CCNP TSHOOT Exam Preparation

CCNP TSHOOT 642-832

Official Certification Guide

- ✔ Master **CCNP® TSHOOT 642-832** exam topics
- ✔ Assess your knowledge with **chapter-opening quizzes**
- ✔ Review key concepts with **Exam Preparation Tasks**
- ✔ Practice with **realistic exam questions** on the CD-ROM

ciscopress.com

Kevin Wallace, CCIE® No. 7945

CCNP TSHOOT 642-832

Official Certification Guide

Kevin Wallace, CCIE No. 7945

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

CCNP TSHOOT 642-832 Official Certification Guide

Kevin Wallace, CCIE No. 7945

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

Printed in the United States of America

Eighth Printing: August 2013

Library of Congress Cataloging-in-Publication Data:

Wallace, Kevin, CCNP.
CCNP TSHOOT 642-832 official certification guide / Kevin Wallace.
p. cm.
Includes index.
ISBN-13: 978-1-58705-844-8
ISBN-10: 1-58705-844-8
1. Computer networks—Management—Examinations—Study guides. 2. Telecommunications engineers—Certification. 3. Cisco Systems, Inc.—Examinations—Study guides. I. Title.
TK5105.8.C57W35 2010
004.6076—dc22

Warning and Disclaimer

This book is designed to provide information about the CCNP TSHOOT Exam (Exam 642-832) 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.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States please contact: **International Sales** international@pearsoned.com

Feedback Information

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

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

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Brett Bartow

Managing Editor: Patrick Kanouse

Senior Project Editor: Tonya Simpson

Business Operation Manager, Cisco Press: Anand Sundaram

Manager Global Certification: Erik Ullanderson

Copy Editors: Gill Editorial Services and Water Crest Publishing, Inc.

Technical Editor: Elan Beer

Proofreader: Williams Woods Publishing Services, LLC

Senior Development Editor: Christopher Cleveland

Editorial Assistant: Vanessa Evans

Book Designer: Louisa Adair

Composition: Mark Shirar

Indexer: Tim Wright

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

About the Author

Kevin Wallace, CCIE No. 7945, is a certified Cisco instructor who holds multiple Cisco certifications, including CCSP, CCVP, CCNP, and CCDP, in addition to multiple security and voice specializations. With Cisco experience dating back to 1989 (beginning with a Cisco AGS+ running Cisco IOS 7.x), Kevin has been a network design specialist for the Walt Disney World Resort, a senior technical instructor for SkillSoft/Thomson NETg/KnowledgeNet, and a network manager for Eastern Kentucky University. Kevin holds a bachelor of science degree in electrical engineering from the University of Kentucky. Kevin has authored multiple books for Cisco Press, including *Routing Video Mentor* and *TSHOOT Video Mentor*, both of which target the current CCNP Routing and Switching certification. Kevin lives in central Kentucky with his wife (Vivian) and two daughters (Stacie and Sabrina).

About the Technical Reviewer

Elan Beer, CCIE No. 1837, CCSI No. 94008, is a senior consultant and Certified Cisco Instructor. His internetworking expertise is recognized internationally through his global consulting and training engagements. As one of the industry's top internetworking consultants and Cisco instructors, Elan has used his expertise for the past 17 years to design, implement, and deploy multiprotocol networks for a wide international clientele. As a senior instructor and course developer, Elan has designed and presented public and implementation-specific technical courses spanning many of today's top technologies. Elan specializes in MPLS, BGP, QoS, and other Internetworking technologies.

Dedications

This book is dedicated to my family. To my beautiful wife Vivian, you have an unbelievably giving spirit. To my daughter Sabrina, you have a keen business mind at only 12 years of age. You're destined for big things. To my daughter Stacie, at the age of 14, you radiate happiness and are maturing into a wonderful young lady.

Acknowledgments

My thanks go out to the team of professionals at Cisco Press. I'm proud to be associated with such a respected organization.

My family is unbelievably supportive of my writing efforts. Thank you to my wife, Vivian, and my daughters, Sabrina and Stacie. You all have been very understanding when I seclude myself to write. Also, I'm grateful to God for surrounding me with such quality people, both personally and professionally.

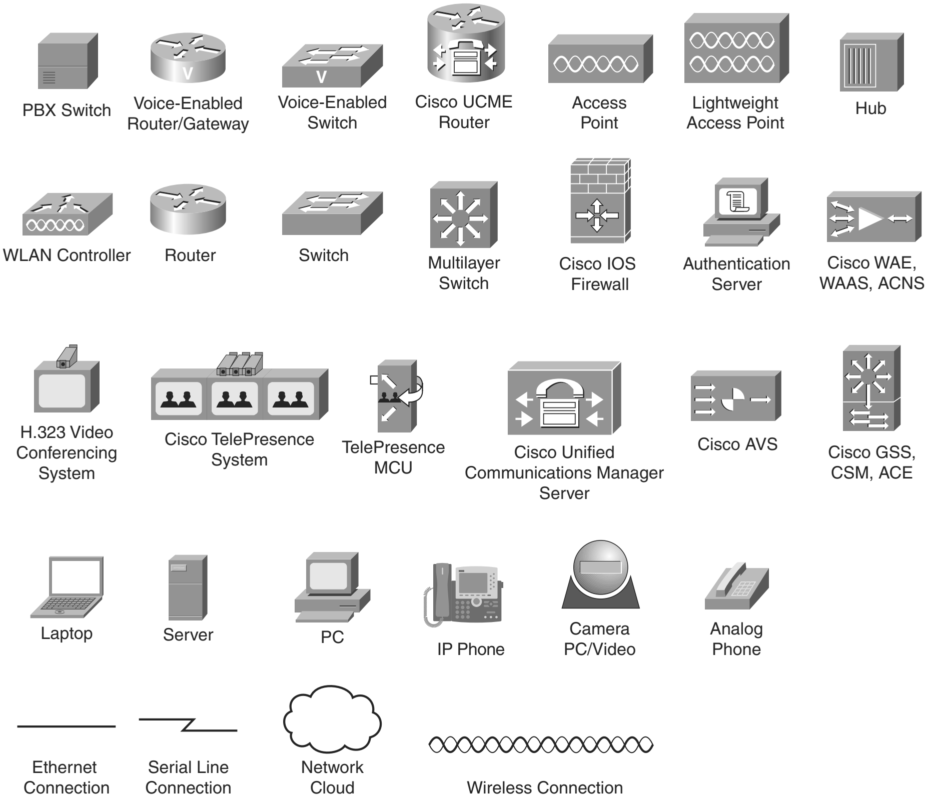
Contents at a Glance

CD-Only Appendixes

Contents

CD-Only Appendixes

Icons Used in This Book



Command Syntax Conventions

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

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

Foreword

CCNP TSHOOT 642-832 Official Certification Guide is an excellent self-study resource for the CCNP TSHOOT 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 TSHOOT exam (Exam 642-832). 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 TSHOOT exam are designed to also make you much more knowledgeable about how to do your job. Although this book and the accompanying CD-ROM 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 TSHOOT 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 TSHOOT exam by using the following methods:

- Covering all of 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 multiple troubleshooting case studies with diagrams and diagnostic output that enhance your ability to resolve trouble tickets presented in the exam environment, in addition to real-world troubleshooting issues you might encounter
- Providing practice exercises on exam topics, presented in each chapter and on the enclosed CD-ROM

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 TSHOOT 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 TSHOOT exam is primarily based on the content of the Cisco TSHOOT course. You should have either taken the course, read through the TSHOOT course material or this book, or have a couple of years of troubleshooting 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 as well, 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 TSHOOT exam might be slightly different than strategies used by other readers, mainly based on the skills, knowledge, and experience you have already obtained. For example, if you have attended the TSHOOT course, you might take a different approach than someone who learned troubleshooting 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 enable you to easily move between 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 TSHOOT exam. The chapters are organized into parts, covering the following topics:

- **Chapter 1, "Introduction to Network Maintenance":** This chapter discusses the importance of proactive maintenance tasks, as opposed to the reactive maintenance required to address a problem. Also discussed in this chapter is a collection of commonly used maintenance approaches.

  Next, this chapter lists common maintenance tasks, emphasizes the importance of regularly scheduled maintenance, and summarizes critical areas of network performance. Finally, this chapter identifies how to compile a set of network maintenance tools that complement your network maintenance plan.

- **Chapter 2, "Introduction to Troubleshooting Processes":** This chapter addresses troubleshooting fundamentals, discusses the benefits of having a structured troubleshooting model, and discusses several popular troubleshooting models.

  Also discussed is each subprocess in a structured troubleshooting approach. Finally, this chapter shows how maintenance processes and troubleshooting process can work in tandem to complement one another.

- **Chapter 3, "The Maintenance and Troubleshooting Toolbox":** This chapter shows how a few readily accessible Cisco IOS commands can be used to quickly gather information, as part of a structured troubleshooting process.

  This chapter also introduces a collection of specialized features, such as SPAN, RSPAN, SMTP, NetFlow, and EEM, which can be used to collect information about a problem.

- **Chapter 4, "Basic Cisco Catalyst Switch Troubleshooting":** This chapter reviews the basics of Layer 2 switch operation and demonstrates a collection of Cisco Catalyst **show** commands that can be used to quickly gather information, as part of a structured troubleshooting process.

  Also, this chapter introduces spanning tree protocol (STP), which allows a Layer 2 topology to have redundant links while avoiding the side effects of a looped Layer 2 topology, such as a broadcast storm. You then learn strategies for troubleshooting an STP issue.

  Finally, troubleshooting an EtherChannel connection is addressed. This chapter concludes with a trouble ticket and an associated topology. You are also given **show** command output (baseline output and output collected after the reported issue occurred). Based on the information provided, you hypothesize an underlying cause for the reported issue and develop a solution. You can then compare your solution with a suggested solution.

- **Chapter 5, "Advanced Cisco Catalyst Switch Troubleshooting":** This chapter begins by contrasting Layer 3 switches and routers. Troubleshooting procedures are also compared for these platforms. Two approaches for routing packets using Layer 3 switches are also discussed. These approaches are using routed ports and using switched virtual interfaces (SVIs).

  Next, this chapter discusses three approaches to providing first-hop router redundancy. Options include HSRP, VRRP, and GLBP. Troubleshooting strategies are discussed for HSRP with suggestions on how to modify those strategies for troubleshooting VRRP and GLBP. Examined next is the architecture of a Cisco Catalyst switch and the different architectural components that could become troubleshooting targets. You are presented with a series of **show** commands used to gather information about different aspects of a switch's performance.

  Finally, this chapter presents you with a trouble ticket and an associated topology. You are also given **show** and **debug** command output (baseline output and output collected after a reported issue occurred). Based on the information provided, you hypothesize an underlying cause for the reported issue and develop a solution. You can then compare your solution with a suggested solution.

