Lab Manual

Scaling Networks

ciscopress.com

Cisco | Networking Academy®
Mind Wide Open™

Scaling Networks Lab Manual

Cisco Networking Academy

Cisco Press
800 East 96th Street
Indianapolis, Indiana 46240

Scaling Networks Lab Manual
Cisco Networking Academy

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

Printed in the United States of America

First Printing December 2013

ISBN-13: 9781587133251

ISBN-10: 1587133253

Warning and Disclaimer

This book is designed to provide information about Scaling Networks. 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.

This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, please visit www.cisco.com/edu.

Feedback Information

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

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

We greatly appreciate your assistance.

Publisher	**Paul Boger**
Associate Publisher	**Dave Dusthimer**
Business Operations Manager, Cisco Press	**Jan Cornelssen**
Executive Editor	**Mary Beth Ray**
Managing Editor	**Sandra Schroeder**
Project Editor	**Seth Kerney**
Editorial Assistant	**Vanessa Evans**
Cover Designer	**Mark Shirar**
Compositor	**TnT Design, Inc.**

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.

Contents

About This Lab Manual

Scaling Networks Lab Manual contains all the labs and class activities from the Cisco Networking Academy course of the same name. It is meant to be used within this program of study.

More Practice

If you would like more practice activities, combine your Lab Manual with the new *CCNA Routing and Switching Practice and Study Guide* ISBN: 9781587133442

Other Related Titles

CCNA Routing and Switching Portable Command Guide ISBN: 9781587204302 (or eBook ISBN: 9780133381368)

Scaling Networks Companion Guide ISBN: 9781587133282 (or eBook ISBN: 9780133476408)

Scaling Networks Course Booklet ISBN: 9781587133244

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.

Chapter 1 — Introduction to Scaling Networks

1.0.1.2 Class Activity – Network by Design

Objective

Explain the need to design a hierarchical network that is scalable.

Scenario

Your employer is opening a new, branch office.

You have been reassigned to the site as the network administrator where your job will be to design and maintain the new branch network.

The network administrators at the other branches used the Cisco three-layer hierarchical model when designing their networks. You decide to use the same approach.

To get an idea of what using the hierarchical model can do to enhance the design process, you research the topic.

Resources

- World Wide Web access
- Word processing software

Directions

Step 1: Use the Internet to find information and take notes about the Cisco three-layer hierarchical model. The site should include information about the:

a. Access layer

b. Distribution layer

c. Core layer

Step 2: In your research, make sure to include:

a. A simple definition of each hierarchical layer

b. Three concise facts about each layer

c. Network device capabilities needed at each layer

d. A detailed graphic that shows a full, three-layer hierarchical model design

Step 3: Create a simple table to organize and share your research with another student, group, the class, or instructor.

1.2.1.8 Lab – Selecting Switching Hardware

Objectives

Part 1: Explore Cisco Switch Products

Part 2: Select an Access Layer Switch

Part 3: Select a Distribution/Core Layer Switch

Background / Scenario

As a Network Engineer, you are part of a team that selects appropriate devices for your network. You need to consider the network requirements for the company as they migrate to a converged network. This converged network supports voice over IP (VoIP), video streaming, and expansion of the company to support a larger customer base.

For a small- to medium-sized company, Cisco hierarchical network design suggests only using a two-tier LAN design. This design consists of an access layer and a collapsed core/distribution layer. Network switches come in different form factors, and with various features and functions. When selecting a switch, the team must choose between fixed configuration or modular configuration, and stackable or non-stackable switches.

Based on a given set of requirements, you will identify the Cisco switch models and features to support the requirements. The scope of this lab will limit the switch models to campus LAN only.

Required Resources

PC with Internet access

Part 1: Explore Cisco Switch Products

In Part 1, you will navigate the Cisco website and explore available switch products.

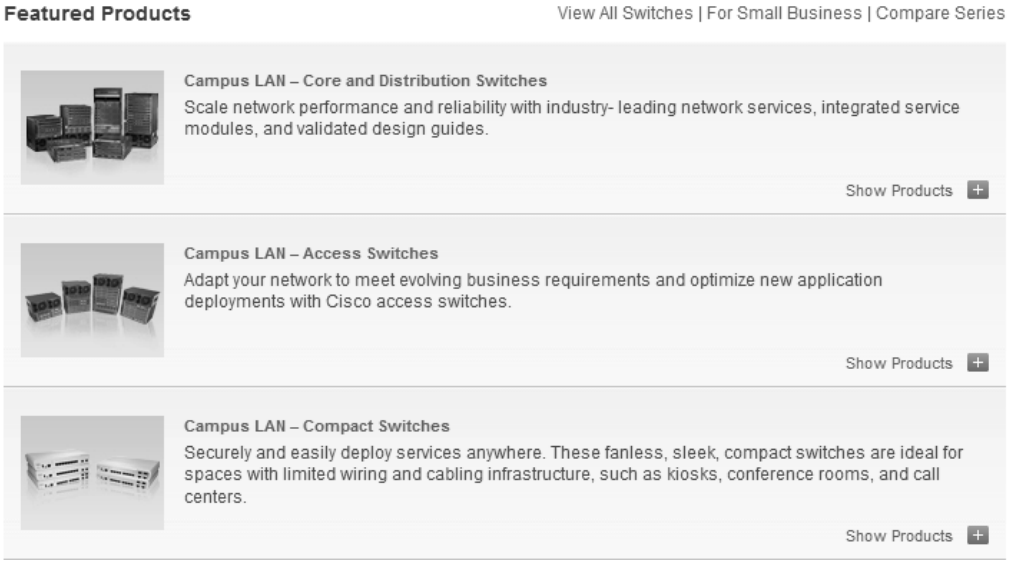
Step 1: Navigate the Cisco website.

At www.cisco.com, a list of available products and information about these products is available.

a. From the home page, click **Products & Services** > **Switches**.

Step 2: Explore switch products.

In the Feature Products section, a list of different categories of switches is displayed. In this lab, you will explore the campus LAN switches. You can click different links to gather information about the different switch models. On this page, the information is organized in different ways. You can view all available switches by clicking **View All Switches**. If you click **Compare Series**, the switches are organized by types: modular vs. fixed configuration.



a. Click the heading **Campus LAN – Core and Distribution Switches**.

List a few models and some of features in the table below.

Model	Uplink Speed	Number of Ports/Speed	Other Features

b. Click the heading **Campus LAN – Access Switches**.

List a few models and some of features in the table below.

Model	Uplink Speed	Number of Ports/Speed	Other Features

c. Click the heading **Campus LAN – Compact Switches**.

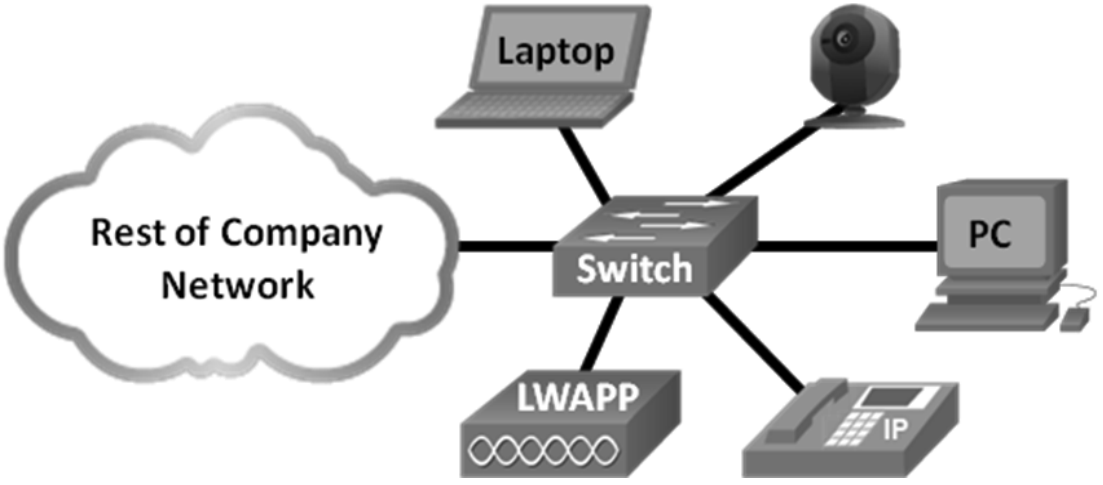
List a few models and some of features in the table below.

Model	Uplink Speed	Number of Ports/Speed	Other Features

Part 2: Select an Access Layer Switch

The main function of an access layer switch is to provide network access to end user devices. This switch connects to the core/distribution layer switches. Access switches are usually located in the intermediate distribution frame (IDF). An IDF is mainly used for managing and interconnecting the telecommunications cables between end user devices and a main distribution frame (MDF). There are typically multiple IDFs with uplinks to a single centralized MDF.

An access switch should have the following capabilities: low cost per switch port, high port density, scalable uplinks to higher layers, and user access functions and resiliency. In Part 2, you will select an access switch based on the requirements set by the company. You have reviewed and become familiar with Cisco switch product line.



a. Company A requires a replacement access switch in the wiring closet. The company requires the switch to support VoIP and multicast, accommodate future growth of users and increased bandwidth usage. The switch must support a minimum of 35 current users and have a high-speed uplink. List a few of models that meet those requirements.

_____

_____

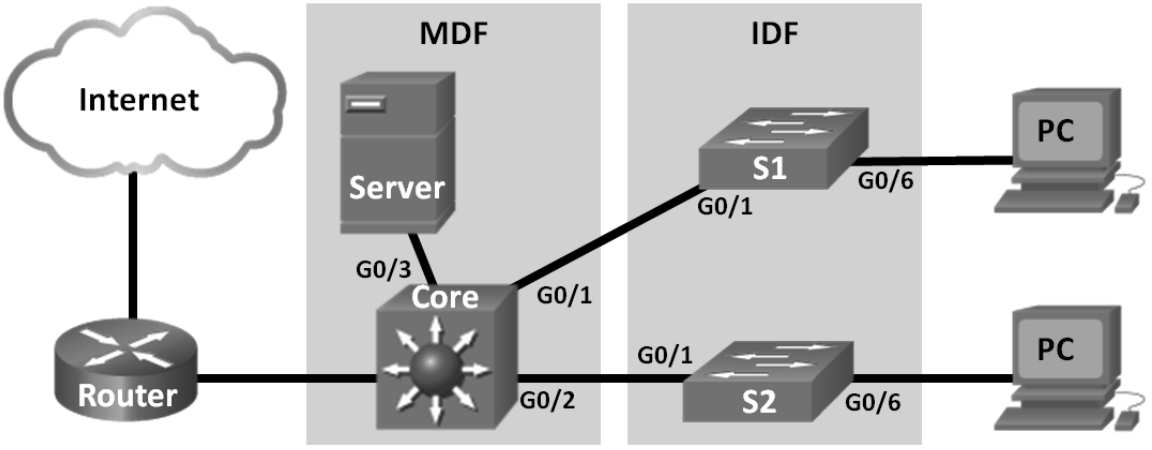
b. Company B would like to extend services to a conference room on an as-needed basis. The switch will be placed on the conference room table, and switch security is a priority.

