Cisco LAN Switching Video Mentor

David Hucaby, CCIE No. 4594

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Cisco LAN Switching Video Mentor

David Hucaby, CCIE No. 4594

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

Printed in the United States of America

First Printing June 2009

ISBN-13: 978-1-58720-223-0

ISBN-10: 1-58720-223-9

Warning and Disclaimer

This Video Mentor is designed to provide information about configuring and using Cisco Catalyst LAN switches. Every effort has been made to make this product as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The author, 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
Anand Sundaram

Manager Global Certification
Erik Ullanderson

Executive Editor
Brett Bartow

Managing Editor
Patrick Kanouse

Development Editor
Andrew Cupp

Project Editor
Jennifer Gallant

Copy Editor
Apostrophe Editing Services

Technical Editor
Geoff Tagg

Editorial Assistant
Vanessa Evans

Book Designer
Louisa Adair

Composition
Mark Shirar

Proofreader
Jennifer Gallant

Trademark Acknowledgments

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

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside the United States please contact:

International Sales
international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical products of the highest quality and value. Each product 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 product, 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.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

About the Author

David Hucaby, CCIE No. 4594, is a network architect for the University of Kentucky, where he works with health-care networks based on Cisco Catalyst LAN switches. He has a B.S. and M.S. in electrical engineering from the University of Kentucky. He is the author of several other books from Cisco Press: *CCNP BCMSN Official Exam Certification Guide; Cisco ASA, PIX, and FWSM Firewall Handbook; Cisco Field Manual: Catalyst Switch Configuration; Cisco Field Manual: Router Configuration;* and *Cisco Firewall Video Mentor*. David lives in Kentucky with his wife and two daughters.

David can be reached at dave@hucaby.net and www.hucaby.net.

About the Technical Reviewer

Geoff Tagg runs a small UK networking company and has worked in the networking industry for nearly 30 years; prior to that, he had 15 years experience of systems programming and management on a wide variety of installations. Geoff has clients ranging from small local businesses to large multinationals and has combined implementation with training for most of his working life. Geoff's main specialties are routing, switching, and networked storage. He lives in Oxford, England, with his wife Christine and family, and is a visiting professor at nearby Oxford Brookes University.

Dedications

To Marci, Lauren, and Kara, who make my life complete as a husband and a daddy. Your love and support make everything easier and worthwhile.

Acknowledgments

I'm very grateful to Geoff Tagg, my old tech editor friend, for agreeing to review this project. His critical eye, thorough work, and good suggestions certainly helped make this project better.

Many thanks to Drew Cupp for taking on another one of my projects. He's been a great editor and a great help in a variety of ways.

It's been my good pleasure to work with the good folks at Cisco Press once again. My thanks to San Dee Phillips and Patrick Kanouse for their editing talents early on, and to Anne Lukens and Vanessa Evans for taking care of a variety of logistics. John Herrin has endured many of my complaints about screen recording issues, and has been a big help in getting my recording and editing stabilized. Louisa Adair always works up a nice cover, in spite of the subject matter.

Brett Bartow has done a super job of organizing this project, of seeing the big picture, and of being patient with me as I made a disaster out of every deadline.

Even though this is my second Video Mentor project, Wendell Odom and Kevin Wallace have generously shared their experiences to iron out more of my wrinkles.

I would also like to acknowledge the folks who have unknowingly provided their assistance. Ajeshwar Sra and Bobby Thekkekandam, of Cisco TAC, were very helpful in answering some obscure questions along the way. Sam Elam, my coworker, was very helpful on several occasions.

Finally, I am thankful that God has given me work that meshes with my interests and talents. The abundant life Jesus gives makes every part of life worthwhile.

Contents at a Glance

Contents

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.

Introduction

Cisco LAN Switching Video Mentor supplies 20 instructional videos that cover a variety of Catalyst switch configuration tasks. Because LAN switching features can be complex and tedious to configure, each video presents a scenario that visually demonstrates a feature configuration step by step, along with a running audio commentary.

This product is one of several in the Cisco Press Video Mentor series. The Video Mentor series offers a learning environment that is different from that of printed books, where you can only read about concepts and look at static examples. With the video labs, you can learn about concepts much as you would in a classroom setting, with a live instructor. As well, you can watch configurations and examples unfold, step by step, with explanations along the way.

Goals and Methods

Cisco LAN Switching Video Mentor shows the author's computer desktop as switches are configured and tested. A running audio commentary accompanies the video so that every activity is explained.

Most of the video labs follow the same format, using the following steps:

1. The video begins with a listing of goals or topics for the lab.
2. An overview of specific LAN switching features is given.
3. A scenario involving a LAN switching feature is presented.
4. A terminal emulator window shows how the LAN switching feature is configured with the command line interface, step by step.

Who Should Use This Product?

Cisco LAN Switching Video Mentor is intended for people who are involved in the installation and administration of LAN switches. Although it is not designed around any specific Cisco course or exam, it can be used to augment self-study books about LAN switching topics, including the CCIE Routing and Switching and the CCNP switching exams.

Because of the multimedia format, the Video Mentor uses the video and audio mediums to deliver information more effectively than printed material alone, especially for visual learners.

This Video Mentor covers the LAN switching features in the Cisco Catalyst product families.

Video Mentor Contents

This Video Mentor product contains a DVD and a printed booklet. The DVD consists of a series of 20 video labs and several introductory video segments. The DVD is viewed on a computer screen and is optimized for display in a 1024 by 768 pixel minimum area.

The booklet contains information that you can use as a reference while watching the video labs. It is not meant to be a standalone tool. The booklet has a chapter for each of the 20 video labs, containing the figures and configuration information used in the video.

Each booklet section includes the following:

- A list of objectives or topics for the video lab
- Copies of figures used in the video
- A description of the scenario, broken down into steps
- The initial configuration entered in relevant switches *before* the video lab begins
- The configuration commands that are entered *during* the video lab

The booklet is also available in PDF format within the Video Mentor application. You can switch between displaying the video and the booklet as you work your way through the video labs.

How the Cisco LAN Switching Video Mentor Is Organized

When the DVD starts, the Video Mentor application displays the list of video labs. From the initial menu, you can also view an introductory video that describes the entire product. The video labs are organized as follows:

- **Lab 1, “Interface Configuration”:** Demonstrates how you can configure a switch interfaces to support connected devices. Use the command line interface (CLI) while the computer connects to the switch console.
- **Lab 2, “Setting Up VLANs”:** Takes a look at Layer 2 switching and covers how to configure virtual networks within a switch.
- **Lab 3, “Setting Up Trunk Links”:** Explores how VLANs are carried over trunk links between switches.

- **Lab 4, "Using the VLAN Trunking Protocol (VTP)":** VTP is leveraged to automate VLAN configuration across multiple switches in a network.
- **Lab 5, "Working with the Spanning Tree Protocol (STP)":** Covers STP operation and how it maintains a loop-free Layer 2 switching topology. STP Root Switch configuration is also covered.
- **Lab 6, "STP Topology Changes":** Explores Per-VLAN STP Plus (PVST+) operation and how STP reacts to a variety of topology changes within a VLAN.
- **Lab 7, "Leveraging Rapid STP":** Covers Rapid PVST+ operation and configuration, with its behavior under several types of topology changes.
- **Lab 8, "Scaling STP with MST":** Explores MST and how you can configure and used it to simplify STP operation in a network.
- **Lab 9, "Protecting the STP Topology":** Covers several features that stabilize the loop-free Layer 2 switching topology. Root Guard, BPDU Guard, Loop Guard, and Unidirectional Link Detection are demonstrated.
- **Lab 10, "Scaling Bandwidth with EtherChannel":** Demonstrates how multiple switch interfaces can be bundled together into a single logical EtherChannel interface. EtherChannels can increase available bandwidth and redundancy.
- **Lab 11, "Setting Up Multilayer Switching":** Moves beyond Layer 2 switching to cover Layer 3 switching and routing.
- **Lab 12, "First-Hop Redundancy with HSRP":** The Layer 3 interface used for multilayer switching is made more redundant for devices within an IP subnet. The Hot Standby Router Protocol (HSRP) is demonstrated by configuring multiple switches to work together and share a common gateway IP address.
- **Lab 13, "First-Hop Redundancy with GLBP":** Explores the Gateway Load Balancing Protocol (GLBP) to provide robust gateway redundancy for devices within an IP subnet.
- **Lab 14, "Private VLANs":** The normal rules of Layer 2 VLANs are stretched to provide new forms of isolation by configuring Private VLANs.
- **Lab 15, "Using ACLs to Control Traffic":** Presents several types of ACLs that can be configured and applied within a switch to control or restrict traffic movement.
- **Lab 16, "Using Port Security":** The Port Security feature is leveraged to control access to switch interfaces.
- **Lab 17, "Preventing Spoofing Attacks":** Demonstrates DHCP Snooping, IP Source Guard, and Dynamic ARP Inspection, which all work to detect and mitigate attempts to spoof network information for malicious purposes.
- **Lab 18, "Qos, Part 1":** Provides an overview of the many Quality of Service (QoS) features available on Catalyst switches. It also demonstrates how you can configure many of the features to identify and handle types of traffic according to QoS policies.

- **Lab 19, "QoS, Part 2":** Explores how packets are put into and taken out of queues at switch interfaces. It also looks at congestion avoidance methods that keep interface queues from becoming too congested.
- **Lab 20, "Monitoring Traffic":** Demonstrates the Switch Port Analyzer (SPAN) family of features. By using one of the SPAN features, a switch can copy or mirror traffic from a source to a destination, either on the same switch or to a different switch. Monitored traffic is normally sent to an external network or protocol analyzer or to the Mini Protocol Analyzer, found within a switch.

Lab 1

Interface Configuration

This LAN Switching Video Mentor lab demonstrates how to configure switch interfaces so that other devices can connect.

The objectives of this lab are as follows:

- Set interface attributes.
- Configure multiple interfaces at one time.
- Configure inline power.
- Manage interface error conditions.

Scenario

This lab contains five main steps, as follows:

Step 1. Survey the interfaces that are available on a switch.

Step 2. Configure the physical interface parameters.

Step 3. Configure a range of interfaces in one pass.

Step 4. Configure inline power operation on some interfaces.

Step 5. Monitor and configure the errdisable error detection feature.

Initial Configurations

The two switches used in this lab have their default configurations in place. There are no relevant initial configuration commands needed.

Video Presentation Reference

Figure 1-1 shows the network topology diagram for this lab. The commands that are entered in each of the lab steps are shown in the following sections.

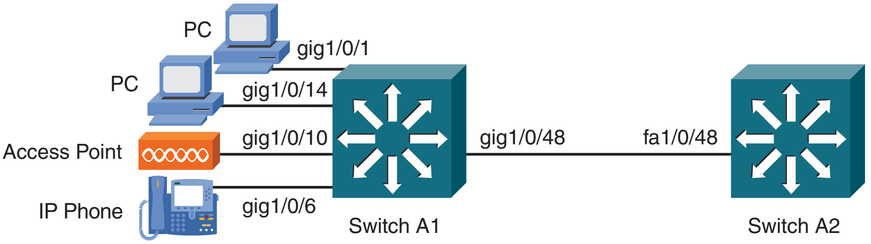

Figure 1-1 Lab 1 Network Topology

Step 1: Surveying the Switch Interfaces

This step lists the available switch interfaces along with their current status. The current interface configuration commands also display. Example 1-1 shows the entered commands.

Example 1-1 Commands That Display Switch Interface Status and Configuration

```
show interfaces status
show running-config interface mod type/num
```

Step 2: Configuring Interface Parameters

This step discusses the commands that configure physical interface parameters. You can configure each interface with a speed, duplex mode, MDIX operation, and a media type, using the commands shown in Example 1-2.

Example 1-2 Commands That Configure Interface Parameters

```
interface gigabitethernet1/0/1
  speed auto
  duplex auto
  mdix auto
  no shutdown
  exit
interface gigabitethernet1/0/48
  speed auto
  duplex auto
  mdix auto
  no shutdown
  exit
```

Step 3: Configuring a Range of Physical Interfaces

This step configures several ranges of physical interfaces using common sets of configuration commands. The configuration commands used in this step of the lab are shown in Example 1-3.

Example 1-3 Configuring Interface Ranges

```
interface range gigabitethernet1/0/1 - 48
  no description
  speed auto
  duplex auto
  no shutdown
  exit
!
interface range gigabitethernet1/0/44 - 47
  shutdown
  exit
!
interface range gigabitethernet1/0/2 - 4 , gigabitethernet1/0/13
  description Reserved for future use
  shutdown
  exit
```

Step 4: Configuring Inline Power

This step configures a range of switch interfaces to offer inline power and configures a single interface to never offer inline power. Example 1-4 shows the entered commands.

Example 1-4 Configuring Inline Power

```
show power inline

interface range gigabitethernet1/0/1 - 47
  power inline auto
  exit
!
interface gigabitethernet1/0/48
  power inline never
  exit
```

Step 5: Working with Interface Error Conditions

This step monitors and configures the errdisable feature.

Example 1-5 shows the commands that monitor the interface error status and the errdisable detection mechanisms.

Example 1-5 Working with Errdisable

```
show interface status errdisable
show errdisable detect

interface gigabitethernet1/0/34
  shutdown
  no shutdown
  exit
```

Next, you explore automatic errdisable recovery. Example 1-6 shows the commands that monitor the automatic recovery state of each errdisable reason. In addition, you see the command that enables automatic recovery of link-flap interface errors.

Example 1-6 Monitoring and Configuring Automatic Errdisable Recovery

```
show errdisable recovery

errdisable recovery cause link-flap
```

Lab 2

Setting Up VLANs

This LAN Switching Video Mentor lab demonstrates how a Layer 2 switch works, and how to configure switch interfaces into virtual LANs (VLANs) or logical networks.

The objectives of this lab are as follows:

- Learn how a Layer 2 switch operates.
- Configure VLANs.

Scenario

This lab contains three main steps, as follows:

Step 1. Create new VLANs.

Step 2. Assign switch interfaces to a VLAN.

Step 3. Query the Layer 2 switching table.

Initial Configurations

The two switches used in this lab have their default configurations in place. Some physical interface parameters were configured as a result of Lab 1, but those interface configuration commands don't necessarily apply in this lab. Therefore, you do not need any relevant initial configuration commands.

Video Presentation Reference

The following sections show the network topology diagram and the commands for each of the lab steps as appropriate.

Step 1: Creating New VLANs

This step creates three new VLANs, in addition to the default VLAN 1. Example 2-1 shows the entered commands on both switches A1 and A2.

Example 2-1 Commands That Create New VLANs

```
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
```

Step 2: Assigning Switch Interfaces to a VLAN

This step assigns switch interfaces GigabitEthernet1/0/1–16 and GigabitEthernet1/0/48 to VLAN 2. Interfaces GigabitEthernet1/0/17–47 are assigned to VLAN 3. Example 2-2 shows the commands that configure the interfaces on switch A1.

Example 2-2 Commands That Assign Switch A1 Interfaces to VLANs

```
interface range gigabitethernet1/0/1 - 16 , gigabitethernet1/0/48
  switchport
  switchport access vlan 2
  switchport mode access
  no shutdown
  exit
interface range gigabitethernet1/0/17 - 47
  switchport
  switchport access vlan 3
  switchport mode access
  no shutdown
  exit
```

Finally, interfaces FastEthernet1/0/1–48 on switch A2 are configured to belong to VLAN 2. Example 2-3 shows the configuration commands used.

Example 2-3 Commands That Assign Switch A2 Interfaces to VLANs

```
vlan 2
  name Engineering
  exit
interface range fastethernet1/0/1 - 48
  switchport
  switchport access vlan 2
  switchport mode access
  no shutdown
  exit
```

Step 3: Querying the Layer 2 Switching Table

This step queries the Layer 2 switching table or CAM table to track the location of PC2. PC2 begins on interface GigabitEthernet1/0/14 on switch A1 and ends up on interface FastEthernet1/0/14 on switch A2, as shown in the network topology depicted in Figure 2-1.

