CCNA Routing and Switching

Practice and Study Guide

Exercises, Activities, and Scenarios to Prepare for the ICND2 200-101 Certification Exam

Allan Johnson

CCNA Routing and Switching Practice and Study Guide:

Exercises, Activities, and Scenarios to Prepare for the ICND2 (200-101) Certification Exam

Allan Johnson

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

CCNA Routing and Switching Practice and Study Guide:
Exercises, Activities, and Scenarios to Prepare for the ICND2 (200-101) Certification Exam
Student Edition

Allan Johnson

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

Printed in the United States of America

First Printing April 2014

ISBN-13: 978-1-58713-344-2

ISBN-10: 1-58713-344-X

Library of Congress Control Number: 2014933142

Warning and Disclaimer

This book is designed to provide information about networking. 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.

Publisher
Paul Boger

Associate Publisher
Dave Dusthimer

Business Operation Manager, Cisco Press
Jan Cornelssen

Executive Editor
Mary Beth Ray

Managing Editor
Sandra Schroeder

Senior Development Editor
Christopher Cleveland

Project Editor
Mandie Frank

Copy Editor
Keith Cline

Technical Editor
Steve Stiles

Editorial Assistant
Vanessa Evans

Designer
Mark Shirar

Composition
Tricia Bronkella

Proofreader
Sarah Kearns

Trademark Acknowledgments

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

Special Sales

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

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

For questions about sales outside the U.S., please contact 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 email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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

Allan Johnson entered the academic world in 1999 after 10 years as a business owner/operator to dedicate his efforts to his passion for teaching. He holds both an MBA and an M.Ed in Occupational Training and Development. He is an information technology instructor at Del Mar College in Corpus Christi, Texas. In 2003, Allan began to commit much of his time and energy to the CCNA Instructional Support Team, providing services to Networking Academy instructors worldwide and creating training materials. He now works full time for Cisco Networking Academy as a Learning Systems Developer.

About the Technical Reviewer

Steve Stiles is a Cisco Network Academy Instructor for Rhodes State College and a Cisco Certified Instructor Trainer, having earned CCNA Security and CCNP level certifications. He was the recipient of the 2012 Outstanding Teacher of the Year by the Ohio Association of Two-Year Colleges and co-recipient for the Outstanding Faculty of the Year at Rhodes State College.

Dedication

For my wife, Becky. Without the sacrifices you made during the project, this work would not have come to fruition. Thank you providing me the comfort and resting place only you can give.

—Allan Johnson

Acknowledgments

When I began to think of whom I would like to have as a technical editor for this work, Steve Stiles immediately came to mind. With his instructor and industry background, and his excellent work building activities for the new Cisco Networking Academy curriculum, he was an obvious choice. Thankfully, when Mary Beth Ray contacted him, he was willing and able to do the arduous review work necessary to make sure that you get a book that is both technically accurate and unambiguous.

The Cisco Network Academy authors for the online curriculum and series of Companion Guides take the reader deeper, past the CCENT exam topics, with the ultimate goal of not only preparing the student for CCENT certification, but for more advanced college-level technology courses and degrees, as well. Thank you especially to Amy Gerrie and her team of authors—Rick Graziani, Wayne Lewis, and Bob Vachon—for their excellent treatment of the material; it is reflected throughout this book.

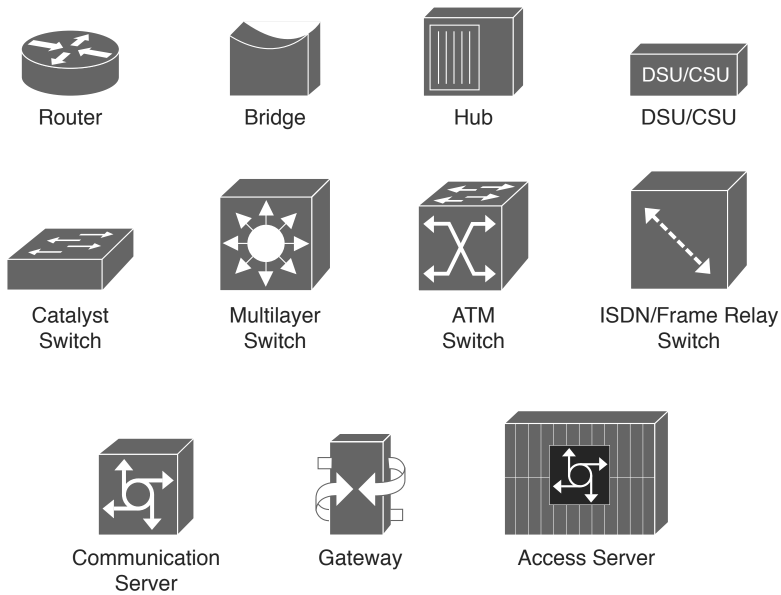
Mary Beth Rey, Executive Editor, you amaze me with your ability to juggle multiple projects at once, steering each from beginning to end. I can always count on you to make the tough decisions.

This is my seventh project with Christopher Cleveland as development editor. His dedication to perfection pays dividends in countless, unseen ways. Thank you again, Chris, for providing me with much-needed guidance and support. This book could not be a reality without your persistence.

Contents at a Glance

Contents

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).
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets [ ] indicate optional elements.
- Braces { } indicate a required choice.
- Braces within brackets [{ }] indicate a required choice within an optional element.

Introduction

The purpose of this book is to provide you with an extra resource for studying the exam topics of the Interconnecting Cisco Networking Devices Part 2 (ICND2) exam that leads to Cisco Certified Networking Associate (CCNA) certification. This book maps to the third and fourth Cisco Networking Academy courses in the CCNA Routing and Switching curricula: *Scaling Networks* (SN) and *Connecting Networks* (CN). Ideally, the reader will have completed the first two courses: *Introduction to Networks* (ITN) and *Routing and Switching Essentials* (RSE). SN continues where RSE left off, taking the student deeper into the architecture, components, and operations of routers and switches in a large and complex network. Successfully completing this course means that you should be able to configure and troubleshoot routers and switches and resolve common issues with OSPF, EIGRP, STP, and VTP in both IPv4 and IPv6 networks. CN pulls everything from the first three courses together as the student learns the WAN technologies and network services required by converged applications in a complex network. Successfully completing this course means that you should be able to configure and troubleshoot network devices and resolve common WAN issues and implement IPsec and virtual private network (VPN) operations in a complex network. To learn more about CCNA Routing and Switching courses and to find an Academy near you, visit http://www.netacad.com.

