CCNAv7: Switching, Routing, and Wireless Essentials

Companion Guide

Networking Academy

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Switching, Routing, and Wireless Essentials Companion Guide (CCNAv7)

Cisco Press
Hoboken, New Jersey

Switching, Routing, and Wireless Essentials Companion Guide (CCNAv7)

Published by:
Cisco Press
Hoboken, New Jersey

ScoutAutomatedPrintCode

Library of Congress Control Number: 2020936826

ISBN-13: 978-0-13-672935-8
ISBN-10: 0-13-672935-5

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy Switching, Routing, and Wireless Essentials course. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

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

For more information on the Cisco Networking Academy or to locate a Networking Academy, Please visit www.netacad.com

Editor-in-Chief
Mark Taub

Alliances Manager, Cisco Press
Arezou Gol

Director, ITP Product Management
Brett Bartow

Senior Editor
James Manly

Managing Editor
Sandra Schroeder

Development Editor
Marianne Bartow

Senior Project Editor
Tonya Simpson

Copy Editor
Barbara Hacha

Technical Editor
Rick Graziani

Editorial Assistant
Cindy Teeters

Cover Designer
Chuti Prasertsith

Composition
codeMantra

Indexer
Cheryl Ann Lenser

Proofreader
Abigail Manheim

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.

Feedback Information

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

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

We greatly appreciate your assistance.

Americas Headquarters
Cisco Systems, Inc.
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 Contributing Authors

Bob Vachon is a professor at Cambrian College (Sudbury, Ontario, Canada) and Algonquin College (Ottawa, Ontario, Canada). He has more than 30 years of teaching experience in computer networking and information technology. He has also collaborated on many Cisco Networking Academy courses, including CCNA, CCNA Security, CCNP, and Cybersecurity as team lead, lead author, and subject matter expert. Bob enjoys family, friends, and being outdoors playing guitar by a campfire.

Allan Johnson entered the academic world in 1999 after 10 years as a business owner/operator to dedicate his efforts to his passion for teaching. He holds both an MBA and an M.Ed. in training and development. He taught CCNA courses at the high school level for seven years and has taught both CCNA and CCNP courses at Del Mar College in Corpus Christi, Texas. In 2003, Allan began to commit much of his time and energy to the CCNA Instructional Support Team providing services to Networking Academy instructors worldwide and creating training materials. He now works full time for Cisco Networking Academy as Curriculum Lead.

Contents at a Glance

Reader Services

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

Switching, Routing, and Wireless Essentials Companion Guide (CCNAv7) is the official supplemental textbook for the Cisco Network Academy CCNA Switching, Routing, and Wireless Essentials version 7 course. Cisco Networking Academy is a comprehensive program that delivers information technology skills to students around the world. The curriculum emphasizes real-world practical application while providing opportunities for you to gain the skills and hands-on experience needed to design, install, operate, and maintain networks in small- to medium-sized businesses as well as enterprise and service provider environments.

As a textbook, this book provides a ready reference to explain the same networking concepts, technologies, protocols, and devices as the online curriculum. This book emphasizes key topics, terms, and activities and provides some alternate explanations and examples compared with the course. You can use the online curriculum as directed by your instructor and then use this Companion Guide's study tools to help solidify your understanding of all the topics.

Who Should Read This Book

The book, as well as the course, is designed as an introduction to data network technology for those pursuing careers as network professionals as well as those who need only an introduction to network technology for professional growth. Topics are presented concisely, starting with the most fundamental concepts and progressing to a comprehensive understanding of network communication. The content of this text provides the foundation for additional Cisco Networking Academy courses and preparation for the CCNA certification.

Book Features

The educational features of this book focus on supporting topic coverage, readability, and practice of the course material to facilitate your full understanding of the course material.

Topic Coverage

The following features give you a thorough overview of the topics covered in each chapter so that you can make constructive use of your study time:

- **Objectives:** Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives stated in the corresponding chapters of the online curriculum; however, the question

format in the Companion Guide encourages you to think about finding the answers as you read the chapter.

- **Notes:** These are short sidebars that point out interesting facts, timesaving methods, and important safety issues.
- **Chapter summaries:** At the end of each chapter is a summary of the chapter's key concepts. It provides a synopsis of the chapter and serves as a study aid.
- **Practice:** At the end of each chapter is a full list of all the labs, class activities, and Packet Tracer activities to refer back to for study time.

Readability

The following features assist your understanding of the networking vocabulary:

- **Key terms:** Each chapter begins with a list of key terms, along with a page-number reference from inside the chapter. The terms are listed in the order in which they are explained in the chapter. This handy reference allows you to find a term, flip to the page where the term appears, and see the term used in context. The Glossary defines all the key terms.
- **Glossary:** This book contains an all-new Glossary with more than 300 terms.

Practice

Practice makes perfect. This Companion Guide offers you ample opportunities to put what you learn into practice. You will find the following features valuable and effective in reinforcing the instruction that you receive:

- **Check Your Understanding questions and answer key:** Review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions that you see in the online course. Appendix A, "Answers to the 'Check Your Understanding' Questions," provides an answer key to all the questions and includes an explanation of each answer.

Interactive Graphic

Video

- **Labs and activities:** Throughout each chapter, you will be directed back to the online course to take advantage of the activities created to reinforce concepts. In addition, at the end of each chapter is a practice section that collects a list of all the labs and activities to provide practice with the topics introduced in the chapter.
- **Page references to online course:** After headings, you will see, for example, (1.1.2). This number refers to the page number in the online course so that you can easily jump to that spot online to view a video, practice an activity, perform a lab, or review a topic.

About Packet Tracer Software and Activities

Interspersed throughout the chapters you'll find a few Cisco Packet Tracer activities. Packet Tracer allows you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available in the course. Packet Tracer software is available only through the Cisco Networking Academy website. Ask your instructor for access to Packet Tracer.

How This Book Is Organized

This book corresponds closely to the Cisco Networking Academy Switching, Routing, and Wireless Essentials course and is divided into 16 chapters, one appendix, and a glossary of key terms:

- **Chapter 1, "Basic Device Configuration":** This chapter explains how to configure devices using security best practices. Included are initial switch and router configuration, switch port configuration, remote access configuration, and how to verify connectivity between two networks.
- **Chapter 2, "Switching Concepts":** This chapter explains how switches forward data. Included are frame forwarding methods and collision and broadcast domain comparison.
- **Chapter 3, "VLANs":** This chapter explains how to implement VLANs and trunking in a switched network. Included are explanations of the purpose of VLANs, how VLANs forward frames in a multiswitched environment, VLAN port assignments, trunk configuration, and DTP configuration.
- **Chapter 4, "Inter-VLAN Routing":** This chapter explains how to implement inter-VLAN routing. Included are descriptions of inter-VLAN routing options, router-on-a-stick configuration, Layer 3 switch inter-VLAN routing, and troubleshooting common inter-VLAN routing configuration issues.
- **Chapter 5, "STP Concepts":** This chapter explains how STP enables redundancy in a Layer 3 network. Included are explanations of common problems in redundant Layer 2 networks, STP operation, and Rapid PVST+ operation.
- **Chapter 6, "EtherChannel":** This chapter explains how to implement EtherChannel on switched links. Included are descriptions of EtherChannel technology, EtherChannel configuration, and troubleshooting EtherChannel.
- **Chapter 7, "DHCPv4":** This chapter explains how to implement DHCPv4 for multiple LANs. Included is an explanation of DHCPv4 operation, as well as configuring a router as a DHCPv4 server or DHCPv4 client.

- **Chapter 8, "SLAAC and DHCPv6":** This chapter explains how to implement dynamic address allocation in an IPv6 network. Included are explanations of how an IPv6 host acquires its addressing, SLAAC operation, DHCPv6 operation, and configuring a router as a stateful or stateless DHCPv6 server.
- **Chapter 9, "FHRP Concepts":** This chapter explains how FHRPs provide default gateway services in a redundant network. Included are explanations of the purpose of FHRPs and HSRP operation.
- **Chapter 10, "LAN Security Concepts":** This chapter explains how vulnerabilities compromise LAN security. Included are explanations of how to use endpoint security, how AAA and 802.1X are used to authenticate, Layer 2 vulnerabilities, MAC address table attacks, and LAN attacks.
- **Chapter 11, "Switch Security Configuration":** This chapter explains how to configure switch security to mitigate LAN attacks. Included is port security implementation as well as mitigating VLAN, DHCP, ARP, and STP attacks.
- **Chapter 12, "WLAN Concepts":** This chapter explains how WLANs enable network connectivity for wireless devices. Included are explanations of WLAN technology, WLAN components, and WLAN operation. In addition, the chapter discusses how CAPWAP is used to manage multiple APs for a WLC. WLAN channel management is discussed. The chapter concludes with a discussion of threats to WLANs and how to secure WLANs.
- **Chapter 13, "WLAN Configuration":** This chapter explains how to implement a WLAN using a wireless router and a WLC. Included are explanations of wireless router configuration and WLC WLAN configuration for both WPA2 PSK and WPA2 Enterprise authentication. The chapter concludes with a discussion of how to troubleshoot common wireless configuration issues.
- **Chapter 14, "Routing Concepts":** This chapter explains how routers use information in packets to make forwarding decisions. Included are explanations of path determination, packet forwarding, basic router configuration, routing table structure, and static and dynamic routing concepts.
- **Chapter 15, "IP Static Routing":** This chapter explains how to implement IPv4 and IPv6 static routes. Included are static route syntax, static and default routing configuration, floating static routing configuration, and static host route configuration.
- **Chapter 16, "Troubleshoot Static and Default Routes":** This chapter explains how to troubleshoot static and default route implementations. Included are explanations of how a router processes packets when a static route is configured, and how to troubleshoot command static and default route configuration issues.