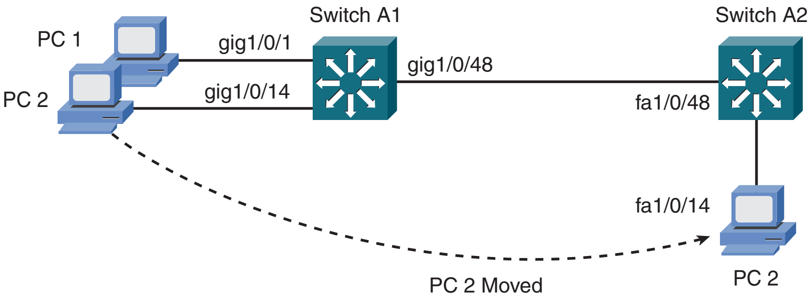

Figure 2-1 Lab 2 Network Topology

The commands in this step of the lab are shown in Example 2-4.

Example 2-4 Querying the Switching Table

```
show mac-address-table dynamic

show mac-address-table dynamic interface gigabitethernet1/0/1

show mac-address-table dynamic address 0014.22f3.dd7d

show mac-address-table count
```

Lab 3

Setting Up Trunk Links

This LAN Switching Video Mentor lab demonstrates how to configure switch interfaces to carry traffic from more than one VLAN, as a trunk link.

The objectives of this lab are as follows:

- Review Trunking operation.
- Select a trunk link encapsulation.
- Set the trunk link mode.
- Prune unnecessary VLANs from a trunk link.

Scenario

This lab contains four main steps, as follows:

Step 1. Configure the trunk link encapsulation.

Step 2. Configure the trunk link mode.

Step 3. Prune VLANs from a trunk link.

Step 4. Configure a special trunk to a Cisco IP Phone.

Initial Configurations

The two switches used in this lab have their initial configurations as a result of Lab 2. The relevant initial configuration commands already in place on switch A1 are shown in Example 3-1. The initial configuration commands for switch A2 are shown in Example 3-2.

Example 3-1 Initial Configuration Commands for Switch A1

```
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/0/48
   switchport
   switchport access vlan 2
   switchport mode access
```

Example 3-2 Initial Configuration Commands for Switch A2

```
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface fastethernet1/0/48
   switchport
   switchport access vlan 2
   switchport mode access
```

Video Presentation Reference

Figure 3-1 shows the network topology used in this lab. In the following sections, the commands entered in each of the lab steps are shown.

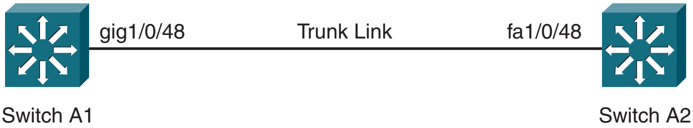

Figure 3-1 Lab 3 Network Topology

Step 1: Configuring the Trunk Link Encapsulation

This step configures interface GigabitEthernet1/0/48 on switch A1 and interface FastEthernet1/0/48 on switch A2 for IEEE 802.1Q trunk encapsulation. VLAN 1 is used as the trunk's native VLAN because it is not used elsewhere in the network. Examples 3-3 and 3-4 show the commands entered on switch A1 and A2, respectively.

Example 3-3 Commands That Set the Trunk Encapsulation on Switch A1

```
interface gigabitethernet1/0/48
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk native vlan 1
   exit
```

Example 3-4 Commands That Set the Trunk Encapsulation on Switch A2

```
interface fastethernet1/0/48
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk native vlan 1
   exit
```

Step 2: Configuring the Trunk Link Mode

In this step, the trunk link begins in the default “auto” mode on both switches A1 and A2. The trunk link is then modified on the switch A1 end to use the “dynamic desirable” mode. The commands that configure the trunk link mode on switch A1 are shown in Example 3-5.

Example 3-5 Commands That Set the Trunk Link Mode on Switch A1

```
interface gigabitethernet1/0/48
  switchport mode dynamic desirable
  exit
```

Finally, the trunk link is configured to operate as an unconditional trunk on both ends. The configuration commands used on switches A1 and A2 are shown in Examples 3-6 and 3-7, respectively.

Example 3-6 Commands That Unconditionally Trunk on Switch A1

```
interface gigabitethernet1/0/48
  switchport mode trunk
  exit
```

Example 3-7 Commands That Unconditionally Trunk on Switch A2

```
interface fastethernet1/0/48
  switchport mode trunk
  exit
```

Step 3: Pruning VLANs from a Trunk Link

This step removes all unnecessary VLANs from the trunk link between switches A1 and A2. By default, all possible VLANs are allowed over the trunk. Only VLANs 2, 3, and 10 are intended for use, so only those VLANs should be allowed. The commands used on switches A1 and A2 in this step of the lab are shown in Examples 3-8 and 3-9, respectively.

Example 3-8 Commands That Prune VLANs on the Switch A1 Trunk

```
interface gigabitethernet1/0/48
   switchport trunk allowed vlan 2,10
   switchport trunk allowed vlan add 3
   exit
```

Example 3-9 Commands That Prune VLANs on the Switch A2 Trunk

```
interface fastethernet1/0/48
   switchport trunk allowed vlan 2-3,10
   exit
```

Example 3-10 shows the commands that verify interface trunk operation.

Example 3-10 Commands That Verify Trunk Link Operation

```
show interface gigabitethernet1/0/48 trunk

show interface gigabitethernet1/0/48 switchport
```

Step 4: Configuring a Special Cisco IP Phone Trunk Link

In this step, a Cisco IP Phone connects to interface GigabitEthernet1/0/6, as shown in Figure 3-2. A PC attached to the IP Phone needs to associate with VLAN 2, for normal data traffic. The voice traffic passing to and from the IP Phone should appear on VLAN 10, the voice VLAN. The commands used on switch A1 in this step of the lab are shown in Example 3-11.

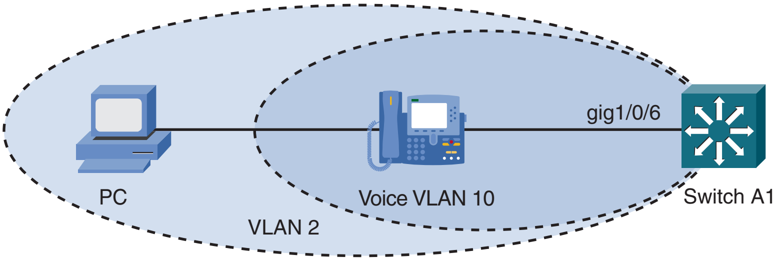

Figure 3-2 Cisco IP Phone Network Topology

Example 3-11 Commands That Configure a Cisco IP Phone Trunk Link

```
interface gigabitethernet1/0/6
   switchport
   switchport access vlan 2
   switchport mode access
   switchport voice vlan 10
   no shutdown
   exit
```

Lab 4

Using the VLAN Trunking Protocol (VTP)

This LAN Switching Video Mentor lab covers the VLAN Trunking Protocol (VTP) and how you can use it to automatically maintain VLAN configurations across multiple switches.

The objectives of this lab are as follows:

- Understand VTP operation.
- Set up a VTP domain.
- Prevent a VTP catastrophe.

Scenario

This lab contains four main steps, as follows:

Step 1. Set up a VTP server and a VTP client; then manage the VLAN configuration on both automatically.

Step 2. Enable VTP pruning.

Step 3. Isolate one switch, make VLAN configuration changes to it, and then introduce it back into the network.

Step 4. Convert the two switches to VTP transparent mode.

Initial Configurations

The two switches used in this lab have their initial configurations as a result of Lab 3. The relevant initial configuration commands already in place on switch A1 are shown in Example 4-1. The initial configuration commands for switch A2 are shown in Example 4-2.

Example 4-1 Initial Configuration Commands for Switch A1

```
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/0/48
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Example 4-2 Initial Configuration Commands for Switch A2

```
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface fastethernet1/0/48
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode access
```

Video Presentation Reference

Figure 4-1 shows the network topology used in this lab. In the following sections, the entered commands in each of the lab steps are shown.

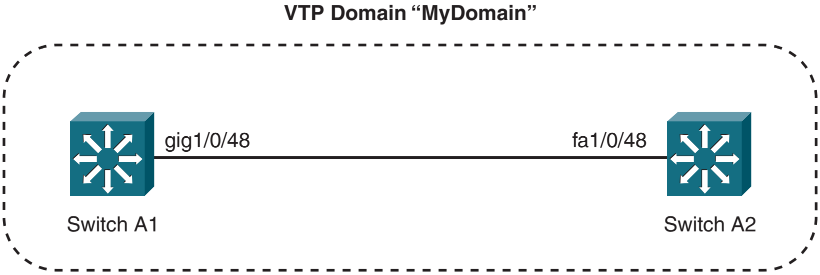

Figure 4-1 Lab 4 Network Topology

Step 1: Setting Up a VTP Server and a VTP Client

This step configures switch A1 to be a VTP server in the VTP domain named **MyDomain**. Switch A2 is configured as a VTP client. Both client and server share a common VTP domain password **b1gs3cr3t**. Examples 4-3 and 4-4 show the commands that are entered on switch A1 and A2, respectively.

Example 4-3 Commands That Make Switch A1 a VTP Server

```
vtp domain MyDomain
vtp mode server
vtp password b1gs3cr3t
```

Example 4-4 Commands That Make Switch A2 a VTP Client

```
vtp domain MyDomain
vtp mode client
vtp password b1gs3cr3t
```

A new VLAN 100 is created on switch A1 (the VTP server) so that the same VLAN will be created automatically on switch A2 (the VTP client). Example 4-5 shows the configuration commands that create the VLAN on switch A1.

Example 4-5 Commands That Create a New VLAN in the VTP Domain

```
vlan 100
   name Lab
   exit
```

Step 2: Enabling VTP Pruning

This step enables VTP pruning on switch A1—the VTP server. Example 4-6 shows the command that configures the trunk link mode on switch A1.

Example 4-6 Command That Sets the Trunk Link Mode on Switch A1

```
vtp pruning
```

Step 3: Isolating, Modifying, and then Reintroducing a Switch into the VTP Domain

This step demonstrates the VTP synchronization issue. Switch A2 is isolated from the network so that it can be reconfigured for a different purpose, using the configuration commands shown in Example 4-7.

Example 4-7 Commands That Isolate Switch A2 from the Network

```
interface fastethernet1/0/48
   shutdown
   exit
```

Switch A2 is converted to a VTP server, and two new VLANs are added to its configuration. Subsequently, the decision is made to delete all the VLANs on switch A2. As each VLAN is deleted from the switch, the VTP configuration revision number is incremented. The commands shown in Example 4-8 make these modifications and introduce switch A2 back into the network. When the switch comes online in the network, it has the highest revision number and becomes the VTP server with the authoritative database. All other switches in the VTP domain accept switch A2s information and delete the full set of VLANs—even as they are in production in the network!

Example 4-8 Commands That Modify Switch A2

```
vtp mode server
vlan 101
   name Lobby
vlan 102
   name Building1
no vlan 101
no vlan 102
no vlan 100
no vlan 3
no vlan 2

interface fastethernet1/0/48
   no shutdown
   exit
```

Step 4: Converting Switches A1 and A2 to VTP Transparent Mode

This step converts both switches A1 and A2 to the VTP transparent mode so that their VLAN configurations can be deliberately set. Because their VLAN configurations were flushed during the VTP synchronization issue demonstration in Step 3, VLANs 2, 3, and 10 must be reconfigured. Example 4-9 shows the commands used on both switches.

Example 4-9 Commands That Convert Switches A1 and A2 to VTP Transparent Mode

```
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
```

Lab 5

Working with the Spanning Tree Protocol (STP)

This LAN Switching Video Mentor lab covers the Spanning Tree Protocol (STP) and how you can use it to automatically prevent bridging loops in a Layer 2 network.

The objectives of this lab are as follows:

- Understand bridging loops.
- Understand the STP.
- Verify STP operation.
- Configure the STP root switch.

Scenario

This lab contains three main steps, as follows:

Step 1. Disable STP and trigger a bridging loop.

Step 2. Verify STP operation and topology.

Step 3. Configure the STP root switch.

Initial Configurations

The switches used in this lab have their initial configurations as a result of Lab 4, with the addition of a third switch, C1. The relevant initial configuration commands already in place on switches A1, A2, and C1 are shown in Examples 5-1 through 5-3, respectively.

Example 5-1 Initial Configuration Commands for Switch A1

```
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/0/48
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
```

Example 5-1 Initial Configuration Commands for Switch A1 continued

```
   switchport mode trunk
interface gigabitethernet1/0/49
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Example 5-2 Initial Configuration Commands for Switch A2

```
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface fastethernet1/0/48
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet1/0/1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Example 5-3 Initial Configuration Commands for Switch C1

```
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet2/1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/3
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Video Presentation Reference

Figure 5-1 shows the network topology used in this lab. In the following sections, the commands that are entered in each of the lab steps are shown.

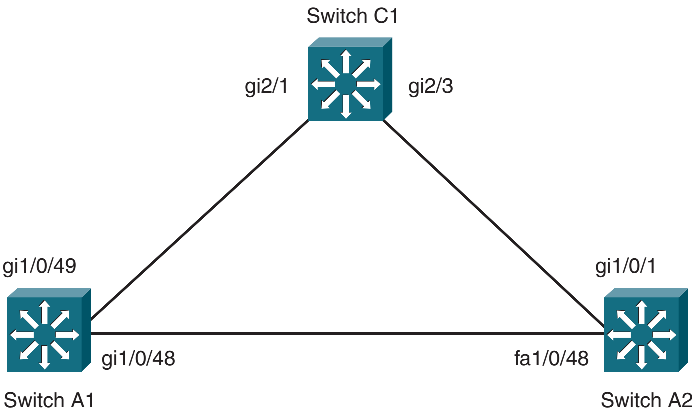

Figure 5-1 Lab 5 Network Topology

Step 1: Disabling STP and Triggering a Bridging Loop

This step disables the Spanning Tree Protocol on switches A1, A2, and C1 to remove the default mechanism to prevent Layer 2 bridging loops from forming. This is done only to demonstrate how a bridging loop can form and how it affects the network.

Example 5-4 shows the command that is entered on switches A1, A2, and C1.

Example 5-4 Command That Disables STP on VLAN 2

```
no spanning-tree vlan 2
```

On the PC connected to Switch A1s gigabitethernet1/0/1 interface, a single ping or ICMP echo request packet is sent to a nonexistent destination. When the packet is flooded by switch A1, the bridging loop begins.

To break the bridging loop, enter the commands on switch A1, as shown in Example 5-5.

Example 5-5 Command That Disables STP and Breaks the Bridging Loop on VLAN 2

```
interface gigabitethernet1/0/48
shutdown
```

The STP is reenabled on each switch before moving to Step 2, using the configuration command shown in Example 5-6.

Example 5-6 Command That Reenables STP

```
spanning-tree vlan 2
```

Step 2: Verifying STP Operation and Topology

This step verifies the STP Root Switch with the command shown in Example 5-7. All three switches should agree on the current Root Switch ID. As well, the STP state of each active interface is shown using the same command output.

Example 5-7 Command That Verifies the STP State

```
show spanning-tree vlan 2
```

On switch A2, interface FastEthernet1/0/48 is shut down and then brought back up to demonstrate how an interface progresses through the STP states. The commands shown in Example 5-8 are used.

Example 5-8 Command That Triggers STP Port State Progression

```
interface fastethernet1/0/48
shutdown
no shutdown
```

Step 3: Configuring the STP Root Switch

Although switch C1 becomes the STP Root Switch in this lab, it does so only by chance. In this step, switch C1 is configured to always take the Root Switch role, using the configuration command shown in Example 5-9.

