CCNP SWITCH 642-813 Official Certification Guide

David Hucaby, CCIE No. 4594

Copyright© 2010 Pearson Education, Inc.

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

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

Printed in the United States of America
First Printing February 2010

Library of Congress Cataloging-in-Publication Data:
Hucaby, Dave.
CCNP SWITCH 642-813 official certification guide / David Hucaby.
p. cm.
TK5103.8.H8327 2010
004.6076—dc22

2009050384

Warning and Disclaimer

This book is designed to provide information about the CCNP SWITCH Exam (Exam 642-813) for the CCNP Routing and Switching certification. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Trademark Acknowledgments

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

*CCNP SWITCH 642-813 Official Certification Guide* is an excellent self-study resource for the CCNP SWITCH exam. Passing this exam is a crucial step to attaining the valued CCNP Routing and Switching certification.

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 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](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  
January 2010
Introduction: Overview of Certification and How to Succeed

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

Objectives and Methods

The most important and somewhat obvious objective of this book is to help you pass the Cisco CCNP SWITCH exam (Exam 642-813). In fact, if the primary objective of this book were different, the book's title would be misleading; however, the methods used in this book to help you pass the SWITCH exam are designed to also make you much more knowledgeable about how to do your job. Although this book and the accompanying CD have many exam preparation tasks and example test questions, the method in which they are used is not to simply make you memorize as many questions and answers as you possibly can.

The methodology of this book helps you discover the exam topics about which you need more review, fully understand and remember exam topic details, and prove to yourself that you have retained your knowledge of those topics. So this book helps you pass not by memorization, but by helping you truly learn and understand the topics. The SWITCH exam is just one of the foundation topics in the CCNP Routing and Switching certification, and the knowledge contained within is vitally important to consider yourself a truly skilled routing and switching engineer or specialist. This book would do you a disservice if it did not attempt to help you learn the material. To that end, the book can help you pass the SWITCH exam by using the following methods:

■ Covering all the exam topics and helping you discover which exam topics you have not mastered
■ Providing explanations and information to fill in your knowledge gaps
■ Supplying exam preparation tasks and example networks with diagrams and sample configurations that all enhance your ability to recall and deduce the answers to test questions
■ Providing practice exercises on the exam topics and the testing process through test questions on the CD
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 Cisco SWITCH exam. Although other objectives can be achieved from using this book, the book is written with one goal in mind: to help you pass the exam.

The SWITCH exam is primarily based on the content of the Cisco SWITCH course. You should have either taken the course, read through the SWITCH coursebook or this book, or have a couple of years of LAN switching experience.

Cisco Certifications and Exams

Cisco offers four levels of routing and switching certification, each with an increasing level of proficiency: Entry, Associate, Professional, and Expert. These are commonly known by their acronyms CCENT (Cisco Certified Entry Networking Technician), CCNA (Cisco Certified Network Associate), CCNP (Cisco Certified Network Professional), and CCIE (Cisco Certified Internetworking Expert). There are others, too, but this book focuses on the certifications for enterprise networks.

For the CCNP Routing and Switching certification, you must pass exams on a series of CCNP topics, including the SWITCH, ROUTE, and TSHOOT exams. For most exams, Cisco does not publish the scores needed for passing. You need to take the exam to find that out for yourself.

To see the most current requirements for the CCNP Routing and Switching certification, go to Cisco.com and click Training and Events. There you can find out other exam details such as exam topics and how to register for an exam.

The strategy you use to prepare for the SWITCH exam might be slightly different from strategies used by other readers, mainly based on the skills, knowledge, and experience you already have obtained. For instance, if you have attended the SWITCH course, you might take a different approach than someone who learned switching through on-the-job training. 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 with the least amount of time required.

How This Book Is Organized

Although this book can 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 only the material that you need more work with. The chapters can be covered in any order, although some chapters are related and build upon each other. If you do intend to read them all, the order in the book is an excellent sequence to use.

Each core chapter covers a subset of the topics on the CCNP SWITCH exam. The chapters are organized into parts, covering the following topics:
Part I: New CCNP Exam Approaches

- **Chapter 1, “The Planning Tasks of the CCNP Exams”**—This chapter explains the roles of a networking professional in the context of the Cisco Lifecycle Model, where network tasks form a cycle over time. The CCNP SWITCH exam covers real-world or practical skills that are necessary as a network is designed, planned, implemented, verified, and tuned.

Part II: Building a Campus Network

- **Chapter 2, “Switch Operation”**—This chapter covers Layer 2 and multilayer switch operation, how various content-addressable memory (CAM) and ternary content-addressable memory (TCAM) tables are used to make switching decisions, and how to monitor these tables to aid in troubleshooting.

- **Chapter 3, “Switch Port Configuration”**—This chapter covers basic Ethernet concepts, how to use scalable Ethernet, how to connect switch and devices together, and how to verify switch port operation to aid in troubleshooting.

- **Chapter 4, “VLANs and Trunks”**—This chapter covers basic VLAN concepts, how to transport multiple VLANs over single links, how to configure VLAN trunks, and how to verify VLAN and trunk operation.

- **Chapter 5, “VLAN Trunking Protocol”**—This chapter covers VLAN management using VTP, VTP configuration, traffic management through VTP pruning, and how to verify VTP operation.

- **Chapter 6, “Aggregating Switch Links”**—This chapter covers switch port aggregation with EtherChannel, EtherChannel negotiation protocols, EtherChannel configuration, and how to verify EtherChannel operation.

- **Chapter 7, “Traditional Spanning Tree Protocol”**—This chapter covers IEEE 802.1D Spanning Tree Protocol (STP) and gives an overview of the other STP types that might be running on a switch.

- **Chapter 8, “Spanning-Tree Configuration”**—This chapter covers the STP root bridge, how to customize the STP topology, how to tune STP convergence, redundant link convergence, and how to verify STP operation.

- **Chapter 9, “Protecting the Spanning Tree Protocol Topology”**—This chapter covers protecting the STP topology using Root Guard, BPDU Guard, and Loop Guard, and also how to use BPDU filtering and how to verify that these STP protection mechanisms are functioning properly.

- **Chapter 10, “Advanced Spanning Tree Protocol”**—This chapter covers Rapid Spanning Tree Protocol (RSTP) for Rapid PVST+ and Multiple Spanning Tree (MST) Protocol.

- **Chapter 11, “Multilayer Switching”**—This chapter covers interVLAN routing, multilayer switching with Cisco Express Forwarding (CEF), and how to verify that multilayer switching is functioning properly.
Part III: Designing Campus Networks

- **Chapter 12, “Enterprise Campus Network Design”**—This chapter covers different campus network models, hierarchical network design, and how to design, size, and scale a campus network using a modular approach.

- **Chapter 13, “Layer 3 High Availability”**—This chapter covers providing redundant router or gateway addresses on Catalyst switches and verifying that redundancy is functioning properly.

Part IV: Campus Network Services

- **Chapter 14, “IP Telephony”**—This chapter covers how a Catalyst switch can provide power to operate a Cisco IP Phone, how voice traffic can be carried over the links between an IP Phone and a Catalyst switch, QoS for voice traffic, and how to verify that IP Telephony features are functioning properly.

- **Chapter 15, “Integrating Wireless LANs”**—This chapter covers different approaches to integrating autonomous and lightweight wireless access points into a switched campus network.

Part V: Securing Switched Networks

- **Chapter 16, “Securing Switch Access”**—This chapter covers switch authentication, authorization, and accounting (AAA); port security using MAC addresses; port-based security using IEEE 802.1x; DHCP snooping; and dynamic ARP inspection.

- **Chapter 17, “Securing with VLANs”**—This chapter covers how to control traffic within a VLAN using access lists, implementing private VLANs, and monitoring traffic on switch ports for security reasons.

Part VI: Final Exam Preparation

- **Chapter 18, “Final Preparation”**—This chapter explains how to use the practice exam CD to enhance your study, along with a basic study plan.

There is also an appendix that has answers to the “Do I Know This Already” quizzes and an appendix that tells you how to find any updates should there be changes to the exam.

Each chapter in the book uses several features to help you make the best use of your time in that chapter. The features are as follows:

- **Assessment**—Each chapter begins with a “Do I Know This Already?” quiz that helps you determine the amount of time you need to spend studying each topic of the chapter. If you intend to read the entire chapter, you can save the quiz for later use. Questions are all multiple choice, to give a quick assessment of your knowledge.

- **Foundation Topics**—This is the core section of each chapter that explains the protocols, concepts, and configuration for the topics in the chapter.

- **Exam Preparation Tasks**—At the end of each chapter, this section collects key topics, references to memory table exercises to be completed as memorization practice, key terms to define, and a command reference that summarizes relevant commands presented in the chapter.
Finally, there is a CD-based practice exam. The companion CD contains a practice CCNP SWITCH exam containing a bank of test questions to reinforce your understanding of the book’s concepts. This is the best tool for helping you prepare for the actual test-taking process.

The CD also contains the Memory Table exercises and answer keys that come up at the end of each chapter.

How to Use This Book for Study

Retention and recall are the two features of human memory most closely related to performance on tests. This exam-preparation guide focuses on increasing both retention and recall of the topics on the exam. The other human characteristic involved in successfully passing the exam is intelligence; this book does not address that issue!

This book is designed with features to help you increase retention and recall. It does this in the following ways:

- By providing succinct and complete methods of helping you decide what you recall easily and what you do not recall at all.

- By giving references to the exact passages in the book that review those concepts you most need to recall, so you can quickly be reminded about a fact or concept. Repeating information that connects to another concept helps retention, and describing the same concept in several ways throughout a chapter increases the number of connectors to the same pieces of information.

- Finally, accompanying this book is a CD that has exam-like questions. These are useful for you to practice taking the exam and to get accustomed to the time restrictions imposed during the exam.

When taking the “Do I Know This Already?” assessment quizzes in each chapter, make sure that you treat yourself and your knowledge fairly. If you come across a question that makes you guess at an answer, mark it wrong immediately. This forces you to read through the part of the chapter that relates to that question and forces you to learn it more thoroughly.

If you find that you do well on the assessment quizzes, it still might be wise to quickly skim through each chapter to find sections or topics that do not readily come to mind. Look for the Key Topics icons. Sometimes even reading through the detailed table of contents will reveal topics that are unfamiliar or unclear. If that happens to you, mark those chapters or topics and spend time working through those parts of the book.

