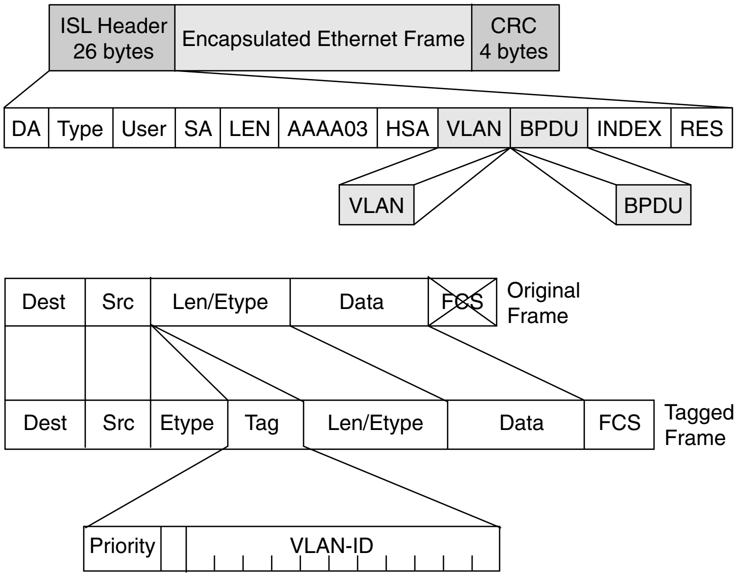
Feature	**ISL**	**802.1Q**
VLANs supported	Normal and extended range[1]	Normal and extended range
Protocol defined by	Cisco	IEEE
Encapsulates original frame or inserts tag	Encapsulates	Inserts tag
Supports native VLAN	No	Yes

[1] ISL originally supported only normal-range VLANs, but was later improved to support extended-range VLANs as well.

ISL and 802.1Q differ in how they add a header to the Ethernet frame before sending it over a trunk. ISL adds a new 26-byte header, plus a new trailer (to allow for the new FCS value), encapsulating the original frame. This encapsulating header uses the source address (listed as SA in Figure 2-3) of the device doing the trunking, instead of the source MAC of the original frame. ISL uses a multicast destination address (listed as DA in Figure 2-3) of either 0100.0C00.0000 or 0300.0C00.0000.

802.1Q inserts a 4-byte header, called a tag, into the original frame (right after the Source Address field). The original frame's addresses are left intact. Normally, an Ethernet controller would expect to find either an Ethernet Type field or 802.3 Length field right after the Source Address field. With an 802.1Q tag, the first 2 bytes after the Address fields holds a registered Ethernet type value of 0x8100, which implies that the frame includes an 802.1Q header. Because 802.1Q does not actually encapsulate the original frame, it is often called *frame tagging*. Figure 2-3 shows the contents of the headers used by both ISL and 802.1Q.

Figure 2-3 *ISL and 802.1Q Frame Marking Methods*



Finally, the last row from Table 2-7 refers to the *native VLAN*. 802.1Q does not tag frames sent inside the native VLAN. The native VLAN feature allows a switch to attempt to use 802.1Q trunking on an interface, but if the other device does not support trunking, the traffic for that one native VLAN can still be sent over the link. By default, the native VLAN is VLAN 1.

ISL and 802.1Q Configuration

Cisco switches use the *Dynamic Trunk Protocol (DTP)* to dynamically learn whether the device on the other end of the cable wants to perform trunking and, if so, which trunking protocol to use. DTP learns whether to trunk based on the DTP mode defined for an interface. Cisco switches default to use the DTP *desirable* mode, which means that the switch initiates sending DTP messages, hoping that the device on the other end of the segment replies with another DTP message. If a reply is received, DTP can detect whether both switches can trunk and, if so, which type of trunking to use. If both switches support both types of trunking, they choose to use ISL. (An upcoming section, "Trunk Configuration Compatibility," covers the different DTP modes and how they work.)

