CCNA Video Mentor

Second Edition

Wendell Odom, CCIE® No. 1624

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

CCNA Video Mentor

Second Edition

Wendell Odom

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

Printed in the United States of America

First Printing December 2007

Library of Congress Cataloging-in-Publication Data is on file.

ISBN-13: 978-1-58720-191-2

ISBN-10: 1-58720-191-7

Publisher
Paul Boger

Associate Publisher
Dave Dusthimer

Cisco Representative
Anthony Wolfenden

Cisco Press Program Manager
Jeff Brady

Executive Editor
Brett Bartow

Managing Editor
Patrick Kanouse

Senior Development Editor
Christopher A. Cleveland

Senior Project Editor
Tonya Simpson

Technical Editor
Stephen Kalman

Editorial Assistant
Vanessa Evans

Book Designer
Louisa Adair

Composition
Mark Shirar

Proofreader
Jennifer Gallant

Warning and Disclaimer

This book and video product is designed to provide information about the CCNA Exam. 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.

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.

Trademark Acknowledgments

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

Corporate and Government Sales

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

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

For sales outside the United States please contact:

International Sales international@pearsoned.com

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

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

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

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

About the Author

Wendell Odom, CCIE No. 1624, splits time between writing Cisco Press books and teaching Cisco authorized training for Skyline Advanced Technology Services (http://www.skyline-ats.com). Wendell has worked in the networking arena for more than 25 years, with jobs in pre- and post-sales technical consulting, teaching, and course development. He is the author of all prior editions of the Cisco Press *CCNA Exam Certification Guides*, most recently the two-book set *CCENT/CCNA ICND1 Official Exam Certification Guide* and *CCNA ICND2 Official Exam Certification Guide*. Wendell has also authored several other titles, including the *CCIE Routing/Switching Written Exam Certification Guide*, *QoS Exam Certification Guide*, and *Computer Networking First-Step*, all from Cisco Press.

About the Technical Reviewer

Stephen Kalman is a data security trainer and the author or technical editor of more than 20 books, courses, and CBT titles. His most recent book is *Web Security Field Guide*, published by Cisco Press. In addition to those responsibilities he runs a consulting company, Esquire Micro Consultants, which specializes in network security assessments and forensics.

Mr. Kalman holds SSCP, CISSP, ISSMP, ISSAP, CEH, CHFI, CCNA, CCSA (Checkpoint), A+, Network+, and Security+ certifications and is a member of the New York State Bar.

Dedications

For Hannah Grace: Thanks for all the help learning how to draw on the computer.

Acknowledgments

I imagine Steve Kalman, my tech editor on yet another project, might need a break—we've worked on a lot of projects together in the last year or two. Thankfully, Steve never seems to tire in helping me with the books and with these videos. Steve did his usual wonderful job of looking at the little details while also looking out for the bigger picture, helping make this product better. Steve, thanks again for all the good work!

Chris Cleveland got the wonderful opportunity (tee hee) to listen to all the videos, even the old ones that Chris had already listened to a dozen times last year. Chris was great at finding every last little picky thing that could be changed in each video, but then helping me pick which ones made sense to change, with a lot of thinking outside the box. Chris, many thanks for the usual wonderful job, and no, you weren't being too picky!

Eric Strom played several roles with this product, from recording and editing the live video sections, to creating the product menus and putting the finishing touches on the video/audio itself. The Cisco Press Video Mentor series owes a lot to the efforts, skills, and knowledge supplied by Eric—thanks much!

As usual, a lot of people have a hand in taking what I submit and causing it to magically appear as a product—a group we generally call "the production folks." Thanks for making my products shine as much as they can!

Thanks to Jeff Doyle for the heads-up on the Rode Podcaster microphone I used for all the new videos—excellent suggestion!

Brett Bartow did his usual wonderful job in talking me through the product from the big-picture perspective, helping determine the organization, size, timing, positioning, and essentially anything to help make the product successful. And he writes our decisions down, so when I forget some of the choices we made after being down in the trenches for a few weeks, he can set me back on the straight and narrow. Thanks, Brett, for keeping our little juggling act in the air.

