CISCO

CCNP SWITCH Exam Preparation

CCNP SWITCH 642-813

Official Certification Guide

- ✔ Master the **CCNP® SWITCH 642-813** exam with this official study guide
- ✔ Assess your knowledge with **chapter-opening quizzes**
- ✔ Review key concepts with **Exam Preparation Tasks**
- ✔ Practice with **realistic exam questions** on the CD-ROM

ciscopress.com

David Hucaby, CCIE® No. 4594

CCNP SWITCH 642-813 Official Certification Guide

David Hucaby, CCIE No. 4594

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

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.

ISBN-13: 978-1-58720-243-8

ISBN-10: 1-58720-243-3

1. Virtual LANs—Examinations—Study guides. 2. Telecommunications engineers—Certification. 3. Cisco Systems, Inc.—Examinations—Study guides. I. Title.

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.

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 fiexible 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

Exam Topic	Part of This Book Where Exam Topic Is Covered
Implement VLAN-based solution, given a network design and a set of requirements	
Determine network resources needed for implementing VLAN-based solution on a network. Create a VLAN-based implementation plan. Create a VLAN-based verification plan. Configure switch-to-switch connectivity for the VLAN-based solution. Configure loop prevention for the VLAN-based solution. Configure access ports for the VLAN-based solution. Verify the VLAN-based solution was implemented properly using **show** and **debug** commands. Document results of VLAN implementation and verification	Part II, "Building a Campus Network" Chapters 2–10
Implement a security extension of a Layer 2 solution, given a network design and a set of requirements	
Determine network resources needed for implementing a security solution. Create a implementation plan for the security solution. Create a verification plan for the security solution. Configure port security features. Configure general switch security features. Configure private VLANs. Configure VACL and PACL. Verify the security solution was implemented properly using **show** and **debug** commands. Document results of security implementation and verification.	Part V, "Securing Switched Networks" Chapters 16–17

Table I-1—CCNP SWITCH Exam Topics

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

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 BPDUs, 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.

CHAPTER 9

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*

Foundation Topics Section	Questions Covered in This Section
Protecting Against Unexpected BPDUs	1–5
Protecting Against Sudden Loss of BPDUs	6–11
Using BPDU Filtering to Disable STP on a Port	12
Troubleshooting STP Protection	13

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 uplink 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 udld**
    b. **udld reset**
    c. **no udld**
    d. **show udld errdisable**

Foundation Topics

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 BPDU 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 PortFast 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 interface 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 errdisable state.

You should use BPDU Guard on all switch ports where STP PortFast is enabled. This prevents any possibility that a switch will be added to the port, either intentionally or by mistake. 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 detected 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 without any STP activity.

You never should enable BPDU Guard on any switch uplink where the root bridge is located. 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 participating 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 domain. The STP topology's integrity then depends on a continuous and regular flow of BPDUs from the root.

What happens if a switch doesn't receive BPDUs in a timely manner or when it doesn't receive 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 Errdisable 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 configuration command:

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

For normal mode, use the **enable** keyword; for aggressive mode, use the **aggressive** keyword. 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 following 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 interface.

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. Obviously, 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*

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

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*

Key Topic Element	Description	Page Number
Paragraph	Discusses the Root Guard feature	180
Paragraph	Discusses the BPDU Guard feature	181
Paragraph	Discusses the Loop Guard feature	183
Paragraph	Discusses the UDLD feature	184
Paragraph	Explains BPDU filtering	186

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:

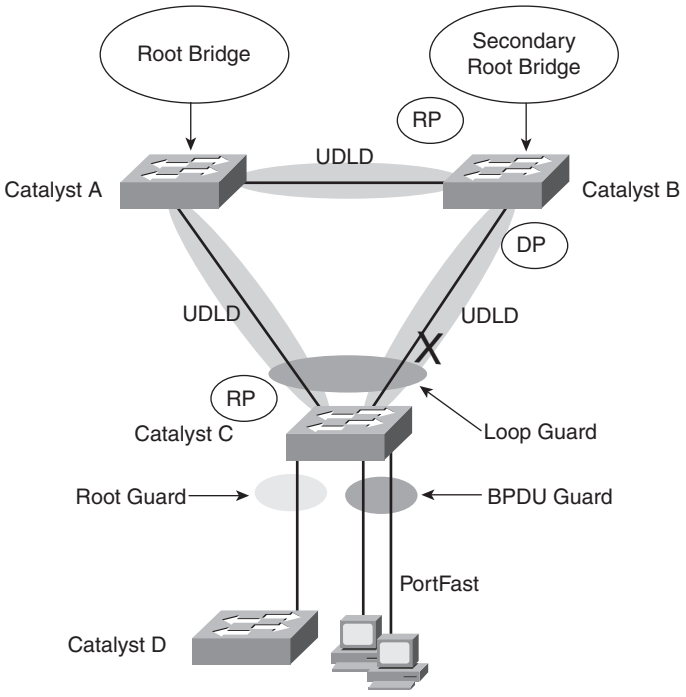
Root Guard, superior BPDU, BPDU Guard, Loop Guard, UDLD, BPDU filtering

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.



Root guard: Apply to ports where root is never expected.

BPDU guard: Apply to all user ports where PortFast is enabled.

Loop guard: Apply to nondesignated ports but okay to apply to all ports.

UDLD: Apply to all fiber-optic links between switches (must be enabled on both ends).

Permissible combinations on a switch port:

Loop guard and UDLD
Root guard and UDLD

Not permissible on a switch port:

Root guard and Loop guard
Root guard and BPDU guard

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*

Task	Global Command Syntax	Interface Command Syntax
Enable Root Guard	—	Switch(config-if)# **spanning-tree guard root**
Enable BPDU Guard	Switch(config)# **spanning-tree portfast bpduguard default**	Switch(config-if)# **spanning-tree bpduguard enable**
Enable Loop Guard	Switch(config)# **spanning-tree loopguard default**	Switch(config-if)# **spanning-tree guard loop**
Enable UDLD	Switch(config)# **udld** {**enable** | **aggressive** | **message time seconds**}	Switch(config-if)# **udld** {**enable** | **aggressive** | **disable**}
Enable BPDU filtering	Switch(config)# **spanning-tree bpdufilter default**	Switch(config-if)# **spanning-tree bpdufilter enable**

Table 9-5 *STP Protection Activity Commands*

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

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

P

Q

R

S

T

U

V

W