- **Appendix A, "Answers to the 'Check Your Understanding' Questions":** This appendix lists the answers to the "Check Your Understanding" review questions that are included at the end of each chapter.
- **Glossary:** The Glossary provides you with definitions for all the key terms identified in each chapter.

Figure Credits

Figure 1-6, screenshot of Telnet Session Capture © Wireshark

Figure 1-7, screenshot of SSH Session Capture © Wireshark

Figure 7-8, screenshot of Configuring a Home Router as a DHCPv4 Client © 2020 Belkin International, Inc.

Figure 8-1, screenshot of Manual Configuration of an IPv6 Windows Host © Microsoft 2020

Figure 8-2, screenshot of Automatic Configuration of an IPv6 Windows Host © Microsoft 2020

Figure 10-1, screenshot of WannaCry Ransomware © Lazarus Group

Figure 10-29, screenshot of Wireshark Capture of a CDP Frame © Wireshark

Figure 12-38, screenshot of Disabling SSID Broadcast (SSID Cloaking) on a Wireless Router © 2020 Belkin International, Inc.

Figure 12-39, screenshot of Configuring MAC Address Filtering on a Wireless Router © 2020 Belkin International, Inc.

Figure 12-41, screenshot of Selecting the Authentication Method on a Wireless Router © 2020 Belkin International, Inc.

Figure 12-42, screenshot of Setting the Encryption Method on a Wireless Router © 2020 Belkin International, Inc.

Figure 12-43, screenshot of Configuring WPA2 Enterprise Authentication on a Wireless Router © 2020 Belkin International, Inc.

Figure 13-3, screenshot of Connecting to a Wireless Router Using a Browser © 2020 Belkin International, Inc.

Figure 13-4, screenshot of Basic Network Setup - Step 1 © 2020 Belkin International, Inc.

Figure 13-5, screenshot of Basic Network Setup - Step 2 © 2020 Belkin International, Inc.

Figure 13-6, screenshot of Basic Network Setup - Step 3 © 2020 Belkin International, Inc.

Figure 13-7, screenshot of Basic Network Setup - Step 4 © 2020 Belkin International, Inc.

Figure 13-8, screenshot of Basic Network Setup - Step 6 © 2020 Belkin International, Inc.

Figure 13-9, screenshot of Basic Wireless Setup - Step 1 © 2020 Belkin International, Inc.

Figure 13-10, screenshot of Basic Wireless Setup - Step 2 © 2020 Belkin International, Inc.

Figure 13-11, screenshot of Basic Wireless Setup - Step 3 © 2020 Belkin International, Inc.

Figure 13-12, screenshot of Basic Wireless Setup - Step 4 © 2020 Belkin International, Inc.

Figure 13-13, screenshot of Basic Wireless Setup - Step 5 © 2020 Belkin International, Inc.

Figure 13-14, screenshot of Basic Wireless Setup - Step 6 © 2020 Belkin International, Inc.

Figure 13-16, screenshot of Verifying the Status of a Wireless Router © 2020 Belkin International, Inc.

Figure 13-18, screenshot of Configuring Port Forwarding on a Wireless Router © 2020 Belkin International, Inc.

CHAPTER 4

Inter-VLAN Routing

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- What are the options for configuring inter-VLAN routing?
- How do you configure router-on-a-stick inter-VLAN routing?
- How do you configure inter-VLAN routing using Layer 3 switching?
- How do you troubleshoot common inter-VLAN configuration issues?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

inter-VLAN routing *Page 98*

legacy inter-VLAN routing *Page 98*

router-on-a-stick *Page 98*

subinterfaces *Page 100*

switched virtual interface (SVI) *Page 112*

routed port *Page 112*

Introduction (4.0)

Now you know how to segment and organize your network into VLANs. Hosts can communicate with other hosts in the same VLAN, and you no longer have hosts sending out broadcast messages to every other device in your network, eating up needed bandwidth. But what if a host in one VLAN needs to communicate with a host in a different VLAN? If you are a network administrator, you know that people will want to communicate with other people outside of your network. This is where inter-VLAN routing can help you. Inter-VLAN routing uses a Layer 3 device, such as a router or a Layer 3 switch. Let's take your VLAN expertise and combine it with your network layer skills and put them to the test!

Inter-VLAN Routing Operation (4.1)

In this section, you learn about two options for configuring for inter-VLAN routing.

What Is Inter-VLAN Routing? (4.1.1)

VLANs are used to segment switched Layer 2 networks for a variety of reasons. Regardless of the reason, hosts in one VLAN cannot communicate with hosts in another VLAN unless there is a router or a Layer 3 switch to provide routing services.

Inter-VLAN routing is the process of forwarding network traffic from one VLAN to another VLAN.

There are three inter-VLAN routing options:

- *Legacy Inter-VLAN routing*: This is a legacy solution. It does not scale well.
- *Router-on-a-Stick*: This is an acceptable solution for a small- to medium-sized network.
- **Layer 3 switch using switched virtual interfaces (SVIs):** This is the most scalable solution for medium to large organizations.

Legacy Inter-VLAN Routing (4.1.2)

The first inter-VLAN routing solution relied on using a router with multiple Ethernet interfaces. Each router interface was connected to a switch port in different VLANs. The router interfaces served as the default gateways to the local hosts on the VLAN subnet.

For example, refer to the topology in Figure 4-1 where R1 has two interfaces connected to switch S1.

Note

The IPv4 addresses of PC1, PC2, and R1 all have a /24 subnet mask.

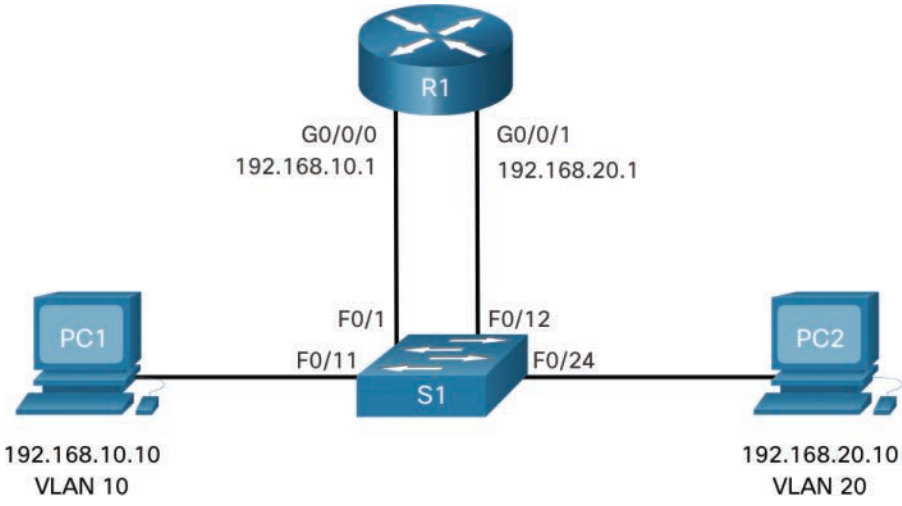

Figure 4-1 Legacy Inter-VLAN Routing Example

As shown in Table 4-1, the example MAC address table of S1 is populated as follows:

- Fa0/1 port is assigned to VLAN 10 and is connected to the R1 G0/0/0 interface.
- Fa0/11 port is assigned to VLAN 10 and is connected to PC1.
- Fa0/12 port is assigned to VLAN 20 and is connected to the R1 G0/0/1 interface.
- Fa0/11 port is assigned to VLAN 20 and is connected to PC2.

Table 4-1 MAC Address Table for S1

Port	MAC Address	VLAN
F0/1	R1 G0/0/0 MAC	10
F0/11	PC1 MAC	10
F0/12	R1 G0/0/1 MAC	20
F0/24	PC2 MAC	20

When PC1 sends a packet to PC2 on another network, it forwards it to its default gateway 192.168.10.1. R1 receives the packet on its G0/0/0 interface and examines the destination address of the packet. R1 then routes the packet out its G0/0/1 interface to the F0/12 port in VLAN 20 on S1. Finally, S1 forwards the frame to PC2.

Legacy inter-VLAN routing using physical interfaces works, but it has a significant limitation. It is not reasonably scalable because routers have a limited number of physical interfaces. Requiring one physical router interface per VLAN quickly exhausts the physical interface capacity of a router.

In our example, R1 required two separate Ethernet interfaces to route between VLAN 10 and VLAN 20. What if there were six (or more) VLANs to interconnect? A separate interface would be required for each VLAN. Obviously, this solution is not scalable.

Note

This method of inter-VLAN routing is no longer implemented in switched networks and is included for explanation purposes only.

Router-on-a-Stick Inter-VLAN Routing (4.1.3)

The "router-on-a-stick" inter-VLAN routing method overcomes the limitation of the legacy inter-VLAN routing method. It requires only one physical Ethernet interface to route traffic between multiple VLANs on a network.

A Cisco IOS router Ethernet interface is configured as an 802.1Q trunk and connected to a trunk port on a Layer 2 switch. Specifically, the router interface is configured using *subinterfaces* to identify routable VLANs.

The configured subinterfaces are software-based virtual interfaces. Each is associated with a single physical Ethernet interface. Subinterfaces are configured in software on a router. Each subinterface is independently configured with an IP address and VLAN assignment. Subinterfaces are configured for different subnets that correspond to their VLAN assignment. This facilitates logical routing.

When VLAN-tagged traffic enters the router interface, it is forwarded to the VLAN subinterface. After a routing decision is made based on the destination IP network address, the router determines the exit interface for the traffic. If the exit interface is configured as an 802.1Q subinterface, the data frames are VLAN-tagged with the new VLAN and sent back out the physical interface.