- **Chapter 6, "Introduction to Troubleshooting Routing Protocols":** This chapter begins by reviewing basic routing concepts. For example, you examine the changes to a frame's header as that frame's data is routed from one network to another. You see how Layer 2 information can be learned and stored in a router. Cisco Express Forwarding (CEF) is also discussed. Additionally, you are presented with a collection of **show** commands, useful for troubleshooting IP routing.

  Next, this chapter generically reviews how an IP routing protocol's data structures interact with a router's IP routing table. Then, EIGRP's data structures are considered, followed by a review of basic EIGRP operation. Again, you are presented with a collection of **show** and **debug** commands useful for troubleshooting various EIGRP operations.

  Finally, this chapter challenges you with a trouble ticket and an associated topology. You are also given **show** command output. Based on the information provided, you hypothesize an underlying cause for the reported issue and develop a solution. You can then compare your solution with a suggested solution.

- **Chapter 7, "OSPF and Route Redistribution Troubleshooting":** This chapter begins by introducing you to OSPF's routing structures, followed by a review of OSPF operation. You are then presented with a collection of **show** and **debug** commands useful for troubleshooting OSPF operations.

  This chapter next presents you with a trouble ticket and an associated topology. You are also given **show** command output. Based on the information provided, you hypothesize an underlying cause for the reported issues and develop solutions. You can then compare your solutions with the suggested solutions.

  This chapter also introduces the concept of route redistribution and discusses how a route from one routing process can be injected into a different routing process. Common route redistribution troubleshooting targets are identified, along with strategies for troubleshooting route redistribution.

  Finally, this chapter challenges you with another trouble ticket and an associated topology. You are also given **show** command output. Based on the information provided, you hypothesize an underlying cause for the reported issue and develop a solution. You can then compare your solution with a suggested solution.

- **Chapter 8, "Troubleshooting BGP and Router Performance Issues":** This chapter begins by introducing you to BGP's data structures, followed by a review of BGP operation. You are then presented with a collection of **show** and **debug** commands useful for troubleshooting BGP operations.

  This chapter next presents you with a trouble ticket and an associated topology. You are given **show** command output. Based on the information provided, you hypothesize an underlying cause for the reported issue and develop a solution. You can then compare your solutions with the suggested solutions.

  Finally, this chapter discusses how to troubleshoot performance issues on a router, focusing on CPU utilization, packet-switching modes, and memory utilization.

- **Chapter 9, "Security Troubleshooting":** This chapter begins by reviewing various security measures that might be put in place on Cisco routers and switches to protect three different planes of network operation. These planes are the management plane, the control plane, and the data plane. Once you review these security measures, this chapter considers how your troubleshooting efforts might be impacted by having various layers of security in place.

  Next, this chapter describes the basic operation and troubleshooting tips for Cisco IOS firewalls and AAA services. Although complete configuration details for Cisco IOS firewalls and AAA is beyond the scope of the TSHOOT curriculum, as a reference, this chapter does provide a couple of basic configuration examples with an explanation of the syntax used.

  Finally, this chapter presents you with a trouble ticket and an associated topology. You are also given **show** command output and a syntax reference. Based on the information provided, you hypothesize how to correct the reported issues. You can then compare your solutions with the suggested solutions.

- **Chapter 10, "IP Services Troubleshooting":** This chapter begins by reviewing the purpose and basic operation of Network Address Translation (NAT). As a reference, sample topologies are provided, along with their configurations. Common NAT troubleshooting targets are identified, and a syntax reference is provided to aid in troubleshooting NAT issues.

  Next, this chapter reviews Dynamic Host Configuration Protocol (DHCP) operation and various types of DHCP messages. You are given three configuration examples corresponding to the three roles a router might play in a DHCP environment: DHCP relay agent, DHCP client, and DHCP server. Common DHCP troubleshooting targets are reviewed, along with recommended DHCP troubleshooting practices. This section also presents a collection of commands that could prove to be useful in troubleshooting a suspected DHCP issue.

  Finally, this chapter presents you with a trouble ticket and an associated topology. You are also given **show** and **debug** command output, which confirms the reported issue. Then, you are challenged to hypothesize how to correct the reported issue. You can then compare your solution with a suggested solution.

- **Chapter 11, "IP Communications Troubleshooting":** This chapter begins by introducing you to design and troubleshooting considerations that arise when adding voice traffic to a data network. Several protocols are involved when a Cisco IP Phone registers with its call agent in order to place and receive voice calls. You review the function of these protocols along with recommendations for troubleshooting voice issues. One of the major troubleshooting targets for voice networks involves quality of service. Therefore, this chapter provides overview of quality of service configuration, verification, and troubleshooting commands. Additionally, this chapter considers video traffic in an IP network, including video's unique design and troubleshooting challenges.

Also, video-based networks often rely on an infrastructure that supports IP multicasting. Because multicasting has not been addressed in any depth thus far in this book, this chapter serves as a primer to multicast technologies. Included in this primer are commands used to configure, monitor, and troubleshoot multicast networks. The chapter next considers common video troubleshooting issues and recommends resolutions for those issues.

Finally, this chapter presents you with two trouble tickets focused on unified communications. You are presented with a topology used by both trouble tickets, in addition to a collection of **show** command output. For each trouble ticket, you are challenged to hypothesize how to correct the reported issue. You can also compare your solutions with suggested solutions.

- **Chapter 12, "IPv6 Troubleshooting":** This chapter introduces the purpose and structure of IP version 6 (IPv6) addressing. You consider the various types of IPv6 addresses, routing protocols supporting IPv6, and basic syntax for enabling a router to route IPv6 traffic. A sample configuration is provided to illustrate the configuration of a router to support IPv6. Additionally, as an organization is migrating from IPv4 to IPv6, there might be portions of the network that are still running IPv4 with other portions of the network running IPv6. For IPv6 traffic to span an IPv4 portion of the network, one option is to create a tunnel spanning the IPv4 network. Then, IPv6 traffic can travel inside the tunnel to transit the IPv4 network. This section discusses the syntax and provides an example of tunneling IPv6 over an IPv4 tunnel.

  This chapter also contrasts the characteristics of two versions of OSPF, specifically OSPFv2 and OSPFv3. OSPFv3 can support the routing of IPv6 networks, whereas OSPFv2 cannot. OSPFv3 configuration syntax is presented, along with a sample configuration. You are also provided with a collection of verification troubleshooting commands and a listing of common OSPFv3 issues.

  Next, this chapter presents you with a trouble ticket addressing a network experiencing OSPF adjacency issues. You are presented with a collection of **show** and **debug** command output and challenged to resolve a series of misconfigurations. Suggested solutions are provided.

  Also, this chapter contrasts the characteristics of RIP next generation (RIPng) with RIPv2. You are given a set of RIPng configuration commands along with a sample configuration. From a troubleshooting perspective, you compare RIPng troubleshooting commands with those commands used to troubleshoot RIPv1 and RIPv2. This chapter also discusses some of the more common RIPng troubleshooting issues you might encounter.

  Finally, this chapter challenges you to resolve a couple of RIPng issues being observed in a network. Specifically, load balancing and default route advertisements are not behaving as expected. To assist in your troubleshooting efforts, you are armed with a collection of **show** and **debug** command output. Your proposed solutions can then be compared with suggested solutions.

- **Chapter 13, "Advanced Services Troubleshooting":** This chapter introduces you to Cisco's Application Network Services (ANS) architecture. Cisco ANS includes multiple pieces of dedicated equipment aimed at optimizing the performance of network-based applications (for example, improving the response time of a corporate web server for users at a remote office). Although this chapter introduces a collection of Cisco ANS components, the primary focus is on Cisco IOS features that can improve application performance. Specifically, the Cisco IOS features addressed are NetFlow, IP SLAs, NBAR, and QoS.

  Also, this chapter addresses the troubleshooting of wireless networks, and it begins by contrasting autonomous and split-MAC wireless network architectures. Wired network issues that could impact wireless networks are then highlighted. These issues include power, VLAN, security, DHCP, and QoS issues.

- **Chapter 14, "Large Enterprise Network Troubleshooting":** This chapter begins by identifying a collection of technologies that might become troubleshooting targets for a remote office network. The primary technologies focused on are Virtual Private Network (VPN) technologies. Sample syntax is provided for a VPN using IPsec and GRE. Also, several useful **show** commands are provided as a troubleshooting reference.

  Finally, this chapter discusses the troubleshooting of complex networks, and begins by identifying how multiple network technologies map to the seven layers of the OSI model. Also, you are given a list of resources a troubleshooter should have prior to troubleshooting a complex enterprise network. Finally, this chapter reviews key points from all trouble tickets previously presented.

- **Chapter 15, "Final Preparation":** This chapter identifies tools for final exam preparation and helps you develop an effective study plan.

Appendix A has the answers to the "Do I Know This Already" quizzes and an online appendix 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, configuration, and troubleshooting strategies 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 any relevant commands presented in the chapter.

Finally, the companion CD-ROM contains practice CCNP TSHOOT questions to reinforce your understanding of the book's concepts. Be aware that the TSHOOT exam will primarily be made up of trouble tickets you need to resolve. Mastery of the topics covered by the CD-based questions, however, will help equip you with the tools needed to effectively troubleshoot the trouble tickets presented on the exam.

The CD also contains the Memory Table exercises and answer keys.

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 determine what you recall easily and what you do not recall at all.
- By referencing the portions of 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-ROM that has questions covering troubleshooting theory, tools, and methodologies. Familiarity with these troubleshooting resources can help you be more efficient when diagnosing and resolving a reported network issue.

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 TSHOOT 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. Also, you can develop a broader knowledge of the subject matter 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 TSHOOT 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 TSHOOT Exam Topics*

Exam Topics	Chapters Where Exam Topics Are Covered
Maintain and monitor network performance	
Develop a plan to monitor and manage a network Perform network monitoring using IOS tools Perform routine IOS device maintenance Isolate sub-optimal internetwork operation at the correctly defined OSI Model layer	Chapters 1–3 and 14
Troubleshooting IPv4 and IPv6 routing protocols and IP services in a multiprotocol system network	
Troubleshoot EIGRP Troubleshoot OSPF Troubleshoot eBGP Troubleshoot routing redistribution solution Troubleshoot a DHCP client and server solution Troubleshoot NAT Troubleshoot first-hop redundancy protocols Troubleshoot IPv6 routing Troubleshoot IPv6 and IPv4 interoperability	Chapters 5–8, 10, and 12
Troubleshoot switch-based features	
Troubleshoot switch-to-switch connectivity for a VLAN-based solution Troubleshoot loop prevention for a VLAN-based solution Troubleshoot access ports for a VLAN-based solution Troubleshoot private VLANS Troubleshoot port security Troubleshoot general switch security Troubleshoot VACL and PACL Troubleshoot switch virtual interfaces (SVIs) Troubleshoot switch supervisor redundancy Troubleshoot switch support of advanced services Troubleshoot a VoIP support solution Troubleshoot a video support solution	Chapters 4–5, 11, and 13

Table I-1 *CCNP TSHOOT Exam Topics* (*Continued*)

Exam Topics	Chapters Where Exam Topics Are Covered
Troubleshoot Cisco router and switch device hardening	
Troubleshoot Layer 3 security Troubleshoot issues related to ACLs used to secure access to Cisco routers Troubleshoot configuration issues related to accessing an AAA server for authentication purposes Troubleshoot security issues related to IOS services	Chapters 9 and 10

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 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 www.ciscopress.com/title/1587058448, where we publish any information pertinent to how you might use this book differently in light of Cisco's future changes. For example, if Cisco decided 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 page intentionally left blank

This chapter covers the following subjects:

Resolving InterVLAN Routing Issues: This section begins by contrasting Layer 3 switches and routers. Troubleshooting procedures are also compared for these platforms. Lastly, this section discusses two approaches for routing packets using Layer 3 switches: routed ports and Switched Virtual Interfaces (SVIs).