CCNP SWITCH Exam Topics

Carefully consider the exam topics Cisco has posted on its website as you study, particularly for clues to how deeply you should know each topic. Beyond that, you cannot go wrong by developing a broader knowledge of the subject matter. You can do that by reading and studying the topics presented in this book. Remember that it is in your best
interest to become proficient in each of the CCNP subjects. When it is time to use what you have learned, being well rounded counts more than being well tested.

Table I-1 shows the official exam topics for the SWITCH exam, as posted on Cisco.com. Note that Cisco has occasionally changed exam topics without changing the exam number, so do not be alarmed if small changes in the exam topics occur over time. When in doubt, go to Cisco.com and click Training and Events.

**Table I-1—CCNP SWITCH Exam Topics**

<table>
<thead>
<tr>
<th>Exam Topic</th>
<th>Part of This Book Where Exam Topic Is Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Implement VLAN-based solution, given a network design and a set of requirements</strong></td>
<td></td>
</tr>
<tr>
<td>Determine network resources needed for implementing VLAN-based solution on a network.</td>
<td>Part II, “Building a Campus Network” Chapters 2–10</td>
</tr>
<tr>
<td>Create a VLAN-based implementation plan.</td>
<td></td>
</tr>
<tr>
<td>Create a VLAN-based verification plan.</td>
<td></td>
</tr>
<tr>
<td>Configure switch-to-switch connectivity for the VLAN-based solution.</td>
<td></td>
</tr>
<tr>
<td>Configure loop prevention for the VLAN-based solution.</td>
<td></td>
</tr>
<tr>
<td>Configure access ports for the VLAN-based solution.</td>
<td></td>
</tr>
<tr>
<td>Verify the VLAN-based solution was implemented properly using show and debug commands.</td>
<td></td>
</tr>
<tr>
<td>Document results of VLAN implementation and verification</td>
<td></td>
</tr>
<tr>
<td><strong>Implement a security extension of a Layer 2 solution, given a network design and a set of requirements</strong></td>
<td></td>
</tr>
<tr>
<td>Determine network resources needed for implementing a security solution.</td>
<td>Part V, “Securing Switched Networks” Chapters 16–17</td>
</tr>
<tr>
<td>Create a implementation plan for the security solution.</td>
<td></td>
</tr>
<tr>
<td>Create a verification plan for the security solution.</td>
<td></td>
</tr>
<tr>
<td>Configure port security features.</td>
<td></td>
</tr>
<tr>
<td>Configure general switch security features.</td>
<td></td>
</tr>
<tr>
<td>Configure private VLANs.</td>
<td></td>
</tr>
<tr>
<td>Configure VACL and PACL.</td>
<td></td>
</tr>
<tr>
<td>Verify the security solution was implemented properly using show and debug commands.</td>
<td></td>
</tr>
<tr>
<td>Document results of security implementation and verification.</td>
<td></td>
</tr>
</tbody>
</table>
Table I-1—CCNP SWITCH Exam Topics

<table>
<thead>
<tr>
<th>Exam Topic</th>
<th>Part of This Book Where Exam Topic Is Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement switch-based Layer 3 services, given a network design and a set of requirements</td>
<td></td>
</tr>
<tr>
<td>Determine network resources needed for implementing a switch-based Layer 3 solution.</td>
<td>Part II, “Building a Campus Network” Chapter 11</td>
</tr>
<tr>
<td>Create an implementation plan for the switch-based Layer 3 solution.</td>
<td></td>
</tr>
<tr>
<td>Create a verification plan for the switch-based Layer 3 solution.</td>
<td></td>
</tr>
<tr>
<td>Configure routing interfaces.</td>
<td></td>
</tr>
<tr>
<td>Configure Layer 3 security.</td>
<td></td>
</tr>
<tr>
<td>Verify the switch-based Layer 3 solution was implemented properly using <code>show</code> and <code>debug</code> commands.</td>
<td></td>
</tr>
<tr>
<td>Document results of switch-based Layer 3 implementation and verification.</td>
<td></td>
</tr>
<tr>
<td>Prepare infrastructure to support advanced services</td>
<td></td>
</tr>
<tr>
<td>Implement a wireless extension of a Layer 2 solution.</td>
<td>Part IV, “Campus Network Services”</td>
</tr>
<tr>
<td>Implement a VoIP support solution.</td>
<td>Chapters 14–15</td>
</tr>
<tr>
<td>Implement video support solution.</td>
<td></td>
</tr>
<tr>
<td>Implement high availability, given a network design and a set of requirements</td>
<td></td>
</tr>
<tr>
<td>Determine network resources needed for implementing high availability on a network.</td>
<td>Part III, “Designing Campus Networks” Chapters 12–13</td>
</tr>
<tr>
<td>Create a high availability implementation plan.</td>
<td></td>
</tr>
<tr>
<td>Create a high availability verification plan.</td>
<td></td>
</tr>
<tr>
<td>Implement first-hop redundancy protocols.</td>
<td></td>
</tr>
<tr>
<td>Implement switch supervisor redundancy.</td>
<td></td>
</tr>
<tr>
<td>Verify high-availability solution was implemented properly using <code>show</code> and <code>debug</code> commands.</td>
<td></td>
</tr>
<tr>
<td>Document results of high-availability implementation and verification.</td>
<td></td>
</tr>
</tbody>
</table>

For More Information

If you have any comments about the book, you can submit those via the Ciscopress.com website. Just go to the website, select Contact Us, and type in your message. Cisco might make changes that affect the CCNP Routing and Switching certification from time to time. You should always check Cisco.com for the latest details. Also, you can look to http://www.ciscopress.com/title/1587202433, where we publish any information pertinent to how you might use this book differently in light of future changes from Cisco. For example, if Cisco decides to remove a major topic from the exam, it might post that on its website; Cisco Press will make an effort to list that information as well via an online updates appendix.
This chapter covers the following topics that you need to master for the CCNP SWITCH exam:

**Protecting Against Unexpected BPDUs**—This section covers the Root Guard and BPDU Guard features, which protect against unexpected root candidates and unexpected BP-DUs, respectively.

**Protecting Against Sudden Loss of BPDUs**—This section discusses the Loop Guard and UDLD features, which detect and protect against the loss of root bridge BPDUs and conditions causing unidirectional links, respectively.

**Using BPDU Filtering to Disable STP on a Port**—This section explains how to filter BPDUs on a switch port to prevent the port from participating in STP altogether. Bridging loops are neither detected nor prevented.

**Troubleshooting STP Protection**—This section summarizes the commands that diagnose or verify actions to protect the topology.
Protecting the Spanning Tree Protocol Topology

Achieving and maintaining a loop-free Spanning Tree Protocol (STP) topology revolves around the simple process of sending and receiving bridge protocol data units (BPDU). Under normal conditions, with all switches playing fairly and according to the rules, a loop-free topology is determined dynamically.

This chapter discusses two basic conditions that can occur to disrupt the loop-free topology (even while STP is running):

On a port that has not been receiving BPDUs, BPDUs are not expected. When BPDUs suddenly appear for some reason, the STP topology can reconverge to give unexpected results.

On a port that normally receives BPDUs, BPDUs always are expected. When BPDUs suddenly disappear for some reason, a switch can make incorrect assumptions about the topology and unintentionally create loops.

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the “Exam Preparation Tasks” section. If you are in doubt based on your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 9-1 outlines the major headings in this chapter and the “Do I Know This Already?” quiz questions that go with them. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes.”

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

<table>
<thead>
<tr>
<th>Foundation Topics Section</th>
<th>Questions Covered in This Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protecting Against Unexpected BPDUs</td>
<td>1–5</td>
</tr>
<tr>
<td>Protecting Against Sudden Loss of BPDUs</td>
<td>6–11</td>
</tr>
<tr>
<td>Using BPDU Filtering to Disable STP on a Port</td>
<td>12</td>
</tr>
<tr>
<td>Troubleshooting STP Protection</td>
<td>13</td>
</tr>
</tbody>
</table>

1. Why is it important to protect the placement of the root bridge?
   a. To keep two root bridges from becoming active
   b. To keep the STP topology stable
c. So all hosts have the correct gateway  
d. So the root bridge can have complete knowledge of the STP topology

2. Which of the following features protects a switch port from accepting superior BPDUs?
   a. STP Loop Guard  
   b. STP BPDU Guard  
   c. STP Root Guard  
   d. UDLD

3. Which of the following commands can you use to enable STP Root Guard on a switch port?
   a. spanning-tree root guard  
   b. spanning-tree root-guard  
   c. spanning-tree guard root  
   d. spanning-tree rootguard enable

4. Where should the STP Root Guard feature be enabled on a switch?
   a. All ports  
   b. Only ports where the root bridge should never appear  
   c. Only ports where the root bridge should be located  
   d. Only ports with PortFast enabled

5. Which of the following features protects a switch port from accepting BPDUs when PortFast is enabled?
   a. STP Loop Guard  
   b. STP BPDU Guard  
   c. STP Root Guard  
   d. UDLD

6. To maintain a loop-free STP topology, which one of the following should a switch up-link be protected against?
   a. A sudden loss of BPDUs  
   b. Too many BPDUs  
   c. The wrong version of BPDUs  
   d. BPDUs relayed from the root bridge

7. Which of the following commands can enable STP Loop Guard on a switch port?
   a. spanning-tree loop guard  
   b. spanning-tree guard loop  
   c. spanning-tree loop-guard  
   d. spanning-tree loopguard enable
8. STP Loop Guard detects which of the following conditions?
   a. The sudden appearance of superior BPDUs
   b. The sudden lack of BPDUs
   c. The appearance of duplicate BPDUs
   d. The appearance of two root bridges

9. Which of the following features can actively test for the loss of the receive side of a link between switches?
   a. POST
   b. BPDU
   c. UDLD
   d. STP

10. UDLD must detect a unidirectional link before which of the following?
    a. The Max Age timer expires.
    b. STP moves the link to the Blocking state.
    c. STP moves the link to the Forwarding state.
    d. STP moves the link to the Listening state.

11. What must a switch do when it receives a UDLD message on a link?
    a. Relay the message on to other switches
    b. Send a UDLD acknowledgment
    c. Echo the message back across the link
    d. Drop the message

12. Which of the following features effectively disables spanning-tree operation on a switch port?
    a. STP PortFast
    b. STP BPDU filtering
    c. STP BPDU Guard
    d. STP Root Guard

13. To reset switch ports that have been put into the errdisable mode by UDLD, which one of the following commands should be used?
    a. clear errdisable udlld
    b. udlld reset
    c. no udlld
    d. show udlld errdisable
Protecting Against Unexpected BPDUs

A network running STP uses BPDUs to communicate between switches (bridges). Switches become aware of each other and of the topology that interconnects them. After a root bridge is elected, BPDUs are generated by the root and are relayed down through the spanning-tree topology. Eventually, all switches in the STP domain receive the root’s BPDUs so that the network converges and a stable loop-free topology forms.