_____

_____

Part 3: Select a Distribution/Core Layer Switch

The distribution/core switch is the backbone of the network for the company. A reliable network core is of paramount importance for the function of the company. A network backbone switch provides both adequate capacity for current and future traffic requirements and resilience in the event of failure. They also require high throughput, high availability, and advanced quality of service (QoS). These switches usually reside in the main wiring closet (MDF) along with high speed servers, routers, and the termination point of your ISP.



a. Company C will replace a backbone switch in the next budget cycle. The switch must provide redundancy features to minimize possible downtime in the event that an internal component fails. What features can accommodate these requirements for the replacement switch?

_____

_____

b. Which Cisco Catalyst switches would you recommend?

_____

c. As Company C grows, high speed, such as 10 GB Ethernet, up to 8 uplink ports, and a modular configuration for the switch will become necessary. Which switch models would meet the requirement?

_____

Reflection

What other factors should be considered during the selection process aside from network requirements and costs?

_____

_____

1.3.1.1 Class Activity – Layered Network Design Simulation

Objective

Explain the need to design a hierarchical network that is scalable.

Scenario

As the network administrator for a very small network, you want to prepare a simulated-network presentation for your branch manager to explain how the network currently operates.

The small network includes the following equipment:

- One Cisco 2911 series router
- One Cisco 3560 switch
- One Cisco 2960 switch
- Four user workstations (PCs or laptops)
- One printer

Resources

- Packet Tracer software

Directions

Step 1: Create a simple network topology using Packet Tracer software. Place the devices at the appropriate levels of the Cisco three-layer hierarchical model design, including:

a. One Cisco 2911 series router

b. One Cisco 3560 switch

c. One Cisco 2960 switch

d. Four user workstations (PCs or laptops)

e. One printer

Step 2: Using Packet Tracer's drawing tool and indicate the hierarchical layers with different color coding and labels:

a. Access layer

b. Distribution layer

c. Core layer

Step 3: Configure the network and user devices. Check for end-to-end connectivity.

Step 4: Share your configuration and hierarchical network design Packet Tracer file with another student, group, the class, or the instructor.

Chapter 2 — LAN Redundancy

2.0.1.2 Class Activity – Stormy Traffic

Objective

Explain the purpose of the Spanning Tree Protocol (STP) in a switched LAN environment with redundant switch links.

Scenario

It is your first day on the job as a network administrator for a small- to medium-sized business. The previous network administrator left suddenly after a network upgrade took place for the business.

During the upgrade, a new switch was added. Since the upgrade, many employees complain that they are having trouble accessing the Internet and servers on your network. In fact, most of them cannot access the network at all. Your corporate manager asks you to immediately research what could be causing these connectivity problems and delays.

So you take a look at the equipment operating on your network at your main distribution facility in the building. You notice that the network topology seems to be visually correct and that cables have been connected correctly, routers and switches are powered on and operational, and switches are connected together to provide backup or redundancy.

However, one thing you do notice is that all of your switches' status lights are constantly blinking at a very fast pace to the point that they almost appear solid. You think you have found the problem with the connectivity issues your employees are experiencing.

Use the Internet to research STP. As you research, take notes and describe:

- Broadcast storm
- Switching loops
- The purpose of STP
- Variations of STP

Complete the reflection questions that accompany the PDF file for this activity. Save your work and be prepared to share your answers with the class.

Resources

- Internet access to the World Wide Web

Reflection

1. What is a definition of a broadcast storm? How does a broadcast storm develop?

   _____

2. What is a definition of a switching loop? What causes a switching loop?

   _____

3. How can you mitigate broadcast storms and switching loops caused by introducing redundant switches to your network?

   _____

4. What is the IEEE standard for STP and some other STP variations, as mentioned in the hyperlinks provided?

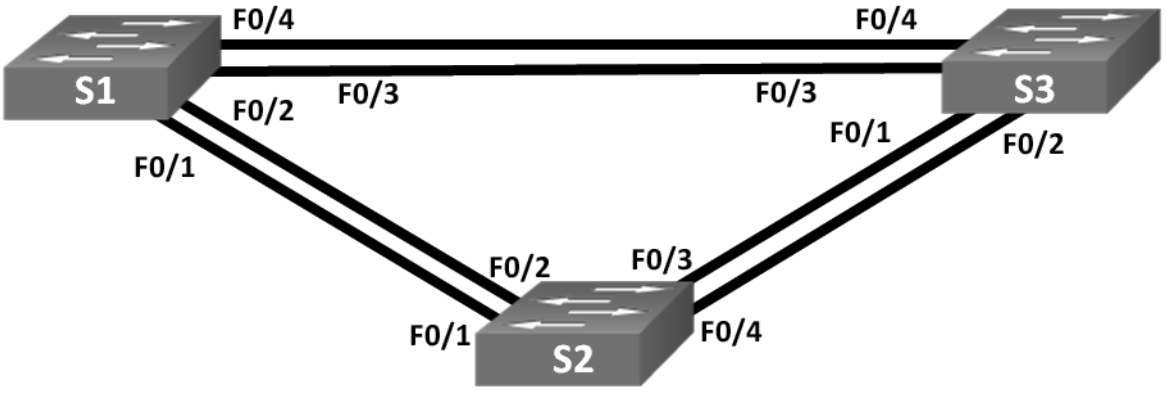
   _____

5. In answer to this scenario, what would be your first step (after visually checking your network) to correcting the described network problem?

   _____

2.1.2.10 Lab – Building a Switched Network with Redundant Links

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.1	255.255.255.0
S2	VLAN 1	192.168.1.2	255.255.255.0
S3	VLAN 1	192.168.1.3	255.255.255.0

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Determine the Root Bridge

Part 3: Observe STP Port Selection Based on Port Cost

Part 4: Observe STP Port Selection Based on Port Priority

Background / Scenario

Redundancy increases the availability of devices in the network topology by protecting the network from a single point of failure. Redundancy in a switched network is accomplished through the use of multiple switches or multiple links between switches. When physical redundancy is introduced into a network design, loops and duplicate frames can occur.

The Spanning Tree Protocol (STP) was developed as a Layer 2 loop-avoidance mechanism for redundant links in a switched network. STP ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop.

In this lab, you will use the **show spanning-tree** command to observe the STP election process of the root bridge. You will also observe the port selection process based on cost and priority.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other

switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the switches.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Initialize and reload the switches as necessary.

Step 3: Configure basic settings for each switch.

a. Disable DNS lookup.

b. Configure the device name as shown in the topology.

c. Assign **class** as the encrypted privileged EXEC mode password.

d. Assign **cisco** as the console and vty passwords and enable login for console and vty lines.

e. Configure logging synchronous for the console line.

f. Configure a message of the day (MOTD) banner to warn users that unauthorized access is prohibited.

g. Configure the IP address listed in the Addressing Table for VLAN 1 on all switches.

h. Copy the running configuration to the startup configuration.

Step 4: Test connectivity.

Verify that the switches can ping one another.

Can S1 ping S2? _____

Can S1 ping S3? _____

Can S2 ping S3? _____

Troubleshoot until you are able to answer yes to all questions.

Part 2: Determine the Root Bridge

Every spanning-tree instance (switched LAN or broadcast domain) has a switch designated as the root bridge. The root bridge serves as a reference point for all spanning-tree calculations to determine which redundant paths to block.

An election process determines which switch becomes the root bridge. The switch with the lowest bridge identifier (BID) becomes the root bridge. The BID is made up of a bridge priority value, an extended system ID, and the MAC address of the switch. The priority value can range from 0 to 65,535, in increments of 4,096, with a default value of 32,768.

Step 1: Deactivate all ports on the switches.

Step 2: Configure connected ports as trunks.

Step 3: Activate ports F0/2 and F0/4 on all switches.

Step 4: Display spanning tree information.