Router Redundancy Troubleshooting: This section discusses three approaches to providing first-hop router redundancy. Options include: Hot Standby Routing Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP). Troubleshooting strategies are discussed for HSRP with suggestions on how to modify those strategies for troubleshooting VRRP and GLBP.

Cisco Catalyst Switch Performance Tuning: This section examines the architecture of a Cisco Catalyst switch and points out different architectural components that could become troubleshooting targets. Also, you are presented with a series of **show** commands used to gather information about different aspects of a switch's performance.

Trouble Ticket: HSRP: This section presents you with a trouble ticket and an associated topology. You are also given **show** and **debug** command output (baseline output and output collected after a reported issue occurred). Based on the information provided, you hypothesize an underlying cause for the reported issue and develop a solution. You can then compare your solution with a suggested solution.

Advanced Cisco Catalyst Switch Troubleshooting

This chapter builds on Chapter 4, "Basic Cisco Catalyst Switch Troubleshooting," by continuing to focus on troubleshooting Cisco Catalyst Switch platforms. Although the term *switch* might conjure up the image of a Layer 2 device, many modern switches can also route. Specifically, many switches can make forwarding decisions based on Layer 3 information (for example, IP address information). Therefore, this chapter starts by discussing a couple of ways to make a Layer 3 (or multilayer) switch perform routing.

Next, because many Layer 3 switches reside in a wiring closet, these switches might very well act as the default gateway for endpoints (for example, user PCs). Rather than having this switch (or perhaps a router at the distribution layer) become a single point of failure for endpoints relying on the IP address maintained by that switch (or router), you can take advantage of a first-hop redundancy protocol. A first-hop redundancy protocol allows clients to continue to reach their default gateway's IP address, even if the Layer 3 switch or router that had been servicing that IP address becomes available. This chapter contrasts three first-hop redundancy protocols and discusses the troubleshooting of first-hop redundancy.

Often a trouble reported by a user comes in some variation of, "The network is slow." Although such a description is less than insightful, troubleshooters are likely to encounter network performance issues resulting in a poor user experience. This chapter focuses on troubleshooting performance problems that originate from a Cisco Catalyst switch.

Finally, this chapter presents another trouble ticket. This trouble ticket describes a first-hop redundancy protocol not operating as expected. Given a collection of **show** and **debug** output, you are challenged to determine the underlying cause of the issue and formulate a solution.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz helps you determine your level of knowledge of this chapter's topics before you begin. Table 5-1 details the major topics discussed in this chapter and their corresponding quiz questions.

Table 5-1 *"Do I Know This Already?" Section-to-Question Mapping*

Foundation Topics Section	Questions
Resolving InterVLAN Routing Issues	1–3

continues

Table 5-1 *"Do I Know This Already?" Section-to-Question Mapping* *(Continued)*

Foundation Topics Section	Questions
Router Redundancy Troubleshooting	4–7
Cisco Catalyst Switch Performance Troubleshooting	8–10

1. What are two differences between Layer 3 switches and routers? (Choose two.)

- **a.** Layer 3 switches do not maintain a routing table.
- **b.** Layer 3 switches usually forward traffic faster than routers.
- **c.** Layer 3 switches support more interface types than routers.
- **d.** Layer 3 switches usually support fewer features than routers.

2. What type of special memory is used by Layer 3 switches, and not routers, that supports very rapid route lookups?

- **a.** NBAR
- **b.** TCAM
- **c.** NetFlow
- **d.** MIB

3. What type of interface can be created on a Layer 3 switch to support routing between VLANs on that switch?

- **a.** BVI
- **b.** VPI
- **c.** SVI
- **d.** VCI

4. What is the default priority for an HSRP interface?

- **a.** 0
- **b.** 100
- **c.** 256
- **d.** 1000

5. What is the name for the router in a VRRP virtual router group that is actively forwarding traffic on behalf of the virtual router group?

- **a.** virtual forwarder
- **b.** active virtual gateway
- **c.** virtual router master
- **d.** active virtual forwarder

6. Which of the following statements is true concerning GLBP?

   a. GLBP is an industrial-standard first-hop redundancy protocol.
   b. GLBP allows multiple routers to simultaneously forward traffic for the group of GLBP routers.
   c. The active virtual forwarder in a GLBP group is responsible for responding to ARP requests with different MAC addresses.
   d. A GLBP group has multiple active virtual gateways.

7. Which of the following are a Cisco proprietary first-hop router redundancy protocols? (Choose two.)

   a. HSRP
   b. VRRP
   c. GLBP
   d. DSCP

8. What are two components of a switch's control plane? (Choose two.)

   a. Backplane
   b. Memory
   c. CPU
   d. Forwarding logic

9. Which three of the following are situations when a switch's TCAM would punt a packet to the switch's CPU? (Choose the three best answers.)

   a. OSPF sends a multicast routing update.
   b. An administrator Telnets to a switch.
   c. An ACL is applied to a switch port.
   d. A switch's TCAM has reached capacity.

10. The output of a **show processes cpu** command on a switch displays the following in the first line of the output:

    ```
    CPU utilization for five seconds: 10%/7%; one minute: 12%; five minutes: 6%
    ```

    Based on the output, what percent of the switch's CPU is being consumed with interrupts?

    a. 10 percent
    b. 7 percent
    c. 12 percent
    d. 6 percent

Foundation Topics

Resolving InterVLAN Routing Issues

As mentioned in Chapter 4, "Basic Cisco Catalyst Switch Troubleshooting," for traffic to pass from one VLAN to another VLAN, that traffic has to be routed. Several years ago, one popular approach to performing interVLAN routing with a Layer 2 switch was to create a *router on a stick* topology, where a Layer 2 switch is interconnected with a router via a trunk connection, as seen in Figure 5-1.

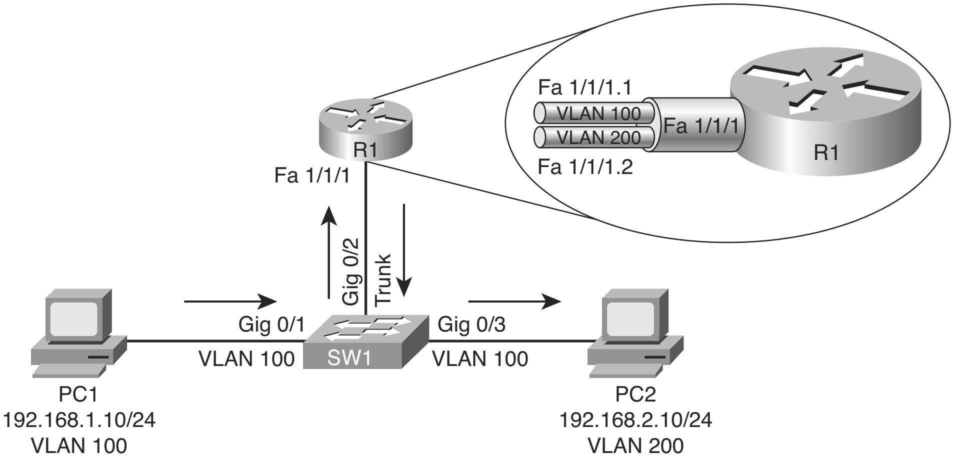


Figure 5-1 *Router on a Stick*

In Figure 5-1, router R1's Fast Ethernet 1/1/1 interface has two subinterfaces, one for each VLAN. Router R1 can route between VLANs 100 and 200, while simultaneously receiving and transmitting traffic over the trunk connection to the switch.

More recently, many switches have risen above their humble Layer 2 beginnings and started to route traffic. Some literature refers to these switches that can route as *Layer 3 switches*. Other sources might call such switches *multilayer switches*, because of the capability of a switch to make forwarding decisions based on information from multiple layers of the OSI model.

This section refers to these switches as Layer 3 switches because the focus is on the capability of the switches to route traffic based on Layer 3 information (that is, IP address information). Specifically, this section discusses troubleshooting Layer 3 switch issues and contrasts troubleshooting a Layer 3 switch versus a router.

Contrasting Layer 3 Switches with Routers

Because a Layer 3 switch performs many of the same functions as a router, it is important for a troubleshooter to distinguish between commonalities and differences in these two platforms.

Table 5-2 lists the characteristics that Layer 3 switches and routers have in common, as well as those characteristics that differ.

Table 5-2 *Layer 3 Switch and Router Characteristics: Compare and Contrast*

Key Topic

Layer 3 Switch/Router Shared Characteristics	Layer 3 Switch/Router Differentiating Characteristics
Both can build and maintain a routing table using both statically configured routes and dynamic routing protocols.	Routers usually support a wider selection of interface types (for example, non-Ethernet interfaces).
Both can make packet forwarding decisions based on Layer 3 information (for example, IP addresses).	Switches leverage application-specific integrated circuits (ASIC) to approach wire speed throughput. Therefore, most Layer 3 switches can forward traffic faster than their router counterparts.
	A Cisco IOS version running on routers typically supports more features than a Cisco IOS version running on a Layer 3 switch, because many switches lack the specialized hardware required to run many of the features available on a router.

Control Plane and Data Plane Troubleshooting

Many router and Layer 3 switch operations can be categorized as control plane or data plane operations. For example, routing protocols operate in a router's control plane, whereas the actual forwarding of data is handled by a router's data plane.

Fortunately, the processes involved in troubleshooting control plane operations are identical on both Layer 3 switch and router platforms. For example, the same command-line interface (CLI) commands could be used to troubleshoot an Open Shortest Path First (OSPF) issue on both types of platforms.

Data plane troubleshooting, however, can vary between Layer 3 switches and routers. For example, if you were troubleshooting data throughput issues, the commands you issued might vary between types of platforms, because Layer 3 switches and routers have fundamental differences in the way traffic is forwarded through the device.

