



LAN Switching and Wireless

CCNA Exploration Labs and Study Guide

Allan Johnson

LAN Switching and Wireless

CCNA Exploration Labs and Study Guide

Allan Johnson

Copyright© 2008 Cisco Systems, Inc.

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

First Printing April 2008

Library of Congress Cataloging-in-Publication Data:

Johnson, Allan, 1962-

LAN switching and wireless : CCNA exploration labs and study guide /

Allan Johnson.

p. cm.

ISBN-13: 978-1-58713-202-5 (pbk.)

ISBN-10: 1-58713-202-8 (pbk.)

1. Wireless LANs—Examinations—Study guides.
2. Packet switching—Examinations—Study guides.
3. Telecommunications engineers—Certification—Examinations—Study guides.
4. Routing (Computer network management)—Examinations—Study guides.
5. Telecommunication—Switching systems Examinations—Study guides. I.

Title.

TK5105.78.J64 2008

004.6'8—dc22

2008014858

ISBN-13: 978-1-58713-202-5

ISBN-10: 1-58713-202-8

Publisher

Paul Boger

Associate Publisher

Dave Dusthimer

Cisco Representative

Anthony Wolfenden

Cisco Press Program Manager

Jeff Brady

Executive Editor

Mary Beth Ray

Production Manager

Patrick Kanouse

Development Editor

Andrew Cupp

Senior Project Editor

Tonya Simpson

Copy Editor

Bill McManus

Technical Editors

Bruce R. Gottwig

Khalid Rubayi

Tara Skibar

Linda C. Watson

Editorial Assistant

Vanessa Evans

Book and Cover Designer

Louisa Adair

Composition

Mark Shirar

Proofreader

Leslie Joseph

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

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



Introduction

The Cisco Networking Academy is a comprehensive e-learning program that provides students with Internet technology skills. A Networking Academy delivers web-based content, online assessment, student performance tracking, and hands-on labs to prepare students for industry-standard certifications. The CCNA curriculum includes four courses oriented around the topics on the Cisco Certified Network Associate (CCNA) certification.

LAN Switching and Wireless, CCNA Exploration Labs and Study Guide is a supplement to your classroom and laboratory experience with the Cisco Networking Academy. In order to be successful on the exam and achieve your CCNA certification, you should do everything in your power to arm yourself with a variety of tools and training materials to support your learning efforts. This Labs and Study Guide is just such a collection of tools. Used to its fullest extent, it will help you gain the knowledge and practice the skills associated with the content area of the CCNA Exploration LAN Switching and Wireless course. Specifically, this book will help you work on these main areas:

- LAN design principles and concepts
- Ethernet operation with switches
- Basic switch configuration and security
- VLAN concepts and configuration
- VTP concepts and configuration
- STP, RSTP, and rapid PVST+ concepts and configuration
- Inter-VLAN routing concepts and configuration
- LAN wireless concepts and security issues
- LAN wireless configuration using Linksys WRT300N routers
- Troubleshooting LAN switching and wireless configurations

Labs and Study Guides similar to this one are also available for the other three courses: *Network Fundamentals, CCNA Exploration Labs and Study Guide, Routing Protocols and Concepts, CCNA Exploration Labs and Study Guide*, and *Accessing the WAN, CCNA Exploration Labs and Study Guide*.

Audience for This Book

This book's main audience is anyone taking the *CCNA Exploration LAN Switching and Wireless course* of the Cisco Networking Academy curriculum. Many Academies use this book as a required tool in the course, while other Academies recommend the Labs and Study Guides as an additional source of study and practice materials.

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

Goals and Methods

The most important goal of this book is to help you pass the CCNA exam (640-802). Passing this foundation exam means that you not only have the required knowledge of the technologies covered by the exam, but that you can plan, design, implement, operate, and troubleshoot these technologies. In other words, these exams are rigorously application based. You can view the exam topics any time at <http://www.cisco.com/go/certifications>. The topics are divided into eight categories:

- Describe how a network works
- Configure, verify, and troubleshoot a switch with VLANs and inter-switch communications
- Implement an IP addressing scheme and IP services to meet network requirements in a medium-sized enterprise branch office network
- Configure, verify, and troubleshoot basic router operation and routing on Cisco devices
- Explain and select the appropriate administrative tasks required for a WLAN
- Identify security threats to a network and describe general methods to mitigate those threats
- Implement, verify, and troubleshoot NAT and ACLs in a medium-sized enterprise branch office network
- Implement and verify WAN links

The LAN Switching and Wireless course focuses on the second, fifth, and sixth bullets.

The Study Guide portion of each chapter offers exercises that help you learn the LAN switching and wireless concepts as well as the configurations crucial to your success as a CCNA exam candidate. Each chapter is slightly different and includes some or all of the following types of exercises:

- Vocabulary matching and completion
- Skill-building activities and scenarios
- Configuration scenarios
- Concept questions
- Internet research



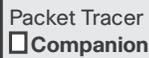
In the configuration chapters, you'll find many Packet Tracer Activities that work with the Cisco Packet Tracer tool. Packet Tracer allows you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available in this book's CD-ROM; Packet Tracer software, however, is available through the Academy Connection website. Ask your instructor for access to Packet Tracer.

The Labs and Activities portion of each chapter includes a Command Reference table, all the online Curriculum Labs, and a Packet Tracer Skills Integration Challenge Activity. The Curriculum Labs are divided into three categories:

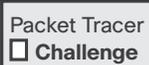
- **Basic:** The Basic Labs are procedural in nature and assume you have no experience configuring the technologies that are the topic of the lab.
- **Challenge:** The Challenge Labs are implementation in nature and assume you have a firm enough grasp on the technologies to "go it alone." These labs often only give you a general requirement that you must implement fully without the details of each small step. In other words, you must use the knowledge and skills you gained in the chapter text, activities, and Basic Lab to successfully complete the Challenge Labs. Avoid the temptation to work through

the Challenge Lab by flipping back through the Basic Lab when you are not sure of a command. Do not try to short-circuit your CCNA training. You need a deep understanding CCNA knowledge and skills to ultimately be successful on the CCNA exam.

- **Troubleshooting:** The Troubleshooting Labs will ask you to fix a broken network. These labs include corrupted scripts you purposefully load onto the routers. Then you use troubleshooting techniques to isolate problems and implement a solution. By the end of the lab, you should have a functional network with full end-to-end connectivity.



Most of the hands-on labs include Packet Tracer Companion Activities where you can use Packet Tracer to complete a simulation of the lab.



Each chapter also includes a culminating activity called the Packet Tracer Skills Integration Challenge. These activities require you to pull together several skills learned from the chapter—and from previous chapters and courses—to successfully complete one comprehensive exercise.

A Word About Packet Tracer

Packet Tracer is a self-paced, visual, interactive teaching and learning tool developed by Cisco. Lab activities are an important part of networking education. However, lab equipment can be a scarce resource. Packet Tracer provides a visual simulation of equipment and network processes to offset the challenge of limited equipment. Students can spend as much time as they like completing standard lab exercises through Packet Tracer, and have the option to work from home. Although Packet Tracer is not a substitute for real equipment, it allows students to practice using a command-line interface. This “e-doing” capability is a fundamental component of learning how to configure routers and switches from the command line.

Packet Tracer v4.x is available only to Cisco Networking Academies through the Academy Connection website.

How This Book Is Organized

Because the content of *LAN Switching and Wireless*, *CCNA Exploration Companion Guide* and the online curriculum is sequential, you should work through this Labs and Study Guide in order beginning with Chapter 1.

The book covers the major topic headings in the same sequence as the online curriculum for the *CCNA Exploration LAN Switching and Wireless course*. This book has seven chapters, with the same numbers and names as the online course chapters.

If necessary, a chapter uses a single topology for the exercises in the Study Guide portion. The single topology per chapter allows for better continuity and easier understanding of switching commands, operations, and outputs. However, the topology is different from the one used in the online curriculum and the *Companion Guide*. A different topology affords you the opportunity to practice your knowledge and skills without just simply recording the information you find in the text.