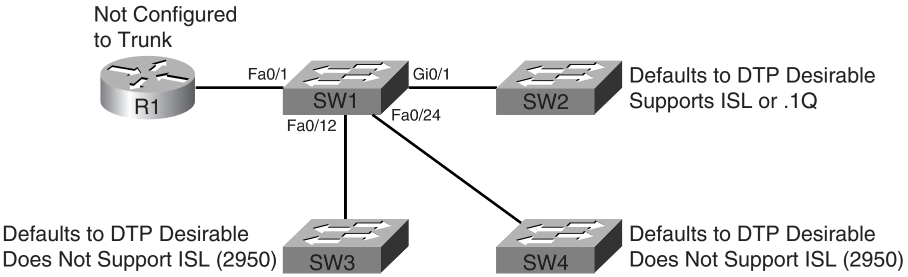
With the DTP mode set to desirable, switches can simply be connected, and they should dynamically form a trunk. You can, however, configure trunking details and verify the results with **show** commands. Table 2-8 lists some of the key Catalyst IOS commands related to trunking.

Table 2-8 *VLAN Trunking–Related Commands*

Command	Function
switchport | **no switchport**	Toggle defining whether to treat the interface as a switch interface (**switchport**) or as a router interface (**no switchport**)
switchport mode	Sets DTP negotiation parameters
switchport trunk	Sets trunking parameters if the interface is trunking
switchport access	Sets nontrunking-related parameters if the interface is not trunking
show interface trunk	Summary of trunk-related information
show interface *type number* **trunk**	Lists trunking details for a particular interface
show interface *type number* **switchport**	Lists nontrunking details for a particular interface

Figure 2-4 lists several details regarding Switch1's trunking configuration and status, as shown in Example 2-5. R1 is not configured to trunk, so Switch1 will fail to negotiate trunking. Switch2 is a Catalyst 3550, which supports both ISL and 802.1Q, so they will negotiate trunking and use ISL. Switch3 and Switch4 are Catalyst 2950s, which support only 802.1Q; as a result, Switch1 negotiates trunking, but picks 802.1Q as the trunking protocol.

Figure 2-4 *Trunking Configuration Reference for Example 2-5*


Not Configured
to Trunk
R1
Fa0/1
SW1
Gi0/1
SW2
Defaults to DTP Desirable
Supports ISL or .1Q
Fa0/12
Fa0/24
Defaults to DTP Desirable
Does Not Support ISL (2950)
SW3
SW4
Defaults to DTP Desirable
Does Not Support ISL (2950)

Example 2-5 *Trunking Configuration and* **show** *Command Example–Switch1*

```
! The administrative mode of dynamic desirable (trunking) and negotiate (trunking
! encapsulation) means that Switch1 attempted to negotiate to trunk, but the
! operational mode of static access means that trunking negotiation failed.
! The reference to "operational trunking encapsulation" of native means that
! no tagging occurs.
```

Example 2-5 *Trunking Configuration and* **show** *Command Example–Switch1 (Continued)*

```
Switch1# show int fa 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

Voice VLAN: none (Inactive)
Appliance trust: none
! Next, the show int gig 0/1 trunk command shows the configured mode
! (desirable), and the current status (N-ISL), meaning negotiated ISL. Note
! that the trunk supports the extended VLAN range as well.
Switch1# show int gig 0/1 trunk
Port      Mode         Encapsulation  Status        Native vlan
Gi0/1     desirable    n-isl          trunking      1

Port      Vlans allowed on trunk
Gi0/1     1-4094

Port      Vlans allowed and active in management domain
Gi0/1     1,21-22

Port      Vlans in spanning tree forwarding state and not pruned
Gi0/1     1,21-22
! Next, Switch1 lists all three trunks - the segments connecting to the other
! three switches - along with the type of encapsulation.
Switch1# show int trunk
Port      Mode         Encapsulation  Status        Native vlan
Fa0/12    desirable    n-802.1q       trunking      1
Fa0/24    desirable    n-802.1q       trunking      1
Gi0/1     desirable    n-isl          trunking      1

Port      Vlans allowed on trunk
Fa0/12    1-4094
```

continues

Example 2-5 *Trunking Configuration and* **show** *Command Example–Switch1 (Continued)*

```
Fa0/24    1-4094
Gi0/1     1-4094

Port      Vlans allowed and active in management domain
Fa0/12    1,21-22
Fa0/24    1,21-22
Gi0/1     1,21-22

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/12    1,21-22
Fa0/24    1,21-22
Gi0/1     1,21-22
```