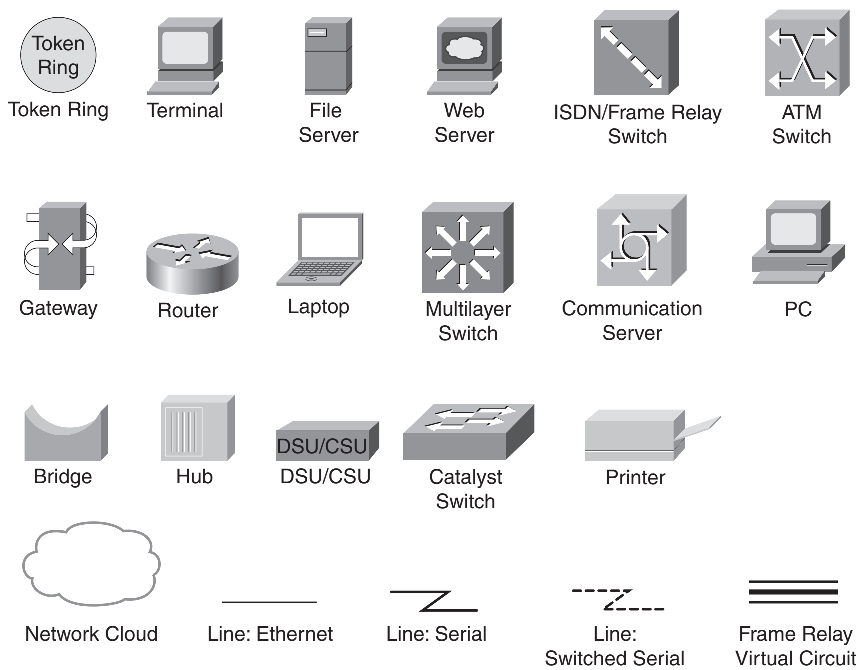
Finally, on a personal note, thanks to wife Kris and daughter Hannah for giving up a few games of chasing around the kitchen when I was recording. I promise to find a way to integrate into the audio track some of the sounds of you two running over my head playing chase in the house. And as always, I'd like to thank Jesus Christ for caring about every part of our lives, including the work and effort spent making these videos.

Contents at a Glance

Contents

ICND2 Labs

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets [ ] indicate optional elements.
- Braces { } indicate a required choice.
- Braces within brackets [{ }] indicate a required choice within an optional element.

Introduction

The *CCNA Video Mentor*, Second Edition (CVM), helps both CCENT and CCNA candidates prepare to pass the ICND1, ICND2, and CCNA exams by supplying 20 instructional videos covering core CCNA exam topics. Each CVM video presents a unique lab scenario, with both visual references and audio explanations of what you should expect to happen in each lab. Most of the videos also show the details of the command-line interface (CLI) commands used to implement the features described in each lab video, along with running commentary. The end result is a set of videos that explain some of the most important CCNA topics, providing you with thorough explanations from a trusted mentor.

This product is one of several products in the Cisco Press Video Mentor series. The Video Mentor series—created because of many requests from Cisco Press book readers—provides something more than just the static written word of a typical book. Many people learn better in a classroom setting, with an instructor explaining the concepts while showing details projected on the wall. This product, along with the other products in the Video Mentor series, provides a product closer to what you might get in a class.

Who Should Use the *CCNA Video Mentor*?

The *CCNA Video Mentor* is primarily intended for people using self-study books as their primary method of preparing to pass the Cisco ICND1, ICND2, and CCNA exams. Additionally, this product should be useful to anyone who is studying basic networking topics, either by reading books or by taking classes.

Goals and Methods

CCNA Video Mentor, Second Edition, has a very specific set of goals. First, these videos help you more completely and thoroughly understand several of the most important CCENT and CCNA exam topics. Although you might have already read about these topics in other books or heard about them in classes, *CCNA Video Mentor* helps you master these particular topics. Using these videos in addition to reading a book or attending a course helps solidify your knowledge and helps you see how to apply the knowledge to better prepare you for the application of that knowledge on the exam.

Note that *CCNA Video Mentor* does not attempt to cover all possible topics on the exams used to achieve CCENT and CCNA certification. It is intended to be used to supplement both self-study efforts and classroom training.