- **Chapter 1, “LAN Design”:** The exercises in the Study Guide portion focus on LAN design concepts, including vocabulary and the three-layer hierarchical model. The Labs and Activities portion includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.
- **Chapter 2, “Basic Switch Concepts and Configuration”:** The exercises in the Study Guide portion help you understand basic Ethernet and switching concepts, including building the MAC address table and collision and broadcast domains. Then, the Packet Tracer exercises

cover, in detail, how to configure a switch, including basic switch management and configuring switch security. The Labs and Activities portion includes two Basic Labs, a Challenge Lab, and a Packet Tracer Skills Integration Challenge activity.

- **Chapter 3, “VLANs”:** The exercises in the Study Guide portion focus on the concepts of VLANs, including benefits of VLANs and types of VLANs. The exercises then cover VLAN trunking concepts before moving into a section devoted to a VLAN and trunk configuration Packet Tracer exercise. The Labs and Activities portion includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.
- **Chapter 4, “VTP”:** The exercises in the Study Guide portion are devoted to VTP concepts and configuration, including vocabulary, VTP modes, an Internet research exercise, and a VTP Packet Tracer exercise. The Labs and Activities portion includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.
- **Chapter 5, “STP”:** The exercises in the Study Guide portion focus on the concept of redundant LAN topologies, using STP and its variants to stop loops, and the commands to manipulate root bridge elections. The Labs and Activities portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.
- **Chapter 6, “Inter-VLAN Routing”:** This short chapter focuses on how to configure inter-VLAN routing, including two Packet Tracer exercises. The Labs and Activities portion includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.
- **Chapter 7, “Basic Wireless Concepts and Configuration”:** The exercises in the Study Guide portion begin with wireless LAN concepts, including standards, operation, and security. The exercises then cover wireless configuration for LAN access using a Linksys WRT300N, including a Packet Tracer exercise. The Labs and Activities portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.

About the CD-ROM

Packet Tracer
 Activity

The CD-ROM included with this book has all the Packet Tracer Activity, Packet Tracer Companion, and Packet Tracer Challenge files that are referenced throughout the book, indicated by the Packet Tracer Activity, Packet Tracer Companion, and Packet Tracer Challenge icons.

Packet Tracer
 Companion

Updates to these files can be obtained from the website for this book at <http://www.ciscopress.com/title/1587132028>. The files will be updated to cover any subsequent releases of Packet Tracer.

Packet Tracer
 Challenge

About the Cisco Press Website for This Book

Cisco Press may provide additional content that can be accessed by registering your individual book at the [Ciscopress.com](http://www.ciscopress.com) website. Becoming a member and registering is free, and you then gain access to exclusive deals on other resources from Cisco Press.

To register this book, go to www.ciscopress.com/bookstore/register.asp and log into your account or create a free account if you do not have one already. Then enter the ISBN located on the back cover of this book.

After you register the book, it will appear on your Account page under Registered Products and you can access any online material from there.

Inter-VLAN Routing

Now that you have a network with many different VLANs, the next question is, “How do you permit devices on separate VLANs to communicate?” The exercises in this chapter review the concepts of inter-VLAN routing and how it is used to permit devices on separate VLANs to communicate.

The Study Guide portion of this chapter uses a combination of fill-in-the-blank, open-ended question, and Packet Tracer exercises to test your knowledge of inter-VLAN routing concepts and configurations.

The Labs and Activities portion of this chapter includes all the online curriculum labs to ensure that you have mastered the hands-on skills needed to understand inter-VLAN routing concepts and configuration.

As you work through this chapter, use Chapter 6 in *LAN Switching and Wireless, CCNA Exploration Companion Guide* or use the corresponding Chapter 6 in the Exploration LAN Switching and Wireless online curriculum for assistance.

Study Guide

Inter-VLAN Routing

The exercise in this section covers what inter-VLAN routing is and some of the different ways to accomplish inter-VLAN routing on a network.

Inter-VLAN Routing Concepts Exercise

Introducing Inter-VLAN Routing

Define inter-VLAN routing:

Briefly explain traditional inter-VLAN routing:

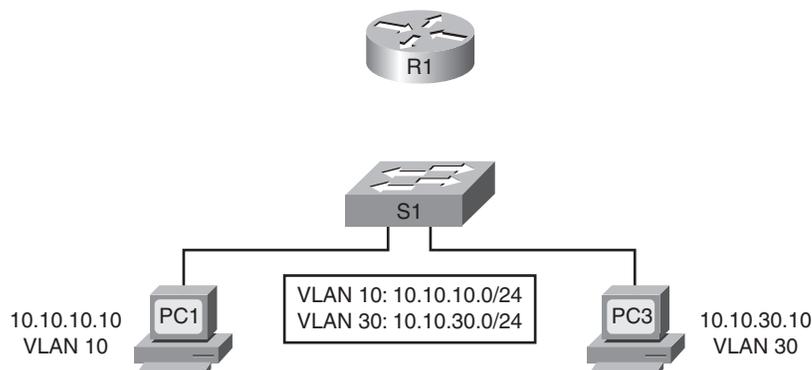
Briefly explain “router-on-a-stick” inter-VLAN routing:

What are subinterfaces?

Interfaces and Subinterfaces

In Figure 6-1, PC1 and PC3 need connectivity between each other. However, each is on a different VLAN. Assume S1 is already configured for traditional inter-VLAN routing. In Figure 6-1, connect S1 and R1 and label the interfaces. Then record the commands to configure R1 with traditional inter-VLAN routing. Use the first available IP addresses in each VLAN for the router interfaces.

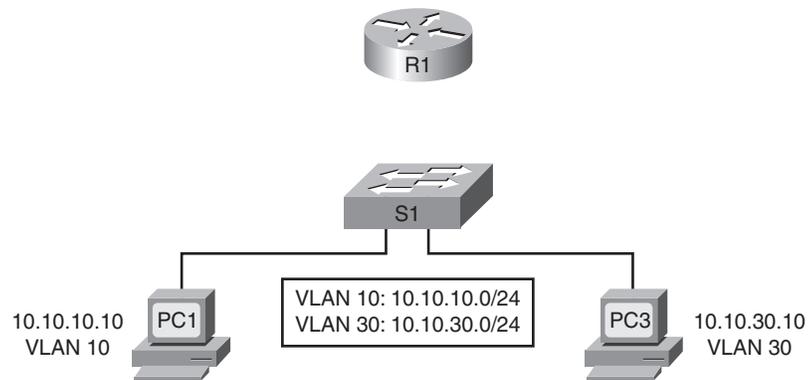
Figure 6-1 Traditional Inter-VLAN Routing Configuration



In the following lines, record the commands to configure R1 with traditional inter-VLAN routing:

In Figure 6-2, PC1 and PC3 need connectivity between each other. However, each is on a different VLAN. Assume S1 is already configured for router-on-a-stick inter-VLAN routing. In Figure 6-2, connect S1 and R1 and label the interfaces. Then record the commands to configure R1 with router-on-a-stick inter-VLAN routing. Use the first available IP addresses in each VLAN for the router interfaces.

Figure 6-2 Router-on-a-Stick Inter-VLAN Routing Configuration



In the following lines, record the commands to configure R1 with router-on-a-stick inter-VLAN routing:

Complete Table 6-1, which compares the characteristics of configuring traditional inter-VLAN routing with router-on-a-stick inter-VLAN routing.

Table 6-1 Comparing Traditional and Router-on-a-Stick Inter-VLAN Routing Characteristics

Characteristic	Traditional	Router-on-a-Stick
Physical interfaces		
Bandwidth		
Switch port configuration		

continues

Table 6-1 Comparing Traditional and Router-on-a-Stick Inter-VLAN Routing Characteristics *continued*

Characteristic	Traditional	Router-on-a-Stick
Expense		
Physical complexity		

Configuring Inter-VLAN Routing

The exercises in this section cover how to configure inter-VLAN routing and review the commands to configure a switch to support inter-VLAN routing.