However, if you are not an Academy student but would like to benefit from the extensive authoring done for these courses, you can buy any or all of CCNA Routing and Switching Companion Guides (CG) and Lab Manuals (LM) of the Academy's popular online curriculum. Although you will not have access to the Packet Tracer network simulator software, you will have access to the tireless work of an outstanding team of Cisco Academy instructors dedicated to providing students with comprehensive and engaging CCNA Routing and Switching preparation course material. The titles and ISBNs for the first two courses of the CCNA Routing and Switching CGs and LMs are as follows:

- *Scaling Networks Companion Guide* (ISBN: 9781587133282)
- *Scaling Networks Lab Manual* (ISBN: 9781587133251)
- *Connecting Networks Companion Guide* (ISBN: 9781587133329)
- *Connecting Networks Lab Manual* (ISBN: 9781587133312)

Goals and Methods

The most important goal of this book is to help you pass the 200-101 Interconnecting Cisco Networking Devices Part 2 (ICND2) exam, which is associated with the Cisco Certified Network Associate (CCNA) certification. Passing the CCNA exam means that you have the knowledge and skills required to successfully install, operate, and troubleshoot a small branch office network. You can view the detailed exam topics any time at http://learningnetwork.cisco.com. They are divided into five broad categories:

- LAN Switching Technologies
- IP Routing Technologies
- IP Services
- Troubleshooting
- WAN Technologies

This book offers exercises that help you learn the concepts, configurations, and troubleshooting skills crucial to your success as a CCNA exam candidate. Each chapter differs slightly and includes some or all of the following types of practice:

- Vocabulary-matching exercises
- Concept question exercises
- Skill-building activities and scenarios
- Configuration scenarios
- Troubleshooting scenarios

Audience for This Book

This book's main audience is anyone taking the CCNA Routing and Switching courses of the Cisco Networking Academy curriculum. Many Academies use this Practice Study Guide as a required tool in the course, whereas other Academies recommend the Practice Study Guide as an additional resource to prepare for class exams and the CCNA certification.

The secondary audiences for this book include people taking CCNA-related classes from professional training organizations. This book can also be used for college- and university-level networking courses, and by anyone wanting to gain a detailed understanding of INCD2 routing and switching concepts.

How This Book Is Organized

Because the content of the *Scaling Networks Companion Guide*, the *Connecting Networks Companion Guide*, and the online curriculum is sequential, you should work through this Practice and Study Guide in order beginning with Chapter 1.

The book covers the major topic headings in the same sequence as the online curriculum. This book has 18 chapters, their names the same as the online course chapters. However, the numbering is sequential in this book, progressing from Chapter 1 to Chapter 18. The online curriculum starts over at Chapter 1 in the *Connecting Networks* course.

Most of the configuration chapters use a single topology where appropriate. This allows for better continuity and easier understanding of routing and switching commands, operations, and outputs. However, the topology differs from the one used in the online curriculum and the Companion Guide. A different topology affords you the opportunity to practice your knowledge and skills without just simply recording the information you find in the text.

Packet Tracer **Activity**

Video **Demonstration**

Note: Throughout the book, you will find references to Packet Tracer and Lab activities. These references are provided so that you can, at that point, complete those activities. The Packet Tracer activities are accessible only if you have access to the online curriculum. However, the Labs are available in the Lab Manuals previously cited.

Part I: Scaling Networks

- **Chapter 1, "Introduction to Scaling Networks":** This chapter provides vocabulary and concept exercises to reinforce your understanding of hierarchical network design and selecting hardware. You will also practice basic router and switch configuration and verification.
- **Chapter 2, "LAN Redundancy":** The exercises in this chapter cover the concepts, operations, configuration, and verification of all the current varieties of STP.
- **Chapter 3, "Link Aggregation":** This chapter's exercises are devoted to the concepts, configuration, verification, and troubleshooting of EtherChannel.
- **Chapter 4, "Wireless LANs":** This chapter is all about wireless connectivity technologies. You will complete exercises that focus on various types of wireless and the standards for 802.11. In addition, you will complete activities focused on WLAN components, topologies, and security.
- **Chapter 5, "Adjust and Troubleshoot Single-Area OSPF":** This chapter focuses on advanced OSPF concepts, configuration, verification, and troubleshooting.
- **Chapter 6, "Multiarea OSPF":** The CCNA exam now includes multiarea OSPF. So, this chapter includes exercises covering multiarea OSPF concepts and configuration, verification, and troubleshooting.
- **Chapter 7, "EIGRP":** The exercises in this chapter are devoted to the basic concepts and configuration of Cisco's routing protocol, EIGRP for IPv4 and IPv6.
- **Chapter 8, "EIGRP Advanced Configurations and Troubleshooting":** This chapter focuses on advanced EIGRP concepts, configuration, verification, and troubleshooting.
- **Chapter 9, "IOS Images and Licensing":** This chapter is devoted to the crucial knowledge and skills you need to manage IOS images. Exercises focus on basic IOS image concepts and management tasks.

Part II: Connecting Networks

- **Chapter 10, "Hierarchical Network Design":** Part II, much like Part I, starts off network design. Exercises focus on the various types of network design models and architectures.
- **Chapter 11, "Connecting to the WAN":** This chapter is a survey of all the various WAN access options and technologies that are available for connecting today's networks. The exercises focus on differentiating between all these WAN options.
- **Chapter 12, "Point-to-Point Connections":** One of the older, and still viable, WAN options is PPP. Exercises in this chapter focus on the serial interface and then the concepts, configuration, verification, and troubleshooting of PPP with PAP and CHAP authentication.
- **Chapter 13, "Frame Relay":** Although some may consider Frame Relay obsolete, it is still a viable option in depending on your location. This chapter includes exercises covering the concepts, configuration, verification, and troubleshooting of Frame Relay.

- **Chapter 14, "Network Address Translation for IPv4":** NAT was created to provide a temporary solution to the limited address space in IPv4. Just about every router connected to the network uses NAT or forwards traffic to a NAT-enabled device for address translation. This chapter focuses on exercises to reinforce your understanding of NAT operation and characteristics. Practice activities include configuring, verifying, and troubleshooting static NAT, dynamic NAT, and PAT.
- **Chapter 15, "Broadband Solutions":** Working from home or away from a central office has largely been made possible by the advent of broadband technologies and VPNs. This exercises in this chapter help you distinguish between the various broadband offerings on the market.
- **Chapter 16, "Securing Site-to-Site Connectivity":** VPNs allow teleworkers and branch sites connect to the corporate network regardless of the underlying WAN access option. The exercises in this chapter are devoted to the concepts of the various VPN solutions, including IPsec and GRE configuration.
- **Chapter 17, "Monitoring the Network":** As a network administrator, you are more likely to be managing a network using a variety of tools rather than designing and building them. The exercises in this chapter cover three popular network monitoring tools: syslog, SNMP, and NetFlow.
- Chapter 18, "**Troubleshooting the Network**": Throughout your CCNA studies, you have practice troubleshooting skills in relation to specific technologies. This chapter reviews troubleshooting methodologies and the tools and commands you use to troubleshoot a network. Troubleshooting is a key skill to fine-tune now that you are close to taking your CCNA exam.

About the Cisco Press Website for This Book

Cisco Press provides additional content that can be accessed by registering your individual book at the ciscopress.com website. Becoming a member and registering is free, and you then gain access to exclusive deals on other resources from Cisco Press.

To register this book, go to http://www.ciscopress.com/bookstore/register.asp and enter the book's ISBN located on the back cover of this book. You'll then be prompted to log in or join ciscopress.com to continue registration.

After you register the book, a link to the supplemental content will be listed on your My Registered Books page.

This page intentionally left blank

CHAPTER 1

Introduction to Scaling Networks

As a business grows, so does its networking requirements. To keep pace with a business's expansion and new emerging technologies, a network must be designed to scale. A network that scales well is not only one that can handle growing traffic demands, but also one designed with the inevitable need to expand. This short chapter sets the stage for the rest of the course. This chapter covers the hierarchical network design model, the Cisco Enterprise Architecture modules, and appropriate device selections that you can use to systematically design a highly functional network.