Figure 4-2 shows an example of router-on-a-stick inter-VLAN routing. PC1 on VLAN 10 is communicating with PC3 on VLAN 30 through router R1 using a single, physical router interface.

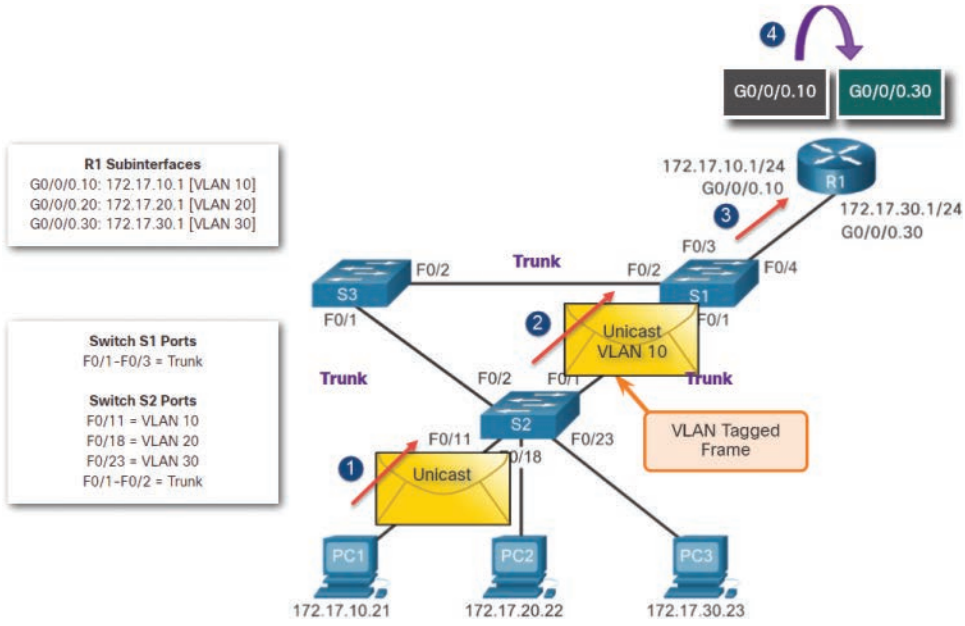

Figure 4-2 Unicast from VLAN 10 Is Route to VLAN 30

Figure 4-2 illustrates the following steps:

Step 1. PC1 sends its unicast traffic to switch S2.

Step 2. Switch S2 tags the unicast traffic as originating on VLAN 10 and forwards the unicast traffic out its trunk link to switch S1.

Step 3. Switch S1 forwards the tagged traffic out the other trunk interface on port F0/3 to the interface on router R1.

Step 4. Router R1 accepts the tagged unicast traffic on VLAN 10 and routes it to VLAN 30 using its configured subinterfaces.

In Figure 4-3, R1 routes the traffic to the correct VLAN.

Figure 4-3 illustrates the following steps:

Step 5. The unicast traffic is tagged with VLAN 30 as it is sent out the router interface to switch S1.

Step 6. Switch S1 forwards the tagged unicast traffic out the other trunk link to switch S2.

Step 7. Switch S2 removes the VLAN tag of the unicast frame and forwards the frame out to PC3 on port F0/23.

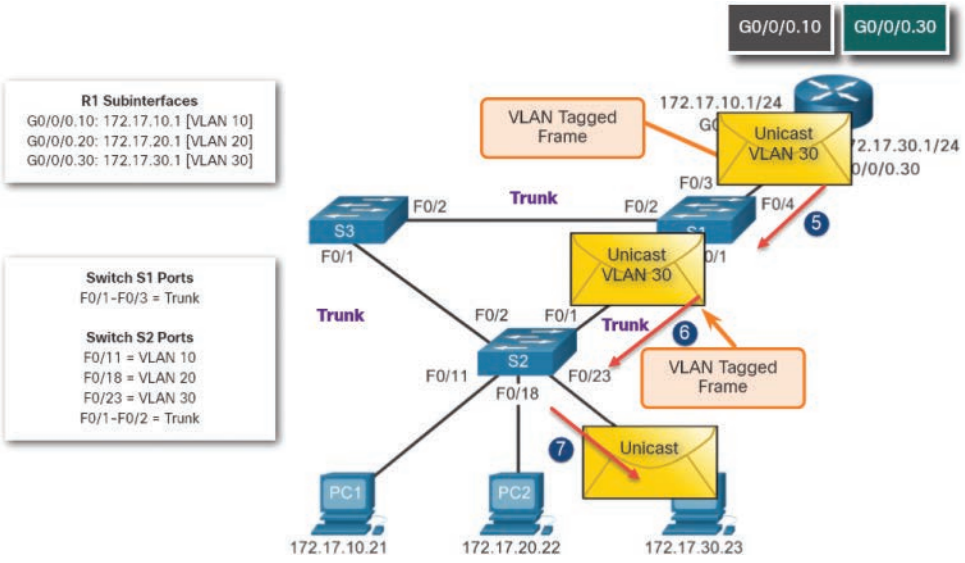

Figure 4-3 Router Tags Unicast Frame with VLAN 30

Note

The router-on-a-stick method of inter-VLAN routing does not scale beyond 50 VLANs.

Inter-VLAN Routing on a Layer 3 Switch (4.1.4)

The modern method of performing inter-VLAN routing is to use Layer 3 switches and switched virtual interfaces (SVI). An SVI is a virtual interface that is configured on a Layer 3 switch, as shown in Figure 4-4.

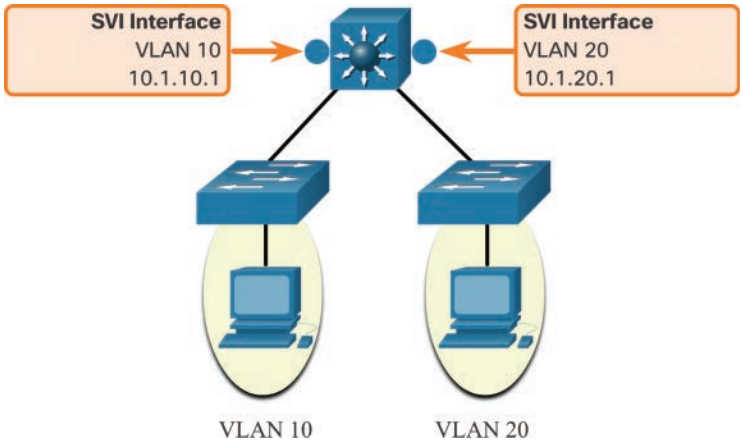

Figure 4-4 Layer 3 Switch Inter-VLAN Routing Example

Note

A Layer 3 switch is also called a multilayer switch because it operates at Layer 2 and Layer 3. However, in this course we use the term Layer 3 switch.

Inter-VLAN SVIs are created the same way that the management VLAN interface is configured. The SVI is created for a VLAN that exists on the switch. Although virtual, the SVI performs the same functions for the VLAN as a router interface would. Specifically, it provides Layer 3 processing for packets that are sent to or from all switch ports associated with that VLAN.

The following are advantages of using Layer 3 switches for inter-VLAN routing:

- They are much faster than router-on-a-stick because everything is hardware switched and routed.
- There is no need for external links from the switch to the router for routing.
- They are not limited to one link because Layer 2 EtherChannels can be used as trunk links between the switches to increase bandwidth.
- Latency is much lower because data does not need to leave the switch to be routed to a different network.
- They are more commonly deployed in a campus LAN than routers.

The only disadvantage is that Layer 3 switches are more expensive than Layer 2 switches, but they can be less expensive than a separate Layer 2 switch and router.

Interactive Graphic

Check Your Understanding—Inter-VLAN Routing Operation (4.1.5)

Refer to the online course to complete this activity.

Router-on-a-Stick Inter-VLAN Routing (4.2)

In this section, you configure router-on-a-stick inter-VLAN routing.

Router-on-a-Stick Scenario (4.2.1)

In the previous section, three ways to create inter-VLAN routing were listed, and legacy inter-VLAN routing was detailed. This section details how to configure router-on-a-stick inter-VLAN routing. You can see in the figure that the router is not in the center of the topology but instead appears to be on a stick near the border, hence the name.

In Figure 4-5, the R1 GigabitEthernet 0/0/1 interface is connected to the S1 FastEthernet 0/5 port. The S1 FastEthernet 0/1 port is connected to the S2 FastEthernet 0/1 port. These are trunk links that are required to forward traffic within and between VLANs.