Allowed, Active, and Pruned VLANs

Although a trunk can support VLANs 1–4094, several mechanisms reduce the actual number of VLANs whose traffic flows over the trunk. First, VLANs can be administratively forbidden from existing over the trunk using the **switchport trunk allowed** interface subcommand. Also, any allowed VLANs must be configured on the switch before they are considered active on the trunk. Finally, VTP can prune VLANs from the trunk, with the switch simply ceasing to forward frames from that VLAN over the trunk.

The **show interface trunk** command lists the VLANs that fall into each category, as shown in the last command in Example 2-5. The categories are summarized as follows:

Key Topic

- **Allowed VLANs**—Each trunk allows all VLANs by default. However, VLANs can be removed or added to the list of allowed VLANs by using the **switchport trunk allowed** command.
- **Allowed and active**—To be active, a VLAN must be in the allowed list for the trunk (based on trunk configuration), and the VLAN must exist in the VLAN configuration on the switch. With PVST+, an STP instance is actively running on this trunk for the VLANs in this list.
- **Active and not pruned**—This list is a subset of the “allowed and active” list, with any VTP-pruned VLANs removed.

Trunk Configuration Compatibility

In most production networks, switch trunks are configured using the same standard throughout the network. For instance, rather than allow DTP to negotiate trunking,, many engineers configure trunk interfaces to always trunk (**switchport mode trunk**) and disable DTP on ports that should not trunk. IOS includes several commands that impact whether a particular segment becomes a trunk. Because many enterprises use a typical standard, it is easy to forget the nuances of how the related commands work. This section covers those small details.

Two IOS configuration commands impact if and when two switches form a trunk. The **switchport mode** and **switchport nonegotiate** interface subcommands define whether DTP even attempts to negotiate a trunk, and what rules it uses when the attempt is made. Additionally, the settings on the switch ports on either side of the segment dictate whether a trunk forms or not.

Table 2-9 summarizes the trunk configuration options. The first column suggests the configuration on one switch, with the last column listing the configuration options on the other switch that would result in a working trunk between the two switches.

Table 2-9 *Trunking Configuration Options That Lead to a Working Trunk*

Key Topic

Configuration Command on One Side[1]	Short Name	Meaning	To Trunk, Other Side Must Be
switchport mode trunk	Trunk	Always trunks on this end; sends DTP to help other side choose to trunk	On, desirable, auto
switchport mode trunk; **switchport nonegotiate**	Nonegotiate	Always trunks on this end; does not send DTP messages (good when other switch is a non-Cisco switch)	On
switchport mode dynamic desirable	Desirable	Sends DTP messages, and trunks if negotiation succeeds	On, desirable, auto
switchport mode dynamic auto	Auto	Replies to DTP messages, and trunks if negotiation succeeds	On, desirable
switchport mode access	Access	Never trunks; sends DTP to help other side reach same conclusion	(Never trunks)
switchport mode access; **switchport nonegotiate**	Access (with nonegotiate)	Never trunks; does not send DTP messages	(Never trunks)

[1] When the **switchport nonegotiate** command is not listed in the first column, the default (DTP negotiation is active) is assumed.

NOTE If an interface trunks, then the type of trunking (ISL or 802.1Q) is controlled by the setting on the **switchport trunk encapsulation** command. This command includes an option for dynamically negotiating the type (using DTP) or configuring one of the two types. See Example 2-5 for a sample of the syntax.

Configuring Trunking on Routers

VLAN trunking can be used on routers and hosts as well as on switches. However, routers do not support DTP, so you must manually configure them to support trunking. Additionally, you must manually configure a switch on the other end of the segment to trunk, because the router does not participate in DTP.

The majority of router trunking configurations use subinterfaces, with each subinterface being associated with one VLAN. The subinterface number does not have to match the VLAN ID; rather, the **encapsulation** command sits under each subinterface, with the associated VLAN ID being part of the **encapsulation** command. Also, because good design calls for one IP subnet per VLAN, if the router wants to forward IP packets between the VLANs, the router needs to have an IP address associated with each trunking subinterface.