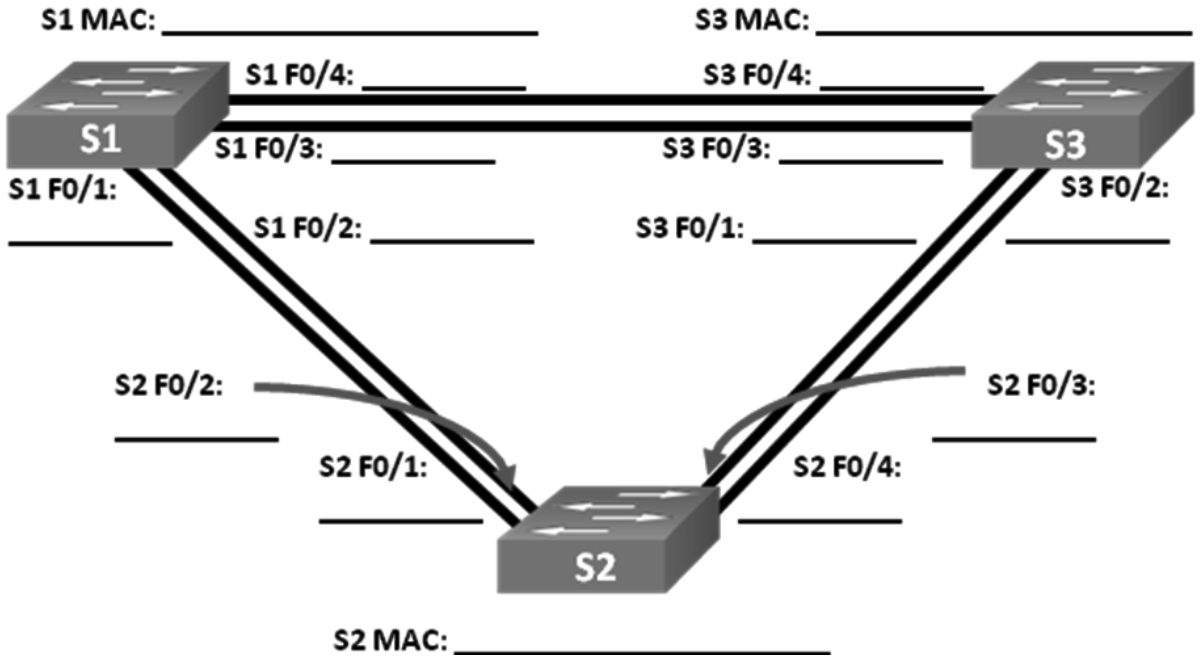
Issue the **show spanning-tree** command on all three switches. The Bridge ID Priority is calculated by adding the priority value and the extended system ID. The extended system ID is always the VLAN number. In the example below, all three switches have equal Bridge ID Priority values (32769 = 32768 + 1, where default priority = 32768, VLAN number = 1); therefore, the switch with the lowest MAC address becomes the root bridge (S2 in the example).

```
S1# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             Cost        19
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0cd9.96e8.8a00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/2               Root FWD 19        128.2    P2p
Fa0/4               Altn BLK 19        128.4    P2p
```

```
S2# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0cd9.96d2.4000
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/2               Desg FWD 19        128.2    P2p
Fa0/4               Desg FWD 19        128.4    P2p

S3# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             Cost        19
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0cd9.96e8.7400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/2               Root FWD 19        128.2    P2p
Fa0/4               Desg FWD 19        128.4    P2p
```

Note: The default STP mode on the 2960 switch is Per VLAN Spanning Tree (PVST).

In the diagram below, record the Role and Status (Sts) of the active ports on each switch in the Topology.



Based on the output from your switches, answer the following questions.

Which switch is the root bridge? _____

Why did spanning tree select this switch as the root bridge?

_____

Which ports are the root ports on the switches? _____

Which ports are the designated ports on the switches? _____

What port is showing as an alternate port and is currently being blocked? _____

Why did spanning tree select this port as the non-designated (blocked) port?

_____

_____

_____

_____

Part 3: Observe STP Port Selection Based on Port Cost

The spanning tree algorithm (STA) uses the root bridge as the reference point and then determines which ports to block, based on path cost. The port with the lower path cost is preferred. If port costs are equal, then spanning tree compares BIDs. If the BIDs are equal, then the port priorities are used to break the tie. Lower values are always preferred. In Part 3, you will change the port cost to control which port is blocked by spanning tree.

Step 1: Locate the switch with the blocked port.

With the current configuration, only one switch should have a port that is blocked by STP. Issue the **show spanning-tree** command on both non-root switches. In the example below, spanning tree is blocking port F0/4 on the switch with the highest BID (S1).

```
S1# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             Cost        19
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0cd9.96e8.8a00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/2               Root FWD 19        128.2    P2p
Fa0/4               Altn BLK 19        128.4    P2p

S3# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             Cost        19
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
```

```
             Address     0cd9.96e8.7400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  15  sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/2               Root FWD 19        128.2    P2p
Fa0/4               Desg FWD 19        128.4    P2p
```

Note: Root bridge and port selection may differ in your topology.

Step 2: Change port cost.

In addition to the blocked port, the only other active port on this switch is the port designated as the root port. Lower the cost of this root port to 18 by issuing the **spanning-tree cost 18** interface configuration mode command.

```
S1(config)# interface f0/2
S1(config-if)# spanning-tree cost 18
```

Step 3: Observe spanning tree changes.

Re-issue the **show spanning-tree** command on both non-root switches. Observe that the previously blocked port (S1 - F0/4) is now a designated port and spanning tree is now blocking a port on the other non-root switch (S3 - F0/4).

```
S1# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             Cost        18
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0cd9.96e8.8a00
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/2               Root FWD 18        128.2    P2p
Fa0/4               Desg FWD 19        128.4    P2p
```

```
S3# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             Cost        19
             Port        2 (FastEthernet0/2)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     0cd9.96e8.7400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Fa0/2               Root FWD 19        128.2    P2p
Fa0/4               Altn BLK 19        128.4    P2p
```

Why did spanning tree change the previously blocked port to a designated port, and block the port that was a designated port on the other switch?

_____

Step 4: Remove port cost changes.

a. Issue the **no spanning-tree cost 18** interface configuration mode command to remove the cost statement that you created earlier.

```
S1(config)# interface f0/2
S1(config-if)# no spanning-tree cost 18
```

b. Re-issue the **show spanning-tree** command to verify that STP has reset the port on the non-root switches back to the original port settings. It takes approximately 30 seconds for STP to complete the port transition process.

Part 4: Observe STP Port Selection Based on Port Priority

If port costs are equal, then spanning tree compares BIDs. If the BIDs are equal, then the port priorities are used to break the tie. The default port priority value is 128. STP aggregates the port priority with the port number to break ties. Lower values are always preferred. In Part 4, you will activate redundant paths to each switch to observe how STP selects a port using the port priority.

a. Activate ports F0/1 and F0/3 on all switches.

b. Wait 30 seconds for STP to complete the port transition process, and then issue the **show spanning-tree** command on the non-root switches. Observe that the root port has moved to the lower numbered port linked to the root switch, and blocked the previous root port.

```
S1# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             Cost        19
             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     0cd9.96e8.8a00
             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 19        128.1    P2p
Fa0/2               Altn BLK 19        128.2    P2p
Fa0/3               Altn BLK 19        128.3    P2p
Fa0/4               Altn BLK 19        128.4    P2p

S3# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0cd9.96d2.4000
             Cost        19
             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     0cd9.96e8.7400
             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 19        128.1    P2p
Fa0/2               Altn BLK 19        128.2    P2p
Fa0/3               Desg FWD 19        128.3    P2p
Fa0/4               Desg FWD 19        128.4    P2p
```

What port did STP select as the root port on each non-root switch? _____

Why did STP select these ports as the root port on these switches?

_____

_____

Reflection

1. After a root bridge has been selected, what is the first value STP uses to determine port selection?

   _____

2. If the first value is equal on the two ports, what is the next value that STP uses to determine port selection?

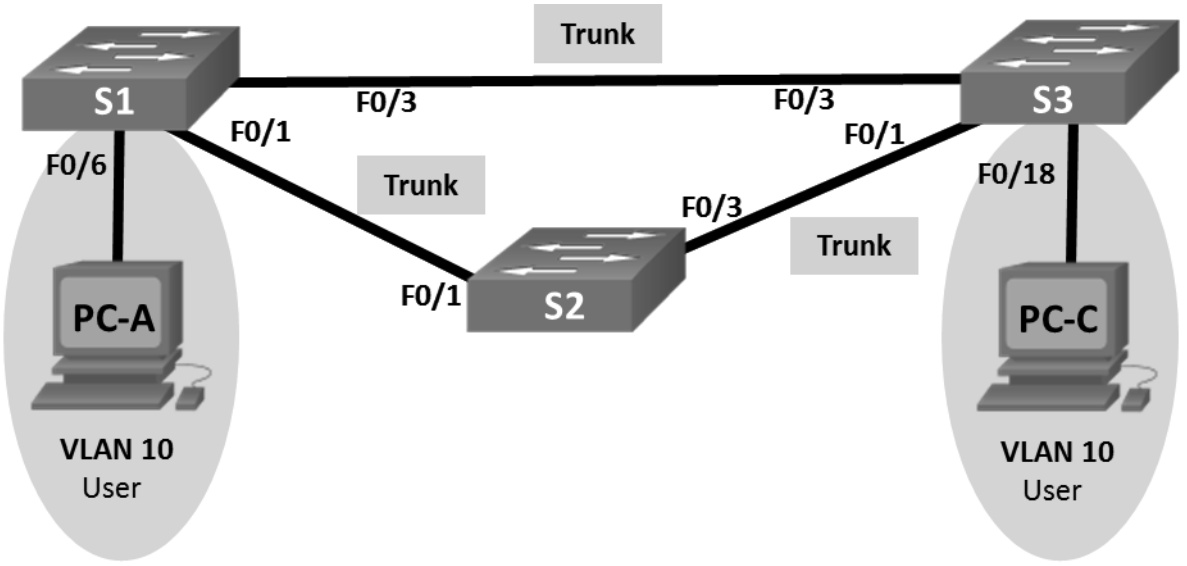
   _____

3. If both values are equal on the two ports, what is the next value that STP uses to determine port selection?

   _____

2.3.2.3 Lab – Configuring Rapid PVST+, PortFast, and BPDU Guard

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 99	192.168.1.11	255.255.255.0
S2	VLAN 99	192.168.1.12	255.255.255.0
S3	VLAN 99	192.168.1.13	255.255.255.0
PC-A	NIC	192.168.0.2	255.255.255.0
PC-C	NIC	192.168.0.3	255.255.255.0

VLAN Assignments

VLAN	Name
10	User
99	Management

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure VLANs, Native VLAN, and Trunks

Part 3: Configure the Root Bridge and Examine PVST+ Convergence

Part 4: Configure Rapid PVST+, PortFast, BPDU Guard, and Examine Convergence

Background / Scenario

The Per-VLAN Spanning Tree (PVST) protocol is Cisco proprietary. Cisco switches default to PVST. Rapid PVST+ (IEEE 802.1w) is an enhanced version of PVST+ and allows for faster spanning-tree calculations and convergence in response to Layer 2 topology changes. Rapid PVST+ defines three port states: discarding, learning, and forwarding, and provides multiple enhancements to optimize network performance.

In this lab, you will configure the primary and secondary root bridge, examine PVST+ convergence, configure Rapid PVST+ and compare its convergence to PVST+. In addition, you will configure edge ports to transition immediately to a forwarding state using PortFast and prevent the edge ports from forwarding BDPUs using BDPU guard.

Note: This lab provides minimal assistance with the actual commands necessary for configuration. However, the required commands are provided in Appendix A. Test your knowledge by trying to configure the devices without referring to the appendix.

Note: The switches used with CCNA hands-on labs are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords.