First, consider how a router uses Cisco Express Forwarding (CEF) to efficiently forward traffic through a router. CEF creates a couple of tables that reside at the data plane. These are the *forwarding information base* (FIB) and the *adjacency table*. These tables are constructed from information collected from the router's control plane (for example, the control plane's IP routing table and Address Resolution Protocol [ARP] cache). When troubleshooting a router, you might check control plane operations with commands such as **show ip route**. However, if the observed traffic behavior seems to contradict information shown in the output of control plane verification commands, you might want to examine information contained in the router's CEF Forwarding Information Base (FIB) and adjacency tables. You can use the commands presented in Table 5-3 to view information contained in a router's FIB and adjacency table.

Key Topic

Table 5-3 *Router Data Plan Verification Commands*

Command	Description
show ip cef	Displays the router's Layer 3 forwarding information, in addition to multicast, broadcast, and local IP addresses.
show adjacency	Verifies that a valid adjacency exists for a connected host.

Example 5-1 and Example 5-2 provide sample output from the **show ip cef** and **show adjacency** commands, respectively.

Example 5-1 **show ip cef** *Command Output*

```
R4# show ip cef
Prefix               Next Hop             Interface
0.0.0.0/0            10.3.3.1             FastEthernet0/0
0.0.0.0/32           receive
10.1.1.0/24          10.3.3.1             FastEthernet0/0
10.1.1.2/32          10.3.3.1             FastEthernet0/0
10.3.3.0/24          attached             FastEthernet0/0
10.3.3.0/32          receive
10.3.3.1/32          10.3.3.1             FastEthernet0/0
10.3.3.2/32          receive
10.3.3.255/32        receive
10.4.4.0/24          10.3.3.1             FastEthernet0/0
10.5.5.0/24          10.3.3.1             FastEthernet0/0
10.7.7.0/24          10.3.3.1             FastEthernet0/0
10.7.7.2/32          10.3.3.1             FastEthernet0/0
10.8.8.0/24          attached             FastEthernet0/1
10.8.8.0/32          receive
10.8.8.1/32          receive
10.8.8.4/32          10.8.8.4             FastEthernet0/1
10.8.8.5/32          10.8.8.5             FastEthernet0/1
10.8.8.6/32          10.8.8.6             FastEthernet0/1
10.8.8.7/32          10.8.8.7             FastEthernet0/1
10.8.8.255/32        receive
192.168.0.0/24       10.3.3.1             FastEthernet0/0
224.0.0.0/4          drop
224.0.0.0/24         receive
255.255.255.255/32   receive
```

Example 5-2 **show adjacency** *Command Output*

```
R4# show adjacency
Protocol  Interface                  Address
IP        FastEthernet0/0            10.3.3.1(21)
IP        FastEthernet0/1            10.8.8.6(5)
IP        FastEthernet0/1            10.8.8.7(5)
IP        FastEthernet0/1            10.8.8.4(5)
IP        FastEthernet0/1            10.8.8.5(5)
```

Although many Layer 3 switches also leverage CEF to efficiently route packets, some Cisco Catalyst switches take the information contained in CEF's FIB and adjacency table and compile that information into Ternary Content Addressable Memory (TCAM). This special memory type uses a mathematical algorithm to very quickly look up forwarding information.

The specific way a switch's TCAM operates depends on the switch platform. However, from a troubleshooting perspective, you can examine information stored in a switch's TCAM using the **show platform** series of commands on Cisco Catalyst 3560, 3750, and 4500 switches. Similarly, TCAM information for a Cisco Catalyst 6500 switch can be viewed with the **show mls cef** series of commands.

Comparing Routed Switch Ports and Switched Virtual Interfaces

On a router, an interface often has an IP address, and that IP address might be acting as a default gateway to hosts residing off of that interface. However, if you have a Layer 3 switch with multiple ports belonging to a VLAN, where should the IP address be configured?

You can configure the IP address for a collection of ports belonging to a VLAN under a virtual VLAN interface. This virtual VLAN interface is called a *Switched Virtual Interface* (SVI). Figure 5-2 shows a topology using SVIs, and Example 5-3 shows the corresponding configuration. Notice that two SVIs are created: one for each VLAN (that is, VLAN 100 and VLAN 200). An IP address is assigned to an SVI by going into interface configuration mode for a VLAN. In this example, because both SVIs are local to the switch, the switch's routing table knows how to forward traffic between members of the two VLANs.

Example 5-3 *SVI Configuration*

Key Topic

```
Cat3550# show run
...OUTPUT OMITTED...
!
interface GigabitEthernet0/7
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/8
 switchport access vlan 100
 switchport mode access
```

```
!
interface GigabitEthernet0/9
 switchport access vlan 200
 switchport mode access
!
interface GigabitEthernet0/10
 switchport access vlan 200
 switchport mode access
!
...OUTPUT OMITTED...
!
interface Vlan100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan200
 ip address 192.168.2.1 255.255.255.0
```

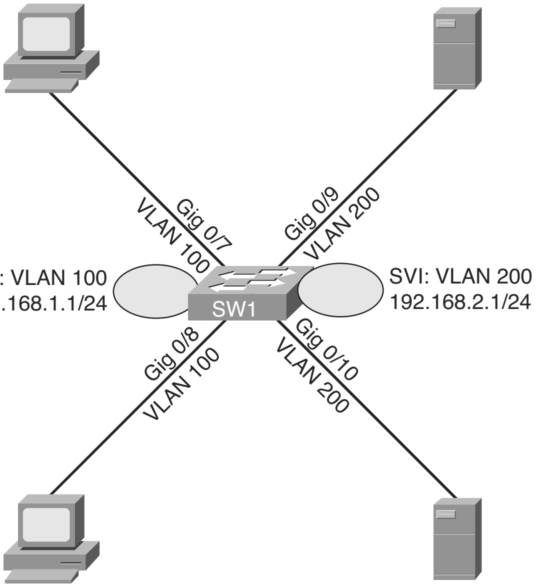


Figure 5-2 *SVI Used for Routing*

Although SVIs can route between VLANs configured on a switch, a Layer 3 switch can be configured to act more as a router (for example, in an environment where you are replacing a router with a Layer 3 switch) by using *routed ports* on the switch. Because the ports on many Cisco Catalyst switches default to operating as switch ports, you can issue the **no switchport** command in interface configuration mode to convert a switch port to a routed port. Figure 5-3 and Example 5-4 illustrate a Layer 3 switch with its Gigabit Ethernet 0/9 and 0/10 ports configured as routed ports.

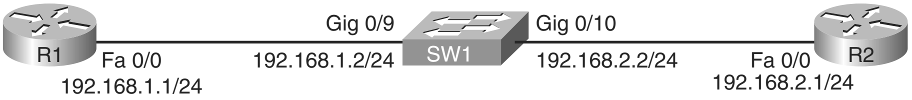


Figure 5-3 *Routed Ports on a Layer 3 Switch*

Example 5-4 *Configuration for Routed Ports on a Layer 3 Switch*

```
Cat3550# show run
...OUTPUT OMITTED...
!
interface GigabitEthernet0/9
 no switchport
 ip address 192.168.1.2 255.255.255.0
!
interface GigabitEthernet0/10
 no switchport
 ip address 192.168.2.2 255.255.255.0
!
...OUTPUT OMITTED...
```

When troubleshooting Layer 3 switching issues, keep the following distinctions in mind between SVIs and routed ports:

Key Topic

- A routed port is considered to be in the down state if it is not operational at both Layer 1 and Layer 2.
- An SVI is considered to be in a down state only when none of the ports in the corresponding VLAN are active.
- A routed port does not run switch port protocols such as Spanning Tree Protocol (STP) or Dynamic Trunking Protocol (DTP).

Router Redundancy Troubleshooting

Many devices, such as PCs, are configured with a *default gateway*. The default gateway parameter identifies the IP address of a next-hop router. As a result, if that router were to become unavailable, devices that relied on the default gateway's IP address would be unable to send traffic off their local subnet.

Fortunately, Cisco offers technologies that provide next-hop gateway redundancy. These technologies include HSRP, VRRP, and GLBP.

This section reviews the operation of these three *first-hop redundancy protocols* and provides a collection of Cisco IOS commands that can be used to troubleshoot an issue with one of these three protocols.

Note that although this section discusses *router* redundancy, keep in mind that the term *router* is referencing a device making forwarding decisions based on Layer 3 information.

Therefore, in your environment, a Layer 3 switch might be used in place of a router to support HSRP, VRRP, or GLBP.

HSRP

Hot Standby Router Protocol (HSRP) uses virtual IP and MAC addresses. One router, known as the *active router*, services requests destined for the virtual IP and MAC addresses. Another router, known as the *standby router*, can service such requests in the event the active router becomes unavailable. Figure 5-4 illustrates a basic HSRP topology.

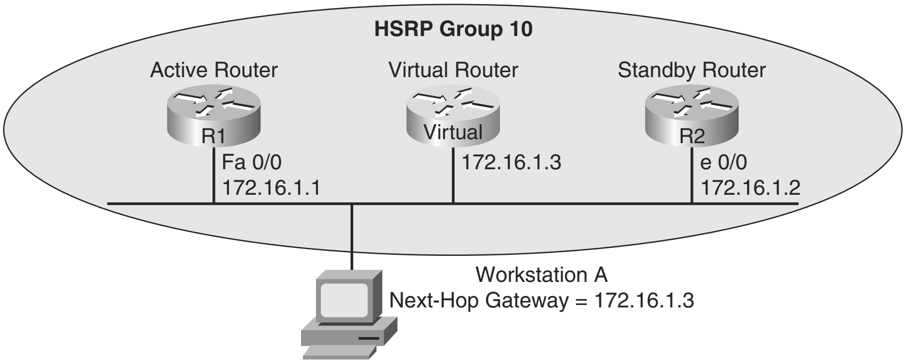


Figure 5-4 *Basic HSRP Operation*

Examples 5-5 and 5-6 show the HSRP configuration for routers R1 and R2.

Key Topic

Example 5-5 *HSRP Configuration on Router R1*

```
R1# show run
...OUTPUT OMITTED...
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 standby 10 ip 172.16.1.3
 standby 10 priority 150
 standby 10 preempt
...OUTPUT OMITTED...
```

Key Topic

Example 5-6 *HSRP Configuration on Router R2*

```
R2# show run
...OUTPUT OMITTED...
interface Ethernet0/0
 ip address 172.16.1.2 255.255.255.0
 standby 10 ip 172.16.1.3
...OUTPUT OMITTED...
```

Notice that both routers R1 and R2 have been configured with the same virtual IP address of 172.16.1.3 for an HSRP group of 10. Router R1 is configured to be the active router with the **standby 10 priority 150** command. Router R2 has a default HSRP priority of 100 for group 10, and with HSRP, higher priority values are more preferable. Also, notice that router R1 is configured with the **standby 10 preempt** command, which means that if router R1 loses its active status, perhaps because it is powered off, it will regain its active status when it again becomes available.