To maintain an efficient topology, the placement of the root bridge must be predictable. Hopefully, you configured one switch to become the root bridge and a second one to be the secondary root. What happens when a “foreign” or rogue switch is connected to the network, and that switch suddenly is capable of becoming the root bridge? Cisco added two STP features that help prevent the unexpected: Root Guard and BPDU Guard.

Root Guard

After an STP topology has converged and becomes loop free, switch ports are assigned the following roles:

- **Root port**—The one port on a switch that is closest (with the lowest root path cost) to the root bridge.
- **Designated port**—The port on a LAN segment that is closest to the root. This port relays, or transmits, BPDUs down the tree.
- **Blocking port**—Ports that are neither root nor designated ports.
- **Alternate port**—Ports that are candidate root ports (they are also close to the root bridge) but are in the Blocking state. These ports are identified for quick use by the STP UplinkFast feature.
- **Forwarding port**—Ports where no other STP activity is detected or expected. These are ports with normal end-user connections.

The root bridge always is expected to be seen on the root port and the alternative ports because these are “closest” (have the best-cost path) to it.

Suppose that another switch is introduced into the network with a bridge priority that is more desirable (lower) than that of the current root bridge. The new switch then would become the root bridge, and the STP topology might reconverge to a new shape. This is entirely permissible by the STP because the switch with the lowest bridge ID always wins the root election.

However, this is not always desirable for you, the network administrator, because the new STP topology might be something totally unacceptable. In addition, while the topology is reconverging, your production network might become unavailable.

The Root Guard feature was developed as a means to control where candidate root bridges can be connected and found on a network. Basically, a switch learns the current root
bridge’s bridge ID. If another switch advertises a superior BPDU, or one with a better bridge ID, on a port where Root Guard is enabled, the local switch will not allow the new switch to become the root. As long as the superior BPDUs are being received on the port, the port will be kept in the root-inconsistent STP state. No data can be sent or received in that state, but the switch can listen to BPDUs received on the port to detect a new root advertising itself.

In essence, Root Guard designates that a port can only forward or relay BPDUs; the port can’t be used to receive BPDUs. Root Guard prevents the port from ever becoming a root port where BPDUs normally would be received from the root bridge.

You can enable Root Guard only on a per-port basis. By default, it is disabled on all switch ports. To enable it, use the following interface configuration command:

```
Switch(config-if)# spanning-tree guard root
```

When the superior BPDUs no longer are received, the port is cycled through the normal STP states to return to normal use.

Use Root Guard on switch ports where you never expect to find the root bridge for a VLAN. In fact, Root Guard affects the entire port so that a root bridge never can be allowed on any VLAN on the port. When a superior BPU is heard on the port, the entire port, in effect, becomes blocked.

**Tip:** You can display switch ports that Root Guard has put into the root-inconsistent state with the following command:

```
Switch# show spanning-tree inconsistentports
```

**BPDU Guard**

Recall that the traditional STP offers the PortFast feature, in which switch ports are allowed to immediately enter the Forwarding state as soon as the link comes up. Normally, PortFast provides quick network access to end-user devices, where bridging loops never are expected to form. Even while PortFast is enabled on a port, STP still is running and can detect a bridging loop. However, a loop can be detected only in a finite amount of time—the length of time required to move the port through the normal STP states.

**Note:** Remember that enabling PortFast on a port is not the same as disabling the STP on it.

By definition, if you enable PortFast, you do not expect to find anything that can cause a bridging loop—especially another switch or device that produces BPDUs. Suppose that a switch is connected by mistake to a port where PortFast is enabled. Now there is a potential for a bridging loop to form. An even greater consequence is that the potential now exists for the newly connected device to advertise itself and become the new root bridge.

The BPDU Guard feature was developed to further protect the integrity of switch ports that have PortFast enabled. If any BPDU (whether superior to the current root or not) is
received on a port where BPDU Guard is enabled, that port immediately is put into the
errdisable state. The port is shut down in an error condition and must be either manually
re-enabled or automatically recovered through the errdisable timeout function.

By default, BPDU Guard is disabled on all switch ports. You can configure BPDU Guard as
a global default, affecting all switch ports with a single command. All ports that have Port-
Fast enabled also have BPDU Guard automatically enabled. You can use the following
global configuration command to enable BPDU Guard as the default:

Switch(config)# spanning-tree portfast bpduguard default

You also can enable or disable BPDU Guard on a per-port basis, using the following inter-
face configuration command:

Switch(config-if)# [no] spanning-tree bpduguard enable

When the BPDUs no longer are received, the port still remains in the errdisable state. See
Chapter 3, “Switch Port Configuration,” for more information about recovering from the
erdisable state.

You should use BPDU Guard on all switch ports where STP PortFast is enabled. This pre-
vents any possibility that a switch will be added to the port, either intentionally or by mis-
take. An obvious application for BPDU Guard is on access-layer switch ports where users
and end devices connect. BPDUs normally would not be expected there and would be de-
tected if a switch or hub inadvertently were connected.

Naturally, BPDU Guard does not prevent a bridging loop from forming if an Ethernet hub
is connected to the PortFast port. This is because a hub doesn’t transmit BPDUs itself; it
merely repeats Ethernet frames from its other ports. A loop could form if the hub became
connected to two locations in the network, providing a path for frames to be looped with-
out any STP activity.

You never should enable BPDU Guard on any switch uplink where the root bridge is lo-
cated. If a switch has multiple uplinks, any of those ports could receive legitimate BPDUs
from the root—even if they are in the Blocking state as a result of the UplinkFast feature.
If BPDU Guard is enabled on an uplink port, BPDUs will be detected and the uplink will
be put into the Errdisable state. This will preclude that uplink port from being used as an
uplink into the network.

**Protecting Against Sudden Loss of BPDUs**

STP BPDUs are used as probes to learn about a network topology. When the switches par-
ticipating in STP converge on a common and consistent loop-free topology, BPDUs still
must be sent by the root bridge and must be relayed by every other switch in the STP do-
main. The STP topology’s integrity then depends on a continuous and regular flow of BP-
DUs from the root.

What happens if a switch doesn’t receive BPDUs in a timely manner or when it doesn’t re-
ceive any? The switch can view that condition as acceptable—perhaps an upstream switch
or an upstream link is dead. In that case, the topology must have changed, so blocked
ports eventually can be unblocked again.
However, if the absence of BPDUs is actually a mistake and BPDUs are not being received even though there is no topology change, bridging loops easily can form.

Cisco has added two STP features that help detect or prevent the unexpected loss of BPDUs:

- Loop Guard
- Unidirectional Link Detection (UDLD)

**Loop Guard**

Suppose that a switch port is receiving BPDUs and the switch port is in the Blocking state. The port makes up a redundant path; it is blocking because it is neither a root port nor a designated port. It will remain in the Blocking state as long as a steady flow of BPDUs is received.

If BPDUs are being sent over a link but the flow of BPDUs stops for some reason, the last-known BPDU is kept until the Max Age timer expires. Then that BPDU is flushed, and the switch thinks there is no longer a need to block the port. After all, if no BPDUs are received, there must not be another STP device connected there.

The switch then moves the port through the STP states until it begins to forward traffic—and forms a bridging loop. In its final state, the port becomes a designated port where it begins to relay or send BPDUs downstream, when it actually should be receiving BPDUs from upstream.

To prevent this situation, you can use the Loop Guard STP feature. When enabled, Loop Guard keeps track of the BPDU activity on nondesignated ports. While BPDUs are received, the port is allowed to behave normally. When BPDUs go missing, Loop Guard moves the port into the loop-inconsistent state. The port is effectively blocking at this point to prevent a loop from forming and to keep it in the nondesignated role.

When BPDUs are received on the port again, Loop Guard allows the port to move through the normal STP states and become active. In this fashion, Loop Guard automatically governs ports without the need for manual intervention.

By default, Loop Guard is disabled on all switch ports. You can enable Loop Guard as a global default, affecting all switch ports, with the following global configuration command:

```
Switch(config)# spanning-tree loopguard default
```

You also can enable or disable Loop Guard on a specific switch port by using the following interface-configuration command:

```
Switch(config-if)# [no] spanning-tree guard loop
```

Although Loop Guard is configured on a switch port, its corrective blocking action is taken on a per-VLAN basis. In other words, Loop Guard doesn't block the entire port; only the offending VLANs are blocked.

You can enable Loop Guard on all switch ports, regardless of their functions. The switch figures out which ports are nondesignated and monitors the BPDU activity to keep them nondesignated. Nondesignated ports are generally the alternative root ports and ports that normally are blocking.
UDLD

In a campus network, switches are connected by bidirectional links, where traffic can flow in two directions. Clearly, if a link has a physical layer problem, the two switches it connects detect a problem, and the link is shown as not connected.

What would happen if just one side of the link (receive or transmit) had an odd failure, such as malfunctioning transmit circuitry in a gigabit interface converter (GBIC) or small form factor pluggable (SFP) modules? In some cases, the two switches still might see a functional bidirectional link, although traffic actually would be delivered in only one direction. This is known as a unidirectional link.

A unidirectional link poses a potential danger to STP topologies because BPDUs will not be received on one end of the link. If that end of the link normally would be in the Blocking state, it will not be that way for long. A switch interprets the absence of BPDUs to mean that the port can be moved safely through the STP states so that traffic can be forwarded. However, if that is done on a unidirectional link, a bridging loop forms and the switch never realizes the mistake.

To prevent this situation, you can use the Cisco-proprietary Unidirectional Link Detection (UDLD) STP feature. When enabled, UDLD interactively monitors a port to see whether the link is truly bidirectional. A switch sends special Layer 2 UDLD frames identifying its switch port at regular intervals. UDLD expects the far-end switch to echo those frames back across the same link, with the far-end switch port’s identification added.

If a UDLD frame is received in return and both neighboring ports are identified in the frame, the link must be bidirectional. However, if the echoed frames are not seen, the link must be unidirectional for some reason.