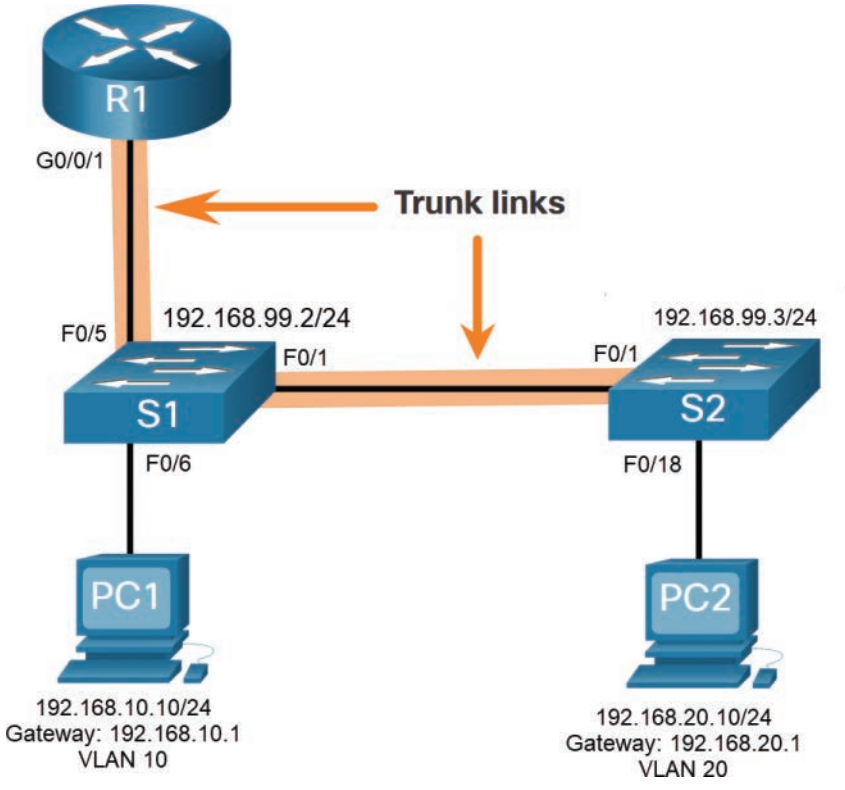

Figure 4-5 Router-on-a-Stick Topology

To route between VLANs, the R1 GigabitEthernet 0/0/1 interface is logically divided into three subinterfaces, as shown in Table 4-2. The table also shows the three VLANs that will be configured on the switches.

Table 4-2 Router R1 Subinterfaces

Subinterface	VLAN	IP Address
G0/0/1.10	10	192.168.10.1/24
G0/0/1.20	20	192.168.20.1/24
G0/0/1.30	99	192.168.99.1/24

Assume that R1, S1, and S2 have initial basic configurations. Currently, PC1 and PC2 cannot **ping** each other because they are on separate networks. Only S1 and S2 can **ping** each other, but they but are unreachable by PC1 or PC2 because they are also on different networks.

To enable devices to ping each other, the switches must be configured with VLANs and trunking, and the router must be configured for inter-VLAN routing.

S1 VLAN and Trunking Configuration (4.2.2)

Complete the following steps to configure S1 with VLANs and trunking:

Step 1. **Create and name the VLANs.** First, the VLANs are created and named, as shown in Example 4-1. VLANs are created only after you exit out of VLAN subconfiguration mode.

Example 4-1 Create and Name VLANs

```
S1(config)# vlan 10
S1(config-vlan)# name LAN10
S1(config-vlan)# exit
S1(config)# vlan 20
S1(config-vlan)# name LAN20
S1(config-vlan)# exit
S1(config)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)#
```

Step 2. **Create the management interface.** Next, the management interface is created on VLAN 99 along with the default gateway of R1, as shown in Example 4-2.

Example 4-2 Create the Management Interface

```
S1(config)# interface vlan 99
S1(config-if)# ip add 192.168.99.2 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.99.1
S1(config)#
```

Step 3. **Configure access ports.** Next, port Fa0/6 connecting to PC1 is configured as an access port in VLAN 10, as shown in Example 4-3. Assume PC1 has been configured with the correct IP address and default gateway.

Example 4-3 Configure Access Ports

```
S1(config)# interface fa0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# no shut
S1(config-if)# exit
S1(config)#
```

Step 4. Configure trunking ports. Finally, ports Fa0/1 connecting to S2 and Fa05 connecting to R1 are configured as trunk ports, as shown in Example 4-4.

Example 4-4 Configure Trunking Ports

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode trunk
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# interface fa0/5
S1(config-if)# switchport mode trunk
S1(config-if)# no shut
S1(config-if)# end
*Mar  1 00:23:43.093: %LINEPROTO-5-UPDOWN: Line protocol on Interface
  FastEthernet0/1, changed state to up
*Mar  1 00:23:44.511: %LINEPROTO-5-UPDOWN: Line protocol on Interface
  FastEthernet0/5, changed state to up
```

S2 VLAN and Trunking Configuration (4.2.3)

The configuration for S2 is similar to S1, as shown in Example 4-5.

Example 4-5 S2 Configuration

```
S2(config)# vlan 10
S2(config-vlan)# name LAN10
S2(config-vlan)# exit
S2(config)# vlan 20
S2(config-vlan)# name LAN20
S2(config-vlan)# exit
S2(config)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)#
S2(config)# interface vlan 99
S2(config-if)# ip add 192.168.99.3 255.255.255.0
```

```
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.99.1
S2(config)# interface fa0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# interface fa0/1
S2(config-if)# switchport mode trunk
S2(config-if)# no shut
S2(config-if)# exit
S2(config-if)# end
*Mar  1 00:23:52.137: %LINEPROTO-5-UPDOWN: Line protocol on Interface
  FastEthernet0/1, changed state to up
```

R1 Subinterface Configuration (4.2.4)

The router-on-a-stick method requires you to create a subinterface for each VLAN to be routed.

A subinterface is created using the **interface** *interface_id.subinterface_id* global configuration mode command. The subinterface syntax is the physical interface followed by a period and a subinterface number. Although not required, it is customary to match the subinterface number with the VLAN number.

Each subinterface is then configured with the following two commands:

- **encapsulation dot1q** *vlan_id* **[native]:** This command configures the subinterface to respond to 802.1Q encapsulated traffic from the specified *vlan-id*. The **native** keyword option is only appended to set the native VLAN to something other than VLAN 1.
- **ip address** *ip-address subnet-mask*: This command configures the IPv4 address of the subinterface. This address typically serves as the default gateway for the identified VLAN.

Repeat the process for each VLAN to be routed. Each router subinterface must be assigned an IP address on a unique subnet for routing to occur.

When all subinterfaces have been created, enable the physical interface using the **no shutdown** interface configuration command. If the physical interface is disabled, all subinterfaces are disabled.

In the configuration in Example 4-6, the R1 G0/0/1 subinterfaces are configured for VLANs 10, 20, and 99.

Example 4-6 R1 Subinterface Configuration

```
R1(config)# interface G0/0/1.10
R1(config-subif)# description Default Gateway for VLAN 10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip add 192.168.10.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.20
R1(config-subif)# description Default Gateway for VLAN 20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip add 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.99
R1(config-subif)# description Default Gateway for VLAN 99
R1(config-subif)# encapsulation dot1Q 99
R1(config-subif)# ip add 192.168.99.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1
R1(config-if)# description Trunk link to S1
R1(config-if)# no shut
R1(config-if)# end
R1#
*Sep 15 19:08:47.015: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed
  state to down
*Sep 15 19:08:50.071: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed
  state to up
*Sep 15 19:08:51.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface
  GigabitEthernet0/0/1, changed state to up
R1#
```

Verify Connectivity Between PC1 and PC2 (4.2.5)

The router-on-a-stick configuration is complete after the switch trunk and the router subinterfaces have been configured. The configuration can be verified from the hosts, router, and switch.

From a host, verify connectivity to a host in another VLAN using the **ping** command. It is a good idea to first verify the current host IP configuration using the **ipconfig** Windows host command, as shown in Example 4-7.

Example 4-7 Verify Windows Host Configuration

```
C:\Users\PC1> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix . :
   Link-local IPv6 Address          : fe80::5c43:ee7c:2959:da68%6
   IPv4 Address                     : 192.168.10.10
   Subnet Mask                      : 255.255.255.0
   Default Gateway                  : 192.168.10.1
C:\Users\PC1>
```

The output confirms the IPv4 address and default gateway of PC1. Next, use **ping** to verify connectivity with PC2 and S1, as shown in Figure 4-5. The **ping** output successfully confirms that inter-VLAN routing is operating, as shown in Example 4-8.

Example 4-8 Verify Inter-VLAN Routing by Pinging from PC1

```
C:\Users\PC1> ping 192.168.20.10
Pinging 192.168.20.10 with 32 bytes of data:
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\PC1>
C:\Users\PC1> ping 192.168.99.2
Pinging 192.168.99.2 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.99.2: bytes=32 time=2ms TTL=254
Reply from 192.168.99.2: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.99.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss).
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\PC1>
```

Router-on-a-Stick Inter-VLAN Routing Verification (4.2.6)

In addition to using **ping** between devices, the following **show** commands can be used to verify and troubleshoot the router-on-a-stick configuration.

- **show ip route**
- **show ip interface brief**
- **show interfaces**
- **show interfaces trunk**

As shown in Example 4-9, verify that the subinterfaces are appearing in the routing table of R1 by using the **show ip route** command. Notice that there are three connected routes (C) and their respective exit interfaces for each routable VLAN. The output confirms that the correct subnets, VLANs, and subinterfaces are active.

Example 4-9 Verify Subinterfaces Are in Routing Table

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/1.10
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/1.10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, GigabitEthernet0/0/1.20
L        192.168.20.1/32 is directly connected, GigabitEthernet0/0/1.20
      192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.99.0/24 is directly connected, GigabitEthernet0/0/1.99
L        192.168.99.1/32 is directly connected, GigabitEthernet0/0/1.99
R1#
```

Another useful router command is **show ip interface brief**, as shown in Example 4-10. The output confirms that the subinterfaces have the correct IPv4 address configured, and that they are operational.

Example 4-10 Verify Subinterface IP Addresses and Status

```
R1# show ip interface brief | include up
GigabitEthernet0/0/1   unassigned      YES unset  up                    up
Gi0/0/1.10             192.168.10.1    YES manual up                    up
Gi0/0/1.20             192.168.20.1    YES manual up                    up
Gi0/0/1.99             192.168.99.1    YES manual up                    up
R1#
```

Subinterfaces can be verified using the **show interfaces** *subinterface-id* command, as shown in Example 4-11.