Step 1: Cable the network as shown in the topology.

Step 2: Configure PC hosts.

Step 3: Initialize and reload the switches as necessary.

Step 4: Configure basic settings for each switch.

a. Disable DNS lookup.

b. Configure the device name as shown in the Topology.

c. Assign **cisco** as the console and vty passwords and enable login.

d. Assign **class** as the encrypted privileged EXEC mode password.

e. Configure **logging synchronous** to prevent console messages from interrupting command entry.

f. Shut down all switch ports.

g. Copy the running configuration to startup configuration.

Part 2: Configure VLANs, Native VLAN, and Trunks

In Part 2, you will create VLANs, assign switch ports to VLANs, configure trunk ports, and change the native VLAN for all switches.

Note: The required commands for Part 2 are provided in Appendix A. Test your knowledge by trying to configure the VLANs, native VLAN, and trunks without referring to the appendix.

Step 1: Create VLANs.

Use the appropriate commands to create VLANs 10 and 99 on all of the switches. Name VLAN 10 as **User** and VLAN 99 as **Management**.

```
S1(config)# vlan 10
S1(config-vlan)# name User
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management

S2(config)# vlan 10
S2(config-vlan)# name User
S2(config-vlan)# vlan 99
S2(config-vlan)# name Management

S3(config)# vlan 10
S3(config-vlan)# name User
S3(config-vlan)# vlan 99
S3(config-vlan)# name Management
```

Step 2: Enable user ports in access mode and assign VLANs.

For S1 F0/6 and S3 F0/18, enable the ports, configure them as access ports, and assign them to VLAN 10.

Step 3: Configure trunk ports and assign to native VLAN 99.

For ports F0/1 and F0/3 on all switches, enable the ports, configure them as trunk ports, and assign them to native VLAN 99.

Step 4: Configure the management interface on all switches.

Using the Addressing Table, configure the management interface on all switches with the appropriate IP address.

Step 5: Verify configurations and connectivity.

Use the **show vlan brief** command on all switches to verify that all VLANs are registered in the VLAN table and that the correct ports are assigned.

Use the **show interfaces trunk** command on all switches to verify trunk interfaces.

What is the default setting for spanning-tree mode on Cisco switches?

_____

Verify connectivity between PC-A and PC-C. Was your ping successful? _____

If your ping was unsuccessful, troubleshoot the configurations until the issue is resolved.

Note: It may be necessary to disable the PC firewall to successfully ping between PCs.

Part 3: Configure the Root Bridge and Examine PVST+ Convergence

In Part 3, you will determine the default root in the network, assign the primary and secondary root, and use the **debug** command to examine convergence of PVST+.

Note: The required commands for Part 3 are provided in Appendix A. Test your knowledge by trying to configure the root bridge without referring to the appendix.

Step 1: Determine the current root bridge.

Which command allows a user to determine the spanning-tree status of a Cisco Catalyst switch for all VLANs? Write the command in the space provided.

_____

Use the command on all three switches to determine the answers to the following questions:

Note: There are three instances of the spanning tree on each switch. The default STP configuration on Cisco switches is PVST+, which creates a separate spanning tree instance for each VLAN (VLAN 1 and any user-configured VLANs).

What is the bridge priority of switch S1 for VLAN 1? _____

What is the bridge priority of switch S2 for VLAN 1? _____

What is the bridge priority of switch S3 for VLAN 1? _____

Which switch is the root bridge? _____

Why was this switch elected as the root bridge?

_____

Step 2: Configure a primary and secondary root bridge for all existing VLANs.

Having a root bridge (switch) elected by MAC address may lead to a suboptimal configuration. In this lab, you will configure switch S2 as the root bridge and S1 as the secondary root bridge.

a. Configure switch S2 to be the primary root bridge for all existing VLANs. Write the command in the space provided.

_____

b. Configure switch S1 to be the secondary root bridge for all existing VLANs. Write the command in the space provided.

_____

Use the **show spanning-tree** command to answer the following questions:

What is the bridge priority of S1 for VLAN 1? _____

What is the bridge priority of S2 for VLAN 1? _____

Which interface in the network is in a blocking state? _____

Step 3: Change the Layer 2 topology and examine convergence.

To examine PVST+ convergence, you will create a Layer 2 topology change while using the **debug** command to monitor spanning-tree events.

a. Enter the **debug spanning-tree events** command in privileged EXEC mode on switch S3.

```
S3# debug spanning-tree events
Spanning Tree event debugging is on
```

b. Create a topology change by disabling interface F0/1 on S3.

```
S3(config)# interface f0/1
S3(config-if)# shutdown
*Mar  1 00:58:56.225: STP: VLAN0001 new root port Fa0/3, cost 38
*Mar  1 00:58:56.225: STP: VLAN0001 Fa0/3 -> listening
*Mar  1 00:58:56.225: STP[1]: Generating TC trap for port FastEthernet0/1
*Mar  1 00:58:56.225: STP: VLAN0010 new root port Fa0/3, cost 38
*Mar  1 00:58:56.225: STP: VLAN0010 Fa0/3 -> listening
*Mar  1 00:58:56.225: STP[10]: Generating TC trap for port FastEthernet0/1
*Mar  1 00:58:56.225: STP: VLAN0099 new root port Fa0/3, cost 38
*Mar  1 00:58:56.225: STP: VLAN0099 Fa0/3 -> listening
*Mar  1 00:58:56.225: STP[99]: Generating TC trap for port FastEthernet0/1
*Mar  1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to down
*Mar  1 00:58:56.242: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to down
*Mar  1 00:58:58.214: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to ad-
ministratively down
*Mar  1 00:58:58.230: STP: VLAN0001 sent Topology Change Notice on Fa0/3
*Mar  1 00:58:58.230: STP: VLAN0010 sent Topology Change Notice on Fa0/3
*Mar  1 00:58:58.230: STP: VLAN0099 sent Topology Change Notice on Fa0/3
*Mar  1 00:58:59.220: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
*Mar  1 00:59:11.233: STP: VLAN0001 Fa0/3 -> learning
*Mar  1 00:59:11.233: STP: VLAN0010 Fa0/3 -> learning
*Mar  1 00:59:11.233: STP: VLAN0099 Fa0/3 -> learning
```

```
*Mar  1 00:59:26.240: STP[1]: Generating TC trap for port FastEthernet0/3
*Mar  1 00:59:26.240: STP: VLAN0001 Fa0/3 -> forwarding
*Mar  1 00:59:26.240: STP[10]: Generating TC trap for port FastEthernet0/3
*Mar  1 00:59:26.240: STP: VLAN0010 sent Topology Change Notice on Fa0/3
*Mar  1 00:59:26.240: STP: VLAN0010 Fa0/3 -> forwarding
*Mar  1 00:59:26.240: STP[99]: Generating TC trap for port FastEthernet0/3
*Mar  1 00:59:26.240: STP: VLAN0099 Fa0/3 -> forwarding
*Mar  1 00:59:26.248: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
*Mar  1 00:59:26.248: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
```

Note: Before proceeding, use the **debug** output to verify that all VLANs on F0/3 have reached a forwarding state then use the command **no debug spanning-tree events** to stop the **debug** output.

Through which port states do each VLAN on F0/3 proceed during network convergence?

_____

Using the time stamp from the first and last STP debug message, calculate the time (to the nearest second) that it took for the network to converge. **Hint**: The debug timestamp format is date hh.mm.ss:msec.

_____

Part 4: Configure Rapid PVST+, PortFast, BPDU Guard, and Examine Convergence

In Part 4, you will configure Rapid PVST+ on all switches. You will configure PortFast and BPDU guard on all access ports, and then use the **debug** command to examine Rapid PVST+ convergence.

Note: The required commands for Part 4 are provided in Appendix A. Test your knowledge by trying to configure the Rapid PVST+, PortFast, and BPDU guard without referring to the appendix.

Step 1: Configure Rapid PVST+.

a. Configure S1 for Rapid PVST+. Write the command in the space provided.

_____

b. Configure S2 and S3 for Rapid PVST+.

c. Verify configurations with the **show running-config | include spanning-tree mode** command.

```
S1# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst

S2# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst

S3# show running-config | include spanning-tree mode
spanning-tree mode rapid-pvst
```

Step 2: Configure PortFast and BPDU Guard on access ports.

PortFast is a feature of spanning tree that transitions a port immediately to a forwarding state as soon as it is turned on. This is useful in connecting hosts so that they can start communicating on the VLAN instantly, rather than waiting on spanning tree. To prevent ports that are configured with PortFast from forwarding BPDUs, which could change the spanning tree topology, BPDU guard can be enabled. At the receipt of a BPDU, BPDU guard disables a port configured with PortFast.

a. Configure interface F0/6 on S1 with PortFast. Write the command in the space provided.

_____

b. Configure interface F0/6 on S1 with BPDU guard. Write the command in the space provided.

_____

c. Globally configure all non-trunking ports on switch S3 with PortFast. Write the command in the space provided.

_____

d. Globally configure all non-trunking PortFast ports on switch S3 with BPDU guard. Write the command in the space provided.