Example 5-9 Command That Forces the STP Root Switch Election

```
spanning-tree vlan 2,3,10 priority 0
```

Lab 6

STP Topology Changes

This LAN Switching Video Mentor lab covers the Spanning Tree Protocol (STP) and how it reacts to changes in the Layer 2 network topology.

The objectives of this lab are as follows:

- Understand Per-VLAN Spanning Tree (PVST+).
- Configure to handle insignificant topology changes.
- Configure to handle direct topology changes.
- Configure to handle indirect topology changes.

Scenario

This lab contains four main steps, as follows:

Step 1. Display the current STP topology in PVST+.

Step 2. Deal with insignificant topology changes.

Step 3. Deal with direct topology changes.

Step 4. Deal with indirect topology changes.

Initial Configurations

The switches in this lab have their initial configurations as a result of Lab 5. The relevant initial configuration commands already in place on switches A1, A2, C1, and C2 are shown in Examples 6-1 through 6-4, respectively.

Example 6-1 Initial Configuration Commands for Switch A1

```
spanning-tree extend system-id
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/0/48
   shutdown
interface gigabitethernet1/0/49
   description to switch C1
```

Example 6-1 Initial Configuration Commands for Switch A1 continued

```
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet1/0/51
   description to switch C2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Example 6-2 Initial Configuration Commands for Switch A2

```
spanning-tree extend system-id
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface fastethernet1/0/48
   shutdown
interface gigabitethernet1/0/1
   description to switch C1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet1/0/3
   description to switch C2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Example 6-3 Initial Configuration Commands for Switch C1

```
spanning-tree extend system-id
spanning-tree vlan 2,3,10 priority 0
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/1
   description to switch C2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/1
   description to switch A1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/3
   description to switch A2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Example 6-4 Initial Configuration Commands for Switch C2

```
spanning-tree extend system-id
spanning-tree vlan 2,3,10 priority 4096
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/1
   description to switch C1
   switchport
   switchport trunk encapsulation dot1q
```

Example 6-4 Initial Configuration Commands for Switch C2 continued

```
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/1
   description to switch A1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/3
   description to switch A2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Video Presentation Reference

Figure 6-1 shows the network topology used in this lab. In the following sections, the commands entered in each of the lab steps are shown.

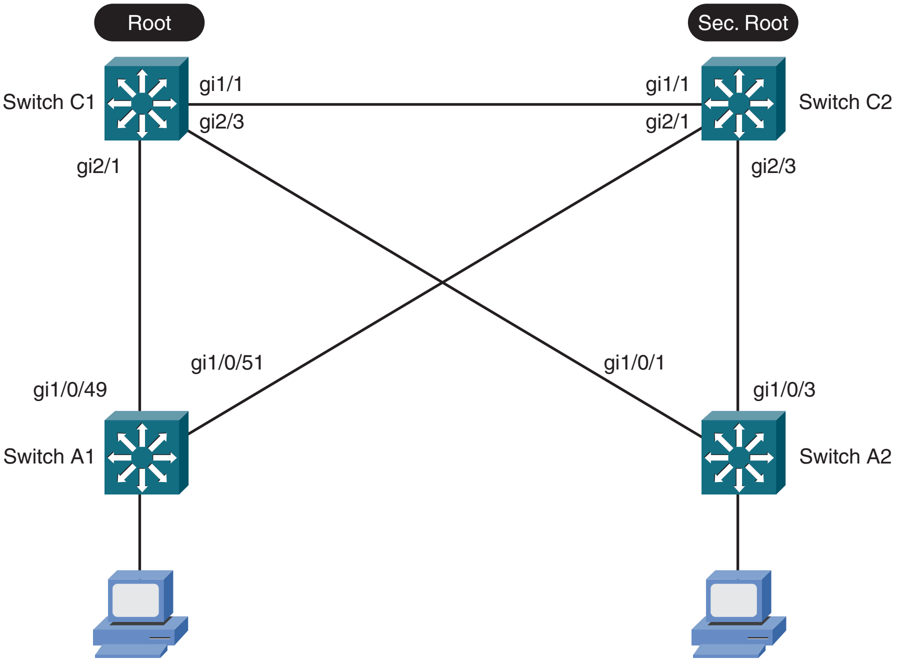

Figure 6-1 Lab 6 Network Topology

Figure 6-2 shows the steady state STP topology as a reference.

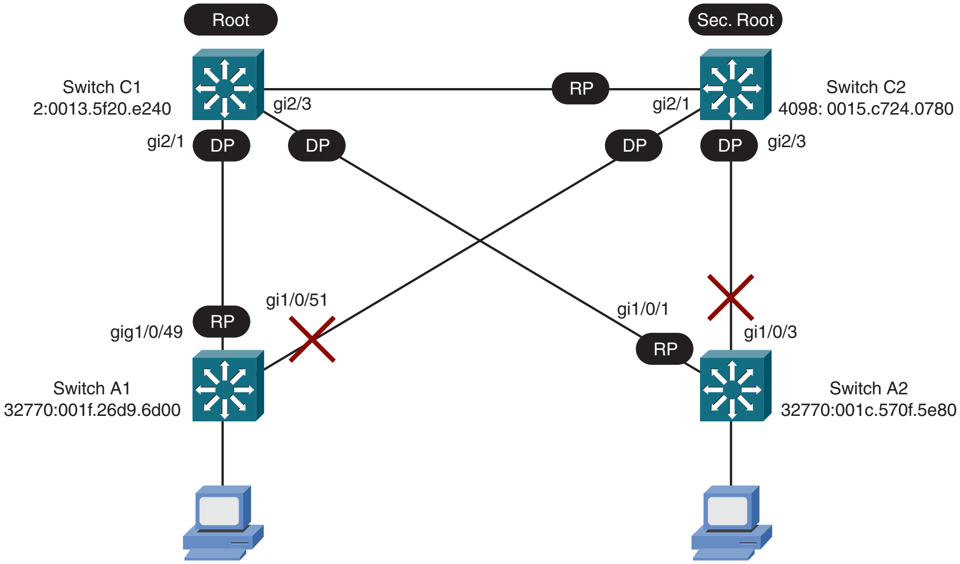

Figure 6-2 Lab 6 STP Topology

Step 1: Displaying the Current STP Topology in PVST+

Due to the nature of Per-VLAN STP+ (PVST+), each VLAN has its own STP topology. In this step, and at various times in the lab, the current STP topology for a VLAN is displayed by entering the commands shown in Example 6-5.

Example 6-5 Commands That Display the Current STP Topology

```
show spanning-tree vlan 2
show spanning-tree vlan 10
show spanning-tree interface gigabitethernet1/0/49
```

Step 2: Dealing with Insignificant Topology Changes

When single hosts are connected to a switch, STP topology changes can be triggered whenever the host goes down or comes up. In this step, the STP PortFast feature identifies ports that have single hosts connected and prevents topology changes from occurring.

Example 6-6 shows the configuration commands used on switch A1 to enable PortFast on interface GigabitEthernet1/0/1.

Example 6-6 Commands That Enable STP PortFast

```
interface gigabitethernet1/0/1
spanning-tree portfast
```

Step 3: Dealing with Direct Topology Changes

A direct topology change is one that STP can detect by monitoring the interface link state. In this step, a link fails, and we see how STP reacts by default. Then the STP UplinkFast feature is enabled on switch A1, using the configuration command shown in Example 6-7, greatly improving the STP reaction time.

Example 6-7 Command That Enables STP UplinkFast

```
spanning-tree uplinkfast
```

Step 4: Dealing with Indirect Topology Changes

An indirect topology change occurs away from a switch so that it can't be easily detected. This step filters STP BPDU packets on the link between C1 and A1, without causing the link to fail or change state.

First, you see how STP reacts by default. Then the STP BackboneFast feature is enabled on all four switches (A1, A2, C1, and C2), using the configuration command shown in Example 6-8.

Example 6-8 Command That Enables STP BackboneFast

```
spanning-tree backbonefast
```

Leveraging Rapid STP

This LAN Switching Video Mentor lab covers the Rapid Spanning Tree Protocol (RSTP) and how you can use it to solve a variety of delays present in the traditional STP.

Note

Sometimes the STP acronyms and modes can be confusing. The following list should help:

- **STP**—The traditional Spanning Tree Protocol defined in IEEE 802.1D
- **PVST+**—Per-VLAN STP, where one instance of STP runs on each VLAN in a network
- **RSTP**—Rapid STP, the next generation of STP, defined in IEEE 802.1w
- **RPVST+**—One instance of RSTP running on each VLAN in a network, similar to PVST+

The objectives of this lab are as follows:

- Learn about Rapid STP operation and configuration.
- Set Rapid STP port types.
- Observe Rapid STP reacting to topology changes.

Scenario

This lab contains three main steps, as follows:

Step 1. Enable the Rapid STP mode.

Step 2. Assign port types.

Step 3. Observe Rapid STP reacting to direct and indirect topology changes.

Initial Configurations

The switches used in this lab have their initial configurations as a result of Lab 5. The relevant initial configuration commands already in place on switches A1, A2, C1, and C2 are shown in Examples 7-1 through 7-4, respectively.

Example 7-1 Initial Configuration Commands for Switch A1

```
spanning-tree extend system-id
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
```

Example 7-1 Initial Configuration Commands for Switch A1 continued

```
vlan 10
   name voice
interface gigabitethernet1/0/48
   shutdown
interface gigabitethernet1/0/49
   description to switch C1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet1/0/51
   description to switch C2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Example 7-2 Initial Configuration Commands for Switch A2

```
spanning-tree extend system-id
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface fastethernet1/0/48
   shutdown
interface gigabitethernet1/0/1
   description to switch C1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet1/0/3
   description to switch C2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Example 7-3 Initial Configuration Commands for Switch C1

```
spanning-tree extend system-id
spanning-tree vlan 2,3,10 priority 0
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/1
   description to switch C2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/1
   description to switch A1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/3
   description to switch A2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Example 7-4 Initial Configuration Commands for Switch C2

```
spanning-tree extend system-id
spanning-tree vlan 2,3,10 priority 4096
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/1
   description to switch C1
   switchport
```

Example 7-4 Initial Configuration Commands for Switch C2 continued

```
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/1
   description to switch A1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/3
   description to switch A2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Video Presentation Reference

Figure 7-1 shows the network topology used in this lab. In the following sections, the entered commands in each of the lab steps are shown.

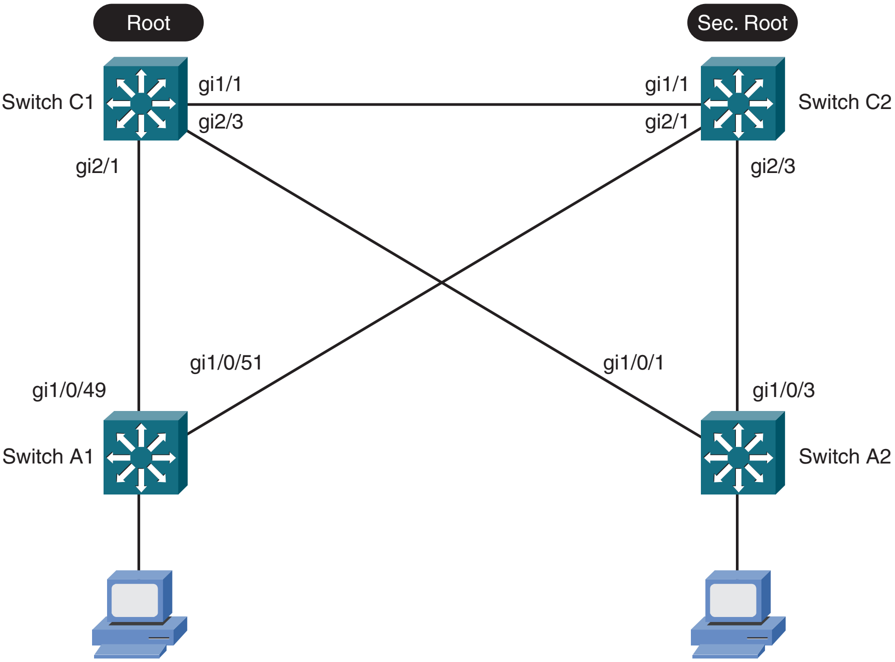

Figure 7-1 Lab 7 Network Topology

The steady state STP topology is shown in Figure 7-2 as a reference.

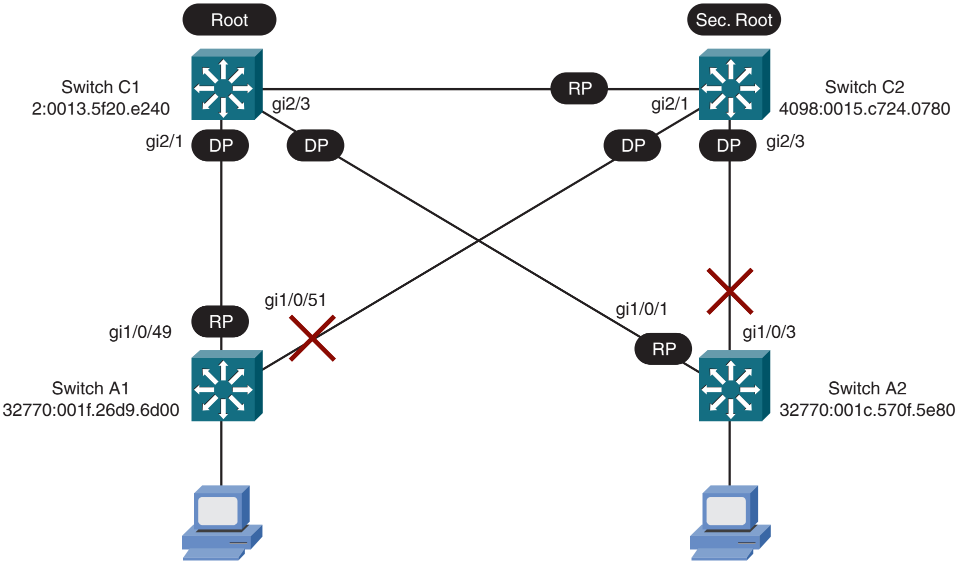

Figure 7-2 Lab 7 STP Topology

Step 1: Enabling the Rapid STP Mode

In this step, you can enable Rapid STP on each switch (A1, A2, C1, and C2) by entering the configuration command shown in Example 7-5. Rapid STP comes up on a per-VLAN basis as Rapid PVST+ or RPVST+.

Example 7-5 Command That Enables Rapid STP Mode

```
spanning-tree mode rapid-pvst
```

Step 2: Assigning Port Types

For switch ports that connect to other switches, the Rapid STP *point-to-point* type is configured. By default, a switch automatically selects the point-to-point type for any interface that is operating in full-duplex mode. In this step, there is no need to enter the **spanning-tree link-type point-to-point** interface configuration command because all switch-to-switch links are full-duplex and are correctly configured automatically.

Where single hosts connect to a switch, Rapid STP should consider the interfaces as *edge* ports. In this step, a single PC connects to interface GigabitEthernet1/0/1 on switch A1, so the interface configuration command shown in Example 7-6 is entered to assign an edge port. Because this is similar to the STP PortFast feature, the interface configuration command can be used for either purpose.

Example 7-6 Commands That Assign a Rapid STP Edge Port

```
interface gigabitethernet1/0/1
spanning-tree portfast
```

Step 3: Observing Topology Changes

In this step, a direct topology change is caused by a link failure between switches C1 and A1. You can see how Rapid STP reacts on switch A1 by entering the command shown in Example 7-7 and observing the STP topology for VLAN 2.

Example 7-7 Command That Displays the Rapid STP Topology

```
show spanning-tree vlan 2
```

An indirect topology change is also demonstrated by filtering Rapid STP BPDU packets between switches C1 and A1. The command shown in Example 7-7 is used again to see how Rapid STP reacts.