Naturally, an echo process such as this requires both ends of the link to be configured for UDLD. Otherwise, one end of the link will not echo the frames back to the originator. In addition, each switch at the end of a link sends its own UDLD messages independently, expecting echoes from the far end. This means that two echo processes are occurring on any given link.

UDLD messages are sent at regular intervals, as long as the link is active. You can configure the message interval UDLD uses. (The default is 15 seconds.) The objective behind UDLD is to detect a unidirectional link condition before STP has time to move a blocked port into the Forwarding state. To do this, the target time must be less than the Max Age timer plus two intervals of the Forward Delay timer, or 50 seconds. UDLD can detect a unidirectional link after about three times the UDLD message interval (45 seconds total, using the default).

UDLD has two modes of operation:

- **Normal mode**—When a unidirectional link condition is detected, the port is allowed to continue its operation. UDLD merely marks the port as having an undetermined state and generates a syslog message.

- **Aggressive mode**—When a unidirectional link condition is detected, the switch takes action to reestablish the link. UDLD messages are sent out once a second for 8
seconds. If none of those messages is echoed back, the port is placed in the Errdis-
able state so that it cannot be used.

You configure UDLD on a per-port basis, although you can enable it globally for all fiber-
optic switch ports (either native fiber or fiber-based GBIC or SFP modules). By default,
UDLD is disabled on all switch ports. To enable it globally, use the following global con-
figuration command:

```
Switch(config)# udld {enable | aggressive | message time seconds}
```

For normal mode, use the `enable` keyword; for aggressive mode, use the `aggressive` key-
word. You can use the `message time` keywords to set the message interval to `seconds`,
ranging from 7 to 90 seconds. (The default interval varies according to switch platform.
For example, the Catalyst 3550 default is 7 seconds; the Catalyst 4500 and 6500 default is
15 seconds.)

You also can enable or disable UDLD on individual switch ports, if needed, using the fol-
lowing interface configuration command:

```
Switch(config-if)# udld {enable | aggressive | disable}
```

Here, you can use the `disable` keyword to completely disable UDLD on a fiber-optic inter-
face.

**Note:** The default UDLD message interval times differ among Catalyst switch platforms.
Although two neighbors might have mismatched message time values, UDLD still works
correctly. This is because each of the two neighbors simply echoes UDLD messages back
as they are received, without knowledge of their neighbor’s own time interval. The time
interval is used only to decide when to send UDLD messages and as a basis for detecting a
unidirectional link from the absence of echoed messages.

If you decide to change the default message time, make sure that UDLD still can detect a
fault before STP decides to move a link to the Forwarding state.

You safely can enable UDLD on all switch ports. The switch globally enables UDLD only
on ports that use fiber-optic media. Twisted-pair or copper media does not suffer from
the physical layer conditions that allow a unidirectional link to form. However, you can
enable UDLD on nonfiber links individually, if you want.

At this point, you might be wondering how UDLD can be enabled gracefully on the two
end switches. Recall that in aggressive mode, UDLD disables the link if the neighbor does
not reflect the messages back within a certain time period. If you are enabling UDLD on a
production network, is there a chance that UDLD will disable working links before you
can get the far end configured?

The answer is no. UDLD makes some intelligent assumptions when it is enabled on a link
for the first time. First, UDLD has no record of any neighbor on the link. It starts sending
out messages, hoping that a neighboring switch will hear them and echo them back. Obvi-
ously, the device at the far end also must support UDLD so that the messages will be
echoed back.
If the neighboring switch does not yet have UDLD enabled, no messages will be echoed. UDLD will keep trying (indefinitely) to detect a neighbor and will not disable the link. After the neighbor has UDLD configured also, both switches become aware of each other and the bidirectional state of the link through their UDLD message exchanges. From then on, if messages are not echoed, the link can accurately be labeled as unidirectional.

Finally, be aware that if UDLD detects a unidirectional condition on a link, it takes action on only that link. This becomes important in an EtherChannel: If one link within the channel becomes unidirectional, UDLD flags or disables only the offending link in the bundle, not the entire EtherChannel. UDLD sends and echoes its messages on each link within an EtherChannel channel independently.

**Using BPDU Filtering to Disable STP on a Port**

Ordinarily, STP operates on all switch ports in an effort to eliminate bridging loops before they can form. BPDUs are sent on all switch ports—even ports where PortFast has been enabled. BPDUs also can be received and processed if any are sent by neighboring switches.

You always should allow STP to run on a switch to prevent loops. However, in special cases when you need to prevent BPDUs from being sent or processed on one or more switch ports, you can use BPDU filtering to effectively disable STP on those ports.

By default, BPDU filtering is disabled on all switch ports. You can configure BPDU filtering as a global default, affecting all switch ports with the following global configuration command:

```
Switch(config)# spanning-tree portfast bpdufilter default
```

The `default` keyword indicates that BPDU filtering will be enabled automatically on all ports that have PortFast enabled. If PortFast is disabled on a port, then BPDU filtering will not be enabled there.

You also can enable or disable BPDU filtering on specific switch ports by using the following interface configuration command:

```
Switch(config-if)# spanning-tree bpdufilter {enable | disable}
```

Be very careful to enable BPDU filtering only under controlled circumstances in which you are absolutely sure that a switch port will have a single host connected and that a loop will be impossible. Enable BPDU filtering only if the connected device cannot allow BPDUs to be accepted or sent. Otherwise, you should permit STP to operate on the switch ports as a precaution.
Troubleshooting STP Protection

With several different types of STP protection features available, you might need to know which (if any) has been configured on a switch port. Table 9-2 lists and describes the EXEC commands useful for verifying the features presented in this chapter.

Table 9-2 Commands for Verifying and Troubleshooting STP Protection Features

<table>
<thead>
<tr>
<th>Display Function</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>List the ports that have been labeled in an inconsistent state.</td>
<td>Switch# show spanning-tree inconsistentports</td>
</tr>
<tr>
<td>Look for detailed reasons for inconsistencies.</td>
<td>Switch# show spanning-tree interface type mod/num [detail]</td>
</tr>
<tr>
<td>Display the global BPDU Guard, BPDU filter, and Loop Guard states.</td>
<td>Switch# show spanning-tree summary</td>
</tr>
<tr>
<td>Display the UDLD status on one or all ports.</td>
<td>Switch# show udld [type mod/num]</td>
</tr>
<tr>
<td>Reenable ports that UDLD aggressive mode has erddisabled.</td>
<td>Switch# udld reset</td>
</tr>
</tbody>
</table>
Exam Preparation Tasks

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 9-3 lists a reference of these key topics and the page numbers on which each is found.

Table 9-3  Key Topics for Chapter 9

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paragraph</td>
<td>Discusses the Root Guard feature</td>
<td>180</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Discusses the BPDU Guard feature</td>
<td>181</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Discusses the Loop Guard feature</td>
<td>183</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Discusses the UDLD feature</td>
<td>184</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Explains BPDU filtering</td>
<td>186</td>
</tr>
</tbody>
</table>

Complete Tables and Lists from Memory

Print a copy of Appendix C, “Memory Tables,” (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, “Memory Tables Answer Key,” also on the CD, 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:

Root Guard, superior BPDU, BPDU Guard, Loop Guard, UDLD, BPDU filtering

Use Command Reference to Check Your Memory

This section includes the most important configuration and EXEC commands covered in this chapter. It might not be necessary to memorize the complete syntax of every command, but you should remember the basic keywords that are needed.

With so many similar and mutually exclusive STP protection features available, you might have a hard time remembering which ones to use where. Use Figure 9-1 as a quick reference.

Figure 9-1 shows two backbone switches (Catalyst A and B), along with an access-layer switch (Catalyst C), with redundant uplinks. Users are connected to the access switch, where PortFast is in use. An additional access switch (Catalyst D) has an uplink to access-layer switch C. All switch-to-switch links are fiber-based Gigabit Ethernet. Obviously, a root bridge never should appear out of Catalyst D.
Figure 9-1  Guidelines for Applying STP Protection Features in a Network

To test your memory of the STP protection feature commands, cover the rightmost columns of Tables 9-4 and 9-5 with a piece of paper, read the description on the left side, then see how much of the command you can remember.

Remember that the CCNP exam focuses on practical or hands-on skills that are used by a networking professional.
Table 9-4  STP Protection Configuration Commands

<table>
<thead>
<tr>
<th>Task</th>
<th>Global Command Syntax</th>
<th>Interface Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Root Guard</td>
<td>—</td>
<td>Switch(config-if)# spanning-tree guard root</td>
</tr>
<tr>
<td>Enable BPDU Guard</td>
<td>Switch(config)# spanning-tree portfast bpduguard default</td>
<td>Switch(config-if)# spanning-tree bpduguard enable</td>
</tr>
<tr>
<td>Enable Loop Guard</td>
<td>Switch(config)# spanning-tree loopguard default</td>
<td>Switch(config-if)# spanning-tree guard loop</td>
</tr>
<tr>
<td>Enable UDLD</td>
<td>Switch(config)# udld {enable</td>
<td>aggressive</td>
</tr>
<tr>
<td>Enable BPDU filtering</td>
<td>Switch(config)# spanning-tree bpdufilter default</td>
<td>Switch(config-if)# spanning-tree bpdufilter enable</td>
</tr>
</tbody>
</table>

Table 9-5  STP Protection Activity Commands

<table>
<thead>
<tr>
<th>Task</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Look for ports that have been put in an inconsistent state</td>
<td>Switch# show spanning-tree inconsistentports</td>
</tr>
<tr>
<td>Display the global BPDU Guard, BPDU filter, and Loop Guard states</td>
<td>Switch# show spanning-tree summary</td>
</tr>
<tr>
<td>Show UDLD status</td>
<td>Switch# show udld [type mod/num]</td>
</tr>
<tr>
<td>Reenable all ports that UDLD has errdisabled</td>
<td>Switch# udld reset</td>
</tr>
</tbody>
</table>
Index

10GbE (10-Gigabit Ethernet), 47–48
10GEC (10-Gigabit EtherChannel), 108
10-Gigabit EtherChannel (10GEC), 108
10-Gigabit Ethernet (10GbE), 47–48
20/80 rule, 70
80/20 rule, 69