Example 4-11 Verify Details of the Subinterface

```
R1# show interfaces g0/0/1.10
GigabitEthernet0/0/1.10 is up, line protocol is up
  Hardware is ISR4221-2x1GE, address is 10b3.d605.0301 (bia 10b3.d605.0301)
  Description: Default Gateway for VLAN 10
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  10.
  ARP type: ARPA, ARP Timeout 04:00:00
  Keepalive not supported
  Last clearing of "show interface" counters never
R1#
```

The misconfiguration could also be on the trunking port of the switch. Therefore, it is also useful to verify the active trunk links on a Layer 2 switch by using the **show interfaces trunk** command, as shown in Example 4-12. The output confirms that the link to R1 is trunking for the required VLANs.

Note

Although VLAN 1 was not explicitly configured, it was automatically included because control traffic on trunk links will always be forwarded on VLAN 1.

Example 4-12 Verify Trunk Link Status

```
S1# show interfaces trunk
Port        Mode             Encapsulation   Status        Native vlan
Fa0/1       on               802.1q          trunking      1
Fa0/5       on               802.1q          trunking      1
Port        Vlans allowed on trunk
Fa0/1       1-4094
Fa0/5       1-4094
Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99
Fa0/5       1,10,20,99
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
Fa0/5       1,10,20,99
S1#
```

Packet Tracer—Configure Router-on-a-Stick Inter-VLAN Routing (4.2.7)

In this Packet Tracer activity, you check for connectivity prior to implementing inter-VLAN routing. Then you configure VLANs and inter-VLAN routing. Finally, you enable trunking and verify connectivity between VLANs.

Lab—Configure Router-on-a-Stick Inter-VLAN Routing (4.2.8)

In this lab, you complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Configure Switches with VLANs and Trunking
- Part 3: Configure Trunk-Based Inter-VLAN Routing

Inter-VLAN Routing using Layer 3 Switches (4.3)

In this section, you configure inter-VLAN routing using Layer 3 switches.

Layer 3 Switch Inter-VLAN Routing (4.3.1)

Modern enterprise networks rarely use router-on-a-stick because it does not scale easily to meet requirements. In these very large networks, network administrators use Layer 3 switches to configure inter-VLAN routing.

Inter-VLAN routing using the router-on-a-stick method is simple to implement for a small- to medium-sized organization. However, a large enterprise requires a faster, much more scalable method to provide inter-VLAN routing.

Enterprise campus LANs use Layer 3 switches to provide inter-VLAN routing. Layer 3 switches use hardware-based switching to achieve higher-packet processing rates than routers. Layer 3 switches are also commonly implemented in enterprise distribution layer wiring closets.

Capabilities of a Layer 3 switch include the ability to do the following:

- Route from one VLAN to another using multiple *switched virtual interfaces (SVIs)*.
- Convert a Layer 2 switchport to a Layer 3 interface (that is, a *routed port*). A routed port is similar to a physical interface on a Cisco IOS router.

To provide inter-VLAN routing, Layer 3 switches use SVIs. SVIs are configured using the same **interface vlan** *vlan-id* command used to create the management SVI on a Layer 2 switch. A Layer 3 SVI must be created for each of the routable VLANs.

Layer 3 Switch Scenario (4.3.2)

In Figure 4-6, the Layer 3 switch, D1, is connected to two hosts on different VLANs. PC1 is in VLAN 10, and PC2 is in VLAN 20, as shown. The Layer 3 switch will provide inter-VLAN routing services to the two hosts.

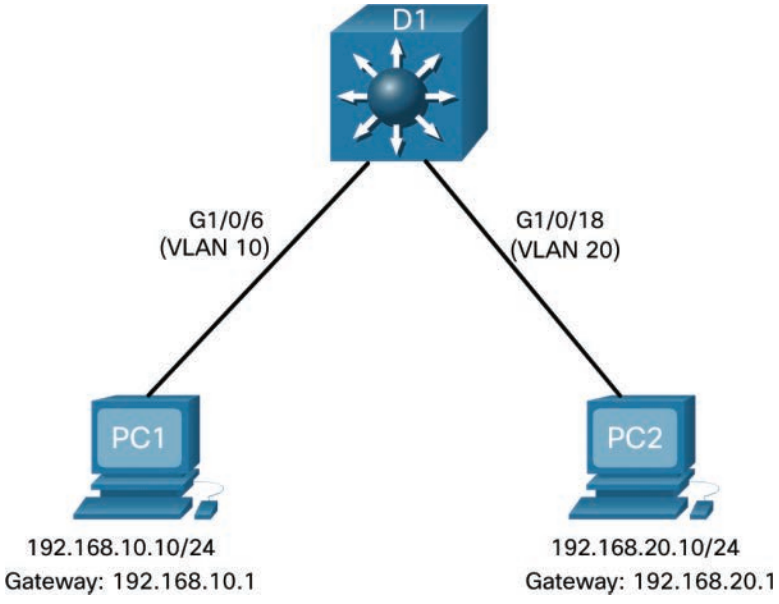

Figure 4-6 Layer 3 Switch Inter-VLAN Routing Topology

Table 4-3 shows the IP addresses for each VLAN.

Table 4-3 D1 VLAN IP Addresses

VLAN Interface	IP Address
10	192.168.10.1/24
20	192.168.20.1/24

Layer 3 Switch Configuration (4.3.3)

Complete the following steps to configure S1 with VLANs and trunking:

Step 1. **Create the VLANs.** First, create the two VLANs as shown in Example 4-13.

Example 4-13 Create the VLANs

```
D1(config)# vlan 10
D1(config-vlan)# name LAN10
D1(config-vlan)# vlan 20
D1(config-vlan)# name LAN20
D1(config-vlan)# exit
D1(config)#
```

Step 2. **Create the SVI VLAN interfaces.** Configure the SVI for VLANs 10 and 20, as shown in Example 4-14. The IP addresses that are configured will serve as the default gateways to the hosts in the respective VLANs. Notice the informational messages showing the line protocol on both SVIs changed to up.

Example 4-14 Create the SVI VLAN Interfaces

```
D1(config)# interface vlan 10
D1(config-if)# description Default Gateway SVI for 192.168.10.0/24
D1(config-if)# ip add 192.168.10.1 255.255.255.0
D1(config-if)# no shut
D1(config-if)# exit
D1(config)#
D1(config)# int vlan 20
D1(config-if)# description Default Gateway SVI for 192.168.20.0/24
D1(config-if)# ip add 192.168.20.1 255.255.255.0
D1(config-if)# no shut
D1(config-if)# exit
D1(config)#
*Sep 17 13:52:16.053: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10,
  changed state to up
*Sep 17 13:52:16.160: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20,
  changed state to up
```

Step 3. **Configure access ports.** Next, configure the access ports connecting to the hosts and assign them to their respective VLANs, as shown in Example 4-15.

Example 4-15 Configure Access Ports

```
D1(config)# interface GigabitEthernet1/0/6
D1(config-if)# description Access port to PC1
D1(config-if)# switchport mode access
D1(config-if)# switchport access vlan 10
D1(config-if)# exit
D1(config)#
D1(config)# interface GigabitEthernet1/0/18
D1(config-if)# description Access port to PC2
D1(config-if)# switchport mode access
D1(config-if)# switchport access vlan 20
D1(config-if)# exit
```

Step 4. **Enable IP routing.** Finally, enable IPv4 routing with the **ip routing** global configuration command to allow traffic to be exchanged between VLANs 10 and 20, as shown in Example 4-16. This command must be configured to enable inter-VAN routing on a Layer 3 switch for IPv4.

Example 4-16 Enable IP Routing

```
D1(config)# ip routing
D1(config)#
```

Layer 3 Switch Inter-VLAN Routing Verification (4.3.4)

Inter-VLAN routing using a Layer 3 switch is simpler to configure than the router-on-a-stick method. After the configuration is complete, the configuration can be verified by testing connectivity between the hosts.

From a host, verify connectivity to a host in another VLAN using the **ping** command. It is a good idea to first verify the current host IP configuration using the **ipconfig** Windows host command. The output in Example 4-17 confirms the IPv4 address and default gateway of PC1.

Example 4-17 Verify Windows Host Configuration

```
C:\Users\PC1> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix .   :
   Link-local IPv6 Address            : fe80::5c43:ee7c:2959:da68%6
   IPv4 Address                       : 192.168.10.10
   Subnet Mask                        : 255.255.255.0
   Default Gateway                    : 192.168.10.1
C:\Users\PC1>
```

Next, verify connectivity with PC2 using the **ping** Windows host command, as shown in Example 4-18. The **ping** output successfully confirms that inter-VLAN routing is operating.

Example 4-18 Verify Inter-VLAN Routing by Pinging from PC1

```
C:\Users\PC1> ping 192.168.20.10
Pinging 192.168.20.10 with 32 bytes of data:
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\PC1>
```

Routing on a Layer 3 Switch (4.3.5)

If VLANs are to be reachable by other Layer 3 devices, they must be advertised using static or dynamic routing. To enable routing on a Layer 3 switch, a routed port must be configured.

A routed port is created on a Layer 3 switch by disabling the switchport feature on a Layer 2 port that is connected to another Layer 3 device. Specifically, configuring the **no switchport** interface configuration command on a Layer 2 port converts it into a Layer 3 interface. Then the interface can be configured with an IPv4 configuration to connect to a router or another Layer 3 switch.

Routing Scenario on a Layer 3 Switch (4.3.6)

In Figure 4-7, the previously configured D1 Layer 3 switch is now connected to R1. R1 and D1 are both in an Open Shortest Path First (OSPF) routing protocol domain. Assume inter-VLAN has been successfully implemented on D1. The G0/0/1 interface of R1 has also been configured and enabled. Additionally, R1 is using OSPF to advertise its two networks, 10.10.10.0/24 and 10.20.20.0/24.