_____

Step 3: Examine Rapid PVST+ convergence.

a. Enter the **debug spanning-tree events** command in privileged EXEC mode on switch S3.

b. Create a topology change by enabling interface F0/1 on switch S3.

```
S3(config)# interface f0/1
S3(config-if)# no shutdown
*Mar  1 01:28:34.946: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 01:28:37.588: RSTP(1): initializing port Fa0/1
*Mar  1 01:28:37.588: RSTP(1): Fa0/1 is now designated
*Mar  1 01:28:37.588: RSTP(10): initializing port Fa0/1
*Mar  1 01:28:37.588: RSTP(10): Fa0/1 is now designated
*Mar  1 01:28:37.588: RSTP(99): initializing port Fa0/1
*Mar  1 01:28:37.588: RSTP(99): Fa0/1 is now designated
*Mar  1 01:28:37.597: RSTP(1): transmitting a proposal on Fa0/1
*Mar  1 01:28:37.597: RSTP(10): transmitting a proposal on Fa0/1
*Mar  1 01:28:37.597: RSTP(99): transmitting a proposal on Fa0/1
*Mar  1 01:28:37.597: RSTP(1): updt roles, received superior bpdu on Fa0/1
*Mar  1 01:28:37.597: RSTP(1): Fa0/1 is now root port
*Mar  1 01:28:37.597: RSTP(1): Fa0/3 blocked by re-root
```

```
*Mar  1 01:28:37.597: RSTP(1): synced Fa0/1
*Mar  1 01:28:37.597: RSTP(1): Fa0/3 is now alternate
*Mar  1 01:28:37.597: RSTP(10): updt roles, received superior bpdu on Fa0/1
*Mar  1 01:28:37.597: RSTP(10): Fa0/1 is now root port
*Mar  1 01:28:37.597: RSTP(10): Fa0/3 blocked by re-root
*Mar  1 01:28:37.597: RSTP(10): synced Fa0/1
*Mar  1 01:28:37.597: RSTP(10): Fa0/3 is now alternate
*Mar  1 01:28:37.597: RSTP(99): updt roles, received superior bpdu on Fa0/1
*Mar  1 01:28:37.605: RSTP(99): Fa0/1 is now root port
*Mar  1 01:28:37.605: RSTP(99): Fa0/3 blocked by re-root
*Mar  1 01:28:37.605: RSTP(99): synced Fa0/1
*Mar  1 01:28:37.605: RSTP(99): Fa0/3 is now alternate
*Mar  1 01:28:37.605: STP[1]: Generating TC trap for port FastEthernet0/1
*Mar  1 01:28:37.605: STP[10]: Generating TC trap for port FastEthernet0/1
*Mar  1 01:28:37.605: STP[99]: Generating TC trap for port FastEthernet0/1
*Mar  1 01:28:37.622: RSTP(1): transmitting an agreement on Fa0/1 as a response to a
proposal
*Mar  1 01:28:37.622: RSTP(10): transmitting an agreement on Fa0/1 as a response to a
proposal
*Mar  1 01:28:37.622: RSTP(99): transmitting an agreement on Fa0/1 as a response to a
proposal
*Mar  1 01:28:38.595: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

Using the time stamp from the first and last RSTP debug message, calculate the time that it took for the network to converge.

_____

Reflection

1. What is the main benefit of using Rapid PVST+?

_____

2. How does configuring a port with PortFast allow for faster convergence?

_____

3. What protection does BPDU guard provide?

_____

Appendix A – Switch Configuration Commands

Switch S1

```
S1(config)# vlan 10
S1(config-vlan)# name User
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)# interface f0/6
S1(config-if)# no shutdown
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/1
S1(config-if)# no shutdown
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# interface f0/3
S1(config-if)# no shutdown
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# exit
S1(config)# spanning-tree vlan 1,10,99 root secondary
S1(config)# spanning-tree mode rapid-pvst
S1(config)# interface f0/6
S1(config-if)# spanning-tree portfast
S1(config-if)# spanning-tree bpduguard enable
```

Switch S2

```
S2(config)# vlan 10
S2(config-vlan)# name User
S2(config-vlan)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)# interface f0/1
S2(config-if)# no shutdown
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 99
```

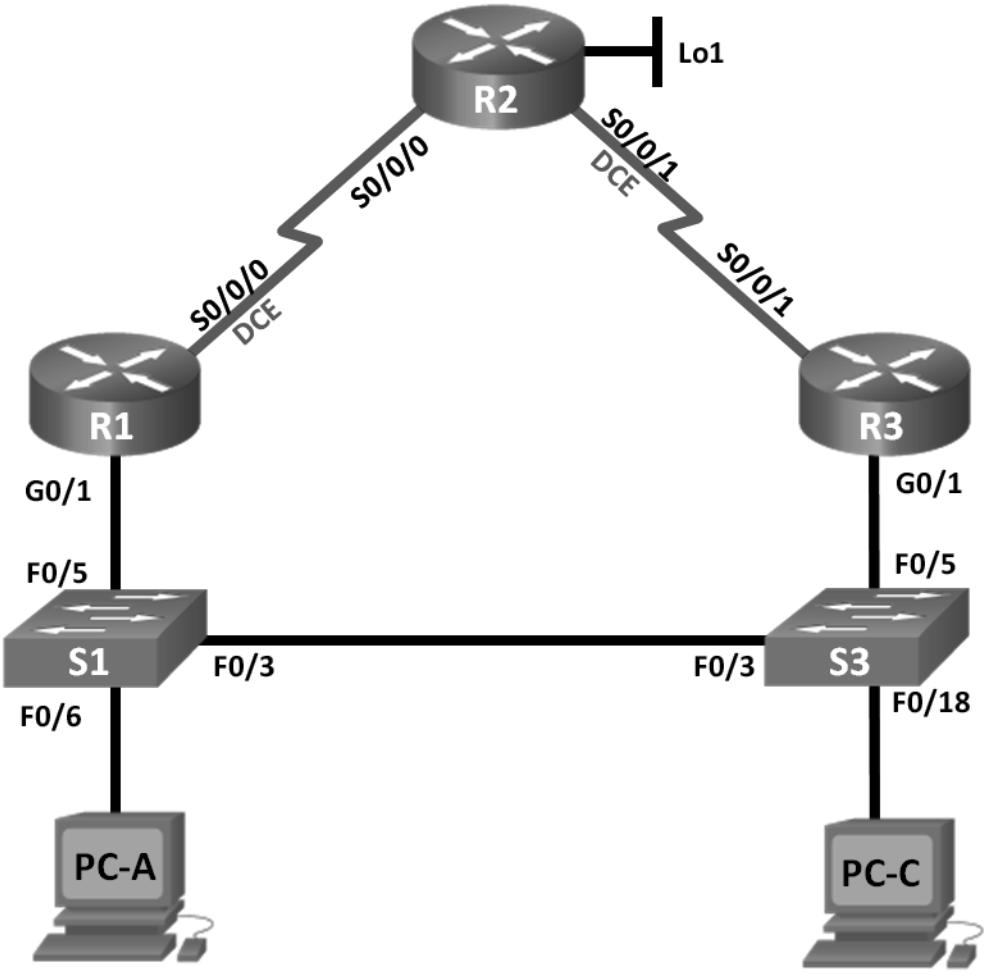
```
S2(config-if)# interface f0/3
S2(config-if)# no shutdown
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# interface vlan 99
S2(config-if)# ip address 192.168.1.12 255.255.255.0
S2(config-if)# exit
S2(config)# spanning-tree vlan 1,10,99 root primary
S2(config)# spanning-tree mode rapid-pvst
```

Switch S3

```
S3(config)# vlan 10
S3(config-vlan)# name User
S3(config-vlan)# vlan 99
S3(config-vlan)# name Management
S3(config-vlan)# exit
S3(config)# interface f0/18
S3(config-if)# no shutdown
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 10
S3(config-if)# spanning-tree portfast
S3(config-if)# spanning-tree bpduguard enable
S3(config-if)# interface f0/1
S3(config-if)# no shutdown
S3(config-if)# switchport mode trunk
S3(config-if)# switchport trunk native vlan 99
S3(config-if)# interface f0/3
S3(config-if)# no shutdown
S3(config-if)# switchport mode trunk
S3(config-if)# switchport trunk native vlan 99
S3(config-if)# interface vlan 99
S3(config-if)# ip address 192.168.1.13 255.255.255.0
S3(config-if)# exit
S3(config)# spanning-tree mode rapid-pvst
```

2.4.3.4 Lab – Configuring HSRP and GLBP

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo1	209.165.200.225	255.255.255.224	N/A
R3	G0/1	192.168.1.3	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.13	255.255.255.0	192.168.1.3
PC-A	NIC	192.168.1.31	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.33	255.255.255.0	192.168.1.3

Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure First Hop Redundancy using HSRP

Part 3: Configure First Hop Redundancy using GLBP

Background / Scenario

Spanning tree provides loop-free redundancy between switches within your LAN. However, it does not provide redundant default gateways for end-user devices within your network if one of your routers fails. First Hop Redundancy Protocols (FHRPs) provide redundant default gateways for end devices with no end-user configuration necessary.

In this lab, you will configure two FHRPs. In Part 2, you will configure Cisco's Hot Standby Routing Protocol (HSRP), and in Part 3 you will configure Cisco's Gateway Load Balancing Protocol (GLBP).

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Verify Connectivity

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Configure PC hosts.

Step 3: Initialize and reload the routers and switches as necessary.

Step 4: Configure basic settings for each router.

a. Disable DNS lookup.

b. Configure the device name as shown in the topology.

c. Configure IP addresses for the routers as listed in the Addressing Table.

d. Set clock rate to **128000** for all DCE serial interfaces.

e. Assign **class** as the encrypted privileged EXEC mode password.

f. Assign **cisco** for the console and vty password and enable login.

g. Configure **logging synchronous** to prevent console messages from interrupting command entry.

h. Copy the running configuration to the startup configuration.

Step 5: Configure basic settings for each switch.

a. Disable DNS lookup.

b. Configure the device name as shown in the topology.

c. Assign **class** as the encrypted privileged EXEC mode password.

d. Configure IP addresses for the switches as listed in the Addressing Table.

e. Configure the default gateway on each switch.

f. Assign **cisco** for the console and vty password and enable login.

g. Configure **logging synchronous** to prevent console messages from interrupting command entry.

h. Copy the running configuration to the startup configuration.

Step 6: Verify connectivity between PC-A and PC-C.

Ping from PC-A to PC-C. Were the ping results successful? _____

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: It may be necessary to disable the PC firewall to successfully ping between PCs.

Step 7: Configure routing.

a. Configure EIGRP on the routers and use AS of 1. Add all the networks, except 209.165.200.224/27 into the EIGRP process.

b. Configure a default route on R2 using Lo1 as the exit interface to 209.165.200.224/27 network and redistribute this route into the EIGRP process.

Step 8: Verify connectivity.

a. From PC-A, you should be able to ping every interface on R1, R2, R3, and PC-C. Were all pings successful? _____

b. From PC-C, you should be able to ping every interface on R1, R2, R3, and PC-A. Were all pings successful? _____

Part 2: Configure First Hop Redundancy Using HSRP

Even though the topology has been designed with some redundancy (two routers and two switches on the same LAN network), both PC-A and PC-C are configured with only one gateway address. PC-A is using R1 and PC-C is using R3. If either of these routers or the interfaces on the routers went down, the PC could lose its connection to the Internet.

In Part 2, you will test how the network behaves both before and after configuring HSRP. To do this, you will determine the path that packets take to the loopback address on R2.

Step 1: Determine the path for Internet traffic for PC-A and PC-C.

a. From a command prompt on PC-A, issue a **tracert** command to the 209.165.200.225 loopback address of R2.