Lab 8

Scaling STP with MST

This LAN Switching Video Mentor lab covers the Multiple Spanning Tree (MST) Protocol and how you can use it to scale an STP operation on switches with many VLANs. MST provides a way to reduce the number of STP instances and group VLANs into those instances.

The objectives of this lab are as follows:

- Observe some possible STP topologies.
- Configure an MST region and add switches to it.
- Configure MST instances.

Scenario

This lab contains four main steps, as follows:

Step 1. Locate the Root Switch deterministically.

Step 2. Enable an MST operation.

Step 3. Configure an MST region.

Step 4. Configure two MST instances.

Initial Configurations

The switches used in this lab have their initial configurations as a result of Lab 7. The relevant initial configuration commands already in place on switches A1, A2, C1, and C2 are shown in Examples 8-1 through 8-4, respectively.

Example 8-1 Initial Configuration Commands for Switch A1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/0/48
   shutdown
interface gigabitethernet1/0/49
   description to switch C1
```

Example 8-1 Initial Configuration Commands for Switch A1 continued

```
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet1/0/51
   description to switch C2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Example 8-2 Initial Configuration Commands for Switch A2

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface fastethernet1/0/48
   shutdown
interface gigabitethernet1/0/1
   description to switch C1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet1/0/3
   description to switch C2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Example 8-3 Initial Configuration Commands for Switch C1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
spanning-tree vlan 2,3,10 priority 0
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/1
   description to switch C2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/1
   description to switch A1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/3
   description to switch A2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Example 8-4 Initial Configuration Commands for Switch C2

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
spanning-tree vlan 2,3,10 priority 4096
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/1
```

Example 8-4 Initial Configuration Commands for Switch C2 continued

```
   description to switch C1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/1
   description to switch A1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/3
   description to switch A2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Video Presentation Reference

Figure 8-1 shows the network topology used in this lab. In the following sections, the entered commands in each of the lab steps are shown.

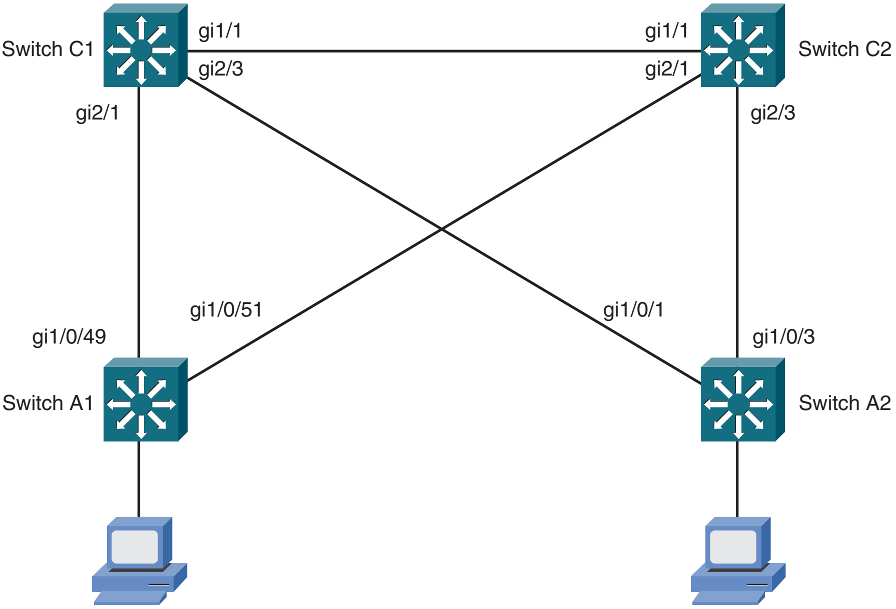

Figure 8-1 Lab 8 Network Topology

Step 1: Locating the Root Switch Deterministically

In this step, Rapid STP is already enabled on switches A1, A2, C1, and C2. Switch C1 is the Root Switch for every active VLAN, and switch C2 is configured to take over the Root role on every active VLAN if C1 fails. By locating the Root and secondary Root Switches in a deterministic fashion, the resulting STP topology will be worked out according to a best practice design. Otherwise, if the default STP priorities are used, the topology will be determined by *any* switch that has the lowest bridge priority—resulting in a topology that might not be expected.

On switch A1, the commands shown in Example 8-5 are entered to display STP topology information. Specifically, the current Root Switch for each active VLAN and the current STP topology for the two access switch uplinks are displayed.

Example 8-5 Commands That Display STP Topology Information

```
show spanning-tree root
show spanning-tree interface gigabitethernet1/0/49
show spanning-tree interface gigabitethernet1/0/51
```

Switch C1 is the current Root Switch for VLANs 2, 3, and 10. The configuration commands shown in Example 8-6 are entered on Switch C2 to make it the Root Switch for VLAN 3. The commands shown in Example 8-7 are entered on switch C1 to make it the secondary Root for VLAN 3.

Example 8-6 Command That Makes Switch C2 the Root for VLAN 3

```
show spanning-tree vlan 3 priority 0
```

Example 8-7 Command That Makes Switch C1 the Secondary Root for VLAN 3

```
show spanning-tree vlan 3 priority 4096
```

Step 2: Enabling MST Operation

The configuration command shown in Example 8-8 is entered on each switch (A1, A2, C1, and C2) to enable the MST mode.

Example 8-8 Commands That Enable MST Mode

```
spanning-tree mode mst
```

Step 3: Configuring an MST Region

In this step, an MST region is defined, and four switches are added to it. The region is named **Region1**. The configuration commands shown in Example 8-9 are entered on switches C1, C2, A1, and A2.

Example 8-9 Commands That Create an MST Region

```
spanning-tree mst configuration
name Region1
revision 1
exit
```

Step 4: Configuring two MST Instances

As a result of Step 3, one MST instance (MSTI 0), or the Integrated Spanning Tree (IST), is created on each switch. All possible VLANs are mapped to it, resulting in a single STP topology.

In this step, a second MST instance is configured so that two distinct topologies can be utilized. The configuration commands shown in Example 8-10 are entered in each switch to create MSTI 1 and map VLAN 3 to it.

Example 8-10 Commands That Create an MST Instance

```
spanning-tree mst configuration
instance 1 vlan 3
revision 2
exit
```

After the instance is created, the Root Switch is purposely located: C1 is the Root for MSTI 0 and the secondary Root for MSTI 1, whereas C2 is the Root for MSTI 1 and the secondary Root for MSTI 0. The configuration commands shown in Example 8-11 are entered into switch C1, whereas the commands shown in Example 8-12 are entered into switch C2.

Example 8-11 Commands That Define the Root Switch in MST Instance 0 on Switch C1

```
spanning-tree mst 0 priority 0
spanning-tree mst 1 priority 4096
```

Example 8-12 Commands That Define the Root Switch in MST Instance 1 on Switch C2

```
spanning-tree mst 1 priority 0
spanning-tree mst 0 priority 4096
```

Note

Recall that with STP, the extended switch system ID is the VLAN number, so the resulting STP bridge priority is the configured priority plus the VLAN number. With MST, the system ID becomes the MST instance number, so the resulting STP bridge priority is the configured priority plus the MST instance number.

Lab 9

Protecting the STP Topology

This LAN Switching Video Mentor lab covers several features that can help protect a stable Spanning Tree topology from changes that could introduce bridging loops.

The objectives of this lab are as follows:

- Protect against unexpected BPDUs with Root Guard.
- Protect against unexpected BPDUs with BPDU Guard.
- Protect against missing BPDUs with Loop Guard.
- Protect against unidirectional links with Unidirectional Link Detection (UDLD).

Scenario

This lab contains four main steps, as follows:

Step 1. Configure Root Guard on interfaces where a Root Switch should not be found.

Step 2. Configure BPDU Guard on interfaces where other switches should not be found.

Step 3. Configure Loop Guard on all switch interfaces.

Step 4. Configure UDLD on all switches in a network.

Initial Configurations

The switches used in this lab have their initial configurations as a result of Lab 7, so Rapid STP is enabled. The relevant initial configuration commands already in place on switches A1, A2, C1, and C2 are shown in Examples 9-1 through 9-4, respectively.

Example 9-1 Initial Configuration Commands for Switch A1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/0/48
   shutdown
interface gigabitethernet1/0/49
```

Example 9-1 Initial Configuration Commands for Switch A1 continued

```
   description to switch C1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet1/0/51
   description to switch C2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Example 9-2 Initial Configuration Commands for Switch A2

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface fastethernet1/0/48
   shutdown
interface gigabitethernet1/0/1
   description to switch C1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet1/0/3
   description to switch C2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Example 9-3 Initial Configuration Commands for Switch C1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
spanning-tree vlan 2,3,10 priority 0
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/1
   description to switch C2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/1
   description to switch A1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/3
   description to switch A2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Example 9-4 Initial Configuration Commands for Switch C2

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
spanning-tree vlan 2,3,10 priority 4096
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/1
```

Example 9-4 Initial Configuration Commands for Switch C2 continued

```
   description to switch C1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/1
   description to switch A1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet2/3
   description to switch A2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
```

Video Presentation Reference

Figure 9-1 shows the network topology used in this lab. In the following sections, the commands that are entered in each of the lab steps are shown.

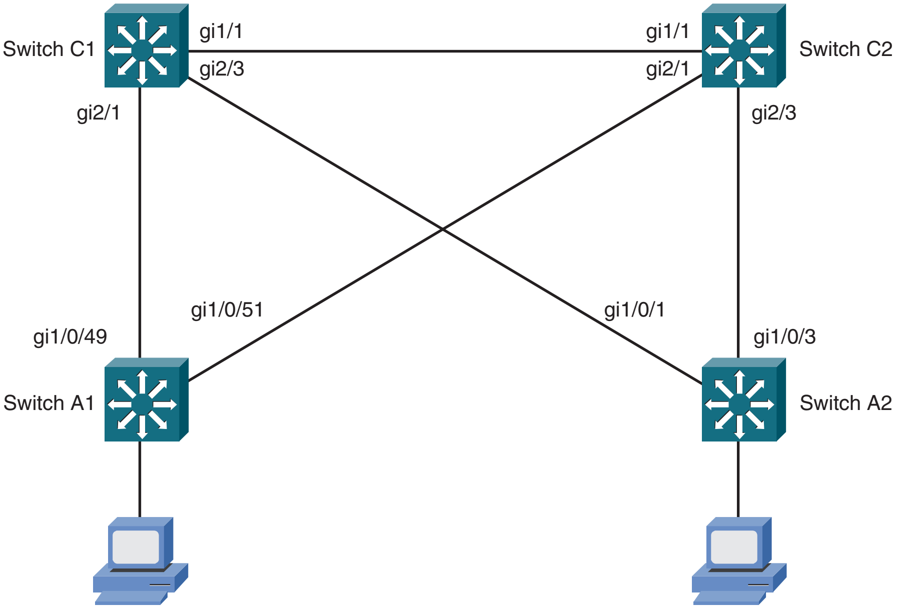

Figure 9-1 Lab 9 Network Topology

Step 1: Configuring Root Guard

In this step, Rapid STP is already enabled on switches A1, A2, C1, and C2. Switch C1 is the Root Switch for every active VLAN, and switch C2 is configured to take over the Root role on every active VLAN if C1 fails. Therefore, on switches A1 and A2, the Root Switch should always be found on either of the two uplinks, but nowhere else.

On switch A1, Root Guard is enabled on interface gigabitethernet1/0/47 to prevent a device that is connected there from ever becoming the Root Switch. The configuration commands shown in Example 9-5 are entered.

Example 9-5 Commands That Enable Root Guard

```
interface gigabitethernet1/0/47
spanning-tree guard root
exit
```

Step 2: Enabling BPDU Guard

In this step, BPDU Guard is enabled on switch A1 interface gigabitethernet1/0/47 to prevent any device running STP from communicating. The configuration commands shown in Example 9-6 are entered to disable Root Guard (which was enabled in Step 1) and enable BPDU Guard instead.

Example 9-6 Commands That Enable BPDU Guard

```
interface gigabitethernet1/0/47
no spanning-tree guard root
spanning-tree bpduguard enable
exit
```

Tip

Rather than configure switch interfaces individually to enable BPDU Guard, you can use the **spanning-tree portfast bpduguard default** global configuration command. This enables BPDU Guard automatically on every switch interface that already has PortFast enabled.

Step 3: Enabling Loop Guard

In this step, the Loop Guard feature is enabled globally on switch A1 to operate on all switch interfaces. In effect, Loop Guard prevents ports that experienced a loss of BPDUs during an indirect STP topology change from inadvertently becoming part of a bridging loop. The configuration command shown in Example 9-7 is entered on switch A1.

Example 9-7 Command That Enables Loop Guard as a Global Default

```
spanning-tree loopguard default
```

Step 4: Enabling UDLD

In this step, the Unidirectional Link Detection (UDLD) feature is enabled on all switches (A1, A2, C1, and C2) to detect unidirectional links over fiber optic media. This prevents unidirectional link faults from causing a bridging loop.

The configuration command shown in Example 9-8 is entered on each switch to enable the UDLD aggressive mode on all fiber optic-based interfaces. Aggressive mode takes action by automatically disabling an interface when unidirectional behavior is detected.

Example 9-8 Command That Enables UDLD Aggressive Mode

```
udld aggressive
```

The EXEC commands shown in Example 9-9 display information about the UDLD status.

Example 9-9 Commands Used to Display UDLD Status

```
show udld
show udld neighbors
```

Lab 10

Scaling Bandwidth with EtherChannel

This LAN Switching Video Mentor lab covers EtherChannel configuration, allowing multiple switch interfaces to be bundled together as a single logical interface.

The objectives of this lab are as follows:

- Build an EtherChannel manually.
- Negotiate an EtherChannel with Port Aggregation Protocol (PAgP).
- Negotiate an EtherChannel with Link Aggregation Control Protocol (LACP).
- Build a Multi-Chassis EtherChannel.

Scenario

This lab contains five main steps, as follows:

Step 1. Configure the EtherChannel load balancing method.

Step 2. Configure an “always on” EtherChannel.

Step 3. Configure PAgP negotiation for an EtherChannel.

Step 4. Configure LACP negotiation for an EtherChannel.

Step 5. Configure a Multi-Chassis EtherChannel.

Initial Configurations

The switches used in this lab have their initial configurations as a result of Lab 9, although only switches A1 and C1 are used. In earlier labs, a Catalyst 6500 is used for C1; in this lab, a Catalyst 3750 is used instead, to leverage its stacking capability.

The relevant initial configuration commands already in place on switches A1 and C1 are shown in Examples 10-1 and 10-2, respectively.

Example 10-1 Initial Configuration Commands for Switch A1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
```

Example 10-1 Initial Configuration Commands for Switch A1 continued

```
interface gigabitethernet1/0/49
   description to switch C1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet1/0/50
interface gigabitethernet1/0/51
   description to switch C2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet1/0/52
```

Example 10-2 Initial Configuration Commands for Switch C1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
spanning-tree vlan 2,3,10 priority 0
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/0/1
interface gigabitethernet1/0/2
interface gigabitethernet1/0/3
interface gigabitethernet1/0/4
interface gigabitethernet1/0/5
interface gigabitethernet1/0/6
interface gigabitethernet1/0/7
interface gigabitethernet1/0/8
```

Video Presentation Reference

Figure 10-1 shows the network topology used in this lab. In the following sections, the entered commands in each of the lab steps are shown.

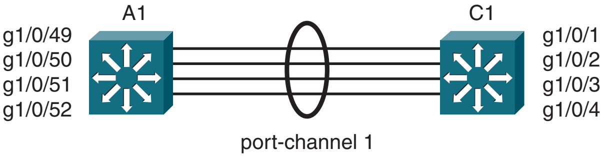

Figure 10-1 Lab 10 Network Topology for Steps 1 Through 4

Step 1: Configuring the EtherChannel Load Balancing Method

In this step, switches A1 and C1 begin with the default EtherChannel load balancing method using only the source MAC address. The method is changed on both switches so that the XOR of the source and destination IP addresses is used, by entering the configuration commands shown in Example 10-3.

Example 10-3 Commands That Configure the EtherChannel Load Balancing Method