Implementing a Network Design

An enterprise network must be designed to support the exchange of various types of network traffic, including data files, email, IP telephony, and video applications for multiple business units.

Hierarchical Network Design

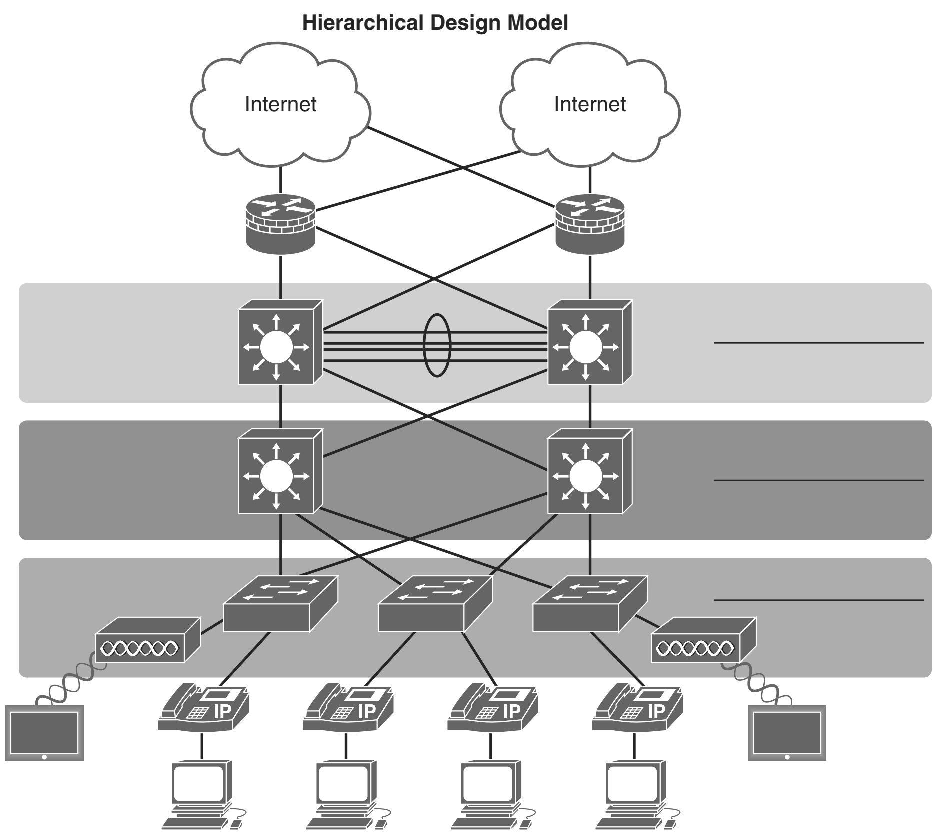
Users expect enterprise networks to be up ________________ percent of the time. To provide this kind of reliability, enterprise class equipment uses ________________ power supplies and has failover capabilities.

Describe what failover capability means for enterprise class equipment.

Why should a network be organized so that traffic stays local and is not propagated unnecessarily on to other portions of the network?

Designing a network using the three-layer hierarchical design model helps optimize the network. In Figure 1-1, label the three layers of the hierarchical design model.

Figure 1-1 Hierarchical Design Model



Briefly describe each layer of the hierarchical design model.

The Cisco Enterprise Architecture divides the network into functional components while still maintaining the core, distribution, and access layers. The primary Cisco Enterprise Architecture modules include Enterprise Campus, Enterprise Edge, Service Provider Edge, and Remote.

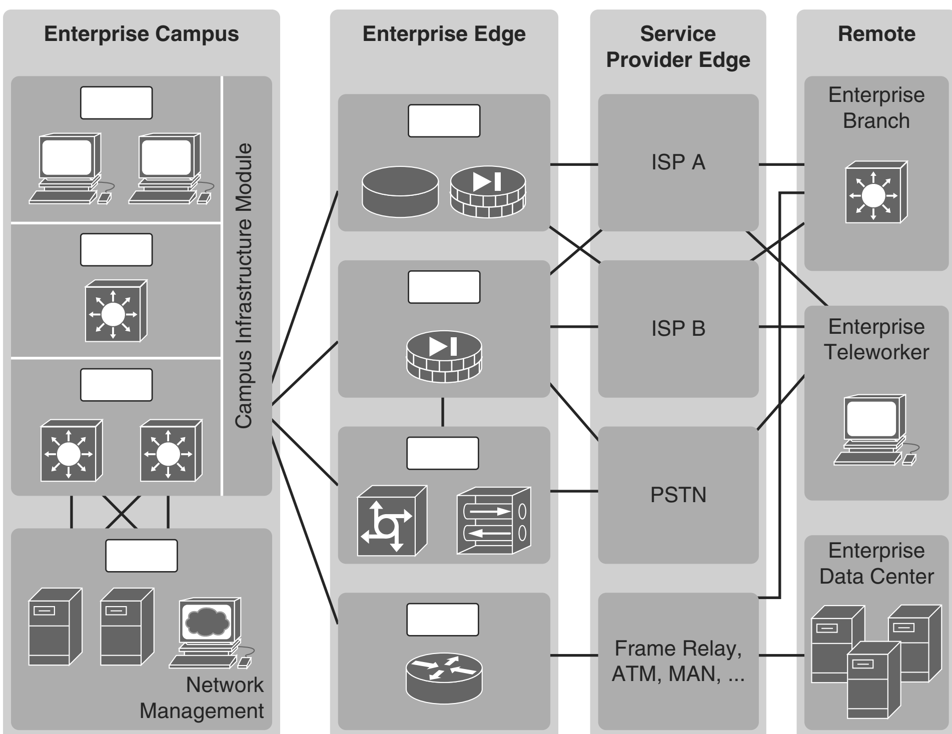
A well-designed network not only controls traffic but also limits the size of failure domains. Briefly describe a failure domain.

Use the list of modules to label the parts of the Cisco Enterprise Architecture in Figure 1-2.

Modules

1 Campus Core
2 Remote Access & VPN
3 Building Distribution
4 Internet Connectivity
5 Building Access
6 Server Farm & Data Center
7 WAN Site-to-Site VPN
8 E-Commerce

Figure 1-2 Cisco Enterprise Architecture



Identify Scalability Terminology

Match the definition on the left with the term on the right. This is a one-to-one matching exercise.

Definition

____ Isolates routing updates and minimizes the size of routing tables

____ Cisco proprietary distance vector routing protocol

____ Allows for redundant paths by eliminating switching loops

____ Technique for aggregating multiple links between equipment to increase bandwidth

____ Minimizes the possibility of a single point of failure

____ Supports new features and devices without requiring major equipment upgrades

____ Link-state routing protocol with a two-layer hierarchical design

____ Increases flexibility, reduces costs, and provides mobility to users

Terms

a. Modular equipment

b. OSPF

c. EIGRP

d. Wireless LANs

e. Redundancy

f. Spanning Tree Protocol

g. Scalable Routing Protocol

h. EtherChannel

Selecting Network Devices

When designing a network, it is important to select the proper hardware to meet current network requirements and to allow for network growth. Within an enterprise network, both switches and routers play a critical role in network communication.

Selecting Switch Hardware

Match the business consideration on the left with the switch feature on the right. This is a one-to-one matching exercise.