You can configure 802.1Q native VLANs under a subinterface or under the physical interface on a router. If configured under a subinterface, you use the **encapsulation dot1q** *vlan-id* **native** subcommand, with the inclusion of the **native** keyword meaning that frames exiting this subinterface should not be tagged. As with other router trunking configurations, the associated IP address would be configured on that same subinterface. Alternately, if not configured on a subinterface, the router assumes that the native VLAN is associated with the physical interface. In this case, the **encapsulation** command is not needed under the physical interface; the associated IP address, however, would need to be configured under the physical interface.

Example 2-6 shows an example configuration for Router1 in Figure 2-1, both for ISL and 802.1Q. In this case, Router1 needs to forward packets between the subnets on VLANs 21 and 22. The first part of the example shows ISL configuration, with no native VLANs, and therefore only a subinterface being used for each VLAN. The second part of the example shows an alternative 802.1Q configuration, using the option of placing the native VLAN (VLAN 21) configuration on the physical interface.

Example 2-6 *Trunking Configuration on Router1*

```
! Note the subinterface on the fa 0/0 interface, with the encapsulation
! command noting the type of trunking, as well as the VLAN number. The
! subinterface does not have to be the VLAN ID. Also note the IP addresses for
! each interface, allowing Router1 to route between VLANs.
interface fastethernet 0/0.1
 ip address 10.1.21.1 255.255.255.0
 encapsulation isl 21
!
interface fastethernet 0/0.2
 ip address 10.1.22.1 255.255.255.0
 encapsulation isl 22
! Next, an alternative 802.1Q configuration is shown. Note that this 802.1Q configuration
! places the IP address
! for VLAN 21 on the physical interface; the router simply associates the
! physical interface with the native VLAN. Alternatively, a subinterface could be
! used, with the encapsulation dot1q 21 native command specifying that the router
! should treat this VLAN as the native VLAN.
interface fastethernet 0/0
  ip address 10.1.21.1 255.255.255.0
!
interface fastethernet 0/0.2
  ip address 10.1.22.1 255.255.255.0
  encapsulation dot1q 22
```

Key Topic

Note also that the router does not have an explicitly defined allowed VLAN list. However, the allowed VLAN list is implied based on the configured VLANs. For instance, in this example, Router1 allows VLAN 1 (because it cannot be deleted), VLAN 21, and VLAN 22. A **show interface trunk** command on Switch1 would show only 1, 21, and 22 as the allowed VLANs on FA0/1.

802.1Q-in-Q Tunneling

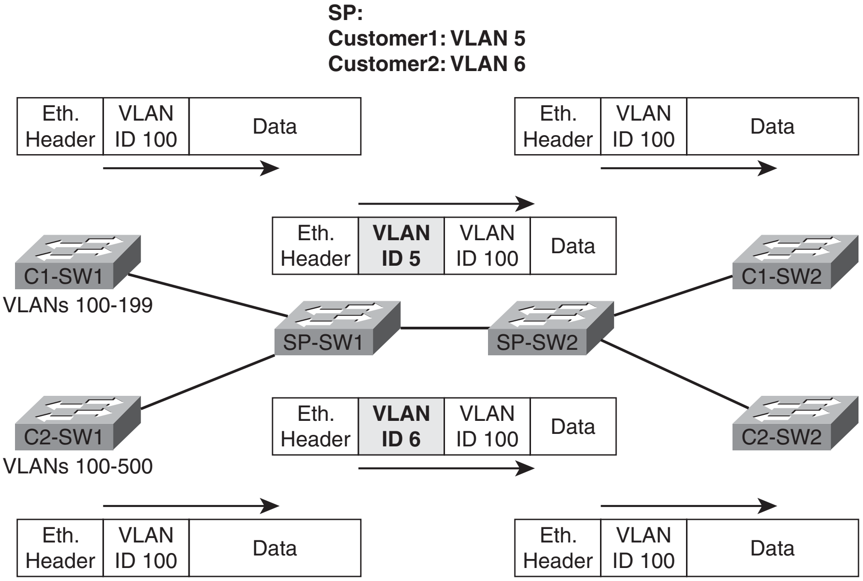
Traditionally, VLANs have not extended beyond the WAN boundary. VLANs in one campus extend to a WAN edge router, but VLAN protocols are not used on the WAN.