A

aaa authentication dot1x default group radius command, 390
Accelerated CEF (aCEF), 225–226
access control lists. See ACLs (access control lists)
access layer in hierarchical network design, 251
access points (WLANs)
autonomous mode AP, 344–346
cells (coverage areas), 341–344
explained, 338–344
aCEF (Accelerated CEF), 225–226
ACLs (access control lists)
QoS ACLs (access control lists)
Layer 2 switching, 24
multilayer switching (MLS), 26
security ACLs (access control lists)
Layer 2 switching, 23
multilayer switching (MLS), 26
VLAN access lists (VACL), 396–397
action command, 408
activating practice exam content, 414
active hosts, determining, 33
active HSRP routers, 269
active virtual forwarder, 282–283
active virtual gateway, 281–282
Address Resolution Protocol. See ARP (Address Resolution Protocol)
adjacency table, 226–229
advertisements (VTP), 89–92
client requests for, 91–92
origination of, 90
aggregation with EtherChannel, 108–112
alternate ports in RSTP (Rapid Spanning Tree Protocol), 197
APs. See access points (WLANs)
arquitectura de WLANs, 344–354
Cisco Unified Wireless Network Architecture
explained, 346–349
LAP (lightweight access point), 350–351
roaming in, 354–361
bridge priorities, setting, 158
bridge protocol data units. See BPDU (bridge protocol data units)
bridging loops
in EtherChannel, 112
explained, 126–129
preventing, 129–130. See also protecting STP (Spanning Tree Protocol)
BSS (basic service set), 338–339
bundling
with EtherChannel, 108–112
ports with EtherChannel, 109

C
cabling
basic Ethernet, 43, 48–49
Fast Ethernet, 44, 48–49
Gigabit Ethernet, 46, 49–50
CAM (content-addressable memory), 27–28
Layer 2 switching, 23
monitoring, 32–34
campus networks, defined, 247
campuswide VLANs, 69–70
canonical format, 74
Canonical Format Indicator (CFI), 74
CAPWAP (Control and Provisioning Wireless Access Points protocol), 348
carrier sense multiple access collision detect (CSMA/CD), 42
Catalyst switches, STP bridge IDs for, 158
CDP, securing, 387–388
CEF (Cisco Express Forwarding), 221–230. See also topology-based MLS
adjacency table, 226–229
configuring, 229–230
FIB (Forwarding Information Base), 222–226
packet rewrite, 229
verifying, 232–233
cells (WLAN coverage areas), 341–344
CFI (Canonical Format Indicator), 74
channel-group mode command, 121
channel-protocol lacp command, 121
channel-protocol pagp command, 121
Cisco Express Forwarding (CEF). See CEF (Cisco Express Forwarding); topology-based MLS
Cisco Hybrid Remote Edge Access Point (HREAP), 351
Cisco Inline Power (ILP), 304
Cisco Learning Network, 416
Cisco Unified Wireless Network Architecture
explained, 346–349
LAP (lightweight access point), configuring, 350–351
roaming in, 354–361
intercontroller roaming, 356–361
intracontroller roaming, 355–356
mobility groups, 361
traffic patterns, 352–354
WLC functions, 349–350
class of service (CoS), 315
classes, packet precedence, 317
clear mac address-table dynamic command, 37
CLI (command-line interface), exam topics not requiring, 6–7
client mode (VTP), 88, 94
client requests for VTP advertisements, 91–92
collapsed core block in modular network design, 259–260
collision domains, 20
collisions, 42, 336–338
Common Spanning Tree (CST), 147
community VLANs, 398
conceding router election in HSRP (Hot Standby Router Protocol), 272–273
Configuration BPDU, 130–131
configuration revision numbers (VTP), 89
  checking settings, 92
configuring. See also tuning
  Auto-QoS, 321–324
  CEF (Cisco Express Forwarding), 229–230
  DHCP relay, 235–236
  DHCP servers, 235
  EtherChannel, 114–116
    LACP (Link Aggregation Control Protocol), 115–116
    PAgP (Port Aggregation Protocol), 114–115
  interVLAN routing, 219–221
    Layer 2 port configuration, 219–220
    Layer 3 port configuration, 220
    SVI port configuration, 221
  LAP (lightweight access point), 350–351
  load-balancing in EtherChannel, 111–112
  MST (Multiple Spanning Tree Protocol), 209–210
  PoE (Power over Ethernet), 307
  port-based authentication, 376–378
  ports
    duplex mode, 52–53
    enabling the port, 55
  error condition management, 53–55
  identifying descriptions, 52
  selecting for configuration, 50–51
  speed, 52
  troubleshooting connectivity, 55–56
  private VLANs, 399–402
  redundancy mode (hardware redundancy), 290–292
  root bridges, 157–161
  RSTP (Rapid Spanning Tree Protocol), 202–203
  static VLANs, 66–68
  supervisor synchronization, 293
  switchports for WLANs, 361–364
    for autonomous APs, 361–362
    for LAPs, 362–363
    for WLCs, 363–364
  trust boundary, 319–321
  VLAN access lists (VACL), 396–397
  VLAN trunks, 75–78
  voice VLANs, 308–311
  VTP (VLAN Trunking Protocol), 92–97
    example of, 96
    management domains, 93
    modes, 93–95
    versions, 95–96
    viewing status, 96–97
connectors
  basic Ethernet, 48–49
  cautions concerning, 50
  Fast Ethernet, 48–49
  Gigabit Ethernet, 49–50
  consistency checks (VTP), 95
content-addressable memory. See CAM (content-addressable memory)
Control and Provisioning Wireless Access Points protocol (CAPWAP), 348

convergence (RSTP), 198–201
- port types, 198–199
- synchronization, 199–201

convergence (STP)
- redundant link convergence, 167–171
  - BackboneFast feature, 170–171
  - PortFast feature, 167–168
  - UplinkFast feature, 168–170
- tuning, 164–166

core blocks in modular network design, 259–262

core layer in hierarchical network design, 249–252

CoS (class of service), 315, 321

CSMA/CD (carrier sense multiple access collision detect), 42

CST (Common Spanning Tree), 147, 207–209

customization of STP (Spanning Tree Protocol), 161–164
- tuning port ID, 163–164
- tuning root path cost, 161–162

dD

DAI (dynamic ARP inspection), 383–385
dCEF (Distributed CEF), 226

DCF (distributed coordination function), 337

describe cdp packets command, 306
describe ipower controller command, 306
describe spanning-tree switch state command, 139
default gateway, 268
default-router command, 238
define interface-range command, 58
delay, 313
demand-based switching. See route caching MLS
deploying VLANs (virtual LANs), 69–70
description command, 58
design phase (planning skills), 10
designated ports
- electing, 135–136
- in RSTP (Rapid Spanning Tree Protocol), 197

DHCP (Dynamic Host Configuration Protocol), multilayer switching (MLS)
- configuring DHCP relay, 235–236
- configuring DHCP server, 235

DHCP snooping, 379–381
differentiated service codepoint (DSCP), 316–318
differentiated services model (DiffServ), 314–318

Layer 2 classification, 315
Layer 3 classification, 316–318
direct topology changes in STP (Spanning Tree Protocol), 142–143

Disabled state (STP ports), 137

disabling STP (Spanning Tree Protocol), 186
discard adjacencies, 228

Discarding state (RSTP ports), 197

Distributed CEF (dCEF), 226
distributed coordination function (DCF), 337
distribution layer in hierarchical network design, 251
documenting results of implementation plan, 12
domains, in VTP (VLAN Trunking Protocol), 88, 93

dot1x host-mode multi-host command, 390
dot1x port-control command, 390
dot1x system-auth-control command, 390
double tagging. See Inter-Switch Link (ISL) protocol
downloading practice exam content, 414

DRM (dual-router mode), 290
drop adjacencies, 228

DSCP (differentiated service codepoint), 316–318

DTP (Dynamic Trunking Protocol), 74, 402–404
dual core in modular network design, 261–262
dual-router mode (DRM), 290
duplex command, 58
duplex mode
   configuring ports, 52–53
   mismatches between ports, 55–56
dynamic ARP inspection, 383–385

Dynamic Host Configuration Protocol. See DHCP (Dynamic Host Configuration Protocol)

Dynamic Trunking Protocol (DTP), 74
dynamic VLANs, 68–69

E

EAPOL (Extensible Authentication Protocol over LANs), 376

edge ports (RSTP), 198
electing
   designated ports, 135–136
   root bridges, 131–132

root ports, 133–135

routers in HSRP (Hot Standby Router Protocol), 269–271

enable secret command, 385

enabling
   GLBP (Gateway Load Balancing Protocol), 284–288
   HTTPS interface, 386
   STP (Spanning Tree Protocol), 154
   VTP pruning, 99–100

everdisable detect cause command, 58

errdisable recovery cause command, 58

errdisable recovery interval command, 58

errdisable state, 53–55

error condition management,
   configuring ports, 53–55

ESS (extended service set), 339–340

EtherChannel
   configuring, 114–116

   LACP (Link Aggregation Control Protocol), 115–116

   PAgP (Port Aggregation Protocol), 114–115

explained, 108

load-balancing in, 108–110

   configuring, 111–112

negotiation protocols, 112–114

troubleshooting, 116–119

Ethernet

10-Gigabit Ethernet (10GbE), 47–48

advantages of, 42

basic Ethernet, 42–43
cabling and connectors, 48–50

Fast Ethernet, 43–44

full-duplex Fast Ethernet, 44–45
Gigabit Ethernet, 45–47
port bundling, 109
Ethernet switches. See switches
exam engine
installing, 413–415
modes of, 416
exam preparation, planning skills
and, 13
exam topics, planning skills needed.
See planning skills
extended service set (ESS), 339–340
extended-range VLANs, 67
Extensible Authentication Protocol over
LANs (EAPOL), 376
external AC adapters, 304