Converging After a Router Failure

By default, HSRP sends hello messages every three seconds. Also, if the standby router does not hear a hello message within ten seconds by default, the standby router considers the active router to be down. The standby router then assumes the active role.

Although this ten-second convergence time applies for a router becoming unavailable for a reason such as a power outage or a link failure, convergence happens more rapidly if an interface is administratively shut down. Specifically, an active router sends a *resign* message if its active HSRP interface is shut down.

Also, consider the addition of another router to the network segment whose HSRP priority for group 10 is higher than 150. If it were configured for preemption, the newly added router would send a *coup* message, to inform the active router that the newly added router was going to take on the active role. If, however, the newly added router were not configured for preemption, the currently active router would remain the active router.

HSRP Verification and Troubleshooting

When verifying an HSRP configuration or troubleshooting an HSRP issue, you should begin by determining the following information about the HSRP group under inspection:

- Which router is the active router
- Which routers, if any, are configured with the preempt option
- What is the virtual IP address
- What is the virtual MAC address

The **show standby brief** command can be used to show a router's HSRP interface, HSRP group number, and preemption configuration. Additionally, this command identifies the router that is currently the active router, the router that is currently the standby router, and the virtual IP address for the HSRP group. Examples 5-7 and 5-8 show the output from the **show standby brief** command issued on routers R1 and R2, where router R1 is currently the active router.

Example 5-7 **show standby brief** *Command Output on Router R1*

```
R1# show standby brief
                       P indicates configured to preempt.
                       |
Interface   Grp  Prio P State    Active          Standby         Virtual IP
Fa0/0       10   150  P Active   local           172.16.1.2      172.16.1.3
```

Example 5-8 **show standby brief** *Command Output on Router R2*

```
R2# show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Prio P State    Active          Standby         Virtual IP
Et0/0       10   100    Standby  172.16.1.1      local           172.16.1.3
```

In addition to an interface's HSRP group number, the interface's state, and the HSRP group's virtual IP address, the **show standby** *interface_id* command also displays the HSRP group's virtual MAC address. Issuing this command on router R1, as shown in Example 5-9, shows that the virtual MAC address for HSRP group 10 is **0000.0c07.ac0a**.

Example 5-9 **show standby fa 0/0** *Command Output on Router R1*

```
R1# show standby fa 0/0
FastEthernet0/0 - Group 10
  State is Active
    1 state change, last state change 01:20:00
  Virtual IP address is 172.16.1.3
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.044 secs
  Preemption enabled
  Active router is local
  Standby router is 172.16.1.2, priority 100 (expires in 8.321 sec)
  Priority 150 (configured 150)
  IP redundancy name is "hsrp-Fa0/0-10" (default)
```

The default virtual MAC address for an HSRP group, as seen in Figure 5-5, is based on the HSRP group number. Specifically, the virtual MAC address for an HSRP group begins with a vendor code of **0000.0c**, followed with a well-known HSRP code of **07.ac**. The last two hexadecimal digits are the hexadecimal representation of the HSRP group number. For example, an HSRP group of 10 yields a default virtual MAC address of **0000.0c07.ac0a**, because **10** in decimal equates to **0a** in hexadecimal.

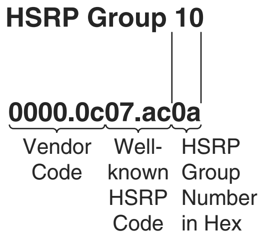


Figure 5-5 *HSRP Virtual MAC Address*

Once you know the current HSRP configuration, you might then check to see if a host on the HSRP virtual IP address' subnet can ping the virtual IP address. Based on the topology previously shown in Figure 5-4, Example 5-10 shows a successful ping from Workstation A.

Example 5-10 *Ping Test from Workstation A to the HSRP Virtual IP Address*

```
C:\>ping 172.16.1.3

Pinging 172.16.1.3 with 32 bytes of data:


Reply from 172.16.1.3: bytes=32 time=2ms TTL=255
Reply from 172.16.1.3: bytes=32 time=1ms TTL=255
Reply from 172.16.1.3: bytes=32 time=1ms TTL=255
Reply from 172.16.1.3: bytes=32 time=1ms TTL=255


Ping statistics for 172.16.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

A client could also be used to verify the appropriate virtual MAC address learned by the client corresponding to the virtual MAC address reported by one of the HSRP routers. Example 5-11 shows Workstation A's ARP cache entry for the HSRP virtual IP address of 172.16.1.3. Notice in the output that the MAC address learned via ARP does match the HSRP virtual MAC address reported by one of the HSRP routers.

Example 5-11 *Workstation A's ARP Cache*

```
C:\>arp -a



Interface: 172.16.1.4 --- 0x4
  Internet Address      Physical Address      Type
  172.16.1.3            00-00-0c-07-ac-0a     dynamic
```

You can use the **debug standby terse** command to view important HSRP changes, such as a state change. Example 5-12 shows this **debug** output on router R2 because router R1's Fast Ethernet 0/0 interface is shut down. Notice that router R2's state changes from Standby to Active.

Example 5-12 **debug standby terse** *Command Output on Router R2: Changing HSRP to Active*

```
R2#
*Mar  1 01:25:45.930: HSRP: Et0/0 Grp 10 Standby: c/Active timer expired
  (172.16.1.1)
```

```
*Mar  1 01:25:45.930: HSRP: Et0/0 Grp 10 Active router is local, was 172.16.1.1
*Mar  1 01:25:45.930: HSRP: Et0/0 Grp 10 Standby router is unknown, was local
*Mar  1 01:25:45.930: HSRP: Et0/0 Grp 10 Standby -> Active
*Mar  1 01:25:45.930: %HSRP-6-STATECHANGE: Ethernet0/0 Grp 10 state Standby ->
   Active
*Mar  1 01:25:45.930: HSRP: Et0/0 Grp 10 Redundancy "hsrp-Et0/0-10" state Standby
   -> Active
*Mar  1 01:25:48.935: HSRP: Et0/0 Grp 10 Redundancy group hsrp-Et0/0-10 state
   Active -> Active
*Mar  1 01:25:51.936: HSRP: Et0/0 Grp 10 Redundancy group hsrp-Et0/0-10 state
   Active -> Active
```

When router R1's Fast Ethernet 0/0 interface is administratively brought up, router R1 reassumes its previous role as the active HSRP router for HSRP group 10, because router R1 is configured with the preempt option. The output shown in Example 5-13 demonstrates how router R2 receives a coup message, letting router R2 know that router R1 is taking back its active role.

Example 5-13 **debug standby terse** *Command Output on Router R2: Changing HSRP to Standby*