The *CCNA Video Mentor's* video labs show the activity on a computer desktop with a running audio commentary from the author. Most of the videos follow the same basic approach, using these steps:

1. The video begins with a description of the goals of the video.
2. The lab scenario steps (usually two or three steps) are listed, giving a general outline of what the viewer should expect to see and hear during the video.
3. The network topology used in the video is described.
4. Then, for each scenario step:

   a) The video shows what the user should expect from the particular part of the lab exercise.

   b) The video shows the CLI details of how to configure and verify that the routers and switches are working properly.

Some of the subnetting videos do not have a CLI component because these videos focus on concepts and processes instead of configuration.

A Brief Word About the Related Exams

This product helps you prepare to achieve a CCNA certification. Two paths exists via which you can become CCNA certified:

- Take the CCNA exam (640-802)
- Take both the ICND1 exam (640-822) and the ICND2 exam (640-816)

Because you might be using the two-exam approach, the videos have been organized based on whether the content is most likely to be seen in the ICND1 exam or the ICND2 exam. All the content could be assessed as part of the 640-802 CCNA exam.

This product also helps you prepare to achieve CCENT certification. Cisco awards a CCENT certification for those passing the ICND1 (640-822) exam.

CVM Contents

The CVM product package contains two components: a DVD and a booklet. The DVD contains the 20 lab videos, plus several introductory videos. The DVD has been optimized for viewing on a computer, with a 1024 × 768 minimum pixel grid.

The booklet lists reference information that can be useful when watching the videos; the booklet is not intended as a standalone tool. The booklet has a section corresponding to each of the 20 CVM video labs, with each section containing a copy of the figures and other material shown in the video. Each section includes the following:

- The list of objectives for the video
- The list of scenario steps
- Copies of all figures shown in the video
- Copies of all reference lists shown in the video
- The beginning configuration on each device
- Any configuration added to each device during the video

How the *CCNA Video Mentor* Is Organized

When the DVD starts, the application displays a menu that lists the two major parts of the product: labs related to the ICND1 exam and labs related to the ICND2 exam. A video introducing the entire product is also available from this initial menu.

Clicking either the ICND1 or ICND2 items moves the user to one of two submenus. Each submenu lists a set of videos, organized into various topics. These submenus also supply clickable links to see an introductory video for each general topic area, plus links to display a PDF for the booklet chapter for each individual lab.

The printed booklet mimics the organization of the labs in the DVD application, organizing the labs into two major groups (ICND1 and ICND2), and smaller topical groupings as well. The groups and labs associated with the ICND1 exam are as follows:

Part I: CLI Basics

- **Lab 1, "Navigating Router/Switch Command-Line Interface"**—This lab demonstrates how to connect to a router or switch console and use both user mode and privileged mode exec commands.
- **Lab 2, "Router Configuration and Managing Configuration Files"**—This lab leads the user through the process of connecting to a router's console, getting into configuration mode, and configuring several features. It also explains the key commands used for copying configuration files.

Part II: LANs

- **Lab 3, "Switching Basics: Learning, Forwarding/Filtering, and Interface Settings"**—This lab shows a sample network with two LAN switches and explains how the switches will learn and forward certain frames. It also shows the MAC address learning process with **show** commands on the switches, along with some basic interface configuration subcommands on switches.

Part III: IP Addressing and Subnetting

- **Lab 4, "Finding the Subnet Number"**—This lab shows how to find the subnet number in which an IP address resides. It emphasizes the use of a process shown in the Cisco Press Exam Certification Guides, a process which shows how to find the answers to subnetting questions without using any binary math.
- **Lab 5, "Finding the Broadcast Address and Range of Addresses in a Subnet"**—This lab shows how to find a subnet's broadcast address and the range of valid addresses in the subnet given the subnet number. This video lab continues the same problem shown in ICND1 video lab 4, again using a decimal-only process from the Cisco Press Exam Certification Guides.
- **Lab 6, "Finding All Subnets of a Network with Less than 8 Subnet Bits"**—This lab shows how to find all the subnet numbers of a single classful network, assuming a single subnet mask is used throughout the classful network. This video emphasizes the use of yet another decimal-only process shown in the Cisco Press Exam Certification Guides. This video uses the same network and subnet mask used in labs 4 and 5.
- **Lab 7, "IP Subnet Design and Implementation"**—This lab explains subnetting from a design perspective, examining how to determine the number of required subnets and reviewing how to find all subnets of a network using a particular static-length mask.