```
port-channel load-balance src-dst-ip
```

Step 2: Configuring an “Always On” EtherChannel

In this step, four interfaces are configured as an unconditional EtherChannel between switches A1 and C1. No EtherChannel negotiation is used. Some configuration commands are entered on switch A1 along the way, while various errors are observed. The resulting configuration commands are shown in Example 10-4. The configuration commands entered on switch C1 are shown in Example 10-5.

Example 10-4 Commands That Enable an Unconditional EtherChannel on Switch A1

```
interface range gigabitethernet1/0/49 - 52
   shutdown
   description etherchannel to C1
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
   channel-group 1 mode on
exit
```

Example 10-5 Commands That Enable an Unconditional EtherChannel on Switch C1

```
interface range gigabitethernet1/0/1 - 4
   description etherchannel to A1
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
   channel-group 1 mode on
exit
```

Finally, the interface range on switch A1 is enabled with the **no shutdown** command. The EtherChannel status displays with the **show etherchannel summary** command.

Step 3: Configuring PAgP Negotiation

In this step, the Port Aggregation Protocol (PAgP) negotiates an EtherChannel between switches A1 and C1. First, the unconditional EtherChannel configuration from Step 2 is removed; then PAgP is enabled on the four-interface EtherChannel. The commands entered on switches A1 and C1 are shown in Examples 10-6 and 10-7, respectively.

Example 10-6 Commands That Enable PAgP Negotiation on Switch A1

```
interface range gigabitethernet1/0/49 - 52
   shutdown
   no channel-group 1
   channel-protocol pagp
   channel-group 1 mode auto
```

Example 10-7 Commands That Enable PAgP Negotiation on Switch C1

```
interface range gigabitethernet1/0/1 - 4
   no channel-group 1
   channel-protocol pagp
   channel-group 1 mode desirable
exit
```

Finally, the interface range on switch A1 is enabled with the **no shutdown** command. The EtherChannel status displays with the **show etherchannel summary** command.

Step 4: Configuring LACP Negotiation

In this step, the Link Aggregation Control Protocol (LACP) negotiates an EtherChannel between switches A1 and C1. First, the PAgP EtherChannel configuration from Step 3 is removed; then LACP is enabled on the four-interface EtherChannel. Switch C1 is given a lower-than-default LACP system priority so that it can make all EtherChannel negotiation decisions for the pair of switches. The commands entered on switches A1 and C1 are shown in Examples 10-8 and 10-9, respectively.

Example 10-8 Commands That Enable LACP Negotiation on Switch A1

```
interface gigabitethernet1/0/49 - 52
   shutdown
   no channel-group 1
   channel-protocol lacp
   channel-group 1 mode passive
```

Example 10-9 Commands That Enable LACP Negotiation on Switch C1

```
lacp system-priority 100
interface gigabitethernet1/0/1 - 4
   no channel-group 1
   channel-protocol lacp
   channel-group 1 mode active
exit
```

Finally, the interface range on switch A1 is enabled with the **no shutdown** command. The EtherChannel status displays with the **show etherchannel summary** command.

Step 5: Configuring a Multi-Chassis EtherChannel

In this step, an additional switch chassis is added to both switches A1 and C1 so that they become stacked pairs. The EtherChannel is expanded so that its member links cross the physical switch chassis within each stacked pair. This creates a Multi-Chassis EtherChannel (MEC) with a high degree of redundancy. Figure 10-2 shows a network diagram used in this step.

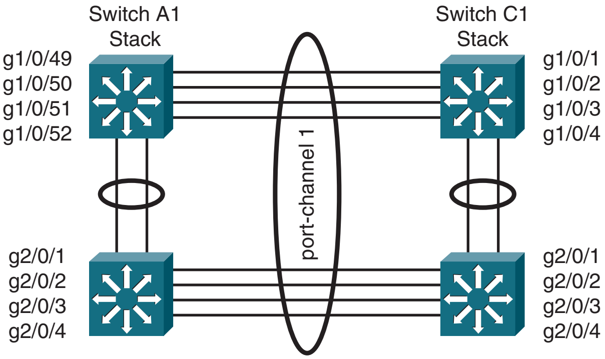

Figure 10-2 Lab 10 Network Topology for Step 5

The configuration commands shown in Examples 10-10 and 10-11 are entered into switches A1 and C1, respectively, to configure the interfaces on the second switch in each stack. The LACP negotiation configured in Step 4 is retained in this step.

Example 10-10 Commands That Configure a Multi-Chassis EtherChannel on Switch A1

```
interface range gigabitethernet2/0/1 - 4
   shutdown
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
   channel-protocol lacp
   channel-group 1 mode passive
```

Example 10-11 Commands That Configure a Multi-Chassis EtherChannel on Switch C1

```
interface range gigabitethernet2/0/1 - 4
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
   channel-protocol lacp
   channel-group 1 mode active
   no shutdown
exit
```

Finally, the interface range on switch A1 is enabled with the **no shutdown** command. The EtherChannel status displays with the **show etherchannel summary** command.

Lab 11

Setting Up Multilayer Switching

This LAN Switching Video Mentor lab moves beyond traditional Layer 2 switching and covers routing between VLANs and IP subnets on Catalyst switches.

The objectives of this lab are as follows:

- Configure Layer 3 switch interfaces.
- Learn about InterVLAN routing.
- Use and monitor Cisco Express Forwarding (CEF).

Scenario

This lab contains five main steps, as follows:

Step 1. Configure a switched virtual interface (SVI).

Step 2. Configure a Layer 3 physical interface.

Step 3. Configure a Layer 3 EtherChannel.

Step 4. Enable IP routing and CEF.

Step 5. Monitor CEF operation.

Initial Configurations

The switches used in this lab have their initial configurations as a result of Lab 10, using only switches A1 and C1.

The relevant initial configuration commands already in place on switches A1 and C1 are shown in Examples 11-1 through 11-2, respectively.

Example 11-1 Initial Configuration Commands for Switch A1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface port-channel1
```

Example 11-1 Initial Configuration Commands for Switch A1 continued

```
   description to switch C1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
   no shutdown
interface range gigabitethernet1/0/49 - 52 , gig2/0/1 - 4
   description to switch C1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
   channel-protocol lacp
   channel-group 1 mode passive
   no shutdown
```

Example 11-2 Initial Configuration Commands for Switch C1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
spanning-tree vlan 2,3,10 priority 0
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface port-channel1
   description to switch A1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
   no shutdown
interface range gigabitethernet1/0/1 - 4 , gig2/0/1 - 4
   description to switch A1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
   channel-protocol lacp
   channel-group 1 mode active
   no shutdown
```

Video Presentation Reference

The following sections show the commands entered in each of the lab steps.

Step 1: Configuring a Switched Virtual Interface (SVI)

In this step, two Layer 3 SVIs are configured on switch C1—one on VLAN 2 and one on VLAN 3. Figure 11-1 shows the network topology used in this step, and Example 11-3 shows the commands entered on switch C1.

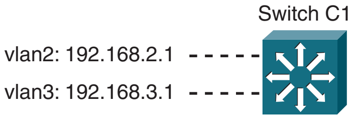

Figure 11-1 Lab 11 Network Topology for Step 1

Example 11-3 Commands That Configure SVIs on Switch C1

```
interface vlan2
   ip address 192.168.2.1 255.255.255.0
   no shutdown
exit
interface vlan 3
   ip address 192.168.3.1 255.255.255.0
   no shutdown
exit
```

You can query Layer 3 interface configurations by using the **show ip interface brief** command.

Step 2: Configuring a Layer 3 Physical Interface

In this step, interface gigabitethernet1/0/10 on switch C1 is configured as a Layer 3 interface. It is given the IP address 192.168.50.1, using the configuration commands shown in Example 11-4.

Example 11-4 Commands That Configure a Layer 3 Interface on Switch C1

```
interface gigabitethernet1/0/10
   no switchport
   ip address 192.168.50.1 255.255.255.0
   no shutdown
exit
```

Step 3: Configuring a Layer 3 EtherChannel

In this step, the 8-port EtherChannel originally configured in Lab 10 is configured for Layer 3 operation. A network diagram is shown in Figure 11-2.

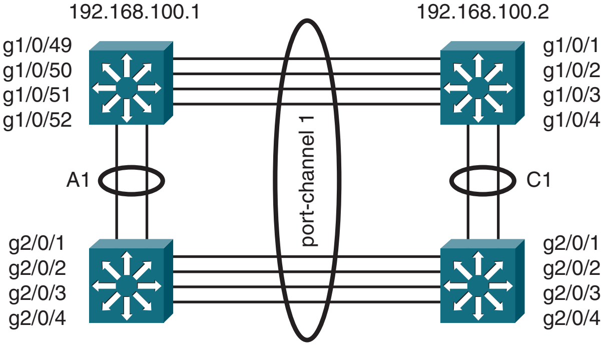

Figure 11-2 Lab 11 Network Topology for Step 3

LACP negotiates an EtherChannel between switches C1 and A1. The commands entered on switches C1 and A1 are shown in Examples 11-5 and 11-6, respectively.

Example 11-5 Commands That Configure a Layer 3 EtherChannel on Switch C1

```
no interface port-channel1
interface port-channel1
   no switchport
   ip address 192.168.100.1 255.255.255.252
   shutdown
!
interface range gigabitethernet1/0/1 - 4 , gigabitethernet2/0/1 - 4
   no switchport
   channel-protocol lacp
   channel-group 1 mode active
   no shutdown
   exit
```

Example 11-6 Commands That Configure a Layer 3 EtherChannel on Switch A1

```
no interface port-channel1
interface port-channel1
   no switchport
   ip address 192.168.100.2 255.255.255.252
   no shutdown
!
interface range gigabitethernet1/0/49 - 52 , gigabitethernet2/0/1 - 4
   no switchport
   channel-protocol lacp
   channel-group 1 mode passive
   no shutdown
exit
```

Finally, interface port-channel1 on switch C1 is brought up for use by entering the configuration commands shown in Example 11-7.

Example 11-7 Commands That Enable a Layer 3 EtherChannel on Switch C1

```
interface port-channel1
   no shutdown
exit
```

Step 4: Enabling IP Routing and Cisco Express Forwarding (CEF)

In this step, IP routing is enabled on switches A1 and C1, which enables CEF in turn. The commands shown in Example 11-8 are entered on switches A1 and C1.

Example 11-8 Commands That Check and Enable IP Routing and CEF

```
show ip cef
configure terminal
ip routing
exit
```

Step 5: Monitoring CEF Operation

In this step, the **show ip cef** command monitors CEF operation and inspects the contents of the Forwarding Information Base (FIB) table.

The **show adjacency** command also inspects the contents of the CEF adjacency table.

Lab 12

First-Hop Redundancy with HSRP

This LAN Switching Video Mentor lab covers the Hot Standby Router Protocol (HSRP) as a method to improve first-hop or gateway redundancy on an IP subnet.

The objectives of this lab are as follows:

- Configure an HSRP group.
- Compare HSRP with Virtual Router Redundancy Protocol (VRRP).
- Configure HSRP load balancing.

Scenario

This lab contains eight main steps, as follows:

Step 1. Define an HSRP group on Switch C1, VLAN 2.

Step 2. Set the HSRP virtual address on Switch C1, VLAN 2.

Step 3. Set the HSRP priority on Switch C1, VLAN 2.

Step 4. Adjust the HSRP timing on Switch C1, VLAN 2.

Step 5. Configure HSRP authentication on Switch C1, VLAN 2.

Step 6. Configure HSRP on Switch C2, VLAN 2.

Step 7. Configure HSRP on VLAN 3.

Step 8. Configure HSRP load balancing.

Initial Configurations

The switches used in this lab are arranged in the redundant topology used in previous labs. Only switches C1 and C2 are used to demonstrate HSRP operation in either the core or distribution layer of a switched network. The link between C1 and C2 is a Layer 2 trunk link so that VLANs 2 and 3 are carried between the two switches.

The relevant initial configuration commands already in place on switches C1 and C2 are shown in Examples 12-1 through 12-2, respectively.

Example 12-1 Initial Configuration Commands for Switch C1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/1
   description to switch C2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
   no shutdown
```

Example 12-2 Initial Configuration Commands for Switch C2

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
spanning-tree vlan 2,3,10 priority 0
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/1
   description to switch C1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
   no shutdown
```

Video Presentation Reference

The network topology for steps 1 through 6 in this lab is shown in Figure 12-1. The following sections show the commands entered in each of the lab steps.

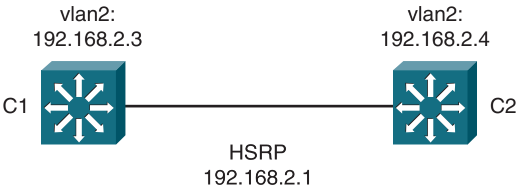

Figure 12-1 Lab 12 Network Topology for Steps 1 Through 6

Step 1: Defining an HSRP Group on Switch C1, VLAN 2

In this step, HSRP group 1 is defined on interface vlan2 of switch C1, using the commands shown in Example 12-3.

Example 12-3 Commands That Define HSRP Group 1 on Switch C1

```
interface vlan2
   ip address 192.168.2.3 255.255.255.0
   no shutdown
   standby 1 name vlan2-gateway
```

Step 2: Setting the HSRP Virtual Address on Switch C1, VLAN 2

In this step, HSRP group 1 is configured to use virtual IP address 192.168.2.1. The interface configuration command shown in Example 12-4 is used on switch C1.

Example 12-4 Command That Configures the HSRP Virtual Address on Switch C1

```
   standby 1 ip 192.168.2.1
```

Step 3: Setting the HSRP Priority on Switch C1, VLAN 2

In this step, switch C1 is given a priority value of 120 for HSRP group 1 on interface vlan2, using the interface configuration command shown in Example 12-5.

Example 12-5 Command That Sets the HSRP Priority on Switch C1

```
   standby 1 priority 120
```

Step 4: Adjusting the HSRP Timing on Switch C1, VLAN 2

In this step, HSRP group 1 on interface vlan2 is configured to use a hello time of 500 milliseconds and a holdtime of 1500 milliseconds. In addition, switch C1 is configured to preempt the HSRP active role after a minimum delay of 60 seconds and a reload delay of 60 seconds. The interface configuration commands shown in Example 12-6 are entered on switch C1.

Example 12-6 Commands That Adjust the HSRP Timing on Switch C1

```
   standby 1 timers msec 500 msec 1500
   standby 1 preempt delay minimum 60 reload 60
```

Step 5: Configuring HSRP Authentication on Switch C1, VLAN 2

In this step, HSRP group 1 on interface vlan2 is configured to use MD5 authentication, based on the single text key-string **b1gs3cr3t**. The interface configuration commands shown in Example 12-7 are entered on switch C1.

Example 12-7 Commands That Enable MD5 Authentication on Switch C1

```
   standby 1 authentication md5 key-string b1gs3cr3t
```

The **show standby** command checks the status of HSRP operation on switch C1.

Step 6: Configuring HSRP on Switch C2, VLAN 2

In this step, Switch C2 is configured for HSRP so that it operates as an HSRP peer with Switch C1 on VLAN 2.

The configuration commands shown in Example 12-8 are entered on switch C2.

Example 12-8 Commands That Configure HSRP Group 1 on Switch C2