```
R2#
*Mar  1 01:27:57.979: HSRP: Et0/0 Grp 10 Coup   in  172.16.1.1 Active  pri 150
  vIP 172.16.1.3
*Mar  1 01:27:57.979: HSRP: Et0/0 Grp 10 Active: j/Coup rcvd from higher pri
   router (150/172.16.1.1)
*Mar  1 01:27:57.979: HSRP: Et0/0 Grp 10 Active router is 172.16.1.1, was local
*Mar  1 01:27:57.979: HSRP: Et0/0 Grp 10 Active -> Speak
*Mar  1 01:27:57.979: %HSRP-6-STATECHANGE: Ethernet0/0 Grp 10 state Active -> Speak
*Mar  1 01:27:57.979: HSRP: Et0/0 Grp 10 Redundancy "hsrp-Et0/0-10" state Active
   -> Speak
*Mar  1 01:28:07.979: HSRP: Et0/0 Grp 10 Speak: d/Standby timer expired (unknown)
*Mar  1 01:28:07.979: HSRP: Et0/0 Grp 10 Standby router is local
*Mar  1 01:28:07.979: HSRP: Et0/0 Grp 10 Speak -> Standby
*Mar  1 01:28:07.979: HSRP: Et0/0 Grp 10 Redundancy "hsrp-Et0/0-10" state Speak
   -> Standby
```

VRRP

Virtual Router Redundancy Protocol (VRRP), similar to HSRP, allows a collection of routers to service traffic destined for a single IP address. Unlike HSRP, the IP address serviced by a VRRP group does not have to be a virtual IP address. The IP address can be the address of a physical interface on the *virtual router master*, which is the router responsible for forwarding traffic destined for the VRRP group's IP address. A VRRP group can have multiple routers acting as *virtual router backups*, as shown in Figure 5-6, any of which could take over in the event of the virtual router master becoming unavailable.

Key Topic

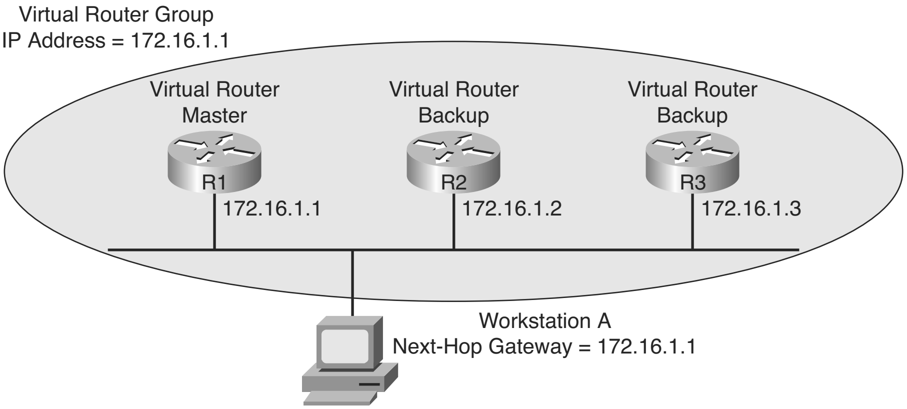


Figure 5-6 *Basic VRRP Operation*

GLBP

Gateway Load Balancing Protocol (GLBP) can load balance traffic destined for a next-hop gateway across a collection of routers, known as a *GLBP group*. Specifically, when a client sends an Address Resolution Protocol (ARP) request, in an attempt to determine the MAC address corresponding to a known IP address, GLBP can respond with the MAC address of one member of the GLBP group. The next such request would receive a response containing the MAC address of a different member of the GLBP group, as depicted in Figure 5-7. Specifically, GLBP has one *active virtual gateway* (AVG), which is responsible for replying to ARP requests from hosts. However, multiple routers acting as *active virtual forwarders* (AVFs) can forward traffic.

Key Topic

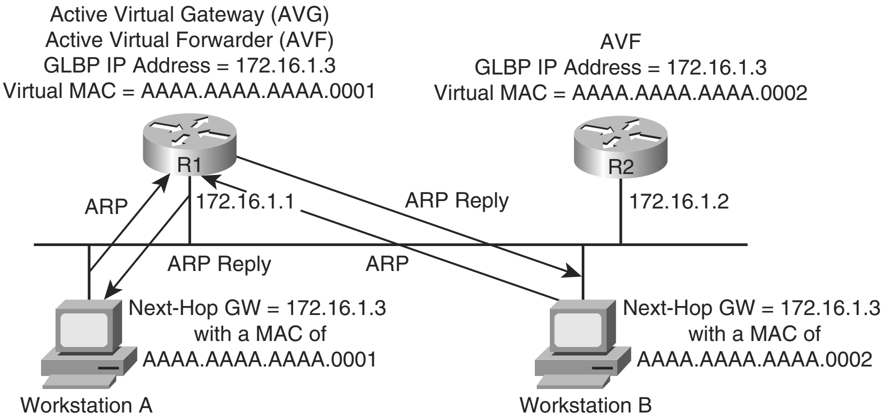


Figure 5-7 *Basic GLBP Operation*

Troubleshooting VRRP and GLBP

Because VRRP and GLBP perform a similar function to HSRP, you can use a similar troubleshooting philosophy. Much like HSRP's **show standby brief** command, similar information can be gleaned for VRRP operation with the **show vrrp brief** command and for GLBP operation with the **show glbp brief** command.

Although HSRP, VRRP, and GLBP have commonalities, it is important for you as a troubleshooter to understand the differences. Table 5-4 compares several characteristics of these first-hop router redundancy protocols.

Key Topic

Table 5-4 *Comparing HSRP, VRRP, and GLBP*

Characteristic	**HSRP**	**VRRP**	**GLBP**
Cisco proprietary	Yes	No	Yes
Interface IP address can act as virtual IP address	No	Yes	No
More than one router in a group can simultaneously forward traffic for that group	No	No	Yes
Hello timer default value	3 seconds	1 second	3 seconds

Cisco Catalyst Switch Performance Troubleshooting

Switch performance issues can be tricky to troubleshoot, because the problem reported is often subjective. For example, if a user reports that the network is running "slow," the user's perception might mean that the network is slow compared to what he expects. However, network performance might very well be operating at a level that is hampering productivity and at a level that is indeed below its normal level of operation. At that point, as part of the troubleshooting process, you need to determine what network component is responsible for the poor performance. Rather than a switch or a router, the user's client, server, or application could be the cause of the performance issue.

If you do determine that the network performance is not meeting technical expectations (as opposed to user expectations), you should isolate the source of the problem and diagnose the problem on that device. This section assumes that you have isolated the device causing the performance issue, and that device is a Cisco Catalyst switch.

Cisco Catalyst Switch Troubleshooting Targets

Cisco offers a variety of Catalyst switch platforms, with different port densities, different levels of performance, and different hardware. Therefore, troubleshooting one of these switches can be platform dependent. Many similarities do exist, however. For example, all Cisco Catalyst switches include the following hardware components:

Key Topic

- **Ports:** A switch's ports physically connect the switch to other network devices. These ports (also known as *interfaces*) allow a switch to receive and transmit traffic.
- **Forwarding logic:** A switch contains hardware that makes forwarding decisions. This hardware rewrites a frame's headers.
- **Backplane:** A switch's backplane physically interconnects a switch's ports. Therefore, depending on the specific switch architecture, frames flowing through a switch

enter via a port (that is, the ingress port), flow across the switch's backplane, and are forwarded out of another port (that is, an egress port).

- **Control plane:** A switch's CPU and memory reside in a control plane. This control plane is responsible for running the switch's operating system.

Figure 5-8 depicts these switch hardware components. Notice that the control plane does not directly participate in frame forwarding. However, the forwarding logic contained in the forwarding hardware comes from the control plane. Therefore, there is an indirect relationship between frame forwarding and the control plane. As a result, a continuous load on the control plane could, over time, impact the rate at which the switch forwards frames. Also, if the forwarding hardware is operating at maximum capacity, the control plane begins to provide the forwarding logic. So, although the control plane does not architecturally appear to impact switch performance, it should be considered when troubleshooting.

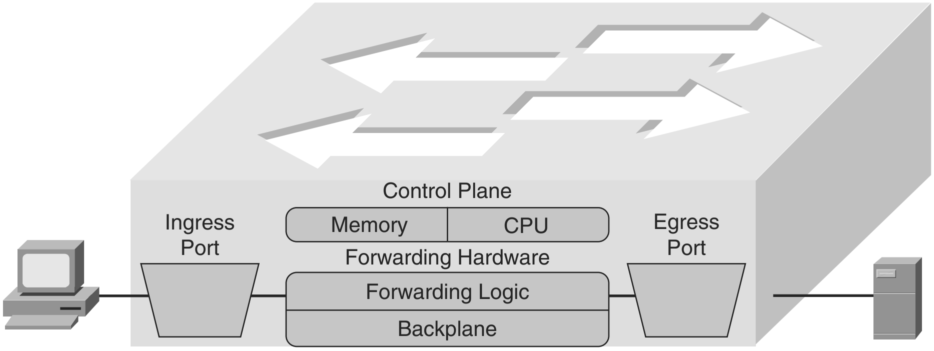


Figure 5-8 *Cisco Catalyst Switch Hardware Components*

The following are two common troubleshooting targets to consider when diagnosing a suspected switch issue:

- Port errors
- Mismatched duplex settings

The sections that follow evaluate these target areas in greater detail.

Port Errors

When troubleshooting a suspected Cisco Catalyst switch issue, a good first step is to check port statistics. For example, examining port statistics can let a troubleshooter know if an excessive number of frames are being dropped. If a TCP application is running slow, the reason might be that TCP flows are going into *TCP slow start*, which causes the window size, and therefore the bandwidth efficiency, of TCP flows to be reduced. A common reason that a TCP flow enters slow start is packet drops. Similarly, packet drops for a UDP flow used for voice or video could result in noticeable quality degradation, because dropped UDP segments are not retransmitted.

Although dropped frames are most often attributed to network congestion, another possibility is that the cabling could be bad. To check port statistics, a troubleshooter could leverage a **show interfaces** command. Consider Example 5-14, which shows the output of the **show interfaces gig 0/9 counters** command on a Cisco Catalyst 3550 switch. Notice that this output shows the number of inbound and outbound frames seen on the specified port.

Example 5-14 **show interfaces gig 0/9 counters** *Command Output*

```
SW1# show interfaces gig 0/9 counters

Port              InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Gi0/9             31265148         20003          3179             1

Port             OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi0/9             18744149          9126            96             6
```

To view errors that occurred on a port, you could add the keyword of **errors** after the **show interfaces** *interface_id* **counters** command. Example 5-15 illustrates sample output from the **show interfaces gig 0/9 counters errors** command.

Example 5-15 **show interfaces gig 0/9 counters errors** *Command Output*

```
SW1# show interfaces gig 0/9 counters errors
Port        Align-Err     FCS-Err    Xmit-Err     Rcv-Err UnderSize
Gi0/9               0           0           0           0         0

Port      Single-Col  Multi-Col   Late-Col Excess-Col Carri-Sen     Runts    Giants
Gi0/9           5603          0       5373          0         0         0         0
```

Table 5-5 provides a reference for the specific errors that might show up in the output of the **show interfaces** *interface_id* **counters errors** command.

Key Topic

Table 5-5 *Errors in the* **show interfaces interface_id counters errors** *Command*

Error Counter	Description
Align-Err	An alignment error occurs when frames do not end with an even number of octets, while simultaneously having a bad Cyclic Redundancy Check (CRC). An alignment error normally suggests a Layer 1 issue, such as cabling or port (either switch port or NIC port) issues.
FCS-Err	A Frame Check Sequence (FCS) error occurs when a frame has an invalid checksum, although the frame has no framing errors. Like the Align-Err error, an FCS-Err often points to a Layer 1 issue.

continues

Table 5-5 *Errors in the* **show interfaces interface_id counters errors** *Command* (*Continued*)

Error Counter	Description
Xmit-Err	A transmit error (that is, Xmit-Err) occurs when a port's transmit buffer overflows. A speed mismatch between inbound and outbound links often results in a transmit error.
Rcv-Err	A receive error (that is, Rcv-Err) occurs when a port's receive buffer overflows. Congestion on a switch's backplane could cause the receive buffer on a port to fill to capacity, as frames await access to the switch's backplane. However, most likely, a Rcv-Err is indicating a duplex mismatch.
UnderSize	An undersize frame is a frame with a valid checksum but a size less than 64 bytes. This issue suggests that a connected host is sourcing invalid frame sizes.
Single-Col	A Single-Col error occurs when a single collisions occurs before a port successfully transmits a frame. High bandwidth utilization on an attached link or a duplex mismatch are common reasons for a Single-Col error.
Multi-Col	A Multi-Col error occurs when more than one collision occurs before a port successfully transmits a frame. Similar to the Single-Col error, high bandwidth utilization on an attached link or a duplex mismatch are common reasons for a Multi-Col error.
Late-Col	A late collision is a collision that is not detected until well after the frame has begun to be forwarded. While a Late-Col error could indicate that the connected cable is too long, this is an extremely common error seen in mismatched duplex conditions.
Excess-Col	The Excess-Col error occurs when a frame experienced sixteen successive collisions, after which the frame was dropped. This error could result from high bandwidth utilization, a duplex mismatch, or too many devices on a segment.
Carri-Sen	The Carri-Sen counter is incremented when a port wants to send data on a half-duplex link. This is normal and expected on a half-duplex port, because the port is checking the wire, to make sure no traffic is present, prior to sending a frame. This operation is the carrier sense procedure described by the Carrier Sense Multiple Access with Collision Detect (CSMA/CD) operation used on half-duplex connections. Full-duplex connections, however, do not use CSMA/CD.
Runts	A runt is a frame that is less than 64 bytes in size and has a bad CRC. A runt could result from a duplex mismatch or a Layer 1 issue.
Giants	A giant is a frame size greater than 1518 bytes (assuming the frame is not a jumbo frame) that has a bad FCS. Typically, a giant is caused by a problem with the NIC in an attached host.

Mismatched Duplex Settings

As seen in Table 5-5, duplex mismatches can cause a wide variety of port errors. Keep in mind that almost all network devices, other than shared media hubs, can run in full-duplex mode. Therefore, if you have no hubs in your network, all devices should be running in full-duplex mode.

A new recommendation from Cisco is that switch ports be configured to autonegotiate both speed and duplex. Two justifications for this recommendation are as follows:

- If a connected device only supported half-duplex, it would be better for a switch port to negotiate down to half-duplex and run properly than being forced to run full-duplex which would result in multiple errors.
- The automatic medium-dependent interface crossover (auto-MDIX) feature can automatically detect if a port needs a crossover or a straight-through cable to interconnect with an attached device and adjust the port to work regardless of which cable type is connected. You can enable this feature in interface configuration mode with the **mdix auto** command on some models of Cisco Catalyst switches. However, the auto-MDIX feature requires that the port autonegotiate both speed and duplex.

In a mismatched duplex configuration, a switch port at one end of a connection is configured for full-duplex, whereas a switch port at the other end of a connection is configured for half-duplex. Among the different errors previously listed in Table 5-5, two of the biggest indicators of a duplex mismatch are a high Rcv-Err counter or a high Late-Col counter. Specifically, a high Rcv-Err counter is common to find on the full-duplex end of a connection with a mismatched duplex, while a high Late-Col counter is common on the half-duplex end of the connection.

To illustrate, examine Examples 5-16 and 5-17, which display output based on the topology depicted in Figure 5-9. Example 5-16 shows the half-duplex end of a connection, and Example 5-17 shows the full-duplex end of a connection.

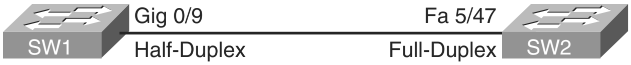


Figure 5-9 *Topology with Duplex Mismatch*

Example 5-16 *Output from the* **show interfaces gig 0/9 counters errors** *and the* **show interfaces gig 0/9 | include duplex** *Commands on a Half-Duplex Port*