Today, several emerging alternatives exist for the passage of VLAN traffic across a WAN, including 802.1Q-in-Q, Ethernet over MPLS (EoMPLS), and VLAN MPLS (VMPLS). While these topics are more applicable to the CCIE Service Provider certification, you should at least know the concept of 802.1 Q-in-Q tunneling.

Also known as Q-in-Q or Layer 2 protocol tunneling, 802.1Q-in-Q allows an SP to preserve 802.1Q VLAN tags across a WAN service. By doing so, VLANs actually span multiple geographically dispersed sites. Figure 2-5 shows the basic idea.

Figure 2-5 *Q-in-Q: Basic Operation*

Key Topic


SP:
Customer1: VLAN 5
Customer2: VLAN 6
Eth. Header | VLAN ID 100 | Data
Eth. Header | VLAN ID 100 | Data
Eth. Header | VLAN ID 5 | VLAN ID 100 | Data
C1-SW1
VLANs 100-199
SP-SW1
SP-SW2
C1-SW2
C2-SW1
VLANs 100-500
C2-SW2
Eth. Header | VLAN ID 6 | VLAN ID 100 | Data
Eth. Header | VLAN ID 100 | Data
Eth. Header | VLAN ID 100 | Data

The ingress SP switch takes the 802.1Q frame, and then tags each frame entering the interface with an additional 802.1Q header. In this case, all of Customer1's frames are tagged as VLAN 5 as they pass over the WAN; Customer2's frames are tagged with VLAN 6. After removing the tag at egress, the customer switch sees the original 802.1Q frame, and can interpret the VLAN ID correctly. The receiving SP switch (SP-SW2 in this case) can keep the various customers' traffic separate based on the additional VLAN tags.

Using Q-in-Q, an SP can offer VLAN services, even when the customers use overlapping VLAN IDs. Customers get more flexibility for network design options, particularly with metro Ethernet services. Plus, CDP and VTP traffic passes transparently over the Q-in-Q service.

Configuring PPPoE

Although it might seem out of place in this chapter on VLANs and VLAN trunking, Point-to-Point Protocol over Ethernet (PPPoE) fits best here because it's an Ethernet encapsulation protocol. PPPoE is widely used for digital subscriber line (DSL) Internet access because the public telephone network uses ATM for its transport protocol; therefore, Ethernet frames must be encapsulated in a protocol supported over both Ethernet and ATM. PPP is the natural choice. The PPP Client feature permits a Cisco IOS router, rather than an endpoint host, to serve as the client in a network. This permits multiple hosts to connect over a single PPPoE connection.

In a DSL environment, PPP interface IP addresses are derived from an upstream DHCP server using IP Configuration Protocol (IPCP). Therefore, IP address negotiation must be enabled on the router's dialer interface. This is done using the **ip address negotiated** command in the dialer interface configuration.

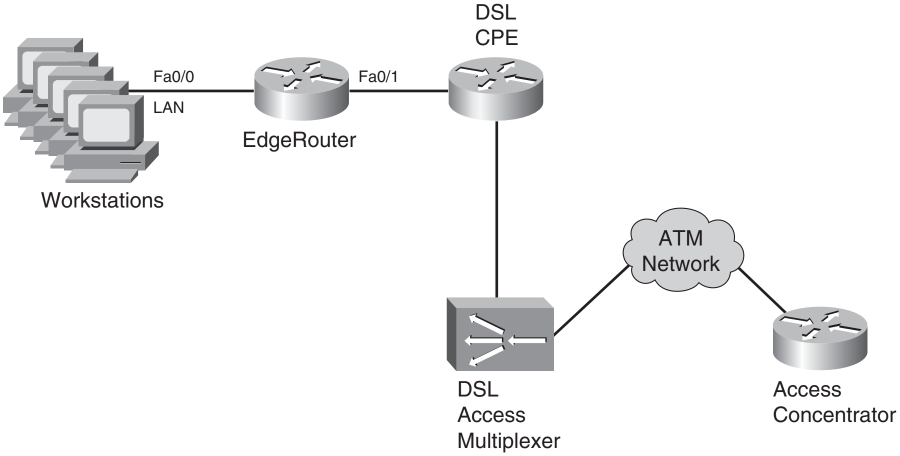
Because of the 8-byte PPP header, the MTU for PPPoE is usually set to 1492 bytes so that the entire encapsulated frame fits within the 1500-byte Ethernet frame. A maximum transmission unit (MTU) mismatch prevents a PPPoE connection from coming up. Checking the MTU setting is a good first step when troubleshooting PPPoE connections.