Business Consideration

____ Should provide continuous access to the network

____ Daisy-chain switches with high-bandwidth throughput

____ Refers to a switch's ability to support the appropriate number of devices on the network

____ Ability to adjust to growth of network users

____ How fast the interfaces will process network data

____ Important consideration in a network where there may be congested ports to servers or other areas of the network

____ Provides electrical current to other device and support redundant power supplies

____ Switches with preset features or options

____ Depends on the number and speed of the interfaces, supported features, and expansion capability

____ Switches with insertable switching line/port cards

Switch Feature

a. Reliability
b. Modular
c. Power
d. Stackable
e. Frame buffers
f. Cost
g. Fixed configuration
h. Scalability
i. Port speed
j. Port density

Packet Tracer Activity

Packet Tracer - Comparing 2960 and 3560 Switches (SN 1.2.1.7/SwN 1.1.2.5)

Selecting Router Hardware

In Table 1-1, select the router category that applies to each description.

Table 1-1 Identify Router Category Features

Router Description	Branch Routers	Network Edge Routers	Service Provider Routers
Fast performance with high security for data centers, campus, and branch networks			
Simple network configuration and management for LANs and WANs			
Optimizes services on a single platform			
End-to-end delivery of subscriber services			
Deliver next-generation Internet experiences across all devices and locations			
High capacity and scalability with hierarchical quality of service			
Maximizes local services and ensures 24/7/365 uptime			
Unites campus, data center, and branch networks			

Managing Devices

A basic router or switch configuration includes the hostname for identification, passwords for security, and assignment of IP addresses to interfaces for connectivity. A router configuration also includes basic routing.

In addition to configuration commands, router and switch verification commands are used to verify the operational status of the router or switch and related network functionality. Use the address scheme in Table 1-2 in the following exercises that review the most common router and switch configuration and verification commands.

Table 1-2 Router and Switch Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
R1	G0/0	172.16.1.1	255.255.255.0	N/A
	S0/0/0	172.16.3.1	255.255.255.252	N/A
	S0/0/1	192.168.10.5	255.255.255.252	N/A
S1	VLAN 1	192.168.1.5	255.255.255.0	192.168.1.1

Basic Router Configuration Review

Using Table 1-2 and the following requirements, record the commands, including the router prompt, to implement a basic router configuration:

- Hostname is R1.
- Console and Telnet line's password is cisco.
- Privileged EXEC password is class.
- Banner message-of-the-day.
- Interface addressing.
- OSPF routing, including an appropriate router ID.
- Save the configuration.

`Router(config)#` ____

Basic Router Verification Review

In Table 1-3, record the verification command that will generate the described output.

Table 1-3 Router Verification Commands

Command	Command Output
	Displays the routing table for known networks, including administrative distance, metric, and outbound interface
	Displays information about routing protocols, including process ID, router ID, and neighbors
	Displays information about directly connected Cisco devices
	Displays all interfaces in an abbreviated format, including IP address and status
	Displays information about neighbors, including router ID, state, IP address, and local interface that learned of neighbor
	Displays one or all interfaces, including status, bandwidth, and duplex type

Basic Switch Configuration Review

Using Table 1-2 and the following requirements, record the commands, including the switch prompt, to implement a basic switch configuration:

- Hostname is S1.
- Console and Telnet line's password is cisco.
- Privileged EXEC password is class.
- Banner message-of-the-day.
- VLAN 1 interface addressing.
- Save the configuration.

```
Switch(config)# ____________________________________________
```

Basic Switch Verification Review

In Table 1-4, record the verification command that will generate the described output.

Table 1-4 Router Verification Commands

Command	Command Output
	Displays information about directly connected Cisco devices
	Displays all secure MAC addresses
	Displays a table of learned MAC addresses, including the port number and VLAN assigned to the port
	Displays one or all interfaces, including status, bandwidth, and duplex type
	Displays information about maximum MAC addresses allowed, current counts, security violation count, and action to be taken

Packet Tracer
☐ Challenge

Packet Tracer - Skills Integration Challenge (SN 1.3.1.2)

CHAPTER 2

LAN Redundancy

Computer networks are inextricably linked to productivity in today's small and medium-sized businesses. Consequently, IT administrators have to implement redundancy in their hierarchical networks. When a switch connection is lost, another link needs to quickly take its place without introducing any traffic loops. This chapter investigates how Spanning Tree Protocol (STP) logically blocks physical loops in the network and how STP has evolved into a robust protocol that rapidly calculates which ports should be blocked in a VLAN-based network. In addition, the chapter briefly explores how Layer 3 redundancy is implemented through First Hop Redundancy Protocols (FHRPs).

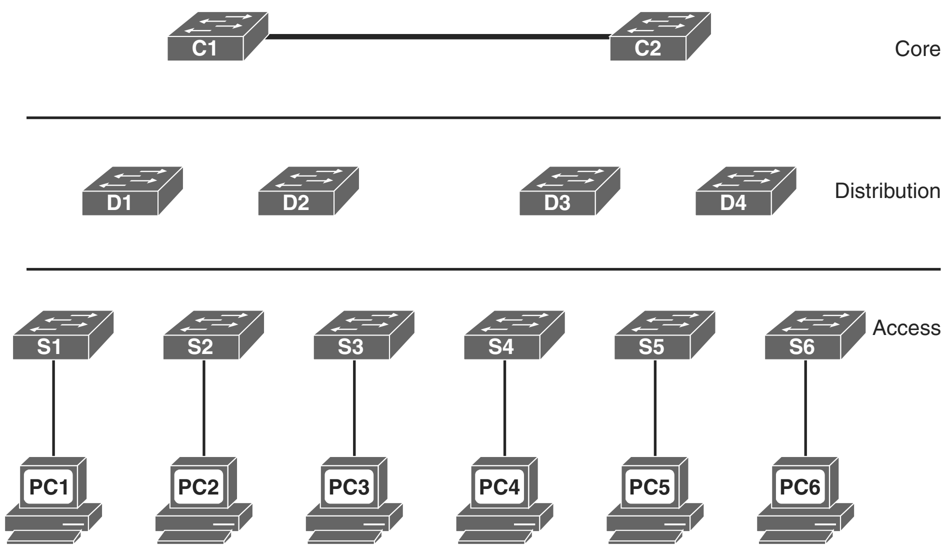
Spanning-Tree Concepts

Redundancy increases the availability of a network topology by protecting the network from a single point of failure, such as a failed network cable or switch. STP was developed to address the issue of loops in a redundant Layer 2 design.

Draw a Redundant Topology

In Figure 2-1, draw redundant links between the access, distribution, and core switches. Each access switch should have two links to the distribution layer with each link connecting to a different distribution layer switch. Each distribution layer switch should have two links to the core layer with each link connecting to a different core layer switch.

Figure 2-1 Redundant Topology



Purpose of Spanning Tree

STP prevents specific types of issues in a redundant topology like the one in Figure 2-1. Specifically, three potential issues would occur if STP was not implemented. Describe each of the following issues:

- MAC database instability:

- Broadcast storms:

- Multiple frame transmission:

You should be prepared to use a topology like Figure 2-1 to explain exactly how these three issues would occur if STP was not implemented.