```
interface vlan2
   ip address 192.168.2.4 255.255.255.0
   no shutdown
   standby 1 name vlan2-gateway
   standby 1 ip 192.168.2.1
   standby 1 timers msec 500 msec 1500
   standby 1 authentication md5 key-string b1gs3cr3t
exit
```

Step 7: Configuring HSRP VLAN 3

In this step, a new HSRP group 1 is brought up on interface vlan3 on both switches C1 and C2. The network topology is shown in Figure 12-2.

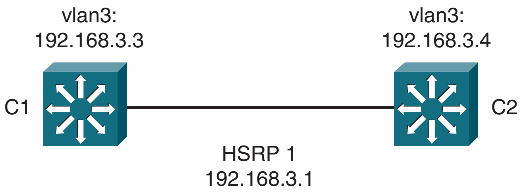

Figure 12-2 Lab 12 Network Topology for Step 7

The configuration commands shown in Examples 12-9 and 12-10 are entered on switches C1 and C2, respectively.

Example 12-9 Commands That Configure HSRP on Switch C1 VLAN 3

```
interface vlan3
   ip address 192.168.3.3 255.255.255.0
   no shutdown
   standby 1 name vlan3-gateway
   standby 1 ip 192.168.3.1
   standby 1 priority 120
   standby 1 timers msec 500 msec 1500
   standby 1 preempt delay minimum 60 reload 60
   standby 1 authentication md5 key-string b1gs3cr3t
exit
```

Example 12-10 Commands That Configure HSRP on Switch C2 VLAN 3

```
interface vlan3
   ip address 192.168.3.4 255.255.255.0
   no shutdown
   standby 1 name vlan3-gateway
   standby 1 ip 192.168.3.1
   standby 1 timers msec 500 msec 1500
   standby 1 authentication md5 key-string b1gs3cr3t
exit
```

Step 8: Configuring HSRP Load Balancing

In this step, two HSRP groups are configured on the same Layer 3 interface so that switches C1 and C2 can load balance gateway traffic. The network topology is shown in Figure 12-3.

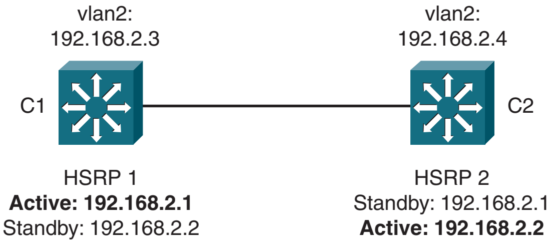

Figure 12-3 Lab 12 Network Topology for HSRP Load Balancing in Step 8

Switch C1 normally has the active role in HSRP group 1, whereas switch C2 is normally active in HSRP group 2. Both switches use virtual IP addresses in the same 192.168.2.0/24 subnet on VLAN 2.

HSRP group 1 in VLAN 2 is already configured as a result of prior steps in this lab. The configuration commands shown in Examples 12-11 and 12-12 are entered on switches C1 and C2, respectively, to configure HSRP group 2.

Example 12-11 Commands That Configure HSRP Load Balancing on Switch C1

```
interface vlan2
   standby 2 name vlan2-gw2
   standby 2 ip 192.168.2.2
   standby 2 priority 100
   standby 2 timers msec 500 msec 1500
   standby 2 authentication md5 key-string b1gs3cr3t
exit
```

Example 12-12 Commands That Configure HSRP Load Balancing on Switch C2

```
interface vlan2
   standby 2 name vlan2-gw2
   standby 2 ip 192.168.2.2
   standby 2 priority 120
   standby 2 timers msec 500 msec 1500
   standby 2 preempt delay minimum 60 reload 60
   standby 2 authentication md5 key-string b1gs3cr3t
exit
```

HSRP—VRRP Comparison

In the video lab, a brief comparison between HSRP and the Virtual Router Redundancy Protocol (VRRP) is made. HSRP was developed by Cisco, whereas VRRP was defined in RFC 3768. VRRP is not covered in detail in this lab because it is so similar to HSRP.

Table 12-1 compares the command syntax between the two first-hop redundancy protocols and can be used as a reference.

Table 12-1 Comparison Between HSRP and VRRP

HSRP	VRRP
standby *group* **priority** *priority*	**vrrp** *group* **priority** *level*
standby *group* **name** *string*	**vrrp** *group* **description** *string*
standby *group* **timers** [**msec**] *hello* [**msec**] *holdtime*	**vrrp** *group* **timers advertise** [**msec**] *interval*
vrrp *group* **timers learn**	
standby *group* **preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]	**vrrp** *group* **preempt** [**delay minimum** *seconds*]
standby *group* **authentication** [**text**] *string*	**vrrp** *group* **authentication** [**text**] *string*
standby *group* **authentication md5 key-string** *string*	**vrrp** *group* **authentication md5 key-string** *string*
standby *group* **authentication md5 key-chain** *chain*	**vrrp** *group* **authentication md5 key-chain** *chain*
standby *group* **ip** *ip-address* [**secondary**]	**vrrp** *group* **ip** *ip-address* [**secondary**]
standby *group* **track** *object-number* [**decrement** [*decrement-value*]]	**vrrp** *group* **track** *object-number* [**decrement** *value*]

First-Hop Redundancy with GLBP

This LAN Switching Video Mentor lab covers the Gateway Load Balancing Protocol (GLBP) as a method to improve first-hop or gateway redundancy on an IP subnet.

The objectives of this lab are as follows:

- Configure the Active Virtual Gateway.
- Configure an Active Virtual Forwarder.
- Monitor GLBP operation.

Scenario

This lab contains seven main steps. In steps 1 through 5, switch C1 is configured as a GLBP Active Virtual Gateway (AVG) and an Active Virtual Forwarder (AVF). In step 6, switch C2 is configured as an AVF and operates as a standby AVG by default.

Step 1. Define a GLBP group and virtual address.

Step 2. Set the GLBP priority.

Step 3. Configure GLBP authentication.

Step 4. Adjust the GLBP timers.

Step 5. Set the GLBP load balancing method.

Step 6. Configure an Active Virtual Forwarder on Switch C2.

Step 7. Monitor GLBP.

Initial Configurations

The switches used in this lab are arranged in the redundant topology used in previous labs. Only switches C1 and C2 are used to demonstrate GLBP operation in either the core or distribution layer of a switched network. The link between C1 and C2 is a Layer 2 trunk link so that VLAN 2 can be carried between the two switches.

The relevant initial configuration commands already in place on switches C1 and C2 are shown in Examples 13-1 through 13-2, respectively.

Example 13-1 Initial Configuration Commands for Switch C1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/1
   description to switch C2
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
   no shutdown
```

Example 13-2 Initial Configuration Commands for Switch C2

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
spanning-tree vlan 2,3,10 priority 0
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/1
   description to switch C1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
   no shutdown
```

Video Presentation Reference

The network topology used in this lab is shown in Figure 13-1. The following sections show the commands entered in each of the lab steps.

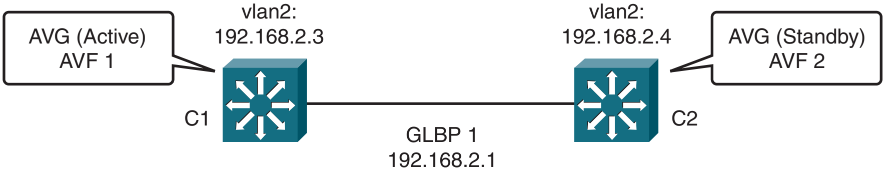

Figure 13-1 Lab 13 Network Topology

Step 1: Defining a GLBP Group and Virtual Address

In this step, GLBP group 1 is defined on interface vlan2 of switch C1, using the commands shown in Example 13-3.

Example 13-3 Commands That Define GLBP Group 1 on Switch C1

```
interface vlan2
   ip address 192.168.2.3 255.255.255.0
   no shutdown
   glbp 1 ip 192.168.2.1
```

Step 2: Setting the GLBP Priority

In this step, switch C1 is given a priority value of 200 for GLBP group 1 on interface vlan2, making it the primary or normally active AVG. C1 is also configured to preempt the active AVG role. The interface configuration commands shown in Example 13-4 are entered on switch C1.

Example 13-4 Commands That Set the GLBP Priority on Switch C1

```
   glbp 1 priority 200
   glbp 1 preempt
```

Step 3: Configuring GLBP Authentication

In this step, GLBP group 1 on interface vlan2 is configured to use MD5 authentication, based on the single text key-string **b1gs3cr3t**. The interface configuration commands shown in Example 13-5 are entered on switch C1.

Example 13-5 Commands That Enable MD5 Authentication on Switch C1

```
   glbp 1 authentication md5 key-string b1gs3cr3t
```

Step 4: Adjusting the GLBP Timers

In this step, GLBP group 1 on interface vlan2 is configured to use a hello time of 500 milliseconds and a holdtime of 1500 milliseconds. The interface configuration commands shown in Example 13-6 are entered on switch C1.

Example 13-6 Commands That Adjust the GLBP Timers on Switch C1

```
   glbp 1 timers msec 500 msec 1500
```

Step 5: Setting the GLBP Load Balancing Method

In this step, GLBP group 1 on interface vlan2 is configured to use the default round robin load balancing method. The interface configuration command shown in Example 13-7 is entered on switch C1.

Example 13-7 Command That Sets the GLBP Load Balancing Method on Switch C1

```
   glbp 1 load-balancing round-robin
```

Step 6: Configuring an AVF on Switch C2

In this step, switch C2 is configured for GLBP operation. GLBP group 1 is defined on interface vlan2, which automatically brings up an AVF function. Switch C2 also becomes a candidate to hold the AVG role, but because it uses the default GLBP priority value, it ends up in the standby AVG role.

The configuration commands shown in Examples 13-8 are entered on switch C2.

Example 13-8 Commands That Configure GLBP on Switch C2

```
interface vlan2
   ip address 192.168.2.4 255.255.255.0
   no shutdown
   glbp 1 ip 192.168.2.1
   glbp 1 priority 100
   glbp 1 authentication md5 key-string b1gs3cr3t
   glbp 1 timers msec 500 msec 1500
   glbp 1 load-balancing round-robin
exit
```

Step 7: Monitoring GLBP Operation

In this step, you can monitor GLBP operation by using the **show glbp brief** and the **show glbp** commands.

Lab 14

Private VLANs

This LAN Switching Video Mentor lab covers Private VLANs and how you can leverage them to isolate hosts within Layer 2 VLANs and IP broadcast domains.

The objectives of this lab are as follows:

- Configure a primary VLAN.
- Configure secondary VLANs.
- Configure switch port modes.

Scenario

This lab contains five main steps, as follows:

Step 1. Configure secondary VLANs.

Step 2. Configure the primary VLAN.

Step 3. Define the host ports and their private VLAN associations.

Step 4. Define promiscuous ports and their private VLAN mapping.

Step 5. Test the private VLAN operation.

Initial Configurations

This lab uses only a single switch. The relevant initial configuration commands already in place on switch A1 are shown in Example 14-1.

Example 14-1 Initial Configuration Commands for Switch A1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/0/49
   description to switch C1
   switchport
```

Example 14-1 Initial Configuration Commands for Switch A1 continued

```
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
   no shutdown
interface range gigabitethernet1/0/1 - 16
   switchport
   switchport access vlan 2
   switchport mode access
   spanning-tree portfast
   no shutdown
```

Video Presentation Reference

The network topology used in this lab is shown in Figure 14-1. The following sections show the commands entered in each of the lab steps.

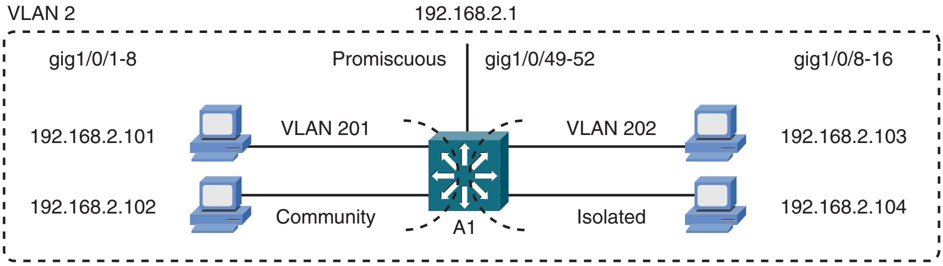

Figure 14-1 Lab 14 Network Topology

Step 1: Configuring Secondary VLANs

In this step, secondary VLANs 201 and 202 are configured using the commands shown in Example 14-2. The VLANs are defined as community and isolated, respectively.

Example 14-2 Commands That Define Secondary VLANs on Switch A1

```
vlan201
   name pvlan_201
   private-vlan community
   exit
vlan 202
   name pvlan_202
   private-vlan isolated
   exit
```

Step 2: Configuring the Primary VLAN

In this step, VLAN 2 is identified as the primary VLAN and is associated with secondary VLANs 201 and 202. The configuration commands shown in Example 14-3 are entered on switch A1.

Example 14-3 Commands That Configure the Primary VLAN on Switch A1

```
vlan 2
   private-vlan primary
   private-vlan association 201,202
   exit
```

Step 3: Defining the Host Ports and Their Private VLAN Associations

In this step, interfaces GigabitEthernet1/0/1 through 1/0/8 are configured as private VLAN host ports associated with primary VLAN 2 and secondary VLAN 201. Interfaces GigabitEthernet1/0/9 through 1/0/16 are also configured as private VLAN host ports, but they are associated with primary VLAN 2 and secondary VLAN 202. The configuration commands shown in Example 14-4 are entered on switch A1.

Example 14-4 Commands That Configure Host Ports on Switch A1

```
interface range gigabitethernet1/0/1 - 8
   switchport mode private-vlan host
   switchport private-vlan host-association 2 201
   exit
interface range gigabitethernet1/0/9 - 16
   switchport mode private-vlan host
   switchport private-vlan host-association 2 202
   exit
```

Step 4: Defining Promiscuous Ports and Their Private VLAN Mapping

In this step, interfaces GigabitEthernet1/0/49 through 1/0/52 are configured as promiscuous ports mapped between primary VLAN 2 and secondary VLANs 201 and 202. The configuration commands shown in Example 14-5 are entered on switch A1.

Example 14-5 Commands That Define Promiscuous Ports on Switch A1

```
interface gigabitethernet1/0/49 - 52
   switchport mode private-vlan promiscuous
   switchport private-vlan mapping 2 201,202
   exit
```

Step 5: Testing the Private VLAN Operation

In this step, private VLAN operation is tested through the use of the **ping** command. The router at 192.168.2.1 is on a promiscuous port and can ping any of the PC hosts.

PCs associated with community secondary VLAN 201 can ping each other and the router but not hosts in any other secondary VLAN.

Finally, PCs associated with isolated secondary VLAN 202 cannot ping each other or hosts in any other secondary VLAN. However, they can ping the router.

Lab 15

Using ACLs to Control Traffic

This LAN Switching Video Mentor lab covers access lists and how they can be leveraged to control or filter packets at various locations within a switch.

The objectives of this lab are as follows:

- Configure a Router ACL (RACL).
- Configure a Port ACL (PACL).
- Configure a VLAN ACL (VACL).

Scenario

This lab contains four main steps, as follows:

Step 1. Configure an outbound RACL for a Layer 3 interface.

Step 2. Configure an inbound RACL for a Layer 3 interface.

Step 3. Configure a PACL for a Layer 2 interface.

Step 4. Configure a VACL to filter within a VLAN.

Initial Configurations

This lab uses only a single switch. The relevant initial configuration commands already in place on switch A1 are shown in Example 15-1.