Those familiar with ISDN BRI configuration will recognize the dialer interface configuration and related commands in Example 2-7. The key difference between ISDN BRI configuration and PPPoE is the **pppoe-client dial-pool-number** command.

Configuring an Ethernet edge router for PPPoE Client mode is the focus of this section. This task requires configuring the Ethernet interface (physical or subinterface) and a corresponding dialer interface. The information in this section applies to Cisco IOS Release 12.2(13)T and later, and 12.3 and 12.4 releases.

Figure 2-6 shows the topology. Example 2-7 shows the configuration steps. The first step is to configure the outside Ethernet interface as a PPPoE client and assign it a dialer interface number. The second step is to configure the corresponding dialer interface. Additional steps, including Network Address Translation (NAT) configuration, are also shown.

Figure 2-6 *PPPoE Topology for Example 2-7*



Example 2-7 *Configuring PPPoE on EdgeRouter*

```
EdgeRouter# conf t
EdgeRouter(config)# interface fa0/1
EdgeRouter(config-if)# ip address 192.168.100.1 255.255.255.0
EdgeRouter(config-if)# ip nat inside
EdgeRouter(config)# interface fa0/1
EdgeRouter(config-if)# pppoe-client dial-pool-number 1
EdgeRouter(config-if)# exit
EdgeRouter(config)# interface dialer1
EdgeRouter(config-if)# mtu 1492
EdgeRouter(config-if)# encapsulation ppp
EdgeRouter(config-if)# ip address negotiated
EdgeRouter(config-if)# ppp authentication chap
!The remaining CHAP commands have been omitted for brevity.
EdgeRouter(config-if)# ip nat outside
EdgeRouter(config-if)# dialer pool 1
```

continues

Example 2-7 *Configuring PPPoE on EdgeRouter* *(Continued)*

```
EdgeRouter(config-if)# dialer-group 1
EdgeRouter(config-if)# exit
EdgeRouter(config)# dialer-list 1 protocol ip permit
EdgeRouter(config)# ip nat inside source list 1 interface dialier1 overload
EdgeRouter(config)# access-list 1 permit 192.168.100.0 0.0.0.255
EdgeRouter(config)# ip route 0.0.0.0 0.0.0.0 dialer1
```

You can verify PPPoE connectivity using the command **show pppoe session**. Cisco IOS includes debug functionality for PPPoE through the **debug pppoe** [**data** | **errors** | **events** | **packets**] command.

Foundation Summary

This section lists additional details and facts to round out the coverage of the topics in this chapter. Unlike most of the Cisco Press *Exam Certification Guides*, this "Foundation Summary" does not repeat information presented in the "Foundation Topics" section of the chapter. Please take the time to read and study the details in the "Foundation Topics" section of the chapter, as well as review items noted with a Key Topic icon.

Table 2-10 lists some of the most popular IOS commands related to the topics in this chapter. (The command syntax was copied from the *Catalyst 3550 Multilayer Switch Command Reference, 12.1(20)EA2*. Note that some switch platforms may have differences in the command syntax.)