Part IV: Routing and Routing Protocols

- **Lab 8, "Static and Connected Routes"—**This lab explains the concept of the details of an IP routing table on a Cisco router. It then shows the requirements for a router to add connected routes to its routing table, as well as how to configure two different styles of static routes.

- **Lab 9, "RIP Configuration"**—This lab shows how to configure RIP in a simple three-router WAN. It focuses on the meaning of the RIP **network** configuration subcommand; in particular, how the **network** command matches a router's interfaces, and what the router does when the **network** command matches an interface. It also explains the default version settings when the **version** command is not configured, and shows how to configure RIP Version 2.

The groups and labs associated with the ICND2 exam are as follows:

Part I: LANs

- **Lab 1, "Configuring VLANs"**—This lab shows two variations of how to configure VLANs on a switch. The lab shows how to configure a VLAN, as well as how to place interfaces into that particular VLAN.
- **Lab 2, "VTP Servers and Clients"**—This lab shows how to configure both VTP servers and VTP clients so that when VLANs are configured on the server, the client dynamically learns about the VLAN. This lab focuses on how to determine whether two neighboring switches meet all the requirements for them to be able to successfully exchange VLAN information.

Part II: Routing Protocols

- **Lab 3, "RIP with Split Horizon, Route Poisoning, and Poison Reverse"**—This lab explains the concepts behind some of the more advanced distance vector loop avoidance features. It also demonstrates these features in a small network using the output of IOS **debug** commands.
- **Lab 4, "Single Area and Multi-area OSPF Configuration"**—This lab shows how to configure OSPF in a five-router WAN. It shows how to configure OSPF as simply as possible, using a single OSPF area, as well as how to configure Area Border Routers (ABR) in a multi-area design.
- **Lab 5, "EIGRP Configuration and Operation"**—This lab shows how to configure EIGRP in a simple three-router WAN. It focuses on the meaning of the EIGRP **network** configuration subcommand; in particular, how the wildcard mask option allows an engineer to control on which interfaces the router enables EIGRP. It also shows the contents of the IP routing table when Variable Length Subnet Masking (VLSM) is used.
- **Lab 6, "Understanding EIGRP Metric Calculations"**—This lab shows how EIGRP calculates its integer metric value based on interface bandwidth and delay. It also shows examples of the metric from the CLI, as well as how to influence the calculated metric—and therefore the routes chosen by EIGRP—by tuning the interface bandwidth.

Part III: Scaling IP Addresses

- **Lab 7, "NAT Overload (PAT)"**—This lab explains how the NAT overload feature (also known as PAT) works, and how it allows the use of a small number of public IP addresses to support a large network. The lab also reviews the NAT overload configuration for a sample network.
- **Lab 8, "IPv6 Subnetting and Address Configuration"**—This lab shows the format of IPv6 global unicast addresses, along with a comparison of how to subnet IPv4 and IPv6 global unicast addresses. The lab also shows how to configure IPv6 addresses on a Cisco router.

Part IV: WAN

- **Lab 9, "PPP and CHAP Configuration"**—This lab explains the two interface status codes and the impact of both correct and incorrect WAN data link configuration parameters. The lab also shows how to configure PPP and CHAP on a serial link.

Part V: Security

- **Lab 10, "Access Lists"**—This lab explains the syntax of the **access-list** command for configuring an extended IP ACL. The video focuses on how to match ranges of IP addresses using a wildcard mask, as well as matching the well-known port number as a destination port.
- **Lab 11, "Access Lists II"**—This lab explains the nuances of matching well-known ports as the source port in an **access-list** command by showing an alternative solution for the scenario described in Lab 10. This video shows how to filter packets going from a server to a client by matching the source port of a packet.

Suggested Times to Use Labs

The *CCNA Video Mentor*, Second Edition, supplements the learning process using CCNA self-study products. The following table suggests the points at which each CVM lab might be best used in conjunction with the Cisco Press CCNA books.