```
C:\ tracert 209.165.200.225
Tracing route to 209.165.200.225 over a maximum of 30 hops


  1     1 ms     1 ms     1 ms  192.168.1.1
  2    13 ms    13 ms    13 ms  209.165.200.225


Trace complete.
```

What path did the packets take from PC-A to 209.165.200.225? ______________________________

b. From a command prompt on PC-C, issue a **tracert** command to the 209.165.200.225 loopback address of R2.

What path did the packets take from PC-C to 209.165.200.225? ______________________________

Step 2: Start a ping session on PC-A, and break the connection between S1 and R1.

a. From a command prompt on PC-A, issue a **ping –t** command to the **209.165.200.225** address on R2. Make sure you leave the command prompt window open.

Note: The pings continue until you press **Ctrl**+**C**, or until you close the command prompt window.

```
C:\ ping –t 209.165.200.225
Pinging 209.165.200.225 with 32 bytes of data:
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
```

```
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
Reply from 209.165.200.225: bytes=32 time=9ms TTL=254
<output omitted>
```

b. As the ping continues, disconnect the Ethernet cable from F0/5 on S1. You can also shut down the S1 F0/5 interface, which creates the same result.

What happened to the ping traffic?

_____

c. Repeat Steps 2a and 2b on PC-C and S3. Disconnect cable from F0/5 on S3.

What were your results?

_____

d. Reconnect the Ethernet cables to F0/5 or enable the F0/5 interface on both S1 and S3, respectively. Re-issue pings to 209.165.200.225 from both PC-A and PC-C to make sure connectivity is re-established.

Step 3: Configure HSRP on R1 and R3.

In this step, you will configure HSRP and change the default gateway address on PC-A, PC-C, S1, and S2 to the virtual IP address for HSRP. R1 becomes the active router via configuration of the HSRP priority command.

a. Configure HSRP on R1.

```
R1(config)# interface g0/1
R1(config-if)# standby 1 ip 192.168.1.254
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt
```

b. Configure HSRP on R3.

```
R3(config)# interface g0/1
R3(config-if)# standby 1 ip 192.168.1.254
```

c. Verify HSRP by issuing the **show standby** command on R1 and R3.

```
R1# show standby
GigabitEthernet0/1 - Group 1
  State is Active
    1 state change, last state change 00:02:11
  Virtual IP address is 192.168.1.254
  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 0.784 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.3, priority 100 (expires in 9.568 sec)
  Priority 150 (configured 150)
  Group name is "hsrp-Gi0/1-1" (default)
```

```
R3# show standby
GigabitEthernet0/1 - Group 1
  State is Standby
    4 state changes, last state change 00:02:20
  Virtual IP address is 192.168.1.254
  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 2.128 secs
  Preemption disabled
  Active router is 192.168.1.1, priority 150 (expires in 10.592 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Gi0/1-1" (default)
```

Using the output shown above, answer the following questions:

Which router is the active router? _____

What is the MAC address for the virtual IP address? _____

What is the IP address and priority of the standby router?

_____

_____

d. Use the **show standby brief** command on R1 and R3 to view an HSRP status summary. Sample output is shown below.

```
R1# show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/1       1    150 P Active  local           192.168.1.3     192.168.1.254

R3# show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/1       1    100   Standby 192.168.1.1     local           192.168.1.254
```

e. Change the default gateway address for PC-A, PC-C, S1, and S3. Which address should you use?

_____

Verify the new settings. Issue a ping from both PC-A and PC-C to the loopback address of R2. Are the pings successful? _____

Step 4: Start a ping session on PC-A and break the connection between the switch that is connected to the Active HSRP router (R1).

a. From a command prompt on PC-A, issue a **ping –t** command to the 209.165.200.225 address on R2. Ensure that you leave the command prompt window open.

b. As the ping continues, disconnect the Ethernet cable from F0/5 on S1 or shut down the F0/5 interface.

What happened to the ping traffic?

_____

_____

_____

Step 5: Verify HSRP settings on R1 and R3.

a. Issue the **show standby brief** command on R1 and R3.

Which router is the active router? _____

b. Reconnect the cable between the switch and the router or enable interface F0/5.

c. Disable the HSRP configuration commands on R1 and R3.

```
R1(config)# interface g0/1
R1(config-if)# no standby 1


R3(config)# interface g0/1
R3(config-if)# no standby 1
```

Part 3: Configure First Hop Redundancy Using GLBP

By default, HSRP does NOT do load balancing. The active router always handles all of the traffic, while the standby router sits unused, unless there is a link failure. This is not an efficient use of resources. GLBP provides nonstop path redundancy for IP by sharing protocol and MAC addresses between redundant gateways. GLBP also allows a group of routers to share the load of the default gateway on a LAN. Configuring GLBP is very similar to HSRP. Load balancing can be done in a variety of ways using GLBP. In this lab, you will use the round-robin method.

Step 1: Configure GLBP on R1 and R3.

a. Configure GLBP on R1.

```
R1(config)# interface g0/1
R1(config-if)# glbp 1 ip 192.168.1.254
R1(config-if)# glbp 1 preempt
R1(config-if)# glbp 1 priority 150
R1(config-if)# glbp 1 load-balancing round-robin
```

b. Configure GLBP on R3.

```
R3(config)# interface g0/1
R3(config-if)# glbp 1 ip 192.168.1.254
R3(config-if)# glbp 1 load-balancing round-robin
```

Step 2: Verify GLBP on R1 and R3.

a. Issue the **show glbp brief** command on R1 and R3.

```
R1# show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Gi0/1       1    -   150 Active   192.168.1.254   local           192.168.1.3
Gi0/1       1    1   -   Active   0007.b400.0101  local           -
Gi0/1       1    2   -   Listen   0007.b400.0102  192.168.1.3     -

R3# show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Gi0/1       1    -   100 Standby  192.168.1.254   192.168.1.1     local
Gi0/1       1    1   -   Listen   0007.b400.0101  192.168.1.1     -
Gi0/1       1    2   -   Active   0007.b400.0102  local           -
```

Step 3: Generate traffic from PC-A and PC-C to the R2 loopback interface.

a. From a command prompt on PC-A, ping the 209.165.200.225 address of R2.