Table 2-10 *Catalyst IOS Commands Related to Chapter 2*

Command	Description
show mac address-table [**aging-time** | **count** | **dynamic** | **static**] [**address** *hw-addr*] [**interface** *interface-id*] [**vlan** *vlan-id*]	Displays the MAC address table; the security option displays information about the restricted or static settings
show interfaces [*interface-id* | **vlan** *vlan-id*] **switchport** | **trunk**]	Displays detailed information about an interface operating as an access port or a trunk
show vlan [**brief** | **id** *vlan-id* | **name** *vlan-name* | *summary*]	EXEC command that lists information about VLAN
show vlan [*vlan*]	Displays VLAN information
show vtp status	Lists VTP configuration and status information
switchport mode {**access** | **dot1q-tunnel** | **dynamic** {**auto** | **desirable**} | **trunk**}	Configuration command setting nontrunking (**access**), trunking, and dynamic trunking (**auto** and **desirable**) parameters
switchport nonegotiate	Interface subcommand that disables DTP messages; interface must be configured as trunk or access port
switchport trunk {**allowed vlan** *vlan-list*} | {**encapsulation** {**dot1q** | **isl** | **negotiate**}} | {**native vlan** *vlan-id*} | {**pruning vlan** *vlan-list*}	Interface subcommand used to set parameters used when the port is trunking
switchport access vlan *vlan-id*	Interface subcommand that statically configures the interface as a member of that one VLAN

Table 2-11 lists the commands related to VLAN creation—both the VLAN database mode configuration commands (reached with the **vlan database** privileged mode command) and the normal configuration mode commands.

> **NOTE** Some command parameters may not be listed in Table 2-11.

Table 2-11 *Catalyst 3550 VLAN Database and Configuration Mode Command List*

VLAN Database	Configuration
vtp {**domain** *domain-name* | **password** *password* | **pruning** | **v2-mode** | {**server** | **client** | **transparent**}}	**vtp** {**domain** *domain-name* | **file** *filename* | **interface** *name* | **mode** {**client** | **server** | **transparent**} | **password** *password* | **pruning** | **version** *number*}
vlan *vlan-id* [**backupcrf** {**enable** | **disable**}] [**mtu** *mtu-size*] [**name** *vlan-name*] [**parent** *parent-vlan-id*] [**state** {**suspend** | **active**}]	**vlan** *vlan-id*[1]
show {**current** | **proposed** | **difference**}	No equivalent
apply | **abort** | **reset**	No equivalent

[1] Creates the VLAN and places the user in VLAN configuration mode, where commands matching the VLAN database mode options of the **vlan** command are used to set the same parameters.

Table 2-12 *Cisco IOS PPPoE Client Commands*

Command	Description
pppoe enable	Enables PPPoE operation on an Ethernet interface or subinterface
pppoe-client dial-pool-number ***number***	Configures the outside Ethernet interface on a router for PPPoE operation and ties it to a dialer interface
debug pppoe [**data** | **errors** | **events** | **packets**]	Enables debugging for PPPoE troubleshooting

Memory Builders

The CCIE Routing and Switching written exam, like all Cisco CCIE written exams, covers a fairly broad set of topics. This section provides some basic tools to help you exercise your memory about some of the broader topics covered in this chapter.

Fill In Key Tables from Memory

Appendix G, “Key Tables for CCIE Study,” on the CD in the back of this book contains empty sets of some of the key summary tables in each chapter. Print Appendix G, refer to this chapter’s tables in it, and fill in the tables from memory. Refer to Appendix H, “Solutions for Key Tables for CCIE Study,” on the CD to check your answers.

Definitions

Next, take a few moments to write down the definitions for the following terms:

> VLAN, broadcast domain, DTP, VTP pruning, 802.1Q, ISL, native VLAN, encapsulation, private VLAN, promiscuous port, community VLAN, isolated VLAN, 802.1Q-in-Q, Layer 2 protocol tunneling, PPPoE, DSL.

Refer to the glossary to check your answers.

Further Reading

The topics in this chapter tend to be covered in slightly more detail in CCNP Switching exam preparation books. For more details on these topics, refer to the Cisco Press CCNP preparation books found at www.ciscopress.com/ccnp.

Cisco LAN Switching, by Kennedy Clark and Kevin Hamilton, is an excellent reference for LAN-related topics in general, and certainly very useful for CCIE written and lab exam preparation.

Index