Table I-1 shows the best timing options when using the *CCNA Official Exam Certification Library*, Third Edition (978-1-58720-183-7), which consists of the *CCENT/CCNA ICND1 Official Exam Certification Guide* and the *CCNA ICND2 Official Exam Certification Guide*.

Table I-1 Using the CVM with the Official CCNA Certification Library

ICND1 Labs

Lab	Book	Chapter(s)
1	ICND1 ECG	8, 13
2	ICND1 ECG	13
3	ICND1 ECG	9
4	ICND1 ECG	12
5	ICND1 ECG	12
6	ICND1 ECG	12
7	ICND1 ECG	12
8	ICND1 ECG	14
9	ICND1 ECG	14

ICND2 Labs

Lab	Book	Chapter(s)
1	ICND2 ECG	1
2	ICND2 ECG	1
3	ICND2 ECG	8
4	ICND2 ECG	9
5	ICND2 ECG	10
6	ICND2 ECG	10
7	ICND2 ECG	16
8	ICND2 ECG	17
9	ICND2 ECG	12
10	ICND2 ECG	6
11	ICND2 ECG	6

ICND1 Labs

The CCNA certification can be achieved through two different paths: by taking the single CCNA (640-802) exam or by taking both the ICND1 (640-822) and ICND2 (640-816) exams. This product separates the video labs into two sections, with labs focusing on the ICND1 exam in this section and labs focusing on the ICND2 exam in the other section. The labs in both sections apply to the CCNA exam.

Part I CLI Basics

Part II LANs

Part III IP Addressing and Subnetting

Part IV Routing and Routing Protocols

Lab 1

Navigating a Router/Switch Command-Line Interface

This *CCNA Video Mentor* (CVM) lab covers the most basic skills for accessing and using the command-line interface (CLI) on a Cisco router or switch. Many of the small, picky details of how the CLI works cannot be seen by reading a book; this lab hopes to complete the coverage of those basics. In particular, the objectives of this lab are as follows:

- Use IOS CLI help features
- Describe the differences between user, enable, and config modes
- Describe the difference between EXEC commands and configuration commands
- Move among user, enable, and configuration modes

Scenario

This lab contains two main steps. The first step focuses on the basics of the CLI, and the second step examines different CLI modes and how to move between them. The video takes the following actions at the two steps:

Step 1. From the console port, the user logs in to a router and experiments with user EXEC mode. This step shows how to get command-line help.

Step 2. The user moves among user EXEC mode, privileged (enable) EXEC mode, and configuration mode. This step demonstrates some commands that might be allowed only in a particular mode.

Initial Configurations

Many labs in the CVIP have meaningful initial configurations. If you use this lab at the suggested point in your study, you will not yet have seen some of the configurations. However, for completeness, Example 1-1 shows the initial configuration of router R1 at the beginning of the lab. The parts of R1's configuration that are not relevant to this lab have been omitted.

Example 1-1 Initial Configuration for R1

```
hostname R1
```

Ending Configurations

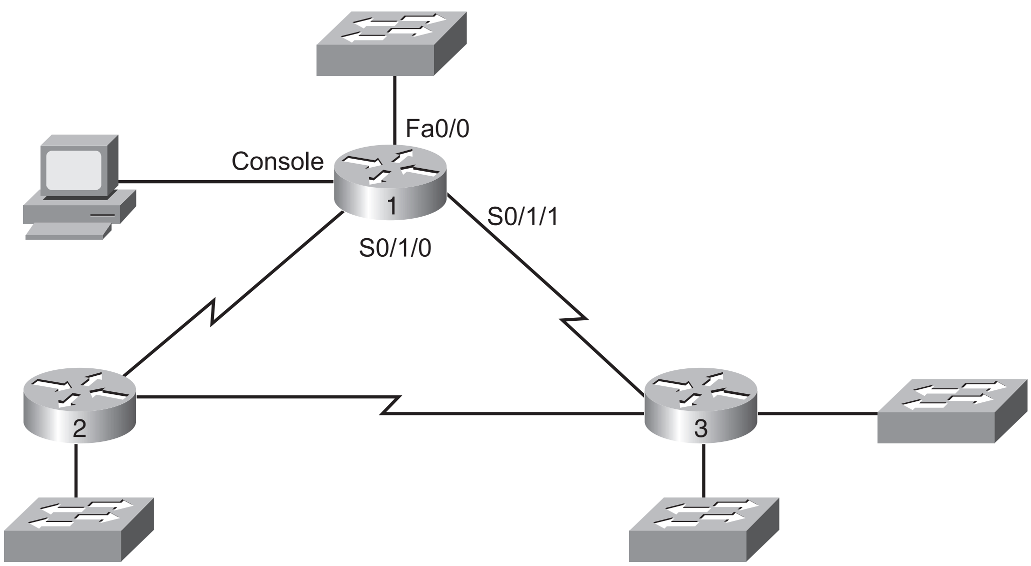
This lab ends with the configuration unchanged.

Video Presentation Reference

The video presents figures, tables, and text with short lectures before showing the CLI of the router. This section simply lists these figures and tables for reference.

Figure 1-1 shows a diagram of the network used in this example.

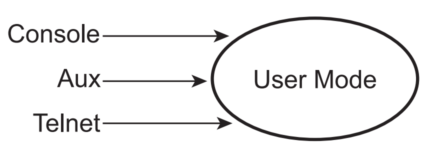
Figure 1-1 Lab 1 Network Topology



Because the video is organized into two separate steps, the reference materials have been organized into two separate sections.

Step 1 Reference

Figure 1-2 Figure for Step 1



- User EXEC Mode Facts:
  - First mode seen by users connected from the console port, aux port, and Telnet.
  - User can type harmless EXEC commands.
  - Characterized by a “>” at the end of the command prompt.

Step 2 Reference

Figure 1-3 Figure for Step 2

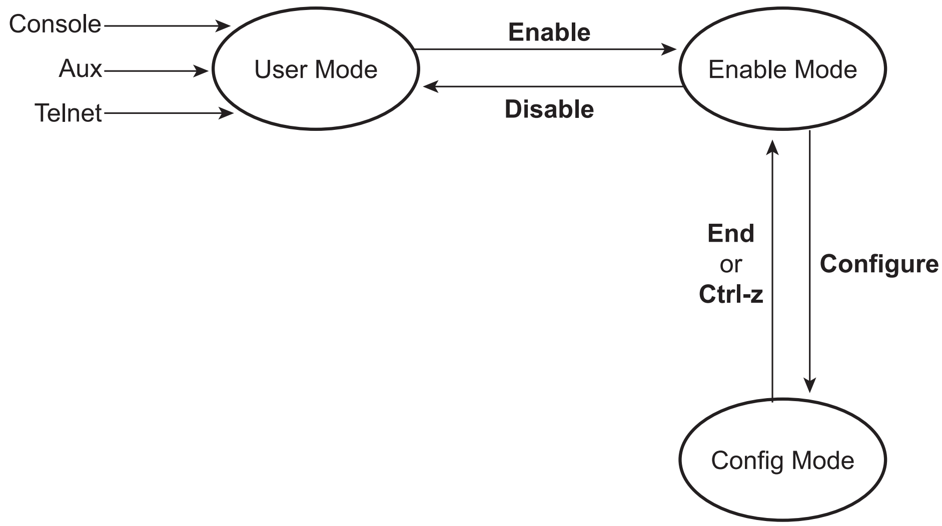


Table 1-1 Comparing EXEC and Config Commands

	EXEC Commands	Config Commands
Mode in which they are used	User or enable	Config
Cisco IOS Software typically responds with a list of messages	Yes	No
Command changes the configuration and behavior of router/switch	No	Yes

Table 1-2 Three Commands That Can Be Used in Different CLI Modes

Command	Modes in Which It Works
show ip route	User, enable
reload	Enable
hostname	Config

Lab 2

Router Configuration and Managing Configuration Files

This *CCNA Video Mentor* lab demonstrates the mechanics of configuring a Cisco router and how to copy configuration files. The objectives of this lab are the following:

- Describe the configuration process using different configuration modes
- Recognize the *command prompts* seen in different configuration modes
- Copy configuration files using the **copy** command

Scenario

This lab contains two primary steps. The first step focuses on an example of moving around in configuration mode, with the goal of explaining the process rather than the specific commands. The second step focuses on how to copy configuration files on a Cisco router. The video references these two main steps as follows:

Step 1. Using configuration mode

Step 2. Viewing and copying configuration files in NVRAM, RAM, and TFTP servers

Initial Configurations

The only router shown in this video begins with almost no configuration other than a host name. Example 2-1 lists the hostname configuration for reference.

Example 2-1 Initial Configuration for Router R1

```
hostname R1
```

Ending Configurations

By the end of the lab, R1's running and startup configuration files should be identical. The video also shows a couple of other configuration items. Example 2-2 lists the ending configuration after all steps in the lab.

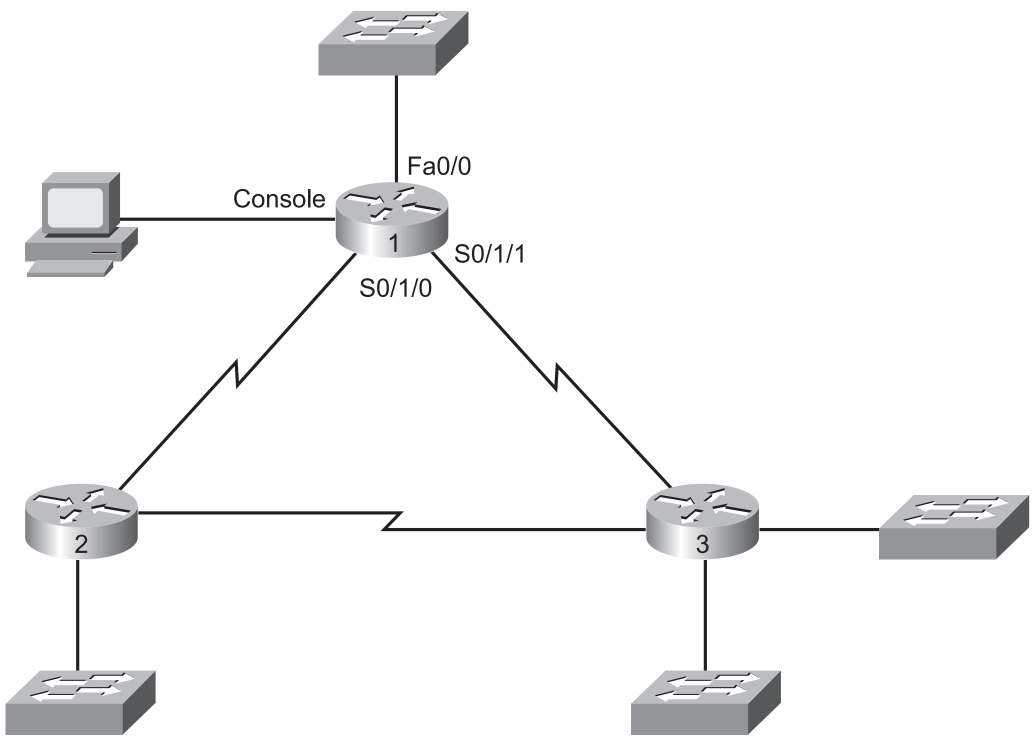
Example 2-2 Ending Configuration for R1

```
hostname Fred
!
interface serial 0/1/0
 ip address 1.1.1.1 255.255.255.0
!
line con 0
 password cisco
 login
```

Video Presentation Reference

The video presents figures, tables, and text with short lectures before showing the CLI of the router. This section simply lists these figures and tables for reference. Figure 2-1 shows a diagram of the network used in this example.

Figure 2-1 Lab 2 Network Topology



Because the video is organized into two separate steps, the reference materials have been organized into two separate sections.

Step 1 Reference

Figure 2-2 Accessing a Router's Config Mode

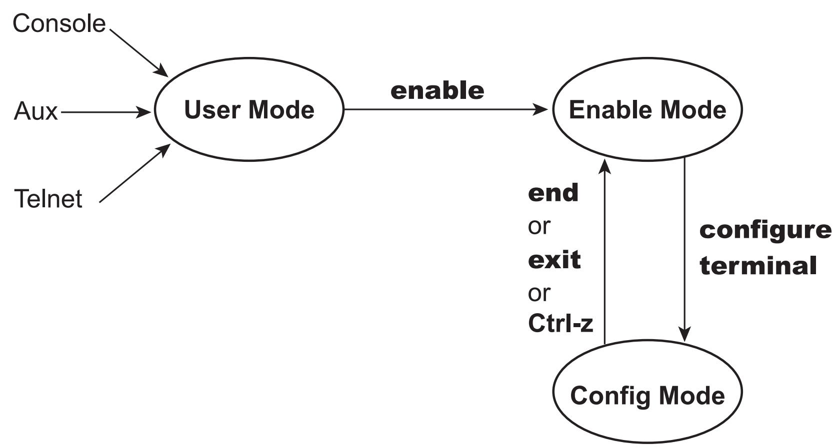
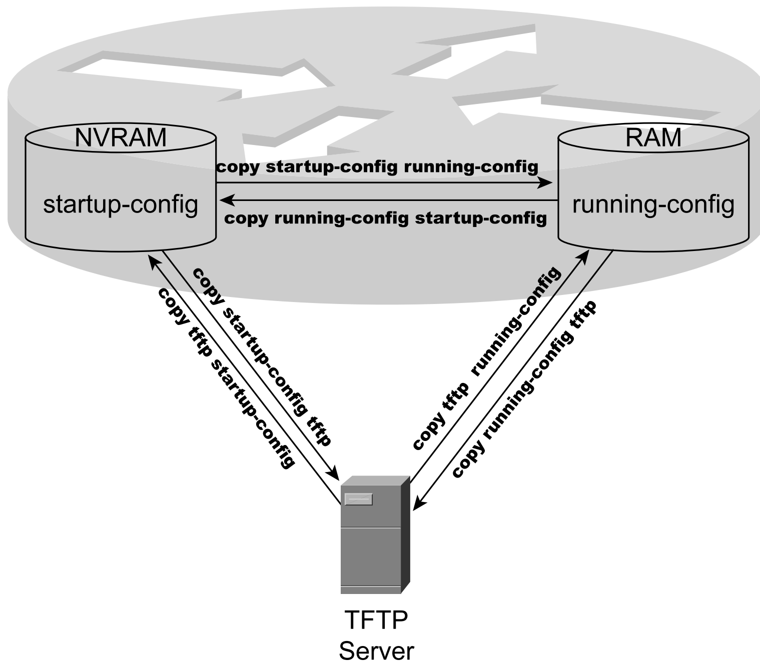


Table 2-1 Example Configuration Sub-modes

Name of Sub-mode	Purpose	Command Prompt
Interface	Configures details about a specific router interface, such as the IP address	Router(config-if)#
Line	Configures details about lines (console, vty, and aux)	Router(config-line)#
Router	Configures details about a particular routing protocol	Router(config-router)#

Step 2 Reference

Figure 2-3 Mechanics of the copy Command



Lab 3

Switch Basics: Learning, Forwarding/Filtering, and Interface Settings

This *CCNA Video Mentor* lab reviews the logic of how switches learn entries for their MAC address tables and make forwarding and filtering decisions based on those tables; it also shows some of the most basic configuration settings on a Cisco LAN switch. In particular, the objectives of this lab are as follows:

- Predict the types of entries to be found in a switch's *MAC address table*
- Describe how switches make forwarding/filtering decisions
- Configure the following:
  - Interface speed and duplex settings
  - Switch IP address and default gateway

Scenario

This lab contains two main steps, as follows:

Step 1. Observe the addition of new MAC address table entries

Step 2. Configure basic settings:

- Interface speed and duplex
- IP address and default gateway

Initial Configurations

The two switches in this lab begin with very little configuration—each switch simply has a hostname configured. Examples 3-1 and 3-2 list the hostname configurations for completeness.

Example 3-1 Initial Configuration for Sw1

```
hostname Sw1
```

Example 3-2 Initial Configuration for Sw2

```
hostname Sw2
```

Ending Configurations

This lab adds some configuration commands to both Sw1 and Sw