```
C:\> ping 209.165.200.225
```

b. Issue an **arp –a** command on PC-A. Which MAC address is used for the 192.168.1.254 address?

_____

c. Generate more traffic to the loopback interface of R2. Issue another **arp –a** command. Did the MAC address change for the default gateway address of 192.168.1.254?

_____

As you can see, both R1 and R3 play a role in forwarding traffic to the loopback interface of R2. Neither router remains idle.

Step 4: Start a ping session on PC-A, and break the connection between the switch that is connected to R1.

a. From a command prompt on PC-A, issue a **ping –t** command to the 209.165.200.225 address on R2. Make sure you leave the command prompt window open.

b. As the ping continues, disconnect the Ethernet cable from F0/5 on S1 or shut down the F0/5 interface.

What happened to the ping traffic?

_____

_____

Reflection

1. Why would there be a need for redundancy in a LAN?

_____

2. If you had a choice, which protocol would you implement in your network, HSRP or GLBP? Explain your choice.

_____

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

2.5.1.1 Class Activity– Documentation Tree

Objective

Identify common STP configuration issues.

Scenario

The employees in your building are having difficulty accessing a web server on the network. You look for the network documentation that the previous network engineer used before he transitioned to a new job; however, you cannot find any network documentation whatsoever.

Therefore, you decide create your own network recordkeeping system. You decide to start at the access layer of your network hierarchy. This is where redundant switches are located, as well as the company servers, printers, and local hosts.

You create a matrix to record your documentation and include access layer switches on the list. You also decide to document switch names, ports in use, cabling connections, and root ports, designated ports, and alternate ports.

For more detailed instructions on how to design your model, use the student PDF that accompanies this activity.

Resources

- Packet Tracer software
- Word processing software

Directions

Step 1: Create the topology diagram with three redundant switches.

Step 2: Connect host devices to the switches.

Step 3: Create the switch documentation matrix.

a. Name and switch location
b. General switch description
c. Model, IOS version, and image name
d. Switch serial number
e. MAC address
f. Ports currently in use
g. Cable connections
h. Root ports
i. Designated ports, status, and cost
j. Alternate ports, status, and cost

Step 4: Use show commands to locate Layer 2 switch information.

a. show version
b. show cdp neighbors detail
c. show spanning-tree

Chapter 3 — Link Aggregation

3.0.1.2 Class Activity – Imagine This

Objective

Explain the operation of link aggregation in a switched LAN environment.

Scenario

It is the end of the work day. In your small- to medium-sized business, you are trying to explain to the network engineers about EtherChannel and how it looks when it is physically set up. The network engineers have difficulties envisioning how two switches could possibly be connected via several links that collectively act as one channel or connection. Your company is definitely considering implementing an EtherChannel network.

Therefore, you end the meeting with an assignment for the engineers. To prepare for the next day's meeting, they are to perform some research and bring to the meeting one graphic representation of an EtherChannel network connection. They are tasked with explaining how an EtherChannel network operates to the other engineers.

When researching EtherChannel, a good question to search for is "What does EtherChannel look like?" Prepare a few slides to demonstrate your research that will be presented to the network engineering group. These slides should provide a solid grasp of how EtherChannels are physically created within a network topology. Your goal is to ensure that everyone leaving the next meeting will have a good idea as to why they would consider moving to a network topology using EtherChannel as an option.

Required Resources

- Internet connectivity for research
- Software program for presentation model

Step 1: Use the Internet to research graphics depicting EtherChannel.

Step 2: Prepare a three-slide presentation to share with the class.

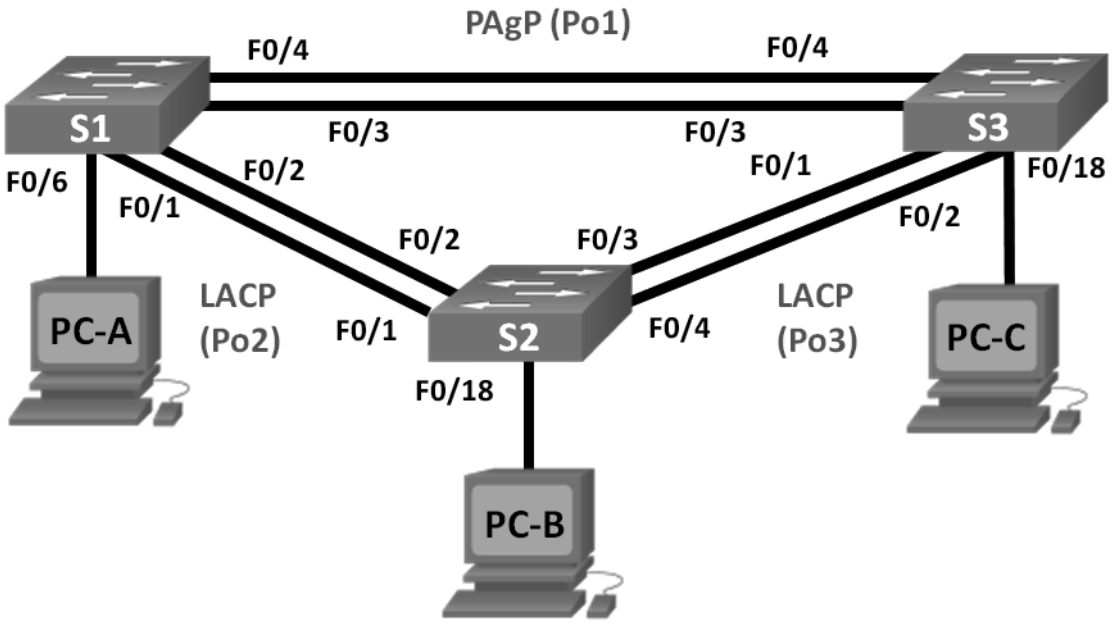
a. The first slide should show a very short, concise definition of a switch-to-switch EtherChannel.

b. The second slide should show a graphic of how a switch-to-switch EtherChannel physical topology would look if used in a small- to medium-sized business.

c. The third slide should list three advantages of using EtherChannel.

3.2.1.4 Lab – Configuring EtherChannel

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 99	192.168.99.11	255.255.255.0
S2	VLAN 99	192.168.99.12	255.255.255.0
S3	VLAN 99	192.168.99.13	255.255.255.0
PC-A	NIC	192.168.10.1	255.255.255.0
PC-B	NIC	192.168.10.2	255.255.255.0
PC-C	NIC	192.168.10.3	255.255.255.0

Objectives

Part 1: Configure Basic Switch Settings

Part 2: Configure PAgP

Part 3: Configure LACP

Background / Scenario

Link aggregation allows the creation of logical links that are comprised of two or more physical links. This provides increased throughput beyond using only one physical link. Link aggregation also provides redundancy if one of the links fails.

In this lab, you will configure EtherChannel, a form of link aggregation used in switched networks. You will configure EtherChannel using Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP).

Note: PAgP is a Cisco-proprietary protocol that you can only run on Cisco switches and on switches that are licensed vendors to support PAgP. LACP is a link aggregation protocol that is defined by IEEE 802.3ad, and it is not associated with any specific vendor.

LACP allows Cisco switches to manage Ethernet channels between switches that conform to the 802.3ad protocol. You can configure up to 16 ports to form a channel. Eight of the ports are in active mode and the other eight are in standby mode. When any of the active ports fail, a standby port becomes active. Standby mode works only for LACP, not for PAgP.

Note: The switches used with CCNA hands-on labs are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Configure Basic Switch Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Initialize and reload the switches.

Step 3: Configure basic settings for each switch.

a. Disable DNS lookup.

b. Configure the device name as displayed in the topology.

c. Encrypt plain text passwords.

d. Create a MOTD banner warning users that unauthorized access is prohibited.

e. Assign **class** as the encrypted privileged EXEC mode password.

f. Assign **cisco** as the console and vty password and enable login.

g. Configure logging synchronous to prevent console message from interrupting command entry.

h. Shut down all switchports except the ports connected to PCs.

i. Configure VLAN 99 and name it **Management**.

j. Configure VLAN 10 and name it **Staff**.

k. Configure the switch ports with attached hosts as access ports in VLAN 10.

l. Assign the IP addresses according to the Addressing Table.

m. Copy the running configuration to startup configuration.

Step 4: Configure the PCs.

Assign IP addresses to the PCs according to the Addressing Table.

Part 2: Configure PAgP

PAgP is a Cisco proprietary protocol for link aggregation. In Part 2, a link between S1 and S3 will be configured using PAgP.

Step 1: Configure PAgP on S1 and S3.

For a link between S1 and S3, configure the ports on S1 with PAgP desirable mode and the ports on S3 with PAgP auto mode. Enable the ports after PAgP modes have been configured.

```
S1(config)# interface range f0/3-4
S1(config-if-range)# channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1

S1(config-if-range)# no shutdown

S3(config)# interface range f0/3-4
S3(config-if-range)# channel-group 1 mode auto
Creating a port-channel interface Port-channel 1

S3(config-if-range)# no shutdown
*Mar  1 00:09:12.792: %LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
*Mar  1 00:09:12.792: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to up
S3(config-if-range)#
*Mar  1 00:09:15.384: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up
*Mar  1 00:09:16.265: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4,
changed state to up
S3(config-if-range)#
*Mar  1 00:09:16.357: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
*Mar  1 00:09:17.364: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1,
changed state to up
*Mar  1 00:09:44.383: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

Step 2: Examine the configuration on the ports.

Currently the F0/3, F0/4, and Po1 (Port-channel1) interfaces on both S1 and S3 are in access operational mode with the administrative mode in dynamic auto. Verify the configuration using the **show run interface** *interface-id* and **show interfaces** *interface-id* **switchport** commands, respectively. The example configuration outputs for F0/3 on S1 are as follows:

```
S1# show run interface f0/3
Building configuration...

Current configuration : 103 bytes
!
interface FastEthernet0/3
 channel-group 1 mode desirable

S1# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access (member of bundle Po1)
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
```

```
Unknown multicast blocked: disabled
Appliance trust: none
```

Step 3: Verify that the ports have been aggregated.

```
S1# show etherchannel summary
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)         PAgP      Fa0/3(P)    Fa0/4(P)

S3# show etherchannel summary
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)          PAgP      Fa0/3(P)    Fa0/4(P)
```

What do the flags, SU and P, indicate in the Ethernet summary?

_____

_____

Step 4: Configure trunk ports.

After the ports have been aggregated, commands applied at the port channel interface affect all the links that were bundled together. Manually configure the Po1 ports on S1 and S3 as trunk ports and assign them to native VLAN 99.

```
S1(config)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99

S3(config)# interface port-channel 1
S3(config-if)# switchport mode trunk
S3(config-if)# switchport trunk native vlan 99
```

Step 5: Verify that the ports are configured as trunk ports.

a. Issue the **show run interface** *interface-id* commands on S1 and S3. What commands are listed for F0/3 and F0/4 on both switches? Compare the results to the running configuration for the Po1 interface? Record your observation.

_____

_____

b. Issue the **show interfaces trunk** and **show spanning-tree** commands on S1 and S3. What trunk port is listed? What is the native VLAN? What is concluding result from the output?

_____

From the **show spanning-tree** output, what is port cost and port priority for the aggregated link?

_____

Part 3: Configure LACP

LACP is an open source protocol for link aggregation developed by the IEEE. In Part 3, the link between S1 and S2, and the link between S2 and S3 will be configured using LACP. Also, the individual links will be configured as trunks before they are bundled together as EtherChannels.

Step 1: Configure LACP between S1 and S2.

```
S1(config)# interface range f0/1-2
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport trunk native vlan 99
S1(config-if-range)# channel-group 2 mode active
Creating a port-channel interface Port-channel 2

S1(config-if-range)# no shutdown

S2(config)# interface range f0/1-2
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99
S2(config-if-range)# channel-group 2 mode passive
Creating a port-channel interface Port-channel 2

S2(config-if-range)# no shutdown
```

Step 2: Verify that the ports have been aggregated.

What protocol is Po2 using for link aggregation? Which ports are aggregated to form Po2? Record the command used to verify.

_____

_____

Step 3: Configure LACP between S2 and S3.

a. Configure the link between S2 and S3 as Po3 and use LACP as the link aggregation protocol.

```
S2(config)# interface range f0/3-4
S2(config-if-range)# switchport mode trunk
S2(config-if-range)# switchport trunk native vlan 99
S2(config-if-range)# channel-group 3 mode active
Creating a port-channel interface Port-channel 3
S2(config-if-range)# no shutdown

S3(config)# interface range f0/1-2
S3(config-if-range)# switchport mode trunk
S3(config-if-range)# switchport trunk native vlan 99
S3(config-if-range)# channel-group 3 mode passive
Creating a port-channel interface Port-channel 3

S3(config-if-range)# no shutdown
```

b. Verify that the EtherChannel has formed.

Step 4: Verify end-to-end connectivity.

Verify that all devices can ping each other within the same VLAN. If not, troubleshoot until there is end-to-end connectivity.

Note: It may be necessary to disable the PC firewall to ping between PCs.