Packet Tracer
☐ **Activity**

Packet Tracer - Examining a Redundant Design (SN 2.1.1.5/SwN 4.1.1.5)

Spanning-Tree Operation

Because ________________ (RSTP), which is documented in IEEE ________________ -2004, supersedes the original STP documented in IEEE ________________ -1998, all references to STP assume RSTP unless otherwise indicated.

STP ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a ________________ . A switch port is considered ________________ when network traffic is prevented from entering or leaving that port.

STP uses the ________________ (STA) to determine which switch ports on a network need to be ________________ to prevent ________________ from occurring. The STA designates a single switch as the ________________ bridge and uses it as the reference point for all subsequent calculations. Switches participating in STP determine which switch has the lowest ________________ (BID) on the network. This switch automatically becomes the ________________ bridge.

A ________________ (BPDU) is a frame containing STP information exchanged by switches running STP. Each BPDU contains a BID that identifies the switch that sent the BPDU. The ________________ BID value determines which switch is root.

After the root bridge has been determined, the STA calculates the shortest path to the root bridge. If there is more than one path to choose from, STA chooses the path with the lowest ______________.

When the STA has determined the "best" paths emanating from the root bridge, it configures the switch ports into distinct port roles. The port roles describe their relation in the network to the root bridge and whether they are allowed to forward traffic:

- __________________ **ports**: Switch ports closest to the root bridge
- __________________ **ports**: Nonroot ports that are still permitted to forward traffic on the network
- __________________ **ports**: Ports in a blocking state to prevent loops
- __________________ **port**: Ports that are administratively shut down

After a switch boots, it sends BPDU frames containing the switch BID and the root ID every _ seconds. Initially, each switch identifies itself as the ____ bridge after boot.

How would a switch determine that another switch is now the root bridge?

How does the STA determine path cost?

Record the default port costs for various link speeds in Table 2-1.

Table 2-1 Port Costs

Link Speed	Cost (Revised IEEE Specification)	Cost (Previous IEEE Specification)
10 Gbps		
1 Gbps		
100 Mbps		
10 Mbps		

Although switch ports have a default port cost associated with them, the port cost is configurable.

To configure the port cost of an interface, enter the ______________________ command in interface configuration mode. The range value can be between ________________ and ________________ .

Record the commands, including the switch prompt, to configure the port cost for F0/1 as 15:

To verify the port and path cost to the root bridge, enter the ________________ privileged EXEC mode command, as shown here:

```
S2# __________________



VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     c025.5cd7.ef00
             Cost        15
             Port        1 (FastEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     c07b.bcc4.a980
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  15  sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/1               Root FWD 15        128.1    P2p
Fa0/2               Altn BLK 19        128.2    P2p
Fa0/3               Desg LIS 19        128.3    P2p
Fa0/4               Desg LIS 19        128.4    P2p
Fa0/6               Desg FWD 19        128.6    P2p<output omitted>
```

The BID field of a BPDU frame contains three separate fields: ________________ , ________________ , and ________________ .

Of these three fields, the ________________ is a customizable value that you can use to influence which switch becomes the root bridge. The default value for this field is ________________ .

Cisco enhanced its implementation of STP to include support for the extended system ID field, which contains the ID of the ________________ with which the BPDU is associated.

Because using the extended system ID changes the number of bits available for the bridge priority, the customizable values can only be multiples of ________________ .

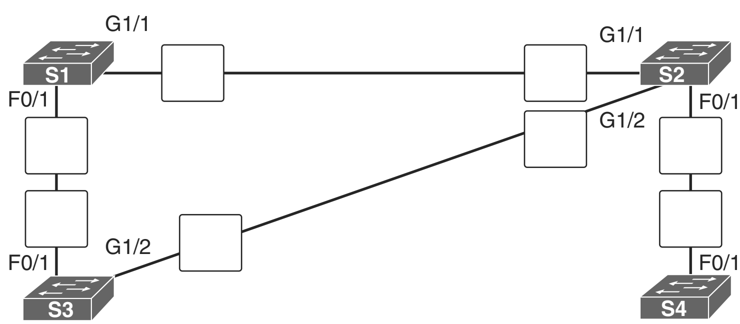
When two switches are configured with the same priority and have the same extended system ID, the switch with the lowest ________________ has the lower BID.

Identify the 802.1D Port Roles

The topologies in the next three figures do not necessarily represent an appropriate network design. However, they provide good exercise topologies for you to practice determining the STP port roles. In Figures 2-2 through 2-4, use the priority values and MAC addresses to determine the root bridge. Then label the ports with one of the following:

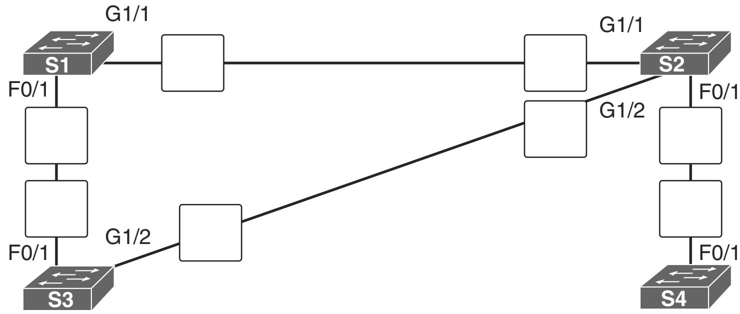
- RP: Root Port
- DP: Designated Port
- AP: Alternate Port

Figure 2-2 802.1D Port Roles - Scenario 1



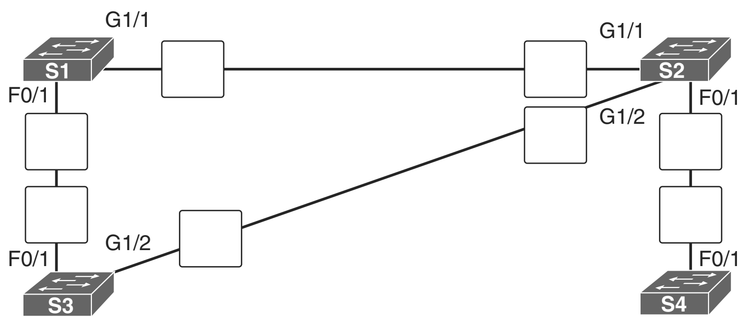
Device	Priority	MAC Address
S1	32769	000a:0001:1111
S2	24577	000a:0002:2222
S3	32769	000a:0003:3333
S4	32769	000a:0004:4444

Figure 2-3 802.1D Port Roles - Scenario 2



Device	Priority	MAC Address
S1	24577	000a:0001:1111
S2	32769	000a:0002:2222
S3	32769	000a:0003:3333
S4	32769	000a:0004:4444

Figure 2-4 802.1D Port Roles - Scenario 3



Device	Priority	MAC Address
S1	32769	000a:0001:1111
S2	32769	000a:0002:2222
S3	24577	000a:0003:3333
S4	32769	000a:0004:4444

Lab – Building a Switched Network with Redundant Links (SN 2.1.2.10/SwN 4.1.2.10)

Varieties of Spanning Tree Protocols

STP has been improved multiple times since its introduction in the original IEEE 802.1D specification. A network administrator should know which type to implement based on the equipment and topology needs.

Comparing the STP Varieties

Identify each of the STP varieties described in the following list:

- ____________________________ : This is an IEEE that maps multiple VLANs into the same spanning tree instance.
- ____________________________ : This is an evolution of STP that provides faster convergence than STP.