Note

OSPF routing configuration is covered in another course. In this module, OSPF configuration commands will be given to you in all activities and assessments. It is not required that you understand the configuration in order to enable OSPF routing on the Layer 3 switch.

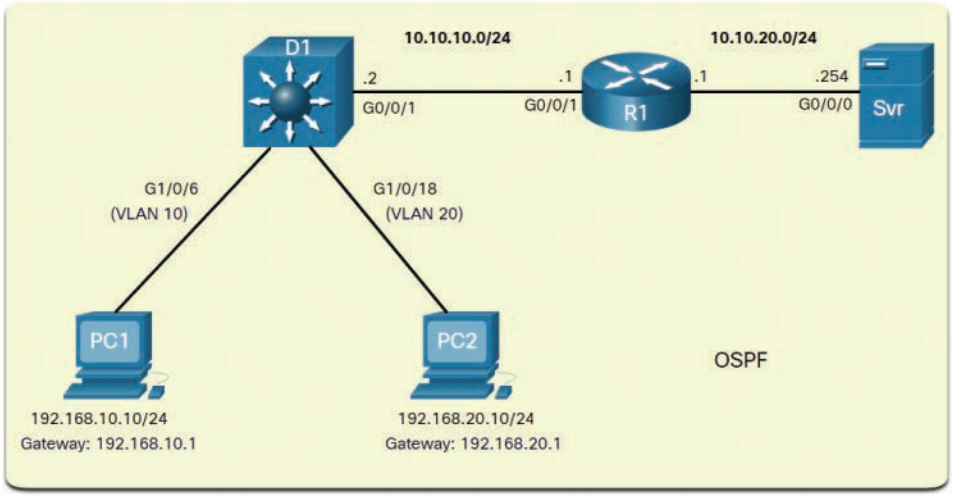

Figure 4-7 Routing Scenario on a Layer 3 Switch Topology

Routing Configuration on a Layer 3 Switch (4.3.7)

Complete the following steps to configure D1 to route with R1:

How To

Step 1. Configure the routed port. Configure G1/0/1 to be a routed port, assign it an IPv4 address, and enable it, as shown in Example 4-19.

Example 4-19 Configure the Routed Port

```
D1(config)# interface GigabitEthernet1/0/1
D1(config-if)# description routed Port Link to R1
D1(config-if)# no switchport
D1(config-if)# ip address 10.10.10.2 255.255.255.0
D1(config-if)# no shut
D1(config-if)# exit
D1(config)#
```

Step 2. Enable routing, as shown in Example 4-20. Ensure IPv4 routing is enabled with the **ip routing** global configuration command.

Example 4-20 Enable Routing

```
D1(config)# ip routing
D1(config)#
```

Step 3. Configure routing. Configure the OSPF routing protocol to advertise the VLAN 10 and VLAN 20 networks, along with the network that is connected to R1, as shown in Example 4-21. Notice the message informing you that an adjacency has been established with R1.

Example 4-21 Configure Routing

```
D1(config)# router ospf 10
D1(config-router)# network 192.168.10.0 0.0.0.255 area 0
D1(config-router)# network 192.168.20.0 0.0.0.255 area 0
D1(config-router)# network 10.10.10.0 0.0.0.3 area 0
D1(config-router)# ^Z
D1#
*Sep 17 13:52:51.163: %OSPF-5-ADJCHG: Process 10, Nbr 10.20.20.1 on
  GigabitEthernet1/0/1 from LOADING to FULL, Loading Done
D1#
```

Step 4. Verify routing. Verify the routing table on D1, as shown in Example 4-22. Notice that D1 now has a route to the 10.20.20.0/24 network.

Example 4-22 Verify Routing

```
D1# show ip route | begin Gateway
Gateway of last resort is not set
      10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C        10.10.10.0/30 is directly connected, GigabitEthernet1/0/1
L        10.10.10.2/32 is directly connected, GigabitEthernet1/0/1
O        10.20.20.0/24 [110/2] via 10.10.10.1, 00:00:06, GigabitEthernet1/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, Vlan10
L        192.168.10.1/32 is directly connected, Vlan10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, Vlan20
L        192.168.20.1/32 is directly connected, Vlan20
D1#
```

Step 5. Verify connectivity. At this time, PC1 and PC2 are able to ping the server connected to R1, as shown in Example 4-23.

Example 4-23 Verify Connectivity

```
C:\Users\PC1> ping 10.20.20.254
Pinging 10.20.20.254 with 32 bytes of data:
Request timed out.
Reply from 10.20.20.254: bytes=32 time<1ms TTL=127
Reply from 10.20.20.254: bytes=32 time<1ms TTL=127
```

```
Reply from 10.20.20.254: bytes=32 time<1ms TTL=127
Ping statistics for 10.20.20.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss).
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\PC1>
!================================================
C:\Users\PC2> ping 10.20.20.254
Pinging 10.20.20.254 with 32 bytes of data:
Reply from 10.20.20.254: bytes=32 time<1ms TTL=127
Reply from 10.20.20.254: bytes=32 time<1ms TTL=127
Reply from 10.20.20.254: bytes=32 time<1ms TTL=127
Reply from 10.20.20.254: bytes=32 time<1ms TTL=127
Ping statistics for 10.20.20.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\PC2>
```

Packet Tracer Activity

Packet Tracer—Configure Layer 3 Switching and Inter-VLAN Routing (4.3.8)

In this Packet Tracer activity, you configure Layer 3 switching and Inter-VLAN routing on a Cisco 3560 switch.

Troubleshoot Inter-VLAN Routing (4.4)

In this section, you learn how to troubleshoot issues in an inter-VLAN routing environment.

Common Inter-VLAN Issues (4.4.1)

By now, you know that when you configure and verify, you must also be able to troubleshoot. This section discusses some common network problems associated with inter-VLAN routing.

There are a number of reasons why an inter-VAN configuration may not work. All are related to connectivity issues. First, check the physical layer to resolve any issues where a cable might be connected to the wrong port. If the connections are correct, use the list in Table 4-4 for other common reasons why inter-VLAN connectivity may fail.

Table 4-4 Common Inter-VLAN Issues

Issue Type	How to Fix	How to Verify

Missing VLANs	■ Create (or re-create) the VLAN if it does not exist.
	■ Ensure host port is assigned to the correct VLAN.
		`show vlan [brief]`
		`show interfaces switchport`
		`ping`

Switch Trunk Port Issues	■ Ensure trunks are configured correctly. ■ Ensure port is a trunk port and enabled.	`show interfaces trunk` `show running-config`

Switch Access Port Issues	■ Assign correct VLAN to access port.
	■ Ensure port is an access port and enabled.
	■ Host is incorrectly configured in the wrong subnet.
		`show interfaces switchport`
		`show running-config interface`
		`ipconfig`

Router Configuration Issues	■ Router subinterface IPv4 address is incorrectly configured. ■ Router subinterface is assigned to the VLAN ID.	`show ip interface brief` `show interfaces`

Troubleshoot Inter-VLAN Routing Scenario (4.4.2)

Next, examples of some of these inter-VLAN routing problems are covered in more detail.

The topology in Figure 4-8 will be used for all of these issues.

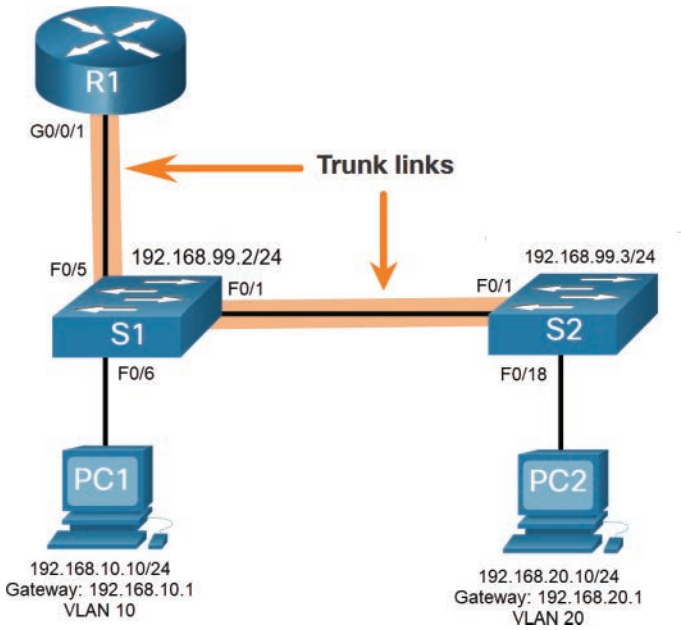

Figure 4-8 Inter-VLAN Routing Troubleshooting Topology

The VLAN and IPv4 addressing information for R1 is shown in Table 4-5.

Table 4-5 Router R1 Subinterfaces

Subinterface	VLAN	IP Address
G0/0/0.10	10	192.168.10.1/24
G0/0/0.20	20	192.168.20.1/24
G0/0/0.30	99	192.168.99.1/24

Missing VLANs (4.4.3)

An inter-VLAN connectivity issue could be caused by a missing VLAN. The VLAN could be missing if it was not created, it was accidently deleted, or it is not allowed on the trunk link.

For example, PC1 is currently connected to VLAN 10, as shown in the **show vlan brief** command output in Example 4-24.

Example 4-24 Verify VLAN for PC1

```
S1# show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gi0/1, Gi0/2
10   LAN10                             active    Fa0/6
20   LAN20                             active
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
S1#
```

Now assume that VLAN 10 is accidently deleted, as shown in Example 4-25.