Inter-VLAN Routing Configuration Exercise

Figure 6-3 shows two topologies. One topology is using traditional inter-VLAN routing and the other topology is using router-on-a-stick inter-VLAN routing. The addressing for both topologies is shown in Table 6-2. For this exercise, you will not configure a separate management or native VLAN.

Figure 6-3 Inter-VLAN Routing Configuration Topology

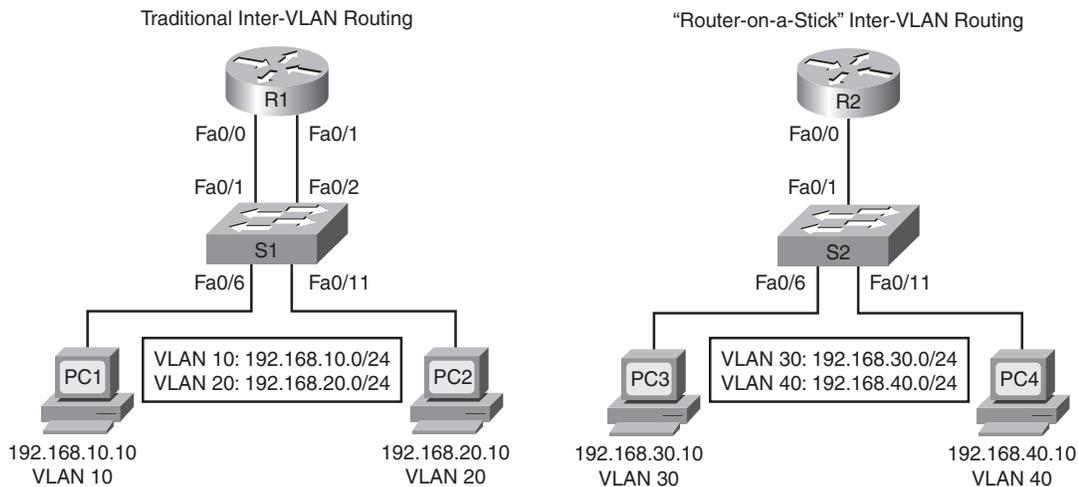


Table 6-2 Addressing Table for Inter-VLAN Routing Configuration Exercise

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.10.1	255.255.255.0	—
	Fa0/1	192.168.20.1	255.255.255.0	—
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.20.10	255.255.255.0	192.168.20.10
R2	Fa0/0.30	192.168.30.1	255.255.255.0	—
	Fa0/0.40	192.168.40.1	255.255.255.0	—
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1
PC4	NIC	192.168.40.10	255.255.255.0	192.168.40.1

Enter the commands, including the router prompt, to configure R1 for traditional inter-VLAN routing:

Enter the commands, including the switch prompt, to configure S1 to forward VLAN traffic. Assume the VLANs are already created in the VLAN database. However, VLANs have not yet been assigned to any ports.

Enter the commands, including the router prompt, to configure R2 for router-on-a-stick inter-VLAN routing:

Enter the commands, including the switch prompt, to configure S2 to forward VLAN traffic. Assume the VLANs are already created in the VLAN database. However, VLANs have not yet been assigned to any ports.



Packet Tracer Exercise 6-1: Inter-VLAN Configuration

Now you are ready to use Packet Tracer to apply your answers to the “Inter-VLAN Routing Configuration Exercise.” Open file LSG03-0601.pka on the CD-ROM that accompanies this book to perform this exercise using Packet Tracer.

Note: The following instructions are also contained within the Packet Tracer Exercise.

Learning Objectives

Upon completion of this Packet Tracer Exercise, you will be able to

- Configure traditional inter-VLAN routing
- Configure router-on-a-stick inter-VLAN routing
- Verify connectivity
- Save the Packet Tracer file

Scenario

In this exercise, you will practice configuring both traditional and router-on-a-stick inter-VLAN routing. The routers and switches have a basic configuration. The passwords are **cisco** for user EXEC mode and **class** for privileged EXEC mode. Use your answers from the “Inter-VLAN Routing Configuration Exercise” to complete the tasks.

Task 1: Configure Traditional Inter-VLAN Routing

- Step 1.** Configure R1 for traditional inter-VLAN routing.
- Step 2.** Configure S1 to forward VLAN traffic.
- Step 3.** Your completion percentage should be 53 percent. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure Router-on-a-Stick Inter-VLAN Routing

- Step 1.** Configure R2 for router-on-a-stick inter-VLAN routing.
- Step 2.** Configure S2 to forward VLAN traffic.
- Step 3.** Your completion percentage should be 100 percent. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Verify Connectivity

PC1 should be able to ping PC2. PC3 should be able to ping PC4. Alternatively, you can click **Check Results** and then the **Connectivity Tests** tab. The status of both connectivity tests should be listed as “Correct.”

Task 4: Save the Packet Tracer File

Save your Packet Tracer file as LSG03-0601-end.pka.

Troubleshooting Inter-VLAN Routing

The exercises in this section explore common issues and troubleshooting methods to identify and correct problems in inter-VLAN routing implementations.

Common Errors and Troubleshooting Tools Exercise

Using the examples shown in the chapter, list at least six common errors in the inter-VLAN routing implementations.

Switch Configuration Issues:

- _____
- _____
- _____

Router Configuration Issues:

- _____
- _____

IP Addressing Issues:

- _____
- _____
- _____

What are some useful commands you can use to isolate problems in an inter-VLAN routing network?

Switch IOS Commands:

- _____
- _____

Router IOS Commands:

- _____
- _____

PC Commands:

- _____

Packet Tracer
Activity

Packet Tracer Exercise 6-2: Troubleshooting Inter-VLAN Routing

Now you are ready to use Packet Tracer to apply your knowledge of troubleshooting techniques. Open file LSG03-0602.pka on the CD-ROM that accompanies this book to perform this exercise using Packet Tracer.

Note: The following instructions are also contained within the Packet Tracer Exercise.

Learning Objectives

Upon completion of this Packet Tracer Exercise, you will be able to

- Test connectivity between the PCs and the router
- Gather data on the problems
- Implement solutions and test connectivity

Scenario

In this exercise, you will practice troubleshooting both traditional and router-on-a-stick inter-VLAN routing. The routers, switches, and PCs are already configured and are using the IP addresses listed in Table 6-2. You cannot access the routers or switches directly. Instead, you must use the available console connections through the PCs. The passwords are **cisco** for user EXEC mode and **class** for privileged EXEC mode. Use connectivity tests and **show** commands to discover problems and troubleshoot the networks. The exercise is complete when you achieve 100 percent and the two PCs on each network can ping each other.

Task 1: Configure Traditional Inter-VLAN Routing

The following tests should be successful at the conclusion of this activity:

- PC1 can ping R1.
- PC2 can ping R1.
- PC1 can ping PC2.
- PC3 can ping R2.
- PC4 can ping R2.
- PC3 can ping PC4.

Each of these tests should fail on the first attempt.

Task 2: Gather Data on the Problems

Step 1. Verify the configuration on the PCs.

Are the following configurations for each PC correct?

- IP address
 - Subnet mask
 - Default gateway
-

Step 2. Verify the configuration on the switches.

Are the configurations on the switches correct? Be sure to verify the following:

- Ports assigned to the correct VLANs
 - Ports configured for the correct mode
 - Ports connected to the correct device
-
-

Step 3. Verify the configuration on the routers.

Are the configurations on the routers correct? Be sure to verify the following:

- IP addresses
 - Interface status
 - Encapsulation and VLAN assignment
-
-

Step 4. Document the problems and suggest solutions.

What are the reasons connectivity failed between the PCs? What are the solutions? There could be more than one problem and more than one solution. All solutions must conform to the topology diagram in Figure 6-3 and the addressing in Table 6-2.

List the problems, if any, and the solutions for the PCs:

List the problems, if any, and the solutions for the switches:

List the problems, if any, and the solutions for routers:

Task 3: Implement the Solution and Test Connectivity

Step 1. Make changes according to the suggested solutions in Task 2.

Note: If you make changes to the switch configuration, you should make the changes in Realtime mode rather than Simulation mode. This is necessary so that the switch port will proceed to the forwarding state.