Example 15-1 Initial Configuration Commands for Switch A1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface vlan2
   ip address 192.168.2.1 255.255.255.0
   no shutdown
interface vlan3
   ip address 192.168.3.1 255.255.255.0
```

Example 15-1 Initial Configuration Commands for Switch A1 continued

```
   no shutdown
interface gigabitethernet1/0/49
   description to switch C1
   no switchport
   ip address 192.168.1.1 255.255.255.252
   no shutdown
interface range gigabitethernet1/0/1 - 24
   switchport
   switchport access vlan 2
   switchport mode access
   spanning-tree portfast
   no shutdown
interface range gigabitethernet1/0/25 - 48
   switchport
   switchport access vlan 3
   switchport mode access
   spanning-tree portfast
   no shutdown
```

Video Presentation Reference

The network topology used in this lab is shown in Figure 15-1. The following sections show the commands entered in each of the lab steps.

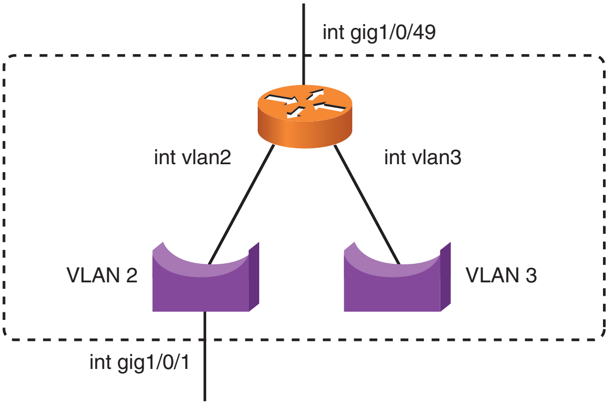

Figure 15-1 Lab 15 Network Topology

Step 1: Configuring an Outbound RACL for a Layer 3 Interface

In this step, a **border-out** extended IP access list is configured, permitting IP traffic sourced by any host in the 192.168.2.0 and 192.168.3.0 subnets, destined for any address. The access list is applied to the GigabitEthernet1/0/49 interface in the outbound direction. The commands shown in Example 15-2 are entered.

Example 15-2 Commands That Define an Outbound RACL on Interface Gig1/0/49

```
ip access-list extended border-out
   permit ip 192.168.2.0 0.0.0.255 any
   permit ip 192.168.3.0 0.0.0.255 any
exit
interface gigabitethernet1/0/49
   ip access-group border-out out
exit
```

Step 2: Configuring an Inbound RACL for a Layer 3 Interface

In this step, a border-in extended IP access list is defined to deny Telnet packets (TCP port 23) between any hosts to deny any IP packets destined for the host at 192.168.2.14 and permit all other IP traffic to any host. The configuration commands shown in Example 15-3 are entered on switch A1.

Example 15-3 Commands That Define an Inbound RACL on Interface Gig1/0/49

```
ip access-list extended border-in
   deny tcp any any eq telnet
   deny ip any host 192.168.2.14
   permit ip any any
exit
interface gigabitethernet1/0/49
   ip access-group border-in in
exit
```

Step 3: Configuring a PACL for a Layer 2 Interface

In this step, an extended IP access list is defined to permit any IP traffic coming from host 192.168.2.100 but nothing else. The access list is applied as a PACL in the inbound direction on interface gigabitethernet1/0/1, which is already in Layer 2-only mode, using the configuration commands shown in Example 15-4.

Example 15-4 Commands That Define a PACL on Interface Gig1/0/1

```
ip access-list extended pacl1
   permit ip host 192.168.2.100 any
exit
interface gigabitethernet1/0/1
   ip access-group pacl1 in
exit
```

Step 4: Configuring a VACL to Filter Within a VLAN

In this step, a VACL is configured to drop any FTP or Telnet packets within VLAN 2, regardless of the traffic direction. Extended IP access list **vacl1-acl** is defined to match the FTP and Telnet traffic, whereas VLAN access map **vacl1** is defined to take action on the matched traffic. The configuration commands shown in Example 15-5 are entered on switch A1.

Example 15-5 Commands That Define a VACL on VLAN 2

```
ip access-list extended vacl1-acl
   permit tcp any any eq ftp
   permit tcp any any eq telnet
exit
vlan access-map vacl1 10
   match ip address vacl1-acl
   action drop
   exit
vlan access-map vacl1 20
   action forward
   exit
vlan filter vacl1 vlan-list 2
```

Lab 16

Using Port Security

This LAN Switching Video Mentor lab covers the port security feature and how it can be leveraged to control host access on switch interfaces.

The objectives of this lab are as follows:

- Configure port security violation modes.
- Limit dynamically learned addresses on switch interfaces.
- Configure static secure addresses on switch interfaces.

Scenario

This lab contains four main steps, as follows:

Step 1. Enable port security.

Step 2. Set the violation mode.

Step 3. Limit the number of secure MAC addresses.

Step 4. Tune secure address aging.

Initial Configurations

This lab uses only a single switch. The relevant initial configuration commands already in place on switch A1 are shown in Example 16-1.

Example 16-1 Initial Configuration Commands for Switch A1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface range gigabitethernet1/0/1 - 24
   switchport
   switchport access vlan 2
   switchport mode access
   spanning-tree portfast
```

Example 16-1 Initial Configuration Commands for Switch A1 continued

```
   no shutdown
interface range gigabitethernet1/0/25 - 48
   switchport
   switchport access vlan 3
   switchport mode access
   spanning-tree portfast
   no shutdown
```

Video Presentation Reference

In the following sections, the entered commands in each of the lab steps are shown.

Step 1: Enabling Port Security

In this step, you can enable port security on switch interface gigabitethernet1/0/1 by entering the commands shown in Example 16-2. The interface must be in the Layer 2-only mode before Port Security can be enabled.

Example 16-2 Commands That Enable Port Security on an Interface

```
interface gigabitethernet1/0/1
   switchport
   switchport port-security
```

Step 2: Setting the Violation Mode

When port security detects a violation on a switch interface, it must take some action. In this step, the **restrict** violation mode is set using the interface configuration command shown in Example 16-3.

Example 16-3 Command That Sets the Port Security Violation Mode

```
switchport port-security violation restrict
```

Step 3: Limiting the Number of Secure MAC Addresses

In this step, the number of secure MAC addresses that can be learned on the interface is set to a maximum of two. In addition, all addresses learned on the interface will be made sticky so that they will be remembered. The interface configuration commands shown in Example 16-4 are entered.

Example 16-4 Commands That Set the Secure Address Limit to Two Sticky MAC Addresses

```
switchport port-security maximum 2
switchport port-security mac-address sticky
```

Step 4: Tuning Secure Address Aging

In this step, port security is tuned so that dynamically learned addresses age out after an inactivity time of two hours. The configuration commands shown in Example 16-5 are entered on switch A1.

Example 16-5 Commands That Tune Secure Address Aging

```
switchport port-security aging type inactivity
switchport port-security aging time 120
```

Lab 17

Preventing Spoofing Attacks

This LAN Switching Video Mentor lab covers switch features that can be leveraged to prevent several different types of spoofing attacks.

The objectives of this lab are as follows:

- Configure DHCP snooping.
- Configure IP Source Guard.
- Configure Dynamic ARP Inspection (DAI).

Scenario

This lab contains three main steps, as follows:

Step 1. Configure DHCP snooping.

Step 2. Configure IP Source Guard.

Step 3. Configure Dynamic ARP Inspection.

Initial Configurations

This lab uses only a single switch. The relevant initial configuration commands already in place on switch A1 are shown in Example 17-1.

Example 17-1 Initial Configuration Commands for Switch A1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface range gigabitethernet1/0/49 - 52
   description to switch C1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
   no shutdown
```

Example 17-1 Initial Configuration Commands for Switch A1 continued

```
interface range gigabitethernet1/0/1 - 48
   switchport
   switchport access vlan 2
   switchport mode access
   spanning-tree portfast
   no shutdown
```

Video Presentation Reference

The network topology used in this lab is shown in Figure 17-1. The following sections show the commands entered in each of the lab steps.

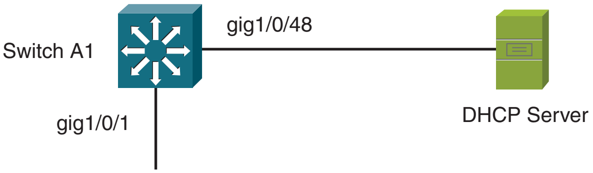

Figure 17-1 Lab 17 Network Topology

Step 1: Configuring DHCP Snooping

In this step, DHCP snooping is enabled on VLAN 2. MAC addresses will be verified to make sure hosts sending DHCP requests are sending consistent MAC addresses in the request packet and in the packet source address. A known, trusted DHCP server can be found on switch interface gigabitethernet1/0/48. All other access switch interfaces are considered to be untrusted. The commands shown in Example 17-2 are entered.

Example 17-2 Commands That Configure DHCP Snooping on Switch A1

```
ip dhcp snooping
ip dhcp snooping vlan 2
ip dhcp snooping verify mac-address
interface gigabitethernet1/0/48
   ip dhcp snooping trust
   exit
interface range gigabitethernet1/0/1 - 47 , gigabitethernet1/0/49 - 52
   no ip dhcp snooping trust
   exit
ip dhcp snooping database flash:/snooping-db
```

Step 2: Configuring IP Source Guard

In this step, the IP Source Guard feature is configured to prevent malicious hosts from spoofing the IP addresses of other hosts. IP Source Guard is enabled on switch interfaces gigabitethernet 1/0/1 through 47. In addition, a static IP source binding is configured for a host on gigabitethernet1/0/16, which uses 192.168.2.198 and 0015.c557.f9bd. The configuration commands shown in Example 17-3 are entered on switch A1.

Example 17-3 Commands That Configure IP Source Guard on Switch A1

```
interface range gigabitethernet1/0/1 - 47
   ip verify source
exit
ip source binding 0015.c557.f9bd vlan 2 192.168.2.198 interface gig1/0/16
```

Step 3: Configuring Dynamic ARP Inspection

In this step, Dynamic ARP Inspection is enabled on VLAN 2 on switch A1. All interfaces connecting to single hosts will be untrusted, whereas uplinks to other switches will be trusted. A static entry is also configured in ARP access list **dai-vlan2** so that the host using 192.168.2.198 will be associated with MAC address 0015.c557.f9bd. The configuration commands shown in Example 17-4 are entered.

Example 17-4 Commands That Configure Dynamic ARP Inspection on Switch A1

```
ip arp inspection vlan 2
interface range gigabitethernet1/0/1 - 48
   no ip arp inspection trust
  exit
interface range gigabitethernet1/0/49 - 52
   ip arp inspection trust
   exit
!
arp access-list dai-vlan2
   permit ip host 192.168.2.198 mac host 0015.c557.f9bd
   exit
ip arp inspection filter dai-vlan2 vlan 2
```

Lab 18

QoS, Part 1

This LAN Switching Video Mentor lab covers a series of switch features that work together to offer quality of service (QoS).

The objectives of this lab are as follows:

- Understand an overview of QoS.
- Configure a trust boundary.
- Classify traffic.
- Police traffic.
- Mark traffic.

Scenario

This lab contains seven main steps, as follows:

Step 1. Enable QoS.

Step 2. Set a trust boundary.

Step 3. Classify traffic.

Step 4. Police traffic.

Step 5. Mark traffic.

Step 6. Apply the policy to an interface.

Step 7. Simplify with AutoQoS.

Initial Configurations

This lab uses only a single switch. The relevant initial configuration commands already in place on switch A1 are shown in Example 18-1.

Example 18-1 Initial Configuration Commands for Switch A1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
vtp mode transparent
vlan 2
   name Engineering
vlan 3
```

Example 18-1 Initial Configuration Commands for Switch A1 continued

```
   name Accounting
vlan 10
   name voice
interface range gigabitethernet1/0/49 - 52
   description Uplinks to Core
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
   no shutdown
interface range gigabitethernet1/0/1 - 48
   switchport
   switchport access vlan 2
   switchport voice vlan 10
   switchport mode access
   spanning-tree portfast
   no shutdown
```

Video Presentation Reference

The network topology used in this lab is shown in Figure 18-1. The following sections show the commands entered in each of the lab steps.

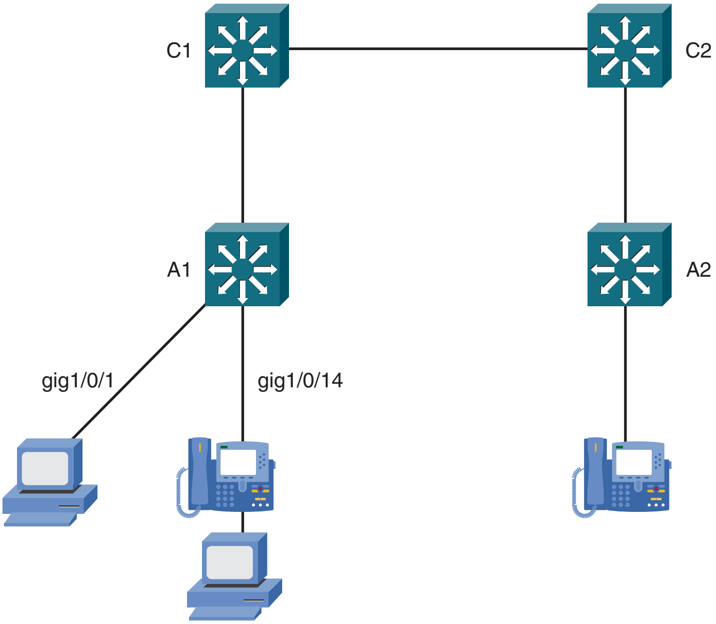

Figure 18-1 Lab 18 Network Topology

Step 1: Enabling QoS

By default, QoS is disabled on a Catalyst switch. In this step, QoS is enabled globally by entering the command shown in Example 18-2.

Example 18-2 Commands Used to Enable QoS on Switch A1

```
mls qos
```

The current QoS status is displayed with the **show mls qos** command.

Step 2: Setting a Trust Boundary

In this step, QoS trust is established on switch interfaces that form a boundary around the network. All access mode interfaces on switch A1 are configured to not trust inbound QoS information and to reset the inbound CoS value to zero. Switch A1's uplinks are configured to trust inbound DSCP values because those interfaces face the trusted, inner portion of the network.

The configuration commands shown in Example 18-3 are entered on switch A1.

Example 18-3 Commands That Configure a QoS Trust Boundary on Switch A1

```
interface range gigabitethernet1/0/1 - 48
   no mls qos trust
   mls qos cos 0
exit
interface range gigabitethernet1/0/49 - 52
   mls qos trust dscp
exit
```

With the commands shown in Example 18-4, QoS trust is extended to the Cisco IP Phone and its attached PC that connects to interface GigabitEthernet1/0/6.

Example 18-4 Commands That Extend QoS Trust to Cisco IP Phones on Switch A1

```
interface gigabitethernet1/0/6
   switchport priority extend trust
```

Step 3: Classifying Traffic

In this step, access lists and class maps are configured to match traffic as part of the following QoS policies:

- Match SIP Control (TCP ports 5060 and 5061)
- Match SIP voice bearer (UDP ports 1024 through 65535)
- Match FTP (TCP port 21 and 20)

The configuration commands shown in Example 18-5 are entered. The class maps are referenced in the QoS policies in Steps 4 and 5.

Example 18-5 Commands That Classify Traffic on Switch A1

```
ip access-list extended sip-control
   permit tcp any any range 5060 5061
exit
class-map class-sip-control
   match access-group name sip-control
exit
!
ip access-list extended sip-bearer
   permit udp any any range 1024 65535
exit
class-map class-sip-bearer
   match access-group name sip-bearer
exit
!
ip access-list extended ftp
   permit tcp any any eq ftp
   permit tcp any any eq ftp-data
exit
class-map class-ftp
   match access-group name ftp
exit
```

Step 4: Policing Traffic

This step defines a **my-qos** policy map that contains the QoS policies as a sequence of class maps and actions. A policer is configured as an action to be taken on traffic classified as FTP. The policer limits the traffic bandwidth to 10 Mbps, with a normal burst of 10,000 bytes. Any traffic that exceeds the rate and burst will be dropped. The configuration commands shown in Example 18-6 are entered.