```
SW1# show interfaces gig 0/9 counters errors

Port         Align-Err    FCS-Err   Xmit-Err     Rcv-Err UnderSize
Gi0/9                0          0          0           0         0


Port       Single-Col Multi-Col  Late-Col Excess-Col Carri-Sen   Runts    Giants
Gi0/9            5603         0      5373          0         0       0         0
```

```
SW1# show interfaces gig 0/9 | include duplex
  Half-duplex, 100Mb/s, link type is auto, media type is 10/100/1000BaseTX
SW1# show interfaces gig 0/9 counters errors
```

Example 5-17 *Output from the* **show interfaces fa 5/47 counters errors** *and the* **show interfaces fa 5/47 | include duplex** *Commands on a Full-Duplex Port*

```
SW2# show interfaces fa 5/47 counters errors



Port         Align-Err    FCS-Err    Xmit-Err    Rcv-Err UnderSize OutDiscards
Fa5/47               0       5248           0       5603        27           0

Port       Single-Col Multi-Col  Late-Col Excess-Col Carri-Sen      Runts    Giants
Fa5/47              0         0         0          0         0        227         0

Port        SQETest-Err Deferred-Tx IntMacTx-Err IntMacRx-Err Symbol-Err
Fa5/47                0           0            0            0          0

SW2# show interfaces fa 5/47 | include duplex
  Full-duplex, 100Mb/s
SW1# show interfaces gig 0/9 counters errors
```

In your troubleshooting, even if you only have access to one of the switches, if you suspect a duplex mismatch, you could change the duplex settings on the switch over which you do have control. Then, you could clear the interface counters to see if the errors continue to increment. You could also perform the same activity (for example, performing a file transfer) the user was performing when he noticed the performance issue. By comparing the current performance to the performance experienced by the user, you might be able to conclude that the problem has been resolved by correcting a mismatched duplex configuration.

TCAM Troubleshooting

As previously mentioned, the two primary components of forwarding hardware are forwarding logic and backplane. A switch's backplane, however, is rarely the cause of a switch performance issue, because most Cisco Catalyst switches have high-capacity backplanes. However, it is conceivable that in a modular switch chassis, the backplane will not have the throughput to support a fully populated modular chassis, where each card in the chassis supports the highest combination of port densities and port speeds.

The architecture of some switches allows groups of switch ports to be handled by separated hardware. Therefore, you might experience a performance gain by simply moving a cable from one switch port to another. However, to strategically take advantage of this design characteristic, you must be very familiar with the architecture of the switch with which you are working.

A multilayer switch's forwarding logic can impact switch performance. Recall that a switch's forwarding logic is compiled into a special type of memory called ternary content addressable memory (TCAM), as illustrated in Figure 5-10. TCAM works with a switch's CEF feature to provide extremely fast forwarding decisions. However, if a switch's TCAM is unable, for whatever reason, to forward traffic, that traffic is forwarded by the switch's CPU, which has a limited forwarding capability.

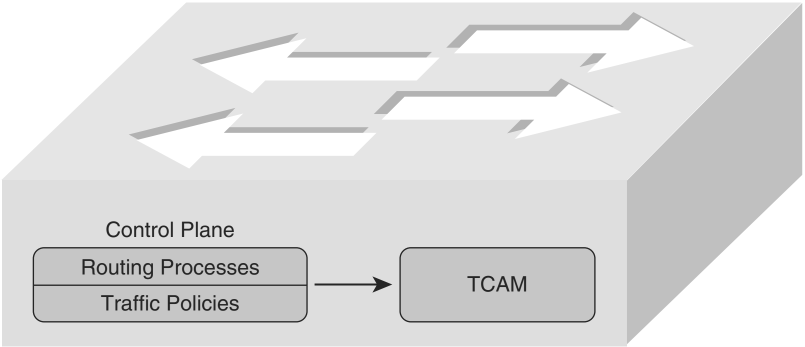


Figure 5-10 *Populating the TCAM*

The process of the TCAM sending packets to a switch's CPU is called *punting*. Consider a few reasons why a packet might be punted from a TCAM to its CPU:

Key Topic

- Routing protocols, in addition to other control plane protocols such as STP, that send multicast or broadcast traffic will have that traffic sent to the CPU.
- Someone connecting to a switch administratively (for example, establishing a Telnet session with the switch) will have their packets sent to the CPU.
- Packets using a feature not supported in hardware (for example, packets traveling over a GRE tunnel) are sent to the CPU.
- If a switch's TCAM has reached capacity, additional packets will be punted to the CPU. A TCAM might reach capacity if it has too many installed routes or configured access control lists.

From the events listed, the event most likely to cause a switch performance issue is a TCAM filling to capacity. Therefore, when troubleshooting switch performance, you might want to investigate the state of the switch's TCAM. Please be sure to check documentation for your switch model, because TCAM verification commands can vary between platforms.

As an example, the Cisco Catalyst 3550 Series switch supports a collection of **show tcam** commands, whereas Cisco Catalyst 3560 and 3750 Series switches support a series of **show platform tcam** commands. Consider the output from the **show tcam inacl 1 statistics** command issued on a Cisco Catalyst 3550 switch, as shown in Example 5-18. The number **1** indicates TCAM number one, because the Cisco Catalyst 3550 has three TCAMs. The **inacl** refers to access control lists applied in the ingress direction. Notice that fourteen masks are allocated, while 402 are available. Similarly, seventeen entries are currently allocated, and 3311 are available. Therefore, you could conclude from this output that TCAM number one is not approaching capacity.

Example 5-18 **show tcam inacl 1 statistics** *Command Output on a Cisco Catalyst 3550 Series Switch*

```
Cat3550# show tcam inacl 1 statistics
Ingress ACL TCAM#1: Number of active labels: 3
Ingress ACL TCAM#1: Number of masks   allocated:   14, available:  402
Ingress ACL TCAM#1: Number of entries allocated:   17, available: 3311
```

On some switch models (for example, a Cisco Catalyst 3750 platform), you can use the **show platform ip unicast counts** command to see if a TCAM allocation has failed. Similarly, you can use the **show controllers cpu-interface** command to display a count of packets being forwarded to a switch's CPU.

On most switch platforms, TCAMs cannot be upgraded. Therefore, if you conclude that a switch's TCAM is the source of the performance problems being reported, you could either use a switch with higher-capacity TCAMs or reduce the number of entries in a switch's TCAM. For example, you could try to optimize your access control lists or leverage route summarization to reduce the number of route entries maintained by a switch's TCAM. Also, some switches (for example, Cisco Catalyst 3560 or 3750 Series switches) enable you to change the amount of TCAM memory allocated to different switch features. For example, if your switch ports were configured as routing ports, you could reduce the amount of TCAM space used for storing MAC addresses, and instead use that TCAM space for Layer 3 processes.

High CPU Utilization Level Troubleshooting

The load on a switch's CPU is often low, even under high utilization, thanks to the TCAM. Because the TCAM maintains a switch's forwarding logic, the CPU is rarely tasked to forward traffic. The **show processes cpu** command that you earlier learned for use on a router can also be used on a Cisco Catalyst switch to display CPU utilization levels, as demonstrated in Example 5-19.

Example 5-19 **show processes cpu** *Command Output on a Cisco Catalyst 3550 Series Switch*

Key Topic