Step 2. Test connectivity between PCs and R1.

If you change any IP configurations, you should create new pings because the prior pings use the old IP address:

- PC1 should be able to ping R1.
- PC2 should be able to ping R1.

- PC1 should be able to ping PC2.
- PC3 should be able to ping R2.
- PC4 should be able to ping R2.
- PC3 should be able to ping PC4.

If any pings fail, return to Task 2 to continue troubleshooting.

Step 3. Check results.

Your completion percentage should be 100 percent. If not, return to Step 1 and continue to implement your suggested solutions. You will not be able to click **Check Results** and see which required components are not yet completed. However, you can click **Check Results** and then the **Connectivity Tests** tab. The status of all six connectivity tests should be listed as “Correct.”

Task 4: Save the Packet Tracer File

Save your Packet Tracer file as LSG03-0602-end.pka.

Labs and Activities

Command Reference

In Table 6-3, record the command, *including the correct prompt*, that fits the description. Fill in any blanks with the appropriate missing information.

Table 6-3 Commands for Inter-VLAN Routing Configuration

Command	Description
	Creates a subinterface numbered 10 on the router for Fa0/0
	Specifies IEEE 801.1Q as the VLAN tagging method for VLAN 10 on this subinterface



Lab 6-1: Basic Inter-VLAN Routing (6.4.1)

Learning Objectives

Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram in Figure 6-4
- Clear configurations and reload a switch and a router to the default state
- Perform basic configuration tasks on a switched LAN and router
- Configure VLANs and VLAN Trunking Protocol (VTP) on all switches
- Demonstrate and explain the impact of Layer 3 boundaries imposed by creating VLANs
- Configure a router to support 802.1Q trunking on a Fast Ethernet interface
- Configure a router with subinterfaces corresponding to the configured VLANs
- Demonstrate and explain inter-VLAN routing

Figure 6-4 shows the topology diagram for this lab.

Figure 6-4 Topology Diagram for Lab 6-1

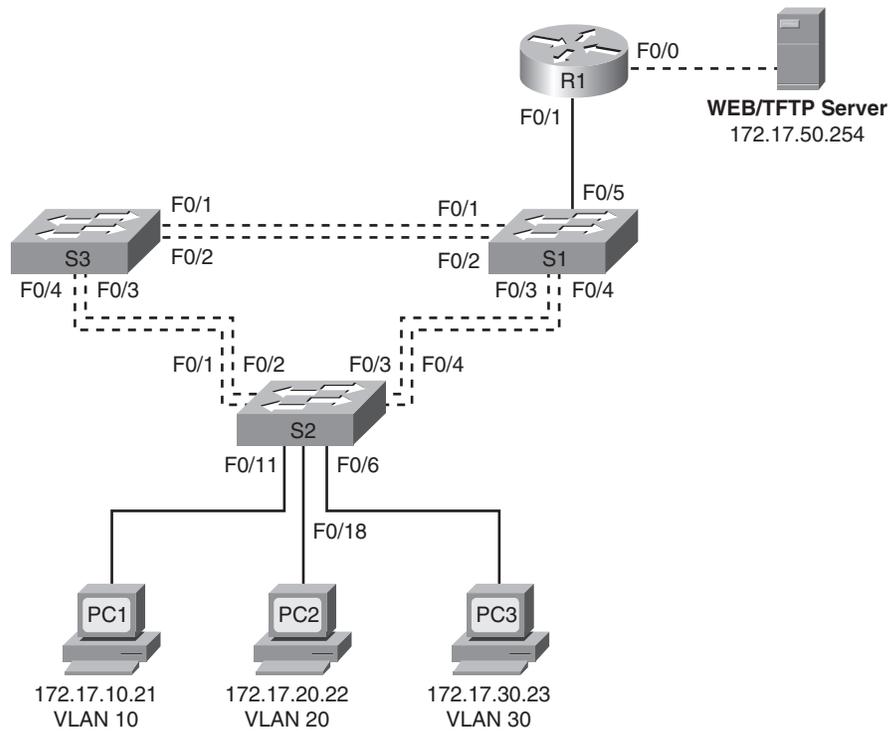


Table 6-4 shows the addressing scheme used in this lab.

Table 6-4 Addressing Table for Lab 6-1

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.17.50.1	255.255.255.0	—
	Fa0/1.1	172.17.1.1	255.255.255.0	—
	Fa0/1.10	172.17.10.1	255.255.255.0	—
	Fa0/1.20	172.17.20.1	255.255.255.0	—
	Fa0/1.30	172.17.30.1	255.255.255.0	—
	Fa0/1.99	172.17.99.1	255.255.255.0	—
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
S3	VLAN 99	172.17.99.13	255.255.255.0	172.17.99.1
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
Web server	NIC	172.17.50.254	255.255.255.0	172.17.50.1

Table 6-5 shows the port assignments used in this lab.

Table 6-5 Port Assignments for S2

Ports	Assignment	Network
Fa0/1–0/4	802.1Q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/5–0/10	VLAN 30—Guest (Default)	172.17.30.0 /24
Fa0/11–0/17	VLAN 10—Faculty/Staff	172.17.10.0 /24
Fa0/18–0/24	VLAN 20—Students	172.17.20.0 /24

Task 1: Prepare the Network

Step 1. Cable a network that is similar to the one shown in Figure 6-4.

You can use any current switch in your lab as long as it has the required interfaces shown in Figure 6-4 and supports 802.1Q encapsulation. The router you choose must support inter-VLAN routing. The output shown in this lab is based on Cisco 2960 switches and an 1841 router. Other switch or router models may produce different output.

Set up console connections to all three switches.

Step 2. Clear any existing configurations on the switches.

Clear NVRAM, delete the `vlan.dat` file, and reload the switches. Refer to “Lab 2-1: Basic Switch Configuration (2.5.1)” if necessary for the procedure. After the reload is complete, use the `show vlan` command to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.

```
S1#show vlan
```

```

VLAN Name                Status    Ports
-----
1    default                  active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, 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
                                           Gig1/1, Gig1/2

1002 fddi-default            active
1003 token-ring-default     active
1004 fddinet-default        active
1005 trnet-default          active

```

Step 3. Disable all ports on the switches using the **shutdown** command.

Ensure that the initial switch port states are inactive by disabling all ports. Use the **interface range** command to simplify this task. Commands for S1 are shown here:

```
S1(config)#interface range fa0/1-24
S1(config-if-range)#shutdown
S1(config-if-range)#interface range gi0/1-2
S1(config-if-range)#shutdown
```

Step 4. Reenable the active user ports on S2 in access mode:

```
S2(config)#interface fa0/6
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/11
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/18
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
```

Task 2: Perform Basic Switch Configurations

Configure the S1, S2, and S3 switches according to the addressing table and the following guidelines:

- Configure the switch hostname.
- Disable DNS lookup.
- Configure an enable secret password of **class**.
- Configure a password of **cisco** for the console connections.
- Configure a password of **cisco** for vty connections.
- Configure the default gateway on each switch.

Only the commands for S1 are shown here:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
S1(config)#ip default-gateway 172.17.99.1
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
```

```
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Task 3: Configure Host PCs

Configure the Ethernet interfaces of PC1, PC2, PC3, and the remote web/TFTP server with the IP addresses in Table 6-4.

Task 4: Configure VTP on the Switches

Step 1. Configure VTP.

Configure VTP on the three switches using the following guidelines:

- S1 is the VTP server; S2 and S3 are VTP clients.
- The VTP domain name is **Lab6**.
- The VTP password is **cisco**.

Remember that VTP domain names and passwords are case sensitive. The default operating mode is server.