- ______________________: This is an updated version of the STP standard, incorporating IEEE 802.1w.
- ______________________: This is a Cisco enhancement of STP that provides a separate 802.1D spanning tree instance for each VLAN configured in the network.
- ______________________: This is a Cisco enhancement that provides a separate instance of 802.1w per VLAN.
- ______________________: This is the original IEEE 802.1D version (802.1D-1998 and earlier) that provides a loop-free topology in a network with redundant links.

Complete the cells in Table 2-2 to identify each the characteristics of each STP variety.

Table 2-2 STP Characteristics - Exercise 1

Protocol	Standard	Resources Needed	Convergence	Tree Calculation
STP		Low		
	Cisco			
	802.1w			
Rapid PVST+				
	802.1s, Cisco	Medium or high		

In Table 2-3, indicate which varieties of STP are best described by the characteristic. Some characteristics apply to more than one STP variety.

Table 2-3 STP Characteristics - Exercise 2

Characteristic	STP	PVST+	RSTP	Rapid PVST+	MSTP	MST
A Cisco implementation of 802.1s that provides up to 16 instances of RSTP.						
Cisco enhancement of RSTP.						
The default STP mode for Cisco Catalyst switches.						
Has the highest CPU and memory requirements.						
Can lead to suboptimal traffic flows.						
Cisco proprietary versions of STP.						
Cisco enhancement of STP. Provides a separate 802.1D spanning-tree instance for each VLAN.						
There is only 1 root bridge and 1 tree.						
Uses 1 IEEE 802.1D spanning-tree instance for the entire bridged network, regardless of the number of VLANs.						
Supports PortFast, BPDU guard, BPDU filter, root guard, and loop guard.						
An evolution of STP that provides faster STP convergence.						

Characteristic	STP	PVST+	RSTP	Rapid PVST+	MSTP	MST
Maps multiple VLANs that have the same traffic flow requirements into the same spanning-tree instance.						
First version of STP to address convergence issues, but still provided only one STP instance.						

PVST+ Operation

After a switch boots, the spanning tree is immediately determined as ports transition through five possible states and three BPDU timers on the way to convergence. Briefly describe each state:

- **Blocking:**
- **Listening:**
- **Learning:**
- **Forwarding:**
- **Disabled:**

Once stable, every active port in the switched network is either in the ________________ state or the ________________ state.

List and briefly describe the four steps PVST+ performs for each VLAN to provide a loop-free logical topology.

In Table 2-4, answer the "Operation Allowed" question with "yes" or "no" for each port state.

Table 2-4 Operations Allowed at Each Port State

Operation Allowed	Port State				
	Blocking	Listening	Learning	Forwarding	Disabled
Can receive and process BPDUs					
Can forward data frames received on interface					
Can forward data frames switched from another interface					
Can learn MAC addresses					

Rapid PVST+ Operation

RSTP (IEEE ________________) is an evolution of the original ________________ standard and is incorporated into the IEEE ________________ -2004 standard. Rapid PVST+ is the Cisco implementation of RSTP on a per-VLAN basis. What is the primary difference between Rapid PVST+ and RSTP?

Briefly describe the RSTP concept that corresponds to the PVST+ PortFast feature.

What command implements Cisco's version of an edge port?

In Table 2-5, indicate whether the characteristic describes PVST+, Rapid PVST+, or both.

Table 2-5 Comparing PVST+ and Rapid PVST+

Characteristic	PVST+	Rapid PVST+	Both
Cisco proprietary protocol.			
Port roles: root, designated, alternate, edge, backup.			
CPU processing and trunk bandwidth usage is greater than with STP.			
Ports can transition to forwarding state without relying on a timer.			
The root bridge is determined by the lowest BID + VLAN ID + MAC.			
Runs a separate IEEE 802.1D STP instance for each VLAN.			
Possible to have load sharing with some VLANS forwarding on each trunk.			
Sends a BPDU "hello message" every 2 seconds.			

Spanning-Tree Configuration

It is crucial to understand the impact of a default switch configuration on STP convergence and what configurations can be applied to adjust the default behavior.

PVST+ and Rapid PVST+ Configuration

Complete Table 2-6 to show the default spanning-tree configuration for a Cisco Catalyst 2960 series switch.

Table 2-6 Default Switch Configuration

Feature	Default Setting
Enable state	Enabled on VLAN 1
Spanning-tree mode	
Switch priority	
Spanning-tree port priority (configurable on a per-interface basis)	
Spanning-tree port cost (configurable on a per-interface basis)	1000 Mbps: 100 Mbps: 10 Mbps:
Spanning-tree VLAN port priority (configurable on a per-VLAN basis)	
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	1000 Mbps: 100 Mbps: 10 Mbps:
Spanning-tree timers	Hello time: seconds Forward-delay time: seconds Maximum-aging time: seconds Transmit hold count: BPDUs

Document the two different configuration commands that you can use to configure the bridge priority value so that the switch is root for VLAN 1. Use the value 4096 when necessary:

Record the command to verify that the local switch is now root:

```
S1# __________________

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
             Address     000A.0033.3333
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
  Bridge ID  Priority    24577  (priority 24576 sys-id-ext 1)
             Address     0019.aa9e.b000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 4        128.1    Shr
Fa0/2            Desg FWD 4        128.2    Shr
```

Explain the purpose of the BPDU guard feature on Cisco switches.

What command interface configuration command enables BPDU guard?

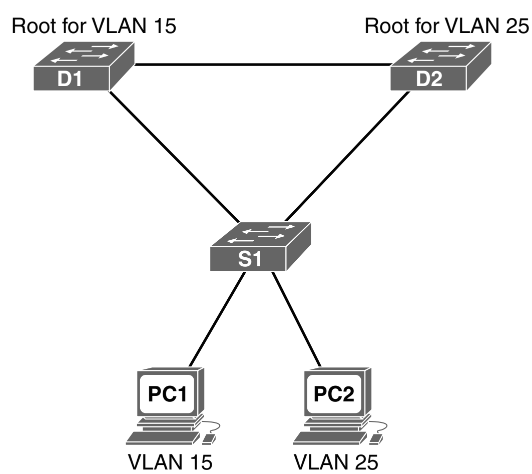
What global configuration command will configure all nontrunking ports as edge ports?

What global configuration command will configure BPDU guard on all PortFast-enabled ports?

The power of PVST+ is that it can load balance across redundant links. By default, the least-favored redundant link is not used. So, you must manually configure PVST+ to use the link.

Figure 2-5 represents a small section of Figure 2-1, showing only two distribution layer switches and one access layer switch. For this example, we have attached PC2 to S1. PC1 is assigned to VLAN 15, and PC2 is assigned to VLAN 25. D1 should be the primary root for VLAN 1 and VLAN 15 and the secondary root for VLAN 25. D2 should be the primary root for VLAN 25 and the secondary root for VLAN 15.

Figure 2-5 PVST+ Configuration Topology



Based on these requirements, document the commands to modify the default PVST+ operation on D1 and D2.

D1 commands

D2 commands

Document the commands to configure all nontrunking ports on S1 as edge ports with BPDU guard enabled.

Now, assume that you want to run rapid PVST+ on all three switches. What command is required?