Example 4-25 VLAN 10 Is Deleted

```
S1(config)# no vlan 10
S1(config)# do show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gi0/1, Gi0/2
20   LAN20                             active
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
S1(config)#
```

Notice that VLAN 10 is now missing from the output in Example 4-25. Also notice that port Fa0/6 has not been reassigned to the default VLAN. The reason is because when you delete a VLAN, any ports assigned to that VLAN become inactive. They remain associated with the VLAN (and thus inactive) until you assign them to a new VLAN or re-create the missing VLAN.

Use the **show interface** *interface-id* **switchport** command to verify the VLAN membership, as shown in Example 4-26.

Example 4-26 Verify an Interface's VLAN Membership

```
S1(config)# do show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
(Output omitted)
```

Re-creating the missing VLAN would automatically reassign the hosts to it, as shown in Example 4-27.

Example 4-27 Attempt to Re-create and Verify VLAN 10

```
S1(config)# vlan 10
S1(config-vlan)# do show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gi0/1, Gi0/2
20   LAN20                             active
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
S1(config-vlan)#
```

Notice that the VLAN has not been created as expected. The reason is because you must exit from VLAN sub-configuration mode to create the VLAN, as shown in Example 4-28.

Example 4-28 Exit VLAN Configuration Mode and Then Re-create and Verify VLAN

```
S1(config-vlan)# exit
S1(config)# vlan 10
S1(config)# do show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gi0/1, Gi0/2
10   VLAN0010                          active    Fa0/6
20   LAN20                             active
99   Management                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
S1(config)#
```

Now notice that the VLAN is included in the list and that the host connected to Fa0/6 is on VLAN 10.

Switch Trunk Port Issues (4.4.4)

Another issue for inter-VLAN routing includes misconfigured switch ports. In a legacy inter-VLAN solution, this could be caused when the connecting router port is not assigned to the correct VLAN.

However, with a router-on-a-stick solution, the most common cause is a misconfigured trunk port.

For example, assume PC1 was able to connect to hosts in other VLANs until recently. A quick look at maintenance logs revealed that the S1 Layer 2 switch was recently accessed for routine maintenance. Therefore, you suspect the problem may be related to that switch.

On S1, verify that the port connecting to R1 (i.e., F0/5) is correctly configured as a trunk link using the **show interfaces trunk** command, as shown in Example 4-29.

Example 4-29 Verify Trunking

```
S1# show interfaces trunk
Port         Mode             Encapsulation  Status         Native vlan
Fa0/1        on               802.1q         trunking       1
Port         Vlans allowed on trunk
Fa0/1        1-4094
Port         Vlans allowed and active in management domain
Fa0/1        1,10,20,99
Port         Vlans in spanning tree forwarding state and not pruned
Fa0/1        1,10,20,99
S1#
```

The Fa0/5 port connecting to R1 is mysteriously missing from the output. Verify the interface configuration using the **show running-config interface fa0/5** command, as shown in Example 4-30.

Example 4-30 Verify Interface Configuration

```
S1# show running-config interface fa0/5
Building configuration...
Current configuration : 96 bytes
!
interface FastEthernet0/5
 description Trunk link to R1
 switchport mode trunk
 shutdown
end
S1#
```

As you can see, the port was accidently shut down. To correct the problem, reenable the port and verify the trunking status, as shown in Example 4-31.

Example 4-31 Reenable and Verify the Port

```
S1(config)# interface fa0/5
S1(config-if)# no shut
S1(config-if)#
*Mar  1 04:46:44.153: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to
  up
S1(config-if)#
*Mar  1 04:46:47.962: %LINEPROTO-5-UPDOWN: Line protocol on Interface
  FastEthernet0/5, changed state to up
S1(config-if)# do show interface trunk
Port         Mode              Encapsulation   Status         Native vlan
Fa0/1        on                802.1q          trunking       1
Fa0/5        on                802.1q          trunking       1
Port         Vlans allowed on trunk
Fa0/1        1-4094
Fa0/5        1-4094
Port         Vlans allowed and active in management domain
Fa0/1        1,10,20,99
Fa0/5        1,10,20,99
Port         Vlans in spanning tree forwarding state and not pruned
Fa0/1        1,10,20,99
Fa0/1        1,10,20,99
S1(config-if)#
```

To reduce the risk of a failed inter-switch link disrupting inter-VLAN routing, redundant links and alternate paths should be part of the network design.

Switch Access Port Issues (4.4.5)

When a problem is suspected with a switch access port configuration, use verification commands to examine the configuration and identify the problem.

Assume PC1 has the correct IPv4 address and default gateway but is not able to **ping** its own default gateway. PC1 is supposed to be connected to a VLAN 10 port.

Verify the port configuration on S1 using the **show interfaces** *interface-id* **switchport** command, as shown in Example 4-32.

Example 4-32 Verify the Port Configuration

```
S1# show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

The Fa0/6 port has been configured as an access port, as indicated by "static access". However, it appears that it has not been configured to be in VLAN 10. Verify the configuration of the interface, as shown in Example 4-33.

Example 4-33 Verify the Port Configuration in the Running-Config

```
S1# show running-config interface fa0/6
Building configuration...
Current configuration : 87 bytes
!
interface FastEthernet0/6
 description PC-A access port
 switchport mode access
end
S1#
```

Assign port Fa0/6 to VLAN 10 and verify the port assignment, as shown in Example 4-34.

Example 4-34 Assign the VLAN to the Port and Verify the Configuration

```
S1# configure terminal
S1(config)# interface fa0/6
S1(config-if)# switchport access vlan 10
S1(config-if)#
S1(config-if)# do show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
```

```
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (VLAN0010)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
(Output omitted)
```

PC1 is now able to communicate with hosts on other VLANs.

Router Configuration Issues (4.4.6)

Router-on-a-stick configuration problems are usually related to subinterface misconfigurations. For instance, an incorrect IP address was configured or the wrong VLAN ID was assigned to the subinterface.

For example, R1 should be providing inter-VLAN routing for users in VLANs 10, 20, and 99. However, users in VLAN 10 cannot reach any other VLAN.

You verified the switch trunk link and all appears to be in order. Verify the subinterface status using the **show ip interface brief** command, as shown in Example 4-35.

Example 4-35 Verify the Status of the Subinterfaces

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  administratively down down
GigabitEthernet0/0/1   unassigned      YES unset  up                    up
Gi0/0/1.10             192.168.10.1    YES manual up                    up
Gi0/0/1.20             192.168.20.1    YES manual up                    up
Gi0/0/1.99             192.168.99.1    YES manual up                    up
Serial0/1/0            unassigned      YES unset  administratively down down
Serial0/1/1            unassigned      YES unset  administratively down down
R1#
```

The subinterfaces have been assigned the correct IPv4 addresses, and they are operational.

Verify which VLANs each of the subinterfaces is on. To do so, the **show interfaces** command is useful, but it generates a great deal of additional unrequired output.

The command output can be reduced using IOS command filters as shown in Example 4-36.

Example 4-36 Verify the VLANs Configured on Each Subinterface

```
R1# show interfaces | include Gig|802.1Q
GigabitEthernet0/0/0 is administratively down, line protocol is down
GigabitEthernet0/0/1 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
GigabitEthernet0/0/1.10 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  100.
GigabitEthernet0/0/1.20 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  20.
GigabitEthernet0/0/1.99 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  99.
R1#
```

The pipe symbol (|) along with some select keywords is a useful method to help filter command output. In this example, the keyword **include** was used to identify that only lines containing the letters "Gig" or "802.1Q" will be displayed. Because of the way the **show interface** output is naturally listed, using these filters produces a condensed list of interfaces and their assigned VLANs.

Notice that the G0/0/1.10 interface has been incorrectly assigned to VLAN 100 instead of VLAN 10. This is confirmed by looking at the configuration of the R1 GigabitEthernet 0/0/1.10 subinterface, as shown in Example 4-37.

Example 4-37 Verify the Configuration of the Subinterface in the Running-Config

```
R1# show running-config interface g0/0/1.10
Building configuration...
Current configuration : 146 bytes
!
interface GigabitEthernet0/0/1.10
 description Default Gateway for VLAN 10
 encapsulation dot1Q 100
 ip address 192.168.10.1 255.255.255.0
end
R1#
```

To correct this problem, configure subinterface G0/0/1.10 to be on the correct VLAN using the **encapsulation dot1q 10** subinterface configuration mode command, as shown in Example 4-38.