Fast EtherChannel (FEC), 45, 108
Fast Ethernet, 43–44
cabling and connectors, 48–49
full-duplex Fast Ethernet, 44–45
Feature Manager (FM), 28
FEC (Fast EtherChannel), 45, 108
FHRP (first-hop redundancy protocols),
268
FIB (Forwarding Information Base),
222–226
first-hop redundancy protocols (FHRP),
268
flat network topology, 65
flooding, unknown unicast flooding, 22
flow-based switching. See route caching
MLS
FM (Feature Manager), 28
Forward Delay timer, 137, 140, 165
forwarding
frames, in Layer 2 switches, 22–24
packets
in multilayer switching (MLS),
25–26, 268
QoS (quality of service),
explained, 313–314
Forwarding Information Base (FIB),
222–226
Forwarding state (RSTP ports), 197
Forwarding state (STP ports), 137
frame distribution. See load-balancing
frame identification, VLANs (virtual
LANs), 71–74
frames
baby giant frames, 74
forwarding in Layer 2 switches, 22–24
full-duplex, 43
full-duplex Fast Ethernet, 44–45
full-duplex ports (RSTP), 199

gateway addressing in HSRP (Hot
Standby Router Protocol), 273–274
Gateway Load Balancing Protocol. See
GLBP (Gateway Load Balancing
Protocol)
GEC (Gigabit EtherChannel), 46, 108
Gigabit EtherChannel (GEC), 46, 108
Gigabit Ethernet, 45–47
cabling and connectors, 49–50
GLBP (Gateway Load Balancing
Protocol), 280–289
active virtual forwarder, 282–283
active virtual gateway, 281–282
enabling, 284–288
load-balancing types, 283–284
verifying redundancy, 289
glbp ip command, 296
intercontroller roaming

glbp load-balancing command, 296
glbp preempt command, 296
glbp priority command, 296
glbp weighting command, 296
glbp weighting track command, 296

gateway addressing, 273–274
load-balancing, 274–277
MD5 authentication, 271–272
plain-text authentication, 271
router election, 269–271
HTTPS interface, enabling, 386

H

half-duplex, 42
half-duplex ports (RSTP), 199
hardware redundancy, 289–294
  configuring redundancy mode, 290–292
  modes of, 289–290
  nonstop forwarding (NSF), 293–294
  supervisor synchronization, 293
Hello Time timer, 140, 164
hierarchical network design, 247–252
  access layer, 251
  core layer, 251–252
  distribution layer, 251
  network segmentation, 247–248
  predictability, 249–250
host dependent load balancing, 284
host location, determining by MAC address, 32–33
host mode (private VLANs), 398
hosts
  active hosts, determining, 33
  multiple hosts, finding on interface, 33
Hot Standby Router Protocol. See HSRP (Hot Standby Router Protocol)
HREAP (Cisco Hybrid Remote Edge Access Point), 351
HSRP (Hot Standby Router Protocol), 269–277
  conceding router election, 272–273
IBSS (Independent basic service set), 338–339
IEEE 802.11 standards. See WLANs (wireless LANs)
IEEE 802.1D standard, 126. See also STP (Spanning Tree Protocol)
IEEE 802.1Q protocol, 73–74, 147, 204, 315
IEEE 802.1s standard. See MST (Multiple Spanning Tree Protocol)
IEEE 802.1w standard, 196. See also RSTP (Rapid Spanning Tree Protocol)
IEEE 802.1x standard, 376–378
IEEE 802.3af standard, 304–305
ILP (Cisco Inline Power), 304
implementation plan phase (planning skills), 10–12
Independent basic service set (IBSS), 338–339
indirect link failures, 170
indirect topology changes in STP (Spanning Tree Protocol), 143–145
inline power. See PoE (Power over Ethernet)
insignificant topology changes in STP (Spanning Tree Protocol), 145–146
installing exam engine, 413–415
integrated services model (IntServ), 314
intercontroller roaming, 356–361
interface command, 58, 83
interface range command, 58
interface range macro command, 58
interface switchport trunk pruning vlan command, 103
interface vlan command, 238
interfaces. See also ports
   active hosts, determining, 33
   in interVLAN routing, 218–219
   multiple hosts, finding, 33
Internal Spanning Tree (IST) instances, 207
internal tagging. See IEEE 802.1Q protocol
Inter-Switch Link (ISL) protocol, 72–73, 315
interVLAN routing, 218–221
   configuring, 219–221
      Layer 2 port configuration, 219–220
      Layer 3 port configuration, 220
      SVI port configuration, 221
   interface types, 218–219
   verifying, 230–232
intracontroller roaming, 355–356
ip arp inspection filter vlan command, 391
ip arp inspection trust command, 391
ip arp inspection validate command, 391
ip arp inspection vlan command, 391
ip dhcp excluded-address command, 238
ip dhcp pool command, 238
ip dhcp snooping command, 390
ip dhcp snooping limit rate command, 390
ip dhcp snooping trust command, 390
ip helper-address command, 238
ip http access-class command, 386
ip http secure server command, 386
IP precedence, mapping to DSCP fields, 316–317
ip source binding vlan interface command, 391
IP source guard, 381–383
IP telephony
   PoE (Power over Ethernet), 304–308
      configuring, 307
      detecting powered devices, 304–305
      supplying power to devices, 305–306
      verifying, 307–308
   voice QoS, 312–326
   voice VLANs, 308–312
      configuring, 308–311
      verifying, 311–312
ip verify source command, 391
ISL (Inter-Switch Link) protocol, 72–73, 315
isolated VLANs, 398
IST (Internal Spanning Tree) instances, 207
J
   jitter, 313
L
   L2 forwarding tables
      Layer 2 switching, 23
      multilayer switching (MLS), 26
   L3 forwarding tables, multilayer switching (MLS), 26
   LACP (Link Aggregation Control Protocol), 113–116
lacp port-priority command, 116, 121
lacp system-priority command, 121
LAN PHY, 47
LAP (lightweight access point), 348
configuring, 350–351
configuring switchports for, 362–363
latency, 313
Layer 2 port configuration, interVLAN routing, 219–220
Layer 2 QoS classification, 315
Layer 2 roaming, 343
Layer 2 switching, 20–24. See also STP (Spanning Tree Protocol)
Layer 3 port configuration, interVLAN routing, 220
Layer 3 QoS classification, 316–318
Layer 3 roaming, 343
Learning state (RSTP ports), 197
Learning state (STP ports), 137
lease command, 238
lightweight access point (LAP), 348
configuring, 350–351
configuring switchports for, 362–363
Lightweight Access Point Protocol (LWAPP), 348
Link Aggregation Control Protocol (LACP), 113–116
listen HSRP routers, 269
Listening state (STP ports), 137
little-endian format, 74
load-balancing. See also GLBP (Gateway Load Balancing Protocol)
in EtherChannel, 108–112
in HSRP (Hot Standby Router Protocol), 274–277
local VLANs, 70
logical network segments, physical network segments versus, 65
Loop Guard feature (STP), 183
loops. See bridging loops
loss (of packets), 313
LWAPP (Lightweight Access Point Protocol), 348

M

MAC addresses
determining by host location, 32–33
port security, 373–376
mac address-table static command, 37
management domains, in VTP (VLAN Trunking Protocol), 88, 93
man-in-the-middle attacks. See spoofing attack prevention
masks (TCAM), 29
master routers in VRRP (Virtual Router Redundancy Protocol), 277
match command, 408
Max Age timer, 140, 165
MD5 authentication, 271–272
membership in VLANs (virtual LANs), 65–69
dynamic VLANs, 68–69
static VLANs, 66–68
microcells (WLAN coverage areas), 344
MLS. See multilayer switching (MLS)
mls qos command, 328
mls qos trust command, 328
mls qos trust device cisco-phone command, 328
mobility groups, 356–361
modes in VTP (VLAN Trunking Protocol), 88–89, 93–95
modular network design, 252–262
core blocks, 259–262
modular network design

- redundant paths versus, 252–254
- switch blocks, 254–259

**monitoring**
- STP (Spanning Tree Protocol), 171–172
- switching tables, 32–35

**MST (Multiple Spanning Tree Protocol), 204–210**
- configuring, 209–210
- regions, 206
- spanning-tree instances in, 207–209

**MST instances (MSTI), 208–209**

**MSTI (MST instances), 208–209**

**multilayer switching (MLS), 24–27**
- CEF (Cisco Express Forwarding), 221–230
  - adjacency table, 226–229
  - configuring, 229–230
  - FIB (Forwarding Information Base), 222–226
  - packet rewrite, 229
  - verifying, 232–233
- DHCP (Dynamic Host Configuration Protocol) and, 233–236
  - configuring DHCP relay, 235–236
  - configuring DHCP server, 235
- interVLAN routing, 218–221
  - configuring, 219–221
  - interface types, 218–219
  - verifying, 230–232
- Netflow LAN switching, 221–222
- router redundancy, 268–289
  - GLBP (Gateway Load Balancing Protocol), 280–289
  - HSRP (Hot Standby Router Protocol), 269–277
  - VRRP (Virtual Router Redundancy Protocol), 277–280
- multiple hosts, finding on interface, 33

**Multiple Spanning Tree Protocol. See MST (Multiple Spanning Tree Protocol)**

**N**

**name command, 83, 212**

**native VLANs, 73, 308**

**negotiation protocols for EtherChannel, 112–114**

**Netflow LAN switching, 221–222. See also route caching MLS**

**network command, 238**

**network connectors. See connectors**

**network design**
- hierarchical network design, 247–252
  - access layer, 251
  - core layer, 251–252
  - distribution layer, 251
  - network segmentation, 247–248
  - predictability, 249–250
- modular network design, 252–262
  - core blocks, 259–262
  - redundant paths versus, 252–254
  - switch blocks, 254–259
- network engineers, role of, 12
- network lifecycle, 7–8
- network segmentation in hierarchical network design, 247–248
- network services, types of, 250
- next hop, 268
- no ip http server command, 386
- no shutdown command, 58
- no switchport command, 238
- no vrrp preempt command, 278, 297
- nonstop forwarding (NSF), 293–294
- NSF (nonstop forwarding), 293–294
- null adjacencies, 228
packet forwarding. See forwarding, packets

packet rewrite, 229

packets, forwarding in multilayer switching (MLS), 25–26

PAgP (Port Aggregation Protocol), 113–115

passwords
  for secure VTP, 94
  security best practices, 385

path cost, 133, 161–162

permit ip host mac host command, 391

Per-VLAN Spanning Tree (PVST), 147

Per-VLAN Spanning Tree Plus (PVST+), 147, 204

Physical Media Dependent (PMD) interfaces, 10-Gigabit Ethernet (10GbE), 47–48

physical network segments, logical network segments versus, 65

picocells (WLAN coverage areas), 344

plain-text authentication in HSRP (Hot Standby Router Protocol), 271

planning skills, 5–13
  company staff example, 9
  design phase, 10
  documenting results, 12
  exam preparation and, 13
  exam topics not requiring CLI, 6–7
  implementation plan phase, 10–11
  need for, 8
  PPDIOO network lifecycle, 7–8
  verification plan phase, 11–12