Lab - Configuring Rapid PVST+, PortFast, and BPDU Guard (SN 2.3.2.3/SwN 4.3.2.3)

Packet Tracer - Configuring PVST+ (SN 2.3.1.5/SwN 4.3.1.5)

Packet Tracer - Configuring Rapid PVST+ (SN 2.3.2.2/SwN 4.3.2.2)

First Hop Redundancy Protocols

Up to this point, we've been reviewing STP and how to manipulate the election of root bridges and load balance across redundant links. In addition to Layer 1 and Layer 2 redundancy, a high-availability network might also implement Layer 3 redundancy by sharing the default gateway responsibility across multiple devices. Through the use of a virtual IP address, two Layer 3 devices can share the default gateway responsibility. The section reviews First Hop Redundancy Protocols (FHRPs) that provide Layer 3 redundancy.

Identify FHRP Terminology

Match the definition on the left with the terms on the right. This is a one-to-one matching exercise.

Definitions

____ The ability to dynamically recover from the failure of a device acting as the default gateway

____ Two or more routers sharing a single MAC and IP address

____ A device that is part of a virtual router group assigned to the role of default gateway

____ Provides the mechanism for determining which router should take the active role in forwarding traffic

____ A device that routes traffic destined to network segments beyond the source network segment

____ A device that is part of a virtual router group assigned the role of alternate default gateway

____ A Layer 3 address assigned to a protocol that shares the single address among multiple devices

____ The Layer 2 address returned by ARP for an FHRP gateway

Terms

- **a.** Default gateway
- **b.** First-hop redundancy
- **c.** Forwarding router
- **d.** Redundancy rrotocol
- **e.** Standby router
- **f.** Virtual IP address
- **g.** Virtual MAC address
- **h.** Virtual router

Identify the Type of FHRP

In Table 2-7, indicate whether the characteristic describes HSRP, VRRP, or GLBP.

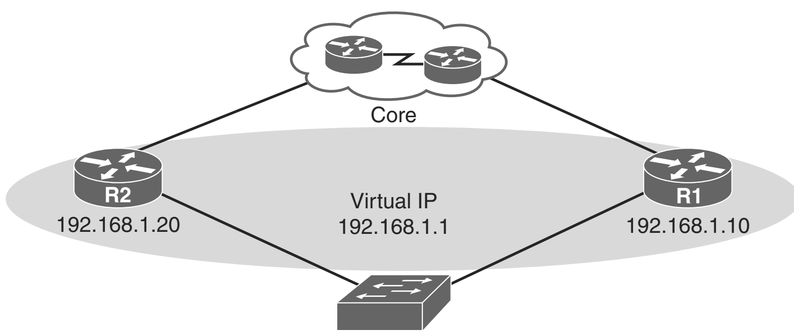
Table 2-7 FHRP Characteristics

FHRP Characteristic	HSRP	VRRP	GLBP
Used in a group of routers for selecting an active device and a standby device.			
A nonproprietary election protocol that allows several routers on a multi-access link to use the same virtual IPv4 address.			
Cisco-proprietary FHRP protocol designed to allow for transparent failover of a first-hop IPv4 devices.			
Cisco-proprietary FHRP protocol that protects data traffic from a failed router or circuit while also allowing load sharing between a group of redundant routers.			
One router is elected as the virtual router master, with the other routers acting as backups in case the virtual router master fails.			

HSRP and GLBP Configuration and Verification

Refer to the topology in Figure 2-6. R2 has been configured for HSRP group 20, priority 120, IP address 192.168.1.20, and virtual IP address 192.168.1.1.

Figure 2-6 HSRP and GLBP Configuration Topology



Example 2-1 shows the HSRP configuration for R2.

Example 2-1 R2 HSRP Configuration

```
R2# show run interface g0/1
<output omitted>
interface GigabitEthernet0/1
 ip address 192.168.1.20 255.255.255.0
 standby 20 ip 192.168.1.1
 standby 20 priority 120
<output omitted>
```

Using the information in Example 2-1, document the commands to configure R1 as the HSRP active router in group 20 using a priority of 210.

What command would generate the following output to verify the HSRP configuration?

```
R1#___________________
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/1       20   210   Active  local           192.168.1.20    192.168.1.1
```

Now assume that all HSRP configurations have been removed. R2 has been configured for GLBP group 20, priority 120, IP address 192.168.1.20, and virtual IP address 192.168.1.1.

Example 2-2 shows the GLBP configuration for R2.

Example 2-2 R2 GLBP Configuration

```
R2# show run interface g0/1
<output omitted>
interface GigabitEthernet0/1
 ip address 192.168.1.20 255.255.255.0
 glbp 20 ip 192.168.1.1
 glbp 20 priority 120
<output omitted>
```

Using the information in Example 2-2, document the commands to configure R1 to be in GLBP group 20 using a priority of 210.

What command would generate the following output to verify the GLBP configuration?

```
R1#___________________
GigabitEthernet0/0 - Group 20
  State is Active
    1 state change, last state change 00:03:05
  Virtual IP address is 192.168.1.1
```

```
Hello time 3 sec, hold time 10 sec
  Next hello sent in 1.792 secs
Redirect time 600 sec, forwarder timeout 14400 sec
Preemption disabled
Active is local
Standby is 192.168.1.20, priority 120 (expires in 9.024 sec)
Priority 210 (configured)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: round-robin
Group members:
  0006.f671.db58 (192.168.1.10) local
  0006.f671.eb38 (192.168.1.20)
There are 2 forwarders (1 active)
Forwarder 1
  State is Active
    1 state change, last state change 00:02:53
  MAC address is 0007.b400.0a01 (default)
  Owner ID is 0006.f671.db58
  Redirection enabled
  Preemption enabled, min delay 30 sec
  Active is local, weighting 100
Forwarder 2
  State is Listen
  MAC address is 0007.b400.0a02 (learnt)
  Owner ID is 0006.f671.eb38
  Redirection enabled, 599.040 sec remaining (maximum 600 sec)
  Time to live: 14399.040 sec (maximum 14400 sec)
  Preemption enabled, min delay 30 sec
  Active is 192.168.1.20 (primary), weighting 100 (expires in 9.312 sec)
```

Lab - Configuring HSRP and GLBP (SN 2.4.3.4/SwN 4.4.3.4)

CHAPTER 3

Link Aggregation

Link aggregation is the ability to create one logical link using multiple physical links between two devices. This allows load sharing among the physical links, rather than having a STP block one or more of the links.

Link Aggregation Concepts

One of the best ways to reduce the time it takes for STP convergence is to simply avoid STP. EtherChannel is a form of link aggregation used in switched networks.

EtherChannel Advantages

EtherChannel technology was originally developed by Cisco as a technique of grouping several Fast Ethernet or Gigabit Ethernet switch ports into one logical channel.

List at least three advantages to using EtherChannel:

-
-
-
-
-

EtherChannel Operation

You can configure EtherChannel as static or unconditional. However, there are also two protocols that can be used to configure the negotiation process: Port Aggregation Protocol (PAgP—Cisco proprietary) and Link Aggregation Control Protocol (LACP—IEEE 802.3ad).

These two protocols ensure that both sides of the link have compatible configurations—same speed, duplex setting, and VLAN information. The modes for each differ slightly.

For PAgP, briefly describe each of the following modes:

- **On:**
- **Desirable:**
- **Auto:**

For LACP, briefly describe each of the following modes:

- **On:**
- **Active:**
- **Passive:**

In Table 3-1, indicate the mode that is described.