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#vtp domain Lab6
Changing VTP domain name from NULL to Lab6
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
```

```
S2(config)#vtp mode client
Setting device to VTP CLIENT mode
S2(config)#vtp domain Lab6
Changing VTP domain name from NULL to Lab6
S2(config)#vtp password cisco
Setting device VLAN database password to cisco
```

```
S3(config)#vtp mode client
Setting device to VTP CLIENT mode
S3(config)#vtp domain Lab6
Changing VTP domain name from NULL to Lab6
S3(config)#vtp password cisco
Setting device VLAN database password to cisco
S3(config)#end
```

Step 2. Configure trunk links and the native VLAN.

For each switch, configure ports Fa0/1 through Fa0/4 as trunking ports. The Fa0/5 port on S1 also needs to be configured as a trunking port because it will trunk to the router, R1. Designate VLAN 99 as the native VLAN for these trunks. Remember to activate the ports.

Only the commands for S1 are shown here:

```
S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
```

Step 3. Configure the VTP server with VLANs.

Configure the following VLANs on the VTP server only:

- VLAN 10: Faculty/Staff
- VLAN 20: Students
- VLAN 30: Guest
- VLAN 99: Management

```
S1(config)#vlan 10
S1(config-vlan)#name faculty/staff
S1(config-vlan)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#end
S1#
```

Step 4. Verify the VLANs.

Verify that all four VLANs have been distributed to the client switches. You should have output similar to the following:

```
S2#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, 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	faculty/staff	active	
20	students	active	
30	guest	active	
99	management	active	

```
S3#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, 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	faculty/staff	active	
20	students	active	
30	guest	active	
99	management	active	

Step 5. Configure the management interface address on all three switches:

```
S1(config)#interface vlan99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
```

```
S2(config)#interface vlan99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown
```

```
S3(config)#interface vlan99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown
```

Verify that the switches are correctly configured by pinging between them. From S1, ping the management interface on S2 and S3. From S2, ping the management interface on S3.

Were the pings successful?

If not, troubleshoot the switch configurations and try again.

Step 6. Assign switch ports to the VLANs.

Assign ports to VLANs on S2 according to Table 6-5 at the beginning of the lab. Activate the ports connected to the PCs.

```
S2(config)#interface range fa0/5-10
S2(config-if-range)#switchport access vlan 30
S2(config-if-range)#interface range fa0/11-17
S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#interface range fa0/18-24
S2(config-if-range)#switchport access vlan 20
S2(config-if-range)#end
S2#
```

Step 7. Check connectivity between VLANs.

Open command windows on the three hosts connected to S2. Ping from PC1 (172.17.10.21) to PC2 (172.17.20.22). Ping from PC2 to PC3 (172.17.30.23).

Are the pings successful?

If not, why do these pings fail?

Task 5: Configure the Router and the Remote Server LAN

Step 1. Clear the configuration on the router and reload.

Step 2. Create a basic configuration on the router:

- Configure the router with hostname R1.
- Disable DNS lookup.
- Configure an EXEC mode password of **cisco**.
- Configure a password of **cisco** for the console connection.
- Configure a password of **cisco** for the vty connections.

Step 3. Configure the trunking interface on R1.

You have demonstrated that connectivity between VLANs requires routing at the network layer, exactly like connectivity between any two remote networks. There are a couple of options for configuring routing between VLANs.

The first is something of a brute-force approach. A Layer 3 device, either a router or a Layer 3-capable switch, is connected to a LAN switch with multiple physical connections—a separate connection for each VLAN that requires inter-VLAN connectivity. Each of the switch ports used by the Layer 3 device is configured in a different VLAN on the switch. After IP addresses are assigned to the interfaces on the Layer 3 device, the routing table has directly connected routes for all VLANs, and inter-VLAN routing is enabled. The limitations to this approach are the lack of sufficient Fast Ethernet ports on routers, underutilization of ports on Layer 3 switches and routers, and excessive wiring and manual configuration. The topology used in this lab does not use this approach.

A better approach is to use one physical Fast Ethernet connection between the Layer 3 device (the router) and the distribution layer switch. This connection is configured as an IEEE 802.1Q trunk to allow all inter-VLAN traffic to be carried to and from the routing device on a single trunk. However, it requires that the Layer 3 interface be configured with multiple IP addresses. This is done by creating “virtual” interfaces, called subinterfaces, on one of the router Fast Ethernet ports. Each subinterface is then configured for 802.1Q encapsulation.

Using the subinterface configuration approach requires these steps:

1. Enter subinterface configuration mode.
2. Establish trunking encapsulation.
3. Associate a VLAN with the subinterface.
4. Assign an IP address from the VLAN to the subinterface.

The commands are as follows:

```
R1(config)#interface fastethernet 0/1
R1(config-if)#no shutdown
R1(config-if)#interface fastethernet 0/1.1
R1(config-subif)#encapsulation dot1q 1
R1(config-subif)#ip address 172.17.1.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/1.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/1.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 172.17.20.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/1.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/1.99
R1(config-subif)#encapsulation dot1q 99 native
R1(config-subif)#ip address 172.17.99.1 255.255.255.0
```

Note the following points highlighted in the preceding configuration:

- The physical interface is enabled using the **no shutdown** command, because router interfaces are down by default. The virtual interfaces are up by default.
- The subinterface can use any number that can be described with 32 bits, but it is good practice to assign the number of the VLAN as the interface number, as has been done here.
- The native VLAN is specified on the Layer 3 device so that it is consistent with the switches. Otherwise, VLAN 1 would be the native VLAN by default, and there would be no communication between the router and the management VLAN on the switches.

Step 4. Configure the server LAN interface on R1:

```
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 172.17.50.1 255.255.255.0
R1(config-if)#description server interface
R1(config-if)#no shutdown
R1(config-if)#end
```

There are now six networks configured. Verify that you can route packets to all six by checking the routing table on R1:

```
R1#show ip route
<output omitted>
```

Gateway of last resort is not set

```

172.17.0.0/24 is subnetted, 6 subnets
C      172.17.50.0 is directly connected, FastEthernet0/0
C      172.17.30.0 is directly connected, FastEthernet0/1.30
C      172.17.20.0 is directly connected, FastEthernet0/1.20
C      172.17.10.0 is directly connected, FastEthernet0/1.10
C      172.17.1.0 is directly connected, FastEthernet0/1.1
C      172.17.99.0 is directly connected, FastEthernet0/1.99

```

If your routing table does not show all six networks, troubleshoot your configuration and resolve the problem before proceeding.

Step 5. Verify inter-VLAN routing.

From PC1, verify that you can ping the remote server (172.17.50.254) and the other two hosts (172.17.20.22 and 172.17.30.23). It may take a couple of pings before the end-to-end path is established.

Are the pings successful?

If not, troubleshoot your configuration. Check to make sure that the default gateways have been set on all PCs and all switches. If any of the hosts have gone into hibernation, the connected interface may go down.

Task 6: Reflection

In Task 5, it was recommended that you configure VLAN 99 as the native VLAN in the router Fa0/0.99 interface configuration. Why would packets from the router or hosts fail when trying to reach the switch management interfaces if the native VLAN were left in default?

Task 7: Document the Switch Configurations

On the router and each switch, capture the running configuration to a text file and save it for future reference. These scripts can be edited to expedite configuring switches in future labs.

Task 8: Clean Up

Unless directed otherwise by your instructor, erase the configurations and reload the router and switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.



Packet Tracer Companion: Basic Inter-VLAN Routing (6.4.1)

You can now open the file LSG03-Lab641.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment.



Lab 6-2: Challenge Inter-VLAN Routing (6.4.2)

Learning Objectives

Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram in Figure 6-5
- Clear configurations and reload a switch and a router to the default state
- Perform basic configuration tasks on a switched LAN and a router
- Configure VLANs and VLAN Trunking Protocol (VTP) on all switches
- Configure a router to support 802.1Q trunking on a Fast Ethernet interface
- Configure a router with subinterfaces corresponding to the configured VLANs
- Demonstrate inter-VLAN routing

Figure 6-5 shows the topology diagram for this lab.

Figure 6-5 Topology Diagram for Lab 6-2

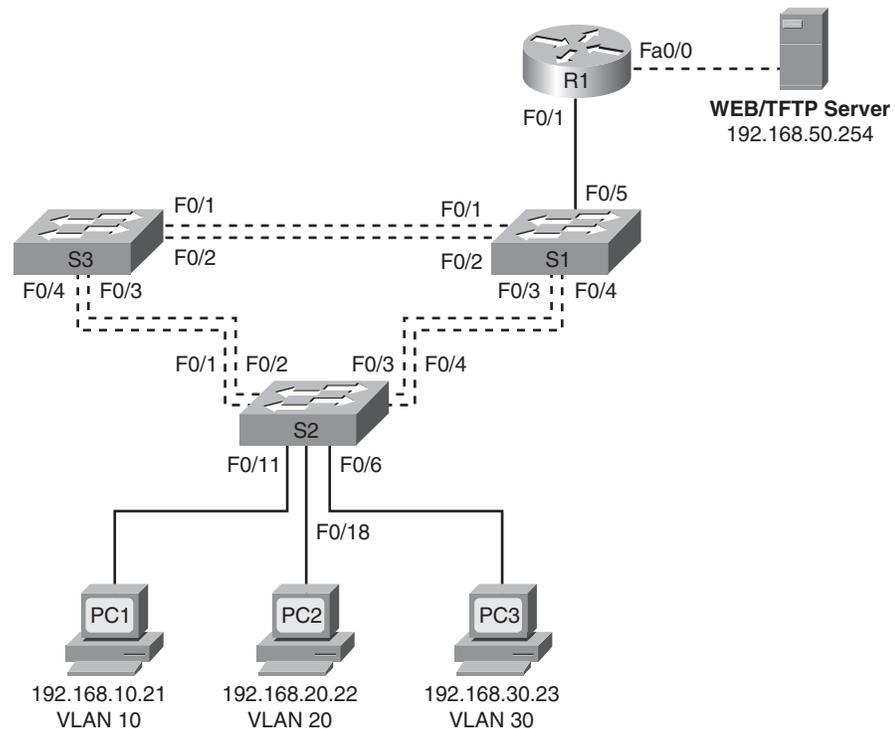


Table 6-6 shows the addressing scheme used in this lab.

Table 6-6 Addressing Table for Lab 6-2

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.50.1	255.255.255.0	—
	Fa0/1.1	192.168.1.1	255.255.255.0	—
	Fa0/1.10	192.168.10.1	255.255.255.0	—
	Fa0/1.20	192.168.20.1	255.255.255.0	—
	Fa0/1.30	192.168.30.1	255.255.255.0	—
	Fa0/1.99	192.168.99.1	255.255.255.0	—
S1	VLAN 99	192.168.99.11	255.255.255.0	192.168.99.1
S2	VLAN 99	192.168.99.12	255.255.255.0	192.168.99.1
S3	VLAN 99	192.168.99.13	255.255.255.0	192.168.99.1
PC1	NIC	192.168.10.21	255.255.255.0	192.168.10.1
PC2	NIC	192.168.20.22	255.255.255.0	192.168.20.1
PC3	NIC	192.168.30.23	255.255.255.0	192.168.30.1
Server	NIC	192.168.50.254	255.255.255.0	192.168.50.1

Table 6-7 shows the port assignments used in this lab.

Table 6-7 Port Assignments for S2

Ports	Assignment	Network
Fa0/1–0/4	802.1Q Trunks (Native VLAN 99)	192.168.99.0 /24
Fa0/5–0/10	VLAN 30—Sales	192.168.30.0 /24
Fa0/11–0/17	VLAN 10—R&D	192.168.10.0 /24
Fa0/18–0/24	VLAN 20—Engineering	192.168.20.0 /24

Task 1: Prepare the Network

- Step 1.** Cable a network that is similar to the one shown in Figure 6-5.
- Step 2.** Clear any existing configurations on the switches, and initialize all ports in the shutdown state.

Task 2: Perform Basic Switch Configurations

- Step 1.** Configure the switches according to the following guidelines:
- Configure the switch hostname.
 - Disable DNS lookup.
 - Configure an EXEC mode password of **class**.

- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Step 2. Reenable the user ports on S2.

Task 3: Configure Host PCs

Configure the PCs. You can complete this lab using only two PCs by simply changing the IP addressing for the two PCs specific to a test you want to conduct. Alternatively, you can configure all three PCs with the IP addresses and default gateways.

Task 4: Configure VTP and VLANs

Step 1. Configure VTP.

Configure VTP on the three switches using the following guidelines:

- S1 is the VTP server; S2 and S3 are VTP clients.
- The VTP domain name is **Lab6**.
- The VTP password is **cisco**.

Remember that VTP domain names and passwords are case sensitive. The default operating mode is server.

Step 2. Configure trunk links and the native VLAN.

For each switch, configure ports Fa0/1 through Fa0/4 as trunking ports. The Fa0/5 port on S1 also needs to be configured as a trunking port because it will trunk to the router, R1. Designate VLAN 99 as the native VLAN for these trunks. Remember to activate the ports.

Step 3. Configure the VTP server with VLANs.

Configure the following VLANs on the VTP server only:

- VLAN 10: R&D
- VLAN 20: Engineering
- VLAN 30: Sales
- VLAN 99: Management

Step 4. Verify the VLANs.

Verify that all four VLANs have been distributed to the client switches. At this point in the lab, all ports should be in VLAN 1. You should have output similar to the following:

S2#show vlan brief

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, 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 R&D active
20 Engineering active
30 Sales active
99 Management active
```

S3#show vlan brief

```
VLAN Name                Status Ports
-----
1    default                active Fa0/1, Fa0/2, Fa0/4, Fa0/5
                                Fa0/6, 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   R&D                    active
20   Engineering            active
30   Sales                  active
99   Management              active
```

Step 5. Configure the management interface address on all three switches.

Verify that the switches are correctly configured by pinging between them. From S1, ping the management interface on S2 and S3. From S2, ping the management interface on S3.

Were the pings successful?

If not, troubleshoot the switch configurations and try again.

Step 6. Assign switch ports to the VLANs.

Assign ports to VLANs on S2 according to Table 6-7 at the beginning of the lab. Activate the ports connected to the PCs.

Step 7. Check connectivity between VLANs.

Open command prompt windows on the three hosts connected to S2. Ping from PC1 (192.168.10.21) to PC2 (192.168.20.22). Ping from PC2 to PC3 (192.168.30.23).

Are the pings successful?

If not, why do these pings fail?

Task 5: Configure the Router

Step 1. Clear the configuration on the router and reload.

Step 2. Create a basic configuration on the router:

- Configure the router with hostname R1.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Step 3. Configure the trunking interface on R1.

Configure the Fa0/1 interface on R1 with five subinterfaces as designated in Table 6-6. Configure these subinterfaces with dot1q encapsulation and assign the correct address. Specify VLAN 99 as the native VLAN on its subinterface. Do not assign an IP address to the physical interface, but be sure to enable it.

Step 4. Configure the server LAN interface on R1.

Refer to Table 6-6 to configure Fa0/0 with the correct IP address and mask.

Step 5. Verify the routing configuration.

At this point, there should be six networks configured on R1. Verify that you can route packets to all six by checking the routing table on R1.

If your routing table does not show all six networks, troubleshoot your configuration and resolve the problem before proceeding.

Step 6. Verify inter-VLAN routing.

From PC1, verify that you can ping the remote server (192.168.50.254) and the other two hosts (192.168.20.22 and 192.168.30.23). It may take a couple of pings before the end-to-end path is established.

Are the pings successful?

If not, troubleshoot your configuration. Check to make sure the default gateways have been set on all PCs and all switches. If any of the hosts have gone into hibernation, the connected interface may go down.

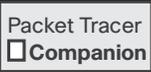
At this point, you should be able to ping any node on any of the six networks configured on your LAN, including the switch management interfaces.

Task 6: Document the Switch Configurations

On the router and each switch, capture the running configuration to a text file and save it for future reference. These scripts can be edited to expedite configuring switches in future labs.

Task 7: Clean Up

Unless directed otherwise by your instructor, erase the configurations and reload the router and switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.



Packet Tracer Companion: Challenge Inter-VLAN Routing (6.4.2)

You can now open the file LSG03-Lab642.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment.