PMD (Physical Media Dependent) interfaces, 10-Gigabit Ethernet (10GbE), 47–48

PoE (Power over Ethernet), 304–308
  configuring, 307
  detecting powered devices, 304–305
  supplying power to devices, 305–306
  verifying, 307–308

point-to-point ports (RSTP), 199

Port Aggregation Protocol (PAgP), 113–115

port IDs, tuning, 163–164

port operations in TCAM (ternary content-addressable memory), 31–32

port priority, 113

port security, 373–376

port state
  finding, 55
  in RSTP (Rapid Spanning Tree Protocol), 197
  in STP (Spanning Tree Protocol), 137–139

port VLAN ID (PVID), 308

port-based authentication, 376–378

port-based membership in static VLANs, 66

port-channel load-balance command, 121

PortFast feature (STP), 167–168
  BPDU Guard feature (STP) and, 181–182

ports. See also interfaces
  associating with private VLANs, 400–401
  bundling, with EtherChannel, 109
  configuring
    duplex mode, 52–53
    enabling the port, 55
    error condition management, 53–55
    identifying descriptions, 52
    selecting for configuration, 50–51
speed, 52
troubleshooting connectivity, 55–56
designated ports. See designated ports
initialization delays, 167
root ports. See root ports
in RSTP (Rapid Spanning Tree Protocol), 196–199
power classes (IEEE 802.3af standard), 305
power inline command, 328
Power over Ethernet. See PoE (Power
er over Ethernet)
power supply redundancy, 289–294
powered devices
detecting, 304–305
supplying power to, 305–306
PPDIOO network lifecycle, 7–8
practice exam content, activating, 414
predictability in hierarchical network
design, 249–250
preparation. See exam preparation
prepare, plan, design, implement,
operate, optimize (PPDIOO) network
lifecycle, 7–8
preventing
bridging loops, 129–130
spoofing attacks, 378–385
DHCP snooping, 379–381
dynamic ARP inspection, 383–385
IP source guard, 381–383
private VLANs, 397–402
private-vlan association command, 408
private-vlan command, 408
private-vlan mapping command, 408
private-vlan primary command, 408
process switching, 27
promiscuous mode (private VLANs), 398
protect mode (port security), 374
protecting STP (Spanning Tree Protocol)
against sudden loss of BPDUs, 182–186
troubleshooting protection, 187
against unexpected BPDUs, 180–182
pruning (VTP), 97–100
punt adjacencies, 228
PVID (port VLAN ID), 308
PVLAN, See private VLANs
PVST (Per-VLAN Spanning Tree), 147
PVST+ (Per-VLAN Spanning Tree Plus), 147, 204
QoS (quality of service)
explained, 313–314
voice QoS, 312–326
Auto-QoS, 321–324
best-effort delivery, 314
differentiated services model, 314–318
implementation, 318–319
integrated services model, 314
trust boundary configuration, 319–321
verifying, 324–326
QoS ACLs (access control lists)
Layer 2 switching, 24
multilayer switching (MLS), 26
quality of service. See QoS (quality of service)
RACLs (router access control lists). See ACLs (access control lists)
range of WLANs, 341–344
Rapid PVST+ (RPVST+), 196, 203–204
Rapid Spanning Tree Protocol. See RSTP (Rapid Spanning Tree Protocol)
redundancy
hardware redundancy, 289–294
configuring redundancy mode, 290–292
modes of, 289–290
nonstop forwarding (NSF), 293–294
supervisor synchronization, 293
router redundancy, 268–289
GLBP (Gateway Load Balancing Protocol), 280–289
HSRP (Hot Standby Router Protocol), 269–277
VRRP (Virtual Router Redundancy Protocol), 277–280
redundant paths
modular network design versus, 252–254
in STP (Spanning Tree Protocol), 130, 167–171
in switch blocks, 256–259
regions (MST), 206
requesting VTP advertisements, 91–92
Resource Reservation Protocol (RSVP), 314
restrict mode (port security), 374
results (TCAM), 29
revision command, 212
revision numbers (VTP), 89, 92

RLQ (Root Link Query) protocol, 170
roaming, 343
in Cisco Unified Wireless Network Architecture, 354–361
intercontroller roaming, 356–361
intracontroller roaming, 355–356
mobility groups, 356–361
root bridges
configuring, 157–161
electing, 131–132
placement of, 154–157
poor choices for, 154
Root Guard feature (STP), 180–181
Root Link Query (RLQ) protocol, 170
root path cost, 133, 161–162
root ports
electing, 133–135
in RSTP (Rapid Spanning Tree Protocol), 197, 199
root-inconsistent STP state, 181
round robin load balancing, 284
route caching MLS, 24, 221–222
route processor redundancy (RPR), 290
route processor redundancy plus (RPR+), 290
router access control lists. See ACLs (access control lists)
router redundancy, 268–289
GLBP (Gateway Load Balancing Protocol), 280–289
HSRP (Hot Standby Router Protocol), 269–277
VRRP (Virtual Router Redundancy Protocol), 277–280
RPR (route processor redundancy), 290
RPR+ (route processor redundancy plus), 290
RPVST+ (Rapid PVST+), 196, 203–204
RSTP (Rapid Spanning Tree Protocol), 196–204
BPDUs in, 197–198
configuring, 202–203
convergence, 198–201
   port types, 198–199
   synchronization, 199–201
port behavior, 196–197
topology changes, 201–202
RSVP (Resource Reservation Protocol), 314
runts, 56

S

SDM (Switching Database Manager), 28
secondary VLANs, associating with primary VLAN SVI, 401–402
secure VTP, passwords for, 94
security
   best practices, 385–388
   port security, 373–376
   port-based authentication, 376–378
   private VLANs, 397–402
   spoofing attack prevention, 378–385
      DHCP snooping, 379–381
      dynamic ARP inspection, 383–385
      IP source guard, 381–383
   VLAN access lists (VACL), 396–397
   for VLAN trunks, 402–406
      switch spoofing, 402–404
      VLAN hopping, 404–406
security ACLs (access control lists)
   Layer 2 switching, 23
   multilayer switching (MLS), 26
segmentation. See network segmentation
selecting ports for configuration, 50–51
server mode (VTP), 88, 93
service password-encryption command, 385
service provider networks, private VLANs and, 398
service set identifier (SSID), 338
   mapping to VLANs, 340–341
service sets (WLANs), 338
show adjacency command, 239
show auto qos command, 328
show cef not-cef-switched command, 239
show dot1x all command, 378
show dtp command, 81, 83
show etherchannel detail command, 119
show etherchannel load-balance command, 119
show etherchannel port command, 117, 119
show etherchannel port-channel command, 112, 119
show etherchannel summary command, 117, 119
show interface command, 239
show interface etherchannel command, 118
show interface pruning command, 101
show interface status err-disabled EXEC command, 55
show interface status EXEC command, 55
show interface switchport command, 80, 83, 101, 239, 328
show interface trunk command, 77, 80, 83
show interface vlan command, 239
show interfaces EXEC command, 55
show ip cef command, 239
spanning-tree mst max-age command

show lACP sys-id command, 119
show mac address-table count command, 37
show mac address-table dynamic address command, 37
show mac address-table dynamic interface command, 37
show mls qos interface command, 328
show neighbor command, 119
show power inline command, 328
show running-config interface command, 118
show spanning-tree backbonefast command, 172
show spanning-tree bridge command, 171
show spanning-tree command, 171
show spanning-tree detail command, 171
show spanning-tree inconsistentports command, 181, 187, 190
show spanning-tree interface command, 139, 172, 187
show spanning-tree root command, 171
show spanning-tree summary command, 171, 187, 190
show spanning-tree uplinkfast command, 172
show udld command, 187, 190
show user all command, 386
show vlan brief command, 101
show vlan command, 68
show vlan id command, 79, 83
show vtp counters command, 97, 101
show vtp status command, 92, 96, 101
shutdown command, 58, 387
shutdown mode (port security), 374
simulation mode (exam engine), 416

single tagging. See IEEE 802.1Q protocol

single-router mode (SRM), 290

size
of CAM tables, checking, 34
of core blocks, 262
of switch blocks, 255–256

SNMP access, securing, 387

Spanning Tree Protocol. See STP (Spanning Tree Protocol)

spanning-tree backbonefast command, 174

spanning-tree bpdufilter enable command, 190

spanning-tree bpduguard enable command, 190

spanning-tree command, 174

spanning-tree cost command, 174

spanning-tree forward-time command, 174

spanning-tree guard loop command, 190

spanning-tree guard root command, 190

spanning-tree hello-time command, 174

spanning-tree instances in MST (Multiple Spanning Tree Protocol), 207–209

spanning-tree link-type point-to-point command, 212

spanning-tree loops. See bridging loops

spanning-tree max-age command, 174

spanning-tree mode mst command, 212

spanning-tree mst configuration command, 212

spanning-tree mst cost command, 210

spanning-tree mst forward-time command, 210

spanning-tree mst hello-time command, 210

spanning-tree mst max-age command, 210

single tagging. See IEEE 802.1Q protocol

single-router mode (SRM), 290

size
of CAM tables, checking, 34
of core blocks, 262
of switch blocks, 255–256

SNMP access, securing, 387

Spanning Tree Protocol. See STP (Spanning Tree Protocol)

spanning-tree backbonefast command, 174

spanning-tree bpdufilter enable command, 190

spanning-tree bpduguard enable command, 190

spanning-tree command, 174

spanning-tree cost command, 174

spanning-tree forward-time command, 174

spanning-tree guard loop command, 190

spanning-tree guard root command, 190

spanning-tree hello-time command, 174

spanning-tree instances in MST (Multiple Spanning Tree Protocol), 207–209

spanning-tree link-type point-to-point command, 212

spanning-tree loops. See bridging loops

spanning-tree max-age command, 174

spanning-tree mode mst command, 212

spanning-tree mst configuration command, 212

spanning-tree mst cost command, 210

spanning-tree mst forward-time command, 210

spanning-tree mst hello-time command, 210

spanning-tree mst max-age command, 210

single tagging. See IEEE 802.1Q protocol

single-router mode (SRM), 290

size
of CAM tables, checking, 34
of core blocks, 262
of switch blocks, 255–256

SNMP access, securing, 387

Spanning Tree Protocol. See STP (Spanning Tree Protocol)