Example 18-6 Commands That Police FTP Traffic on Switch A1

```
policy-map my-qos
   class class-ftp
      police 10000000 10000 exceed-action drop
   exit
```

Step 5: Marking Traffic

In this step, the SIP control traffic classified by class map class-sip-control will be marked with DSCP AF31. SIP voice bearer packets classified with the class-sip-bearer class map will be marked with DSCP EF. The configuration commands shown in Example 18-7 are entered as a continuation of the **my-qos** policy map.

Example 18-7 Commands That Mark Traffic on Switch A1

```
   class class-sip-control
      set dscp af31
   exit
   class class-sip-bearer
      set dscp ef
   exit
exit
```

Step 6: Applying the Policy to an Interface

In this step, the **my-qos** policy map is applied as a service policy on interface GigabitEthernet1/0/1 in the input direction. The configuration commands shown in Example 18-8 are entered.

Example 18-8 Commands That Apply a Policy Map on Switch A1

```
interface gigabitethernet1/0/1
   service-policy input my-qos
exit
```

Step 7: Simplifying with AutoQoS

In this step, AutoQoS sets QoS policies on interface GigabitEthernet1/0/8 for a Cisco IP Phone and on interface GigabitEthernet1/0/14 for a PC running the Cisco IP Communicator application. The configuration commands shown in Example 18-9 are entered.

Example 18-9 Commands That Configure AutoQoS on Switch A1

```
interface gigabitethernet1/0/8
   auto qos voip cisco-phone
exit

interface gigabitethernet1/0/14
   auto qos voip cisco-softphone
exit
```

Lab 19

QoS, Part 2

This LAN Switching Video Mentor lab covers interface queuing, rounding out the series of quality of service features and mechanisms. Most of the lab is devoted to displaying and verifying queuing configuration and operation as an aid to understanding how QoS works within a switch.

The objectives of this lab are as follows:

- Identify the interface queue structure.
- Verify queue scheduling.
- Verify congestion avoidance.
- Verify the mapping of packets into queues.
- Verify the priority queue status.

Scenario

This lab contains five main steps, as follows:

Step 1. Display the interface queue structure.

Step 2. Verify the interface queue scheduling configuration.

Step 3. Verify the congestion avoidance configuration.

Step 4. Verify the queue mapping configuration.

Step 5. Enable the priority queues.

Initial Configurations

This lab uses only a single switch: Switch C1, which is a Catalyst 6500. Because QoS configuration information is verified in the lab, only the **mls qos** command is necessary. Other commands found in the initial switch configuration are not relevant here.

Video Presentation Reference

The following sections show the commands entered in each of the lab steps.

Step 1: Displaying the Interface Queue Structure

In this step, you can see the ingress and egress queue structure by entering the command shown in Example 19-1 on switch C1.

Example 19-1 Command That Displays the Interface Queue Structure

```
show interface gigabitethernet1/1 capabilities
```

Step 2: Verifying the Interface Queue Scheduling Configuration

In this step, you can see the interface queues and their weights by entering the command shown in Example 19-2 on switch C1.

Example 19-2 Command That Displays the Interface Queue Scheduling Configuration

```
show queueing interface gigabitethernet1/1
```

Step 3: Verifying the Congestion Avoidance Configuration

In this step, the interface queue threshold configuration is verified as part of the congestion avoidance mechanism. The command shown in Example 19-3 is entered on switch C1.

Example 19-3 Command That Displays the Congestion Avoidance Threshold Configuration

```
show queueing interface gigabitethernet1/1
```

Step 4: Verifying the Queue Mapping Configuration

In this step, the DSCP-to-CoS map configuration displays. Where the CoS values map packets into ingress and egress queues, the configuration is displayed and verified. Enter the commands shown in Example 19-4.

Example 19-4 Commands That Display the Queue Mapping Configuration

```
show mls qos maps dscp-cos
show queueing interface gigabitethernet1/1
```

Step 5: Enabling the Priority Queues

Priority queues on switch platforms such as the Catalyst 6500 are always enabled and ready for use. On some other switch platforms, such as the Catalyst 3750, priority queues are available but are disabled by default.

In this step, the priority queue status on Switch A1 interface GigabitEthernet1/0/1 is verified with the command shown in Example 19-5. The priority queue is enabled by entering the interface configuration command shown in Example 19-6 on switch A1.

Example 19-5 Command That Displays the Priority Queue Status

```
show mls qos interface gigabitethernet1/0/1 queueing
```

Example 19-6 Command That Enables the Priority Queue

```
interface gigabitethernet1/0/1
   priority-queue out
```

Lab 20

Monitoring Traffic

This LAN Switching Video Mentor lab covers several features that allow traffic from a source to be mirrored or copied to a destination so that the traffic can be monitored or analyzed. The Switched Port Analyzer (SPAN) features make this possible.

The objectives of this lab are as follows:

- Configure and use a Local SPAN session.
- Configure and use a Remote SPAN (RSPAN) session.
- Configure and use an Encapsulated RSPAN (ERSPAN) session.
- Configure and use the Mini Protocol Analyzer.

Scenario

This lab contains four main steps, as follows:

Step 1. Configure a Local SPAN session.

Step 2. Configure an RSPAN session.

Step 3. Configure an ERSPAN session.

Step 4. Configure the Mini Protocol Analyzer.

Initial Configurations

The switches used in this lab are A1 (a Catalyst 3750) and C1 and C2 (both Catalyst 6500s). The relevant commands from their initial configurations are shown in Examples 20-1 through 20-3, respectively.

Example 20-1 Initial Configuration Commands for Switch A1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
vtp mode transparent
vlan 2
   name Engineering
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/0/1
   switchport
```

Example 20-1 Initial Configuration Commands for Switch A1 continued

```
   switchport access vlan 2
   switchport mode access
   spanning-tree portfast
interface gigabitethernet1/0/48
   switchport
   switchport access vlan 2
   switchport mode access
   spanning-tree portfast
interface gigabitethernet1/0/49
   description to switch C1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,3,10
   switchport mode trunk
interface gigabitethernet1/0/50
interface gigabitethernet1/0/51
interface gigabitethernet1/0/52
```

Example 20-2 Initial Configuration Commands for Switch C1

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
spanning-tree vlan 2,10 priority 0
vtp mode transparent
vlan 2
   name Engineering
vlan 10
   name voice
interface gigabitethernet1/1
   description to switch A1
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 2,10
   switchport mode trunk
interface gigabitethernet1/3
   description to switch C2
   no switchport
   ip address 192.168.100.1 255.255.255.252
interface vlan2
   ip address 192.168.2.1 255.255.255.0
router eigrp 1
   network 192.168.2.0
   network 192.168.100.0 0.0.0.3
   passive-interface vlan2
```

Example 20-3 Initial Configuration Commands for Switch C2

```
spanning-tree extend system-id
spanning-tree mode rapid-pvst
vtp mode transparent
vlan 3
   name Accounting
vlan 10
   name voice
interface gigabitethernet1/3
   description to switch C1
   no switchport
   ip address 192.168.100.2 255.255.255.252
interface vlan3
   ip address 192.168.3.1 255.255.255.0
router eigrp 1
   network 192.168.3.0
   network 192.168.100.0 0.0.0.3
   passive-interface vlan3
```

Video Presentation Reference

The following sections show the commands entered in each of the lab steps. A network diagram is also provided for each of Steps 1 through 3. Be aware that the network topology used in this video lab is somewhat different than previous labs.

Step 1: Configuring a Local SPAN Session

In this step, a Local SPAN session monitors traffic on switch A1's source interface GigabitEthernet1/0/1. The monitored traffic is sent to destination interface GigabitEthernet1/0/48, also on switch A1. Figure 20-1 shows the network topology used in this step.

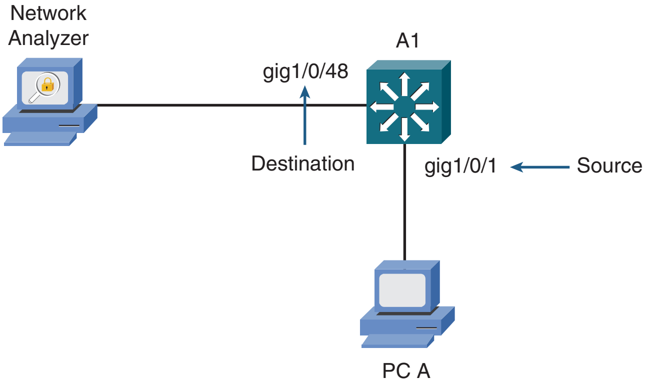

Figure 20-1 Lab 20 Network Topology for Step 1: Local SPAN

To configure the Local SPAN session, the commands shown in Example 20-4 are entered on switch A1.

Example 20-4 Commands That Configure Local SPAN on Switch A1

```
monitor session 1 source interface gigabitethernet1/0/1 both
monitor session 1 destination interface gigabitethernet1/0/48
```

When the Local SPAN session is no longer needed, you can remove it from the running configuration with the **no monitor session 1** command.

Step 2: Configuring a Remote SPAN Session

In this step, a Remote SPAN (RSPAN) session monitors traffic on switch A1's source interface GigabitEthernet1/0/1. The monitored traffic is sent over RSPAN VLAN 99 to destination interface GigabitEthernet2/8 on switch C1. Figure 20-2 shows the network topology used in this step.

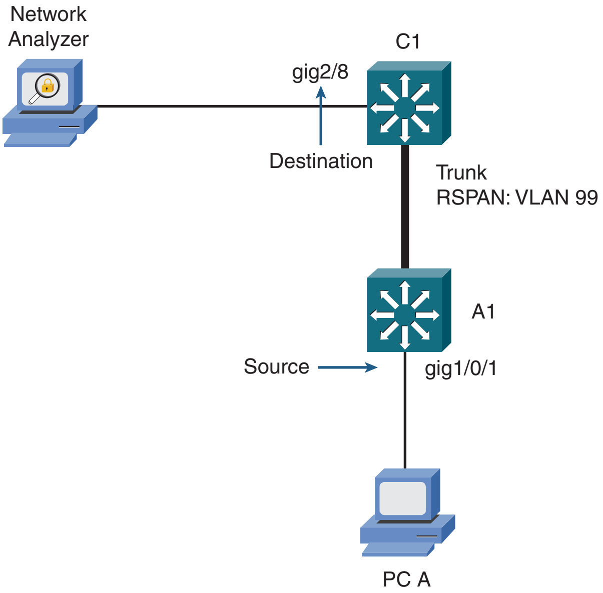

Figure 20-2 Lab 20 Network Topology for Step 2: RSPAN

To configure the RSPAN session, the commands shown in Examples 20-5 and 20-6 are entered on switches A1 and C1, respectively. Because switch A1 is a Catalyst 3750, RSPAN is configured using the global configuration mode.

Example 20-5 Commands That Configure RSPAN on Switch A1

```
vlan 99
   remote-span
   exit
interface gigabitethernet1/0/49
   switchport trunk allowed vlan add 99
   exit
monitor session 1 source interface gigabitethernet1/0/1 both
monitor session 1 destination remote vlan 99
```

Switch C1 is a Catalyst 6500, so RSPAN is configured using the SPAN configuration mode.

Example 20-6 Commands That Configure RSPAN on Switch C1

```
vlan 99
   remote-span
   exit
interface gigabitethernet1/1
   switchport trunk allowed vlan add 99
   exit
monitor session 1 type rspan-destination
   source remote vlan 99
   destination interface gigabitethernet2/8
```

When the RSPAN session is no longer needed, it is removed from the running configuration on A1 and C1 with the **no monitor session 1** command.

Step 3: Configuring an Encapsulated RSPAN Session

In this step, an Encapsulated Remote SPAN (ERSPAN) session monitors traffic on switch C1's source interface GigabitEthernet1/1. The monitored traffic is sent across an IP network to destination switch C2 and then to the network analyzer connected to interface GigabitEthernet2/8 on switch C2. Figure 20-3 shows the network topology used in this step.

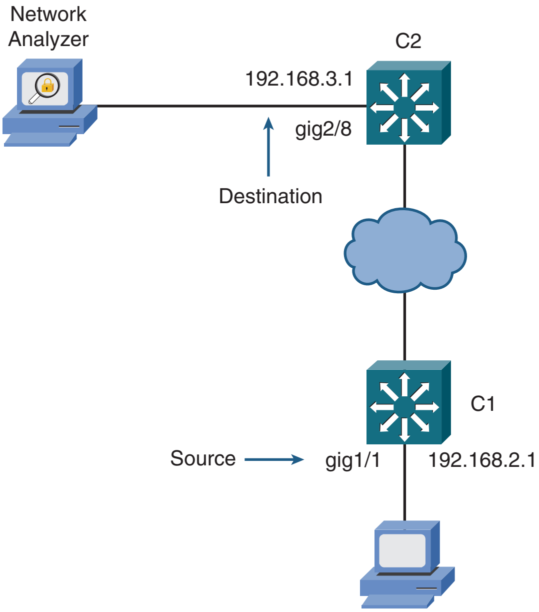

Figure 20-3 Lab 20 Network Topology for Step 3: ERSPAN

To configure the ERSPAN session, the commands shown in Examples 20-7 and 20-8 are entered on switches C1 and C2, respectively. The ERSPAN source interface is GigabitEthernet1/1 on switch C1. Because that interface is a trunk, a VLAN filter monitors only VLAN 2 within the trunk.

The ERSPAN destination is switch C2 at IP address 192.168.3.1. Switch C1 uses its own IP address 192.168.2.1 as the ERSPAN origination address.

Example 20-7 Commands That Configure ERSPAN on Switch C1

```
monitor session 1 type erspan-source
   source interface gigabitethernet1/1 both
      filter vlan 2
      exit
   destination
      ip address 192.168.3.1
      erspan-id 1
      origin ip address 192.168.2.1
      exit
   no shutdown
```

On switch C2, the ERSPAN source is an IP address on C2 (192.168.3.1), where monitored traffic can be accepted from the ERSPAN GRE tunnel. The ERSPAN destination is interface GigabitEthernet 2/8 on switch C2.

Example 20-8 Commands That Configure ERSPAN on Switch C2

```
monitor session 1 type erspan-destination
   source
      ip address 192.168.3.1
      erspan-id 1
      exit
   destination interface gigabitethernet2/8
      exit
   no shutdown
```

After the ERSPAN session is no longer needed, it is removed from the running configuration on C1 and C2 with the **no monitor session 1** command.

Step 4: Configuring the Mini Protocol Analyzer

In this step, the Mini Protocol Analyzer feature is used on switch C1 (a Catalyst 6500) in the place of an external network analyzer.

The commands shown in Example 20-9 are entered in switch C1. Traffic is monitored on interface GigabitEthernet1/1 and sent to switch C1's internal capture buffer.

Example 20-9 Commands That Configure the Mini Protocol Analyzer on Switch C1

```
monitor session 1 type capture
   source interface gigabitethernet1/1 both
   exit
ip access-list extended capture1
   permit ip host 192.168.2.10 any
   permit ip any host 192.168.2.10
   exit
monitor session 1 type capture
   filter access-group capture1
   exit
exit
```

The **monitor capture start** command starts the capture. During the capture, you can use the **show monitor capture status** and **show monitor capture buffer** commands to see how many packets have been captured and their source and destination addresses.

Use the **show monitor capture buffer detail** command to display more information found within the IP header portion of the captured packets.

Finally, a **test1** access list is configured and used as a display filter so that only captured packets involving TCP port 23 are shown. The configuration commands listed in Example 20-10 configures the display filter.

Example 20-10 Commands That Configure a Display Filter for the Mini Protocol Analyzer

```
ip access-list extended test1
   permit tcp any any eq 23
   permit tcp any eq 23 any
   exit
exit
show monitor capture buffer detail acl test1
```