Lab 6-3: Troubleshooting Inter-VLAN Routing (6.4.3)

Learning Objectives

Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram in Figure 6-6
- Erase any existing configurations and reload switches and the router to the default state
- Load the switches and the router with supplied scripts
- Find and correct all configuration errors
- Document the corrected network

Scenario

The network is designed and configured to support five VLANs and a separate server network. Inter-VLAN routing is provided by an external router in a router-on-a-stick configuration. However, the network is not working as designed and complaints from your users do not provide much insight into the source of the problems. You must first define what is not working as expected, and then analyze the existing configurations to determine and correct the source of the problems.

This lab is complete when you can demonstrate IP connectivity between each of the user VLANs and the external server network, and between the switch management VLAN and the server network.

Figure 6-6 shows the topology diagram for this lab.

Figure 6-6 Topology Diagram for Lab 6-3

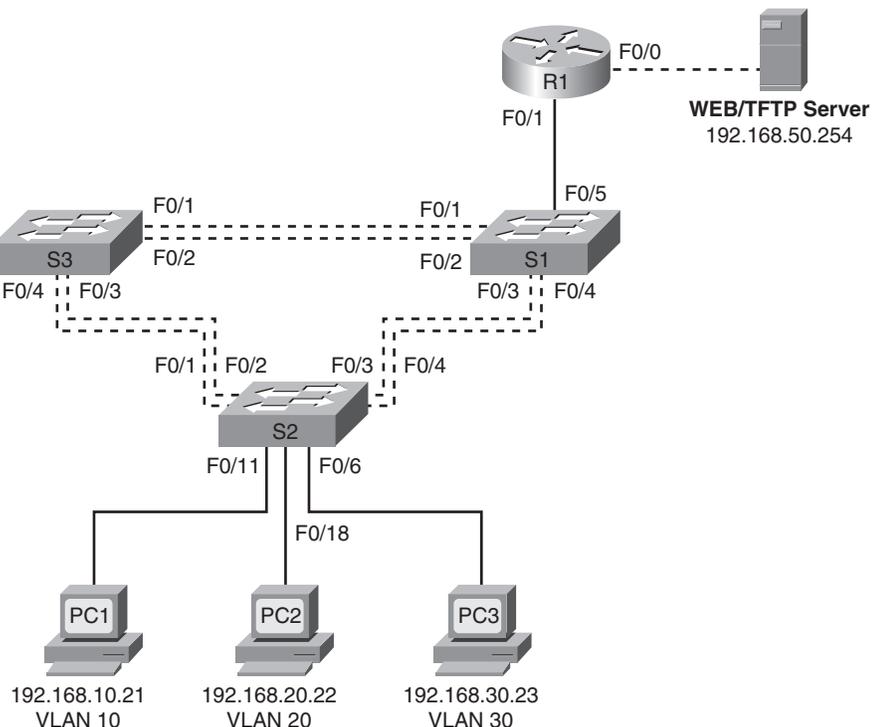


Table 6-8 shows the addressing scheme used in this lab.

Table 6-8 Addressing Table for Lab 6-3

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.50.1	255.255.255.0	—
	Fa0/1.1	192.168.1.1	255.255.255.0	—
	Fa0/1.10	192.168.10.1	255.255.255.0	—
	Fa0/1.20	192.168.20.1	255.255.255.0	—
	Fa0/1.30	192.168.30.1	255.255.255.0	—
	Fa0/1.99	192.168.99.1	255.255.255.0	—
S1	VLAN 99	192.168.99.11	255.255.255.0	192.168.99.1
S2	VLAN 99	192.168.99.12	255.255.255.0	192.168.99.1
S3	VLAN 99	192.168.99.13	255.255.255.0	192.168.99.1
PC1	NIC	192.168.10.21	255.255.255.0	192.168.10.1
PC2	NIC	192.168.20.22	255.255.255.0	192.168.20.1
PC3	NIC	192.168.30.23	255.255.255.0	192.168.30.1
Server	NIC	192.168.50.254	255.255.255.0	192.168.50.1

Table 6-9 shows the port assignments used in this lab.

Table 6-9 Port Assignments for S2

Ports	Assignment	Network
Fa0/1–0/4	802.1Q Trunks (Native VLAN 99)	192.168.99.0 /24
Fa0/5–0/10	VLAN 30—Sales	192.168.30.0 /24
Fa0/11–0/17	VLAN 10—R&D	192.168.10.0 /24
Fa0/18–0/24	VLAN 20—Engineering	192.168.20.0 /24

Task 1: Prepare the Network

- Step 1.** Cable a network that is similar to the one shown in Figure 6-6.
- Step 2.** Clear any existing configurations on the router and switches.
- Step 3.** Configure the Ethernet interfaces on the host PCs and the server.
- Step 4.** Apply the following configurations to the router and each switch. Alternatively, you can open the file LSG03-Lab643-Scripts.txt on the CD-ROM that accompanies this book and copy in the scripts for each of the switches.

R1 Configuration

```
hostname R1
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 192.168.50.1 255.255.255.192
!
interface FastEthernet0/1
 no ip address
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1
 ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/1.10
 encapsulation dot1Q 11
 ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
!
interface FastEthernet0/1.30
 ip address 192.168.30.1 255.255.255.0
!
interface FastEthernet0/1.99
 encapsulation dot1Q 99 native
 ip address 192.168.99.1 255.255.255.0
!
line con 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
!
end
```

S1 Configuration

```
hostname S1
!
```

```

vtp mode server
vtp domain lab6_3
vtp password cisco
!
vlan 99
name Management
vlan 10
name R&D
vlan 30
name Sales
exit
!
interface FastEthernet0/1
  switchport trunk native vlan 99
  switchport mode trunk
  no shutdown
!
interface FastEthernet0/2
  switchport trunk native vlan 99
  switchport mode trunk
  no shutdown
!
interface FastEthernet0/3
  switchport trunk native vlan 99
  switchport mode trunk
  no shutdown
!
interface FastEthernet0/4
  switchport trunk native vlan 99
  switchport mode trunk
  no shutdown
!
!
interface range FastEthernet0/5 - 24
  shutdown
!
interface Vlan99
  ip address 192.168.99.11 255.255.255.0
  no shutdown
!
exit
!
ip default-gateway 192.168.99.1
!
```

```
line con 0
  logging synchronous
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
line vty 5 15
  password cisco
  login
!
end
```

S2 Configuration

```
!
hostname S2
no ip domain-lookup
enable secret class
!
vtp mode client
vtp domain lab6_3
vtp password cisco
!
interface FastEthernet0/1
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/2
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/3
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/4
  switchport trunk native vlan 99
  switchport mode trunk
!
interface range FastEthernet0/5 - 11
  switchport access vlan 30
  switchport mode access
```

```
!  
interface range FastEthernet0/12 - 17  
  switchport access vlan 10  
!  
interface range FastEthernet0/18 -24  
  switchport mode access  
  switchport access vlan 20  
!  
interface Vlan99  
  ip address 192.168.99.12 255.255.255.0  
  no shutdown  
!  
ip default-gateway 192.168.99.1  
!  
line con 0  
  password cisco  
  logging synchronous  
  login  
line vty 0 4  
  password cisco  
  login  
line vty 5 15  
  password cisco  
  login  
!  
end
```

S3 Configuration

```
!  
hostname S3  
!  
enable secret class  
!  
vtp mode client  
vtp domain lab6_3  
vtp password cisco  
!  
interface FastEthernet0/1  
  switchport trunk native vlan 99  
  switchport mode trunk  
  no shutdown  
!
```

```
interface FastEthernet0/2
  switchport trunk native vlan 99
  switchport mode trunk
  no shutdown
!
interface FastEthernet0/3
  switchport trunk native vlan 99
  switchport mode trunk
  no shutdown
!
interface FastEthernet0/4
  switchport trunk native vlan 99
  switchport mode trunk
  no shutdown
!
interface range FastEthernet0/5 - 24
  shutdown
  exit
!
!
ip default-gateway 192.168.99.1
!
line con 0
  logging synchronous
  password cisco
  login
!
line vty 0 4
  password cisco
  login
!
line vty 5 15
  password cisco
  login
!
end
```

Task 2: Troubleshoot and Correct the Inter-VLAN Configuration

The following is a suggested method for approaching the connectivity problems in the network:

Step 1. Evaluate any console messages.