spanning-tree backbonefast command, 174

spanning-tree bpdufilter enable command, 190

spanning-tree bpduguard enable command, 190

spanning-tree command, 174

spanning-tree cost command, 174

spanning-tree forward-time command, 174

spanning-tree guard loop command, 190

spanning-tree guard root command, 190

spanning-tree hello-time command, 174

spanning-tree instances in MST (Multiple Spanning Tree Protocol), 207–209

spanning-tree link-type point-to-point command, 212

spanning-tree loops. See bridging loops

spanning-tree max-age command, 174

spanning-tree mode mst command, 212

spanning-tree mst configuration command, 212

spanning-tree mst cost command, 210

spanning-tree mst forward-time command, 210

spanning-tree mst hello-time command, 210

spanning-tree mst max-age command, 210
spanning-tree mst port-priority command, 210
spanning-tree mst priority command, 210
spanning-tree mst root command, 210
spanning-tree portfast command, 174, 212
spanning-tree port-priority command, 174
spanning-tree uplinkfast command, 174
spanning-tree vlan command, 174
spanning-tree vlan root command, 160, 174
speed
  configuring ports, 52
  mismatches between ports, 55–56
speed command, 58
split-MAC architecture, 348
spoofing attack prevention, 378–385
  DHCP snooping, 379–381
  dynamic ARP inspection, 383–385
  IP source guard, 381–383
SRM (single-router mode), 290
SSH, Telnet versus, 386–387
SSID (service set identifier), 338
  mapping to VLANs, 340–341
SSO (stateful switchover), 290
stale entries, 27
standards. See names of specific standards
standby addresses in HSRP (Hot Standby Router Protocol), 273
standby authentication command, 296
standby HSRP routers, 269
standby ip command, 296
standby preempt command, 296
standby priority command, 296
standby timers command, 296
standby track command, 296
stateful switchover (SSO), 290
static VLANs, 66–68
sticky MAC addresses, 373
store-and-forward switching, 20
STP (Spanning Tree Protocol)
  BPDU (bridge protocol data units), 130–131
  bridge priorities, setting, 158
  bridging loops, preventing, 129–130
  convergence, tuning, 164–166
  customization, 161–164
    tuning port ID, 163–164
    tuning root path cost, 161–162
designated ports, electing, 135–136
disabling, 186
enabling, 154
IEEE 802.1D standard, 126
manually computing, 139
monitoring, 171–172
MST (Multiple Spanning Tree Protocol). See MST (Multiple Spanning Tree Protocol)
port states, 137–139
protecting
  against sudden loss of BPDU, 182–186
  troubleshooting protection, 187
  against unexpected BPDU, 180–182
redundant link convergence, 167–171
  BackboneFast feature, 170–171
  PortFast feature, 167–168
  UplinkFast feature, 168–170
root bridges
  configuring, 157–161
  electing, 131–132
  placement of, 154–157
  poor choices for, 154
root ports, electing, 133–135
RSTP (Rapid Spanning Tree Protocol), See RSTP (Rapid Spanning Tree Protocol)
securing, 387
tie-breaking process, 135
timers, 139–141
tuning, 164–166
topology changes, 141–146
types of, 146–148
study mode (exam engine), 416
study plan, 415–416
subset advertisements (VTP), 90–91
sudden loss of BPDUs, protecting against, 182–186
summary advertisements (VTP), 90
superior BPDUs, 181
supervisor engine redundancy, 289–294
supervisor synchronization, configuring, 293
SVI (switched virtual interface), 219
SVI port configuration, interVLAN routing, 221
switch blocks in modular network design, 254–259
switch console, securing, 386
switch spoofing, 402–404
switched virtual interface (SVI), 219
switches
Layer 2 switching, 20–24
multilayer switching (MLS), 24–27
process switching, 27
tables in
CAM (content-addressable memory), 27–28
monitoring, 32–35
TCAM (ternary content-addressable memory), 28–32
Switching Database Manager (SDM), 28
switchport access vlan command, 68, 83
switchport command, 68, 75, 238
switchport host command, 387
switchport mode access command, 68, 83, 387
switchport mode command, 76, 83
switchport mode private-vlan command, 408
switchport nonegotiate command, 76
switchport port-security command, 390
switchport port-security mac-address command, 390
switchport port-security maximum command, 390
switchport port-security violation command, 390
switchport priority extend command, 328
switchport private-vlan host-association command, 408
switchport private-vlan mapping command, 408
switchport trunk allowed vlan command, 75–76, 83, 99
switchport trunk encapsulation command, 75, 83
switchport trunk native vlan command, 75, 83
switchport voice vlan command, 328
switchports, configuring for WLANs, 361–364
for autonomous APs, 361–362
for LAPs, 362–363
for WLCs, 363–364
synchronization
in RSTP convergence, 199–201
supervisor synchronization, configuring, 293
synchronization problems (VTP), 90
system banners, 385
system priority, 113
Tag Control Information (TCI) field, 74
Tag Protocol Identifier (TPID), 74
tagging. See frame identification
TCAM (ternary content-addressable memory), 28–32
example of, 30–31
Layer 2 switching, 23
monitoring, 35
port operations in, 31–32
structure of, 28–30
TCI (Tag Control Information) field, 74
TCN BPDU, 141–146
telephony. See IP telephony
Telnet, SSH versus, 386–387
ternary content-addressable memory.
See TCAM (ternary content-addressable memory)
throttling adjacency, 228
tie-breaking process in STP (Spanning Tree Protocol), 135
timers in STP (Spanning Tree Protocol), 139–141, 164–166
Token Ring, VTP support for, 96
topology changes
in RSTP (Rapid Spanning Tree Protocol), 201–202
in STP (Spanning Tree Protocol), 141–146
topology-based MLS, 24–25
TPID (Tag Protocol Identifier), 74
track interface command, 296
traditional WLAN architecture, 344–346
traffic patterns in Cisco Unified Wireless Networks, 352–354
transparent bridging, 20–22, 126–127
transparent mode (VTP), 88–89, 94–95
troubleshooting
EtherChannel, 116–119
port connectivity, 55–56
STP protection, 187
VLAN trunks, 79–81
VLANs (virtual LANs), 79–81
VTP (VLAN Trunking Protocol), 100–101
trunk links. See VLAN trunks
trust boundary, configuring, 319–321
tuning. See also configuring
convergence (STP), 164–166
port IDs, 163–164
root path cost, 161–162
STP timers, 164–166

UDLD (Unidirectional Link Detection) feature (STP), 184–186
udld command, 190
udld reset command, 187, 190
unexpected BPDUs, protecting against, 180–182
Unidirectional Link Detection (UDLD) feature (STP), 184–186
unidirectional links, 54, 184
unknown unicast flooding, 22, 97–99, 127
unrecognized Type-Length-Value, VTP support for, 96
unused switch ports, securing, 387
UplinkFast feature (STP), 168–170

VACL (VLAN access lists), 396–397
values (TCAM), 29
voice QoS

verification plan phase (planning skills), 11–12
verifying
  CEF (Cisco Express Forwarding), 232–233
  GLBP (Gateway Load Balancing Protocol) redundancy, 289
  interVLAN routing, 230–232
  PoE (Power over Ethernet), 307–308
  voice QoS, 324–326
  voice VLANs, 311–312
versions (VTP), configuring, 95–96
VID (VLAN identifier), 74
violations of port security, handling, 374
virtual LANs. See VLANs (virtual LANs)
Virtual Router Redundancy Protocol. See VRRP (Virtual Router Redundancy Protocol)
virtual terminal access, securing, 386
VLAN access lists (VACL), 396–397
vlan access-map command, 408
vlan command, 83, 408
vlan database EXEC command, 93
vlan filter vlan-list command, 408
VLAN hopping, 404–406
VLAN identifier (VID), 74
VLAN Trunking Protocol (VTP), 67, 74, 88–92
  advertisements, 89–92
  configuring, 92–97
    example of, 96
    management domains, 93
    modes, 93–95
    versions, 95–96
    viewing status, 96–97
domains, 88
modes, 88–89
pruning, 97–100

synchronization problems, 90
troubleshooting, 100–101
VLAN trunks, 70–74
  configuring, 75–78
  DTP (Dynamic Trunking Protocol), 74
  frame identification, 71–74
  IEEE 802.1Q protocol, 73–74
  Inter-Switch Link (ISL) protocol, 72–73
  securing, 402–406
  switch spoofing, 402–404
  VLAN hopping, 404–406
troubleshooting, 79–81
VLANs (virtual LANs)
deploying, 69–70
exam topics, 6
explained, 65–66
interVLAN routing, 218–221
  configuring, 219–221
  interface types, 218–219
  verifying, 230–232
mapping to SSIDs, 340–341
membership, 65–69
  dynamic VLANs, 68–69
  static VLANs, 66–68
private VLANs, 397–402
troubleshooting, 79–81
voice VLANs, 308–312
  configuring, 308–311
  verifying, 311–312
voice QoS
  Auto-QoS, 321–324
  best-effort delivery, 314
differentiated services model, 314–318
implementation, 318–319
integrated services model, 314
trust boundary configuration, 319–321
verifying, 324–326
voice VLAN ID (VVID), 308
voice VLANs, 308–312
  configuring, 308–311
  verifying, 311–312
VoIP (Voice over IP). See IP telephony
VRRP (Virtual Router Redundancy Protocol), 277–280
vrrp authentication command, 278, 297
vrrp ip command, 278, 297
vrrp preempt command, 278, 297
vrrp priority command, 278, 297
vrrp timers advertise command, 278, 297
vrrp timers learn command, 278, 297
VTP (VLAN Trunking Protocol), 67, 74, 88–92
  advertisements, 89–92
  configuring, 92–97
    example of, 96
    management domains, 93
    modes, 93–95
    versions, 95–96
  viewing status, 96–97
  domains, 88
  modes, 88–89
  pruning, 97–100
  synchronization problems, 90
  troubleshooting, 100–101
vtp domain command, 103
vtp mode command, 103
vtp mode transparent global configuration command, 67
vtp password command, 103
vtp pruning command, 103
vtp version command, 103
VVID (voice VLAN ID), 308

W
“wall warts,” 304
WAN PHY, 47
web interface, securing, 386
weighted load balancing, 284
wired LANs, wireless LANs versus, 335
wireless LAN controller. See WLC (wireless LAN controller)
WLANs (wireless LANs)
  access points, explained, 338–344
  architecture of, 344–354
    Cisco Unified Wireless Network Architecture, 346–354
    traditional architecture, 344–346
  cells (coverage areas), 341–344
  collisions, avoiding, 336–338
  switchport configuration, 361–364
    for autonomous APs, 361–362
    for LAPs, 362–363
    for WLCs, 363–364
  wired LANs versus, 335
WLC (wireless LAN controller), 348
  configuring switchports for, 363–364
  functions of, 349–350
  intercontroller roaming, 356–361
  intracontroller roaming, 355–356
  mobility groups, 356–361