```
Cat3550# show processes cpu
CPU utilization for five seconds: 19%/15%; one minute: 20%; five minutes: 13%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         4          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2           0       610          0  0.00%  0.00%  0.00%   0 Load Meter
   3         128         5      25600  0.00%  0.00%  0.00%   0 crypto sw pk pro
   4        2100       315       6666  0.00%  0.05%  0.05%   0 Check heaps
...OUTPUT OMITTED...
```

Notice in the output in Example 5-19 that the switch is reporting a 19 percent CPU load, with 15 percent of the CPU load used for interrupt processing. The difference between these two numbers is 4, suggesting that 4 percent of the CPU load is consumed with control plane processing.

Although such load utilization values might not be unusual for a router, these values might be of concern for a switch. Specifically, a typical CPU load percentage dedicated to interrupt processing is no more than five percent. A value as high as ten percent is considered acceptable. However, the output given in Example 5-19 shows a fifteen percent utilization. Such a high level implies that the switch's CPU is actively involved in forwarding packets that should normally be handled by the switch's TCAM. Of course, this value might only be of major concern if it varies from baseline information. Therefore, your troubleshooting efforts benefit from having good baseline information.

Periodic spikes in processor utilization are also not a major cause for concern if such spikes can be explained. Consider the following reasons that might cause a switch's CPU utilization to spike:

- The CPU processing routing updates
- Issuing a **debug** command (or other processor-intensive commands)
- Simple Network Management Protocol (SNMP) being used to poll network devices

If you determine that a switch's high CPU load is primarily the result of interrupts, you should examine the switch's packet switching patterns and check the TCAM utilization. If, however, the high CPU utilization is primarily the result of processes, you should investigate those specific processes.

A high CPU utilization on a switch might be a result of STP. Recall that an STP failure could lead to a broadcast storm, where Layer 2 broadcast frames endlessly circulate through a network. Therefore, when troubleshooting a performance issue, realize that a switch's high CPU utilization might be a symptom of another issue.

Trouble Ticket: HSRP

This trouble ticket focuses on HSRP. HSRP was one of three first-hop redundancy protocols discussed in this chapter's "Router Redundancy Troubleshooting" section.

Trouble Ticket #2

You receive the following trouble ticket:

> A new network technician configured HSRP on routers BB1 and BB2, where BB1 was the active router. The configuration was initially working; however, now BB2 is acting as the active router, even though BB1 seems to be operational.

This trouble ticket references the topology shown in Figure 5-11.

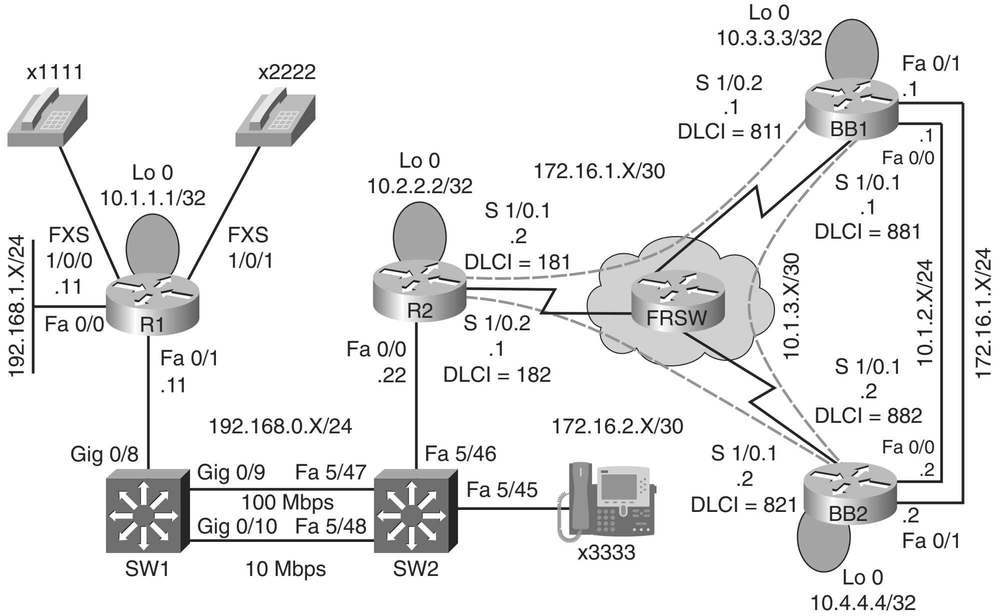


Figure 5-11 *Trouble Ticket #2 Topology*

As you investigate this issue, you examine baseline data collected after HSRP was initially configured. Examples 5-20 and 5-21 provide **show** and **debug** command output collected when HSRP was working properly. Notice that router BB1 was acting as the active HSRP router, whereas router BB2 was acting as the standby HSRP router.

Example 5-20 *Baseline Output for Router BB1*

```
BB1# show standby brief
                       P indicates configured to preempt.
                       |
Interface    Grp  Prio P State    Active           Standby          Virtual IP
Fa0/1         1    150    Active   local             172.16.1.3       172.16.1.4

BB1# debug standby
HSRP debugging is on
*Mar  1 01:14:21.487: HSRP: Fa0/1 Grp 1 Hello  in  172.16.1.3 Standby pri 100 vIP
   172.16.1.4
*Mar  1 01:14:23.371: HSRP: Fa0/1 Grp 1 Hello  out 172.16.1.1 Active  pri 150 vIP
   172.16.1.4
```

```
BB1# u all
All possible debugging has been turned off

BB1# show standby fa 0/1 1
FastEthernet0/1 - Group 1
  State is Active
    10 state changes, last state change 00:12:40
  Virtual IP address is 172.16.1.4
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.536 secs
  Preemption disabled
  Active router is local
  Standby router is 172.16.1.3, priority 100 (expires in 9.684 sec)
  Priority 150 (configured 150)
  IP redundancy name is "hsrp-Fa0/1-1" (default)

BB1# show run
...OUTPUT OMITTED...
hostname BB1
!
interface Loopback0
 ip address 10.3.3.3 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.1.2.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 standby 1 ip 172.16.1.4
 standby 1 priority 150
!
router ospf 1
 network 0.0.0.0 255.255.255.255 area 0
```

Example 5-21 *Baseline Output for Router BB2*

```
BB2# show standby brief
                       P indicates configured to preempt.
                       |
Interface    Grp  Prio P State    Active           Standby          Virtual IP
Fa0/1         1   100    Standby  172.16.1.1       local            172.16.1.4

BB2# show run
...OUTPUT OMITTED...
hostname BB2
!
interface Loopback0
 ip address 10.4.4.4 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.1.2.2 255.255.255.0
!
interface FastEthernet0/1
 ip address 172.16.1.3 255.255.255.0
 standby 1 ip 172.16.1.4
!
router ospf 1
 network 0.0.0.0 255.255.255.255 area 0
```

As part of testing the initial configuration, a ping was sent to the virtual IP address of 172.16.1.4 from router R2 in order to confirm that HSRP was servicing requests for that IP address. Example 5-22 shows the output from the **ping** command.

Example 5-22 *PINGing the Virtual IP Address from Router R2*

```
R2# ping 172.16.1.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.4, timeout is 2 seconds:
!!!!!
```

As you begin to gather information about the reported problem, you reissue the **show standby brief** command on routers BB1 and BB2. As seen in Examples 5-23 and 5-24, router BB1 is administratively up with an HSRP priority of 150, whereas router BB2 is administratively up with a priority of 100.

Example 5-23 *Examining the HSRP State of Router BB1's FastEthernet 0/1 Interface*

```
BB1# show standby brief
                       P indicates configured to preempt.
                       |
Interface    Grp  Prio P State    Active          Standby         Virtual IP
Fa0/1        1    150    Standby  172.16.1.3      local           172.16.1.4
```

Example 5-24 *Examining the HSRP State of Router BB2's FastEthernet 0/1 Interface*

```
BB2# show standby brief
                       P indicates configured to preempt.
                       |
Interface   Grp  Prio P State    Active          Standby         Virtual IP
Fa0/1       1    100    Active   local           172.16.1.1      172.16.1.4
```

Take a moment to look through the baseline information, the topology, and the **show** command output. Then, hypothesize the underlying cause, explaining why router BB2 is currently the active HSRP router, even thought router BB1 has a higher priority. Finally, on a separate sheet of paper, write out a proposed action plan for resolving the reported issue.

Suggested Solution

Upon examination of BB1's output, it becomes clear that the preempt feature is not enabled for the Fast Ethernet 0/1 interface on BB1. The absence of the preempt feature explains the reported symptom. Specifically, if BB1 had at one point been the active HSRP router for HSRP group 1, and either router BB1 or its Fast Ethernet 0/1 interface became unavailable, BB2 would have become the active router. Then, if BB1 or its Fast Ethernet 0/1 interface once again became available, BB1 would assume a standby HSRP role, because BB1's FastEthernet 0/1 interface was not configured for the preempt feature.

To resolve this configuration issue, the preempt feature is added to BB1's Fast Ethernet 0/1 interface, as shown in Example 5-25. After enabling the preempt feature, notice that router BB1 regains its active HSRP role.

Example 5-25 *Enabling the Preempt Feature on Router BB1's FastEthernet 0/1 Interface*

```
BB1# conf term
Enter configuration commands, one per line.  End with CNTL/Z.
BB1(config)#int fa 0/1
BB1(config-if)#standby 1 preempt
BB1(config-if)#end
BB1#
*Mar  1 01:17:39.607: %HSRP-5-STATECHANGE: FastEthernet0/1 Grp 1 state Standby ->
  Active

BB1#show standby brief
                       P indicates configured to preempt.
                       |
Interface   Grp  Prio P State    Active           Standby          Virtual IP
Fa0/1       1    150  P Active   local            172.16.1.3       172.16.1.4
```

Exam Preparation Tasks

Review All Key Topics

Review the most important topics from inside the chapter, noted with the Key Topics icon in the outer margin of the page. Table 5-6 lists these key topics and the page numbers where each is found.

Table 5-6 *Key Topics for Chapter 5*

Key Topic Element	Description	Page Number
Table 5-2	Similarities and differences between routers and Layer 3 switches	111
Table 5-3	Router data plane verification commands	112
Example 5-3	SVI configuration	113
List	Differences between SVIs and routed ports	115
Examples 5-5 and 5-6	HSRP configuration	116
Figure 5-6	Basic VRRP Operation	121
Figure 5-7	Basic GLBP Operation	121
Table 5-4	Comparing HSRP, VRRP, and GLBP	122
List	Cisco Catalyst hardware components	122
Table 5-5	Errors in the **show interfaces** *interface_id* **counters errors** command	124
List	Reasons why a packet might be punted from a TCAM to its CPU	128
Example 5-19	Output from the **show processes cpu** command on a Cisco Catalyst 3550 Series switch	129

Complete Tables and Lists from Memory

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

Layer 3 switch, switched virtual interface (SVI), Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), Global Load Balancing Protocol (GLBP), control plane, backplane, Ternary Content Addressable Memory (TCAM)

Command Reference to Check Your Memory

This section includes the most important configuration and EXEC commands covered in this chapter. To determine how well you have memorized the commands as a side effect of your other studies, cover the left side of Tables 5-7 and 5-8 with a piece of paper, read the descriptions on the right side, and see whether you remember the command.

Table 5-7 *Chapter 5 Configuration Command Reference*

Command	Description
standby *group ip virtual-ip-address*	Interface configuration mode command, used to specify the virtual IP address to be serviced by an HSRP group.
standby group **priority** priority	Interface configuration mode command, used to configure an interface's HSRP priority (which defaults to 100).
standby group **preempt**	Interface configuration mode command, which causes a previously active HSRP router to regain its active status if it becomes available.
mdix auto	Interface configuration mode command for a switch that allows the switch port to automatically detect and adjust to the connected cable type (that is, either straight-through or cross-over).

Table 5-8 *Chapter 5 EXEC Command Reference*

Command	Description
show standby *interface-id group*	Displays the HSRP configuration applied to a specified interface in a specified HSRP group.
show standby brief	Provides a summary view of a router's HSRP configuration.
debug standby	Shows HSRP state changes and information about sent and received HSRP packets.
show vrrp brief	Provides a summary view of a router's VRRP configuration.
show glbp brief	Provides a summary view of a router's GLBP configuration.
show ip cef	Displays the router's Layer 3 forwarding information, in addition to multicast, broadcast, and local IP addresses.
show adjacency	Verifies that a valid adjacency exists for a connected host.
show tcam inacl *tcam_number* **statistics**	A Cisco Catalyst 3550 Series switch command that displays the amount of TCAM memory allocated and used for inbound access control lists.
show platform ip unicast counts	A Cisco Catalyst 3750 Series switch command that can be used to see if a TCAM allocation has failed.
show controllers cpu-interface	A Cisco Catalyst 3750 Series switch command that can be used to display a count of packets being forwarded to a switch's CPU.

Index