Example 4-38 Correct and Verify the Subinterface Configuration

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface gigabitEthernet 0/0/1.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# end
R1#
R1# show interfaces | include Gig|802.1Q
GigabitEthernet0/0/0 is administratively down, line protocol is down
GigabitEthernet0/0/1 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
GigabitEthernet0/0/1.10 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  10.
GigabitEthernet0/0/1.20 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  20.
GigabitEthernet0/0/1.99 is up, line protocol is up
R1#
```

When the subinterface has been assigned to the correct VLAN, it is accessible by devices on that VLAN, and the router can perform inter-VLAN routing.

With verification, router configuration problems are quickly addressed, allowing inter-VLAN routing to function properly.

Interactive Graphic

Check Your Understanding—Troubleshoot Inter-VLAN Routing (4.4.7)

Refer to the online course to complete this activity.

Packet Tracer Activity

Packet Tracer—Troubleshoot Inter-VLAN Routing (4.4.8)

In this Packet Tracer activity, you complete the following objectives:

- Part 1: Locate Network Problems
- Part 2: Implement the Solution
- Part 3: Verify Network Connectivity

Lab—Troubleshoot Inter-VLAN Routing (4.4.9)

In this lab, you complete the following objectives:

- Part 1: Build the Network and Load Device Configurations
- Part 2: Troubleshoot the Inter-VLAN Routing Configuration
- Part 3: Verify VLAN Configuration, Port Assignment, and Trunking
- Part 4: Test Layer 3 Connectivity

Summary (4.5)

The following is a summary of each section in the chapter:

Inter-VLAN Routing Operation

Hosts in one VLAN cannot communicate with hosts in another VLAN unless there is a router or a Layer 3 switch to provide routing services. Inter-VLAN routing is the process of forwarding network traffic from one VLAN to another VLAN. Three options include legacy, router-on-a-stick, and a Layer 3 switch using SVIs. Legacy used a router with multiple Ethernet interfaces. Each router interface was connected to a switch port in different VLANs. Requiring one physical router interface per VLAN quickly exhausts the physical interface capacity of a router. The router-on-a-stick inter-VLAN routing method requires only one physical Ethernet interface to route traffic between multiple VLANs on a network. A Cisco IOS router Ethernet interface is configured as an 802.1Q trunk and connected to a trunk port on a Layer 2 switch. The router interface is configured using subinterfaces to identify routable VLANs. The configured subinterfaces are software-based virtual interfaces associated with a single physical Ethernet interface. The modern method is Inter-VLAN routing on a Layer 3 switch using SVIs. The SVI is created for a VLAN that exists on the switch. The SVI performs the same functions for the VLAN as a router interface. It provides Layer 3 processing for packets being sent to or from all switch ports associated with that VLAN.

Router-on-a-Stick Inter-VLAN Routing

To configure a switch with VLANs and trunking, complete the following steps: create and name the VLANs, create the management interface, configure access ports, and configure trunking ports. The router-on-a-stick method requires a subinterface to be created for each VLAN to be routed. A subinterface is created using the **interface** *interface_id.subinterface_id* global configuration mode command. Each router subinterface must be assigned an IP address on a unique subnet for routing to occur. When all subinterfaces have been created, the physical interface must be enabled using the **no shutdown** interface configuration command. From a host, verify connectivity to a host in another VLAN using the **ping** command. Use **ping** to verify connectivity with the host and the switch. To verify and troubleshoot, use the **show ip route**, **show ip interface brief**, **show interfaces**, and **show interfaces trunk** commands.

Inter-VLAN Routing Using Layer 3 Switches

Enterprise campus LANs use Layer 3 switches to provide inter-VLAN routing. Layer 3 switches use hardware-based switching to achieve higher-packet processing rates than routers. Capabilities of a Layer 3 switch include routing from one VLAN

to another using multiple switched virtual interfaces (SVIs) and converting a Layer 2 switch port to a Layer 3 interface (that is, a routed port). To provide inter-VLAN routing, Layer 3 switches use SVIs. SVIs are configured using the same **interface vlan** *vlan-id* command used to create the management SVI on a Layer 2 switch. A Layer 3 SVI must be created for each of the routable VLANs. To configure a switch with VLANS and trunking, complete the following steps: create the VLANS, create the SVI VLAN interfaces, configure access ports, and enable IP routing. From a host, verify connectivity to a host in another VLAN using the **ping** command. Next, verify connectivity with the host using the **ping** Windows host command. VLANs must be advertised using static or dynamic routing. To enable routing on a Layer 3 switch, a routed port must be configured. A routed port is created on a Layer 3 switch by disabling the switch port feature on a Layer 2 port that is connected to another Layer 3 device. The interface can be configured with an IPv4 configuration to connect to a router or another Layer 3 switch. To configure a Layer 3 switch to route with a router, follow these steps: configure the routed port, enable routing, configure routing, verify routing, and verify connectivity.

Troubleshoot Inter-VLAN Routing

There are a number of reasons why an inter-VAN configuration may not work. All are related to connectivity issues such as missing VLANs, switch trunk port issues, switch access port issues, and router configuration issues. A VLAN could be missing if it was not created, it was accidently deleted, or it is not allowed on the trunk link. Another issue for inter-VLAN routing includes misconfigured switch ports. In a legacy inter-VLAN solution, a misconfigured switch port could be caused when the connecting router port is not assigned to the correct VLAN. With a router-on-a-stick solution, the most common cause is a misconfigured trunk port. When a problem is suspected with a switch access port configuration, use **ping** and **show interfaces** *interface-id* **switchport** commands to identify the problem. Router configuration problems with router-on-a-stick configurations are usually related to subinterface misconfigurations. Verify the subinterface status using the **show ip interface brief** command.

Packet Tracer—Inter-VLAN Routing Challenge (4.5.1)

In this activity, you demonstrate and reinforce your ability to implement inter-VLAN routing, including configuring IP addresses, VLANs, trunking, and subinterfaces.

Lab—Implement Inter-VLAN Routing (4.5.2)

In this lab, you complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Create VLANs and Assign Switch Ports

- Part 3: Configure an 802.1Q Trunk between the Switches
- Part 4: Configure Inter-VLAN Routing on the S1 Switch
- Part 5: Verify Inter-VLAN Routing is Working

Practice

The following activities provide practice with the topics introduced in this chapter. The Labs are available in the companion *Switching, Routing, and Wireless Essentials Labs and Study Guide (CCNAv7)* (ISBN 9780136634386). The Packet Tracer Activity instructions are also in the Labs & Study Guide. The PKA files are found in the online course.

Labs

Lab 4.2.8: Configure Router-on-a-Stick Inter-VLAN Routing

Lab 4.4.9: Troubleshoot Inter-VLAN Routing

Lab 4.5.2: Implement Inter-VLAN Routing

Packet Tracer Activities

Packet Tracer 4.2.7: Configure Router-on-a-Stick Inter-VLAN Routing

Packet Tracer 4.3.8: Configure Layer 3 Switching and Inter-VLAN Routing

Packet Tracer 4.4.8: Troubleshoot Inter-VLAN Routing

Packet Tracer 4.5.1: Inter-VLAN Routing Challenge

Check Your Understanding Questions

Complete all the review questions listed here to test your understanding of the sections and concepts in this chapter. The appendix "Answers to the 'Check Your Understanding' Questions" lists the answers.

1. A router has two FastEthernet interfaces and needs to connect to four VLANs in the local network. How can this be accomplished using the fewest number of physical interfaces without unnecessarily decreasing network performance?

   A. Add a second router to handle the inter-VLAN traffic.
   B. Implement a router-on-a-stick configuration.
   C. Interconnect the VLANs via the two additional FastEthernet interfaces.
   D. Use a hub to connect the four VLANS with a FastEthernet interface on the router.

2. What distinguishes traditional legacy inter-VLAN routing from router-on-a-stick?

   A. Traditional routing is able to use only a single switch interface, whereas a router-on-a-stick can use multiple switch interfaces.
   B. Traditional routing requires a routing protocol, whereas a router-on-a-stick only needs to route directly connected networks.
   C. Traditional routing uses one port per logical network, whereas a router-on-a-stick uses subinterfaces to connect multiple logical networks to a single router port.
   D. Traditional routing uses multiple paths to the router and therefore requires STP, whereas router-on-a-stick does not provide multiple connections and therefore eliminates the need for STP.

3. Subinterface G0/1.10 on R1 must be configured as the default gateway for the VLAN 10 192.168.10.0/24 network. Which command should be configured on the subinterface to enable inter-VLAN routing for VLAN 10?

   A. **encapsulation dot1q 10**
   B. **encapsulation vlan 10**
   C. **switchport mode access**
   D. **switchport mode trunk**

4. What is important to consider while configuring the subinterfaces of a router when implementing inter-VLAN routing?

   A. The IP address of each subinterface must be the default gateway address for each VLAN subnet.
   B. The **no shutdown** command must be given on each subinterface.
   C. The physical interface must have an IP address configured.
   D. The subinterface numbers must match the VLAN ID number.

5. What are the steps that must be completed in order to enable inter-VLAN routing using router-on-a-stick?

   A. Configure the physical interfaces on the router and enable a routing protocol.
   B. Create the VLANs on the router and define the port membership assignments on the switch.
   C. Create the VLANs on the switch to include port membership assignment and enable a routing protocol on the router.
   D. Create the VLANs on the switch to include port membership assignment and configure subinterfaces on the router matching the VLANs.

6. What two statements are true regarding the use of subinterfaces for inter-VLAN routing? (Choose two.)

   A. Fewer router Ethernet ports required than in traditional inter-VLAN routing
   B. Less complex physical connection than in traditional inter-VLAN routing
   C. More switch ports required than in traditional inter-VLAN routing
   D. Simpler Layer 3 troubleshooting than with traditional inter-VLAN routing
   E. Subinterfaces have no contention for bandwidth

7. Which router-on-a-stick command and prompt on R1 correctly encapsulates 802.1Q traffic for VLAN 20?

   A. R1(config-if)# **encapsulation 802.1q 20**
   B. R1(config-if)# **encapsulation dot1q 20**
   C. R1(config-subif)# **encapsulation 802.1q 20**
   D. R1(config-subif)# **encapsulation dot1q 20**

8. What are two disadvantages of using the router-on-a-stick inter-VLAN routing method in a large network? (Choose two.)

   A. A dedicated router is required.
   B. It does not scale well.
   C. It requires multiple physical interfaces on a router.
   D. It requires subinterfaces to be configured on the same subnets.
   E. Multiple SVIs are needed.

9. What is a characteristic of a routed port on a Layer 3 switch? (Choose two.)

   A. It requires the **switchport mode access interface** config command.
   B. It requires the **no switchport interface** config command.
   C. It requires the **switchport access vlan** *vlan-id* interface config command.
   D. It supports trunking.

10. What are two advantages of using a Layer 3 switch with SVIs for inter-VLAN routing? (Choose two.)

A. A router is not required.

B. It switches packets faster than using the router-on-a-stick method.

C. SVIs can be bundled into EtherChannels.

D. SVIs can be divided using subinterfaces.

E. SVIs eliminate the need for a default gateway in the hosts.

Index

SYMBOLS

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Y

Z