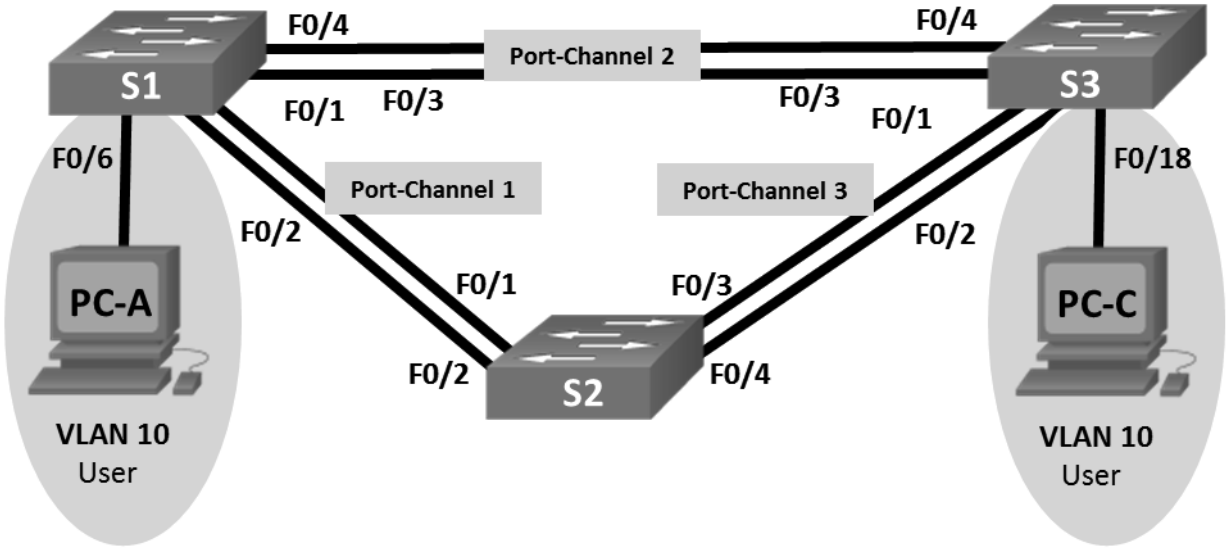
Reflection

What could prevent EtherChannels from forming?

_____

3.2.2.4 Lab – Troubleshooting EtherChannel

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 99	192.168.1.11	255.255.255.0
S2	VLAN 99	192.168.1.12	255.255.255.0
S3	VLAN 99	192.168.1.13	255.255.255.0
PC-A	NIC	192.168.0.2	255.255.255.0
PC-C	NIC	192.168.0.3	255.255.255.0

VLAN Assignments

VLAN	Name
10	User
99	Management

Objectives

Part 1: Build the Network and Load Device Configurations

Part 2: Troubleshoot EtherChannel

Background / Scenario

The switches at your company were configured by an inexperienced network administrator. Several errors in the configuration have resulted in speed and connectivity issues. Your manager has asked you to troubleshoot and correct the configuration errors and document your work. Using your knowledge of EtherChannel and standard testing methods, find and correct the errors. Ensure that all of the EtherChannels use Port Aggregation Protocol (PAgP), and that all hosts are reachable.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with a terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Load Device Configurations

In Part 1, you will set up the network topology, configure basic settings on the PC hosts, and load configurations on the switches.

Step 1: Cable the network as shown in the topology.

Step 2: Configure the PC hosts.

Step 3: Erase the startup and VLAN configurations and reload the switches.

Step 4: Load switch configurations.

Load the following configurations into the appropriate switch. All switches have the same passwords. The privileged EXEC password is **class**. The password for console and vty access is **cisco**. As all switches are Cisco devices, the network administrator decided to use Cisco's PAgP on all port channels configured with EtherChannel. Switch S2 is the root bridge for all VLANs in the topology.

Switch S1 Configuration:

```
hostname S1
interface range f0/1-24, g0/1-2
shutdown
exit
enable secret class
no ip domain lookup
line vty 0 15
password cisco
```

```
login
line con 0
 password cisco
 logging synchronous
 login
 exit
vlan 10
 name User
vlan 99
 Name Management
interface range f0/1-2
 switchport mode trunk

 channel-group 1 mode active
 switchport trunk native vlan 99
 no shutdown
interface range f0/3-4
 channel-group 2 mode desirable
 switchport trunk native vlan 99

 no shutdown
interface f0/6
 switchport mode access
 switchport access vlan 10
 no shutdown
interface vlan 99
 ip address 192.168.1.11 255.255.255.0
interface port-channel 1
 switchport trunk native vlan 99
 switchport mode trunk
interface port-channel 2
 switchport trunk native vlan 99
 switchport mode access
```

Switch S2 Configuration:

```
hostname S2
interface range f0/1-24, g0/1-2
 shutdown
 exit
```

```
enable secret class
no ip domain lookup
line vty 0 15
 password cisco
 login
line con 0
 password cisco
 logging synchronous
 login
 exit
vlan 10
 name User
vlan 99
 name Management
spanning-tree vlan 1,10,99 root primary
interface range f0/1-2
 switchport mode trunk
 channel-group 1 mode desirable
 switchport trunk native vlan 99
 no shutdown
interface range f0/3-4
 switchport mode trunk
 channel-group 3 mode desirable
 switchport trunk native vlan 99

interface vlan 99
 ip address 192.168.1.12 255.255.255.0
interface port-channel 1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 1,99

interface port-channel 3
 switchport trunk native vlan 99
 switchport trunk allowed vlan 1,10,99
 switchport mode trunk
```

Switch S3 Configuration:

```
hostname S3
interface range f0/1-24, g0/1-2
```

```
 shutdown
 exit
enable secret class
no ip domain lookup
line vty 0 15
 password cisco
 login
line con 0
 password cisco
 logging synchronous
 login
 exit
vlan 10
 name User
vlan 99
 name Management
interface range f0/1-2




interface range f0/3-4
 switchport mode trunk

 channel-group 3 mode desirable
 switchport trunk native vlan 99
 no shutdown
interface f0/18
 switchport mode access
 switchport access vlan 10
 no shutdown
interface vlan 99
 ip address 192.168.1.13 255.255.255.0
interface port-channel 3
 switchport trunk native vlan 99
 switchport mode trunk
```

Step 5: Save your configuration.

Part 2: Troubleshoot EtherChannel

In Part 2, you must examine the configurations on all switches, make corrections if needed, and verify full functionality.

Step 1: Troubleshoot S1.

a. Use the **show interfaces trunk** command to verify that the port channels are functioning as trunk ports.

Do port channels 1 and 2 appear as trunked ports? _____

b. Use the **show etherchannel summary** command to verify that interfaces are configured in the correct port channel, the proper protocol is configured, and the interfaces are in use.

Based on the output, are there any EtherChannel issues? If issues are found, record them in the space provided below.

_____

_____

c. Use the command **show run | begin interface Port-channel** command to view the running configuration beginning with the first port channel interface.

d. Resolve all problems found in the outputs from the previous **show** commands. Record the commands used to correct the configurations.

_____

_____

_____

_____

_____

e. Use the **show interfaces trunk** command to verify trunk settings.

f. Use the **show etherchannel summary** command to verify that the port channels are up and in use.

Step 2: Troubleshoot S2.

a. Issue the command to verify that the port channels are functioning as trunk ports. Record the command used in the space provided below.

_____

Based on the output, are there any issues with the configurations? If issues are found, record them in the space provided below.

_____

_____

b. Issue the command to verify that interfaces are configured in the correct port channel and the proper protocol is configured.

Based on the output, are there any EtherChannel issues? If issues are found, record them in the space provided below.

_____

c. Use the command **show run | begin interface Port-channel** to view the running configuration beginning with the first port-channel interface.

d. Resolve all problems found in the outputs from the previous **show** commands. Record the commands used to correct the configuration.

_____

_____

_____

_____

_____

e. Issue the command to verify trunk settings.

f. Issue the command to verify that the port channels are functioning. Remember that port channel issues can be caused by either end of the link.

Step 3: Troubleshoot S3.

a. Issue the command to verify that the port channels are functioning as trunk ports.

Based on the output, are there any issues with the configurations? If issues are found, record them in the space provided below.

_____

_____

b. Issue the command to verify that the interfaces are configured in the correct port channel and that the proper protocol is configured.

Based on the output, are there any EtherChannel issues? If issues are found, record them in the space provided below.

_____

_____

c. Use the command **show run | begin interface Port-channel** command to view the running configuration beginning with the first port channel interface.

d. Resolve all problems found. Record the commands used to correct the configuration.

_____

_____

_____

_____

_____

_____

_____

e. Issue the command to verify trunk settings. Record the command used in the space provided below.

_____

f. Issue the command to verify that the port channels are functioning. Record the command used in the space provided below.

_____

Step 4: Verify EtherChannel and Connectivity.

a. Use the **show interfaces etherchannel** command to verify full functionality of the port channels.

b. Verify connectivity of the management VLAN.

Can S1 ping S2? _____

Can S1 ping S3? _____

Can S2 ping S3? _____

c. Verify connectivity of PCs.

Can PC-A ping PC-C? _____

If EtherChannels are not fully functional, connectivity between switches does not exist, or connectivity between hosts does not exist. Troubleshoot to resolve any remaining issues.

Note: It may be necessary to disable the PC firewall for pings between the PCs to succeed.

3.3.1.1 Class Activity – Linking Up

Objective

Describe link aggregation.

Scenario

Many bottlenecks occur on your small- to medium-sized business network, even though you have configured VLANs, STP, and other network traffic options on the company's switches.

Instead of keeping the switches as they are currently configured, you would like to try EtherChannel as an option for, at least, part of the network to see if it will lesson traffic congestion between your access and distribution layer switches.

Your company uses Catalyst 3560 switches at the distribution layer and Catalyst 2960 and 2950 switches at the access layer of the network. To verify if these switches can perform EtherChannel, you visit the *System Requirements to Implement EtherChannel on Catalyst Switches*. This site allows you to gather more information to determine if EtherChannel is a good option for the equipment and network currently in place.

After researching the models, you decide to use a simulation software program to practice configuring EtherChannel before implementing it live on your network. As a part of this procedure, you ensure that the equipment simulated in Packet Tracer will support these practice configurations.

Resources

- World Wide Web connectivity
- Packet Tracer software
- Word processing or spreadsheet software

Directions

Step 1: Visit *System Requirements to Implement EtherChannel on Catalyst Switches*.

a. Pay particular attention to the Catalyst 3560, 2960, and 2950 model information.

b. Record any information you feel would be useful to deciding whether to use EtherChannel in your company.

Step 2: Create a matrix to record the information you recorded in Step 1b, including:

a. Number of ports allowed to bundled for an EtherChannel group

b. Maximum group bandwidth supported by bundling the ports

c. IOS version needed to support EtherChannel on the switch model

d. Load balancing availability

e. Load balancing configuration options

f. Network layers supported for EtherChannel operation

Step 3: Open Packet Tracer.

a. Notice how many ports are available to bundle for EtherChannel on all three switch models.

b. Check all three models to see how many EtherChannel groups you could create on each model.

c. Make sure the IOS version is recent enough to support all EtherChannel configurations.

d. Do not configure your simulated network, but do check the models available in the Packet Tracer to make sure they will support all the EtherChannel configuration options.

Step 4: Share your matrix with another group or the class.