When pasting or typing in the scripts, did you get any console messages from the system?
If so, what were they and what is the solution?

Step 2. Test and establish connectivity between devices.

When all errors are corrected, you should be able to freely ping and telnet between R1, S1, S2, and S3. PCs should be able to ping each other and the server.

Do you have connectivity between any of the devices?

If yes, which ones?

Step 3. Investigate connectivity issues between the devices and implement solutions. Document the results of your investigation and the solutions you implemented.

Packet Tracer
Companion

Packet Tracer Companion: Troubleshooting Inter-VLAN Routing (6.4.3)

You can now open the file LSG03-Lab643.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment.

Packet Tracer
Challenge

Packet Tracer Skills Integration Challenge

Open the file LSG03-PTSkills6.pka on the CD-ROM that accompanies this book. You will use the topology in Figure 6-7 and the addressing table in Table 6-10 to document your design.

Figure 6-7 Packet Tracer Skills Integration Challenge Topology

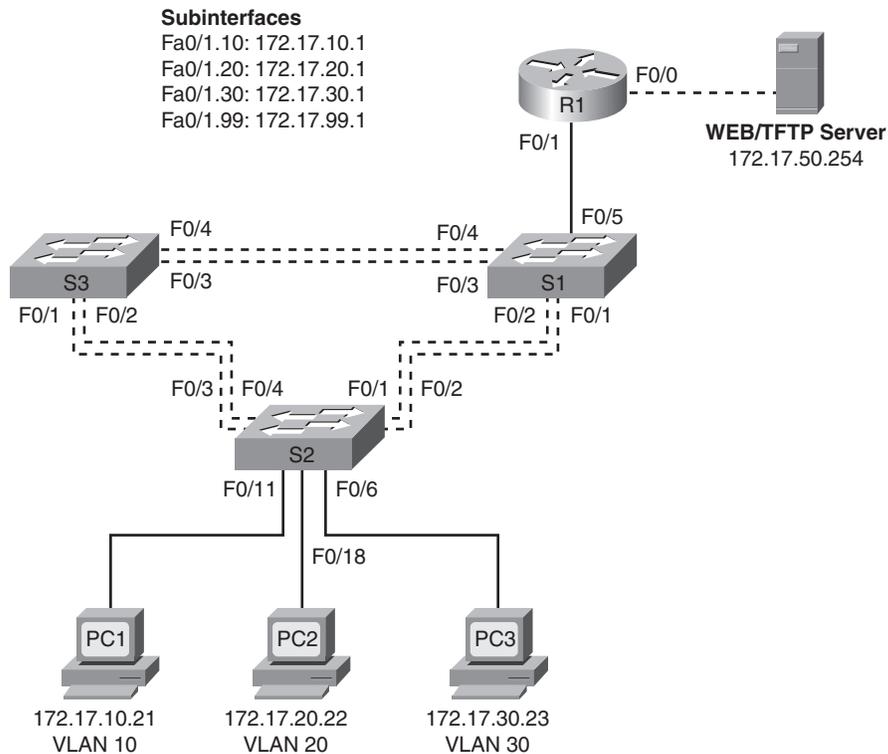


Table 6-10 Addressing Table for the Packet Tracer Skills Integration Challenge Activity

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.17.50.1	255.255.255.0	—
	Fa0/1.10	172.17.10.1	255.255.255.0	—
	Fa0/1.20	172.17.20.1	255.255.255.0	—
	Fa0/1.30	172.17.30.1	255.255.255.0	—
	Fa0/1.99	172.17.99.1	255.255.255.0	—
S1	VLAN 99	172.17.99.31	255.255.255.0	172.17.99.1

Table 6-10 Addressing Table for the Packet Tracer Skills Integration Challenge Activity *continued*

Device	Interface	IP Address	Subnet Mask	Default Gateway
S2	VLAN 99	172.17.99.32	255.255.255.0	172.17.99.1
S3	VLAN 99	172.17.99.33	255.255.255.0	172.17.99.1
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1

Learning Objectives

Upon completion of this lab, you will be able to

- Configure and verify basic device configurations
- Configure VTP
- Configure trunking
- Configure VLANs
- Assign VLANs to ports
- Configure STP
- Configure router-on-a-stick Inter-VLAN routing
- Verify end-to-end connectivity

Introduction

In this activity, you will demonstrate and reinforce your ability to configure switches and routers for inter-VLAN communication. Among the skills you will demonstrate are configuring VLANs, VTP, and trunking on switches. You will also administer STP on switches and configure a router-on-a-stick using subinterfaces.

Task 1: Configure and Verify Basic Device Configurations

Step 1. Configure basic commands.

Configure the router and each switch with the following basic commands. Packet Tracer grades only the hostnames and default gateways.

- Hostnames
- Banner
- Enable secret password
- Line configurations
- Service password encryption
- Switch default gateways

Step 2. Configure the management VLAN interface on S1, S2, and S3.

Create and enable interface VLAN 99 on each switch. Use the addressing table for address configuration.

Step 3. Check results.

Your completion percentage should be 17 percent. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure VTP

Step 1. Configure the VTP mode on all three switches.

Configure S1 as the server. Configure S2 and S3 as clients.

Step 2. Configure the VTP domain name on all three switches.

Use **CCNA** as the VTP domain name.

Step 3. Configure the VTP domain password on all three switches.

Use **cisco** as the VTP domain password.

Step 4. Check results.

Your completion percentage should be 28 percent. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure Trunking

Step 1. Configure trunking on S1, S2, and S3.

Configure the appropriate interfaces in trunking mode and assign VLAN 99 as the native VLAN.

Step 2. Check results.

Your completion percentage should be 62 percent. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure VLANs

Step 1. Create the VLANs on S1.

Create and name the following VLANs on S1 only. VTP advertises the new VLANs to S1 and S2.

- VLAN 10, name = **Faculty/Staff**
- VLAN 20, name = **Students**
- VLAN 30, name = **Guest(Default)**
- VLAN 99, name = **Management&Native**

Step 2. Verify that VLANs have been sent to S2 and S3.

Use the appropriate commands to verify that S2 and S3 now have the VLANs you created on S1. It may take a few minutes for Packet Tracer to simulate the VTP advertisements.

Step 3. Check results.

Your completion percentage should be 67 percent. If not, click **Check Results** to see which required components are not yet completed.

Task 5: Assign VLANs to Ports

Step 1. Assign VLANs to access ports on S2.

Assign the PC access ports to VLANs:

- VLAN 10: PC1 connected to Fa0/11
- VLAN 20: PC2 connected to Fa0/18
- VLAN 30: PC3 connected to Fa0/6

Step 2. Verify the VLAN implementation.

Use the appropriate commands to verify your VLAN implementation.

Step 3. Check results.

Your completion percentage should be 75 percent. If not, click **Check Results** to see which required components are not yet completed.

Task 6: Configure STP

Step 1. Ensure that S1 is the root bridge.

Set priorities to 4096.

Step 2. Verify that S1 is the root bridge.

Step 3. Check results.

Your completion percentage should be 82 percent. If not, click **Check Results** to see which required components are not yet completed.

Task 7: Configure Router-on-a-Stick Inter-VLAN Routing

Step 1. Configure the subinterfaces.

Configure the Fa0/1 subinterfaces on R1 using the information from the addressing table.

Step 2. Check results.

Your completion percentage should be 100 percent. If not, click **Check Results** to see which required components are not yet completed.

Task 8: Verify End-to-End Connectivity

Step 1. Verify that PC1 and the web/TFTP server can ping each other.

Step 2. Verify that PC1 and PC2 can ping each other.

Step 3. Verify that PC3 and PC1 can ping each other.

Step 4. Verify that PC2 and PC3 can ping each other.

Step 5. Verify that the switches can ping R1.