Table 3-1 PAgP and LACP Modes

Mode	PAgP and/or LACP Mode Description
	Initiates LACP negotiations with other interfaces.
	Forces EtherChannel state without PAgP or LACP initiated negotiations.
	Places an interface in a passive, responding state. Does not initiate PAgP negotiations.
	Actively initiates PAgP negotiations with other interfaces.
	Places an interface in a passive, responding state. Does not initiate LACP negotiations.

The mode that is configured on each side of the EtherChannel link determines whether EtherChannel will be operational.

In Table 3-2, two switches are using PAgP. Indicate with "yes" or "no" whether EtherChannel is established.

Table 3-2 EtherChannel Negotiation Using PAgP

Switch 1 Mode	Switch 2 Mode	EtherChannel Established?
Auto	Auto	
Auto	Desirable	
On	Desirable	
On	Off	
Desirable	Desirable	

In Table 3-3, two switches are using LACP. Indicate with "yes" or "no" whether EtherChannel is established.

Table 3-3 EtherChannel Negotiation Using LACP

Switch 1 Mode	Switch 2 Mode	EtherChannel Established?
Passive	On	
Passive	Active	
On	On	
Passive	Passive	
On	Active	

Link Aggregation Configuration

EtherChannel configuration is rather straightforward once you decide on which protocol you will use. In fact, the easiest method is to just force both sides to be on.

Configuring EtherChannel

To configure EtherChannel, complete the following steps:

Step 1. Specify the interfaces that, participate in the EtherChannel group using the **interface range** *interface* command.

What are the requirements for each interface before they can form an EtherChannel?

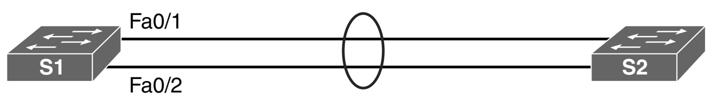
Step 2. Create the port channel interface with the **channel-group** *identifier* **mode** {**on** | **auto** | **desirable** | **active** | **passive**} command in interface range configuration mode. The keyword ________________ forces the port to channel without PAgP or LACP. The keywords ________________ and ________________ enable PAgP. The keywords ________________ and ________________ enable LACP.

Step 3. The **channel-group** command automatically creates a port channel interface using the *identifier* as the number. Use the **interface port-channel** *identifier* command to configure channel-wide settings like trunking, native VLANs, or allowed VLANs.

As you can see from the configuration steps, the way you specify whether to use PAgP, LACP, or no negotiations is by configuring one keyword in the **channel-group** command.

So, with those steps in mind, consider Figure 3-1 in each of the following configuration scenarios.

Figure 3-1 EtherChannel Topology



EtherChannel Configuration Scenario 1

Record the commands, including the switch prompt, to configure the S1 Fa0/1 and Fa0/2 into an EtherChannel without negotiations. Then force the channel to trunking using native VLAN 99.

```
S1(config)#
```

EtherChannel Configuration Scenario 1

Record the commands, including the switch prompt, to configure the S1 Fa0/1 and Fa0/2 into an EtherChannel using PAgP. S1 should initiate the negotiations. The channel should trunk, allowing only VLANs 1, 10, and 20.

```
S1(config)#
```

EtherChannel Configuration Scenario 1

Record the commands, including the switch prompt, to configure the S1 Fa0/1 and Fa0/2 into an EtherChannel using LACP. S1 should not initiate the negotiations. The channel should trunk, allowing all VLANs.

```
S1(config)#
```

Lab - Configuring EtherChannel (SN 3.2.1.4/SwN 5.2.1.4)

Packet Tracer Activity

Packet Tracer - Configuring EtherChannel (SN 3.2.1.3/SwN 5.2.1.3)

Verifying and Troubleshooting EtherChannel

Record the commands used to display the output in Example 3-1.

Example 3-1 EtherChannel Verification Commands

```
S1# ________________________________________________
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0cd9.96e8.8a01 (bia 0cd9.96e8.8a01)
  MTU 1500 bytes, BW 200000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<output omitted>

S1# ________________________________________________
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1
```

```
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Fa0/1(P)    Fa0/2(P)

S1# ______________________________________________________________________________
               Channel-group listing:
               ----------------------

Group: 1
----------
               Port-channels in the group:
               ---------------------------

Port-channel: Po1    (Primary Aggregator)

------------

Age of the Port-channel   = 0d:00h:25m:17s
Logical slot/port   = 2/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa0/1    Active             0
  0     00     Fa0/2    Active             0

Time since last port bundled:    0d:00h:05m:41s    Fa0/2
Time since last port Un-bundled: 0d:00h:05m:48s    Fa0/2

S1# ______________________________________________________________________________
Port state    = Up Mstr Assoc In-Bndl
Channel group = 1           Mode = Active          Gcchange = -
Port-channel  = Po1         GC   =   -             Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol =   LACP

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
```

```
Local information:
                              LACP port     Admin     Oper     Port        Port
Port       Flags    State     Priority      Key       Key      Number      State
Fa0/1      SA       bndl      32768         0x1       0x1      0x102       0x3D

Partner's information:

                  LACP port                        Admin   Oper    Port     Port
Port       Flags    Priority  Dev ID          Age    key     Key     Number   State
Fa0/1      SA       32768     0cd9.96d2.4000   4s    0x0     0x1     0x102    0x3D

Age of the port in the current state: 0d:00h:24m:59s
S1#
```

When troubleshooting an EtherChannel issue, keep in mind the configuration restrictions for interfaces that participate in the channel. List at least four restrictions.

-
-
-
-
-

Refer to the output for S1 and S2 in Example 3-2. Record the command that generated the output.

Example 3-2 Troubleshooting an EtherChannel Issue

```
S1# ______________________________________________________________________________
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SD)          -        Fa0/1(D)    Fa0/2(D)
S1# show run | begin interface Port-channel
```

```
interface Port-channel1
 switchport mode trunk
!
interface FastEthernet0/1
 switchport mode trunk
 channel-group 1 mode auto
!
interface FastEthernet0/2
 switchport mode trunk
 channel-group 1 mode auto
!
<output omitted>
S 1#
```

```
S2# show run | begin interface Port-channel
interface Port-channel1
 switchport mode trunk
!
interface FastEthernet0/1
 switchport mode trunk
 channel-group 1 mode auto
!
interface FastEthernet0/2
 switchport mode trunk
 channel-group 1 mode auto
!
<output omitted>
S2#
```

Explain why the EtherChannel between S1 and S2 is down.

EtherChannel and spanning tree must interoperate. For this reason, the order in which EtherChannel-related commands are entered is important. To correct this issue, you must first remove the port channel. Otherwise, spanning-tree errors cause the associated ports to go into blocking or errdisabled state. With that in mind, what would you suggest to correct the issue shown in Example 3-2 if the requirement is to use PAgP? What commands would be required?

Lab - Troubleshooting EtherChannel (SN 3.2.2.4/SwN 5.2.2.4)

Packet Tracer **Activity**

Packet Tracer - Troubleshooting EtherChannel (SN 3.2.2.3/SwN 5.2.2.3)

Packet Tracer - Skills Integration Challenge (SN 3.3.1.2/SwN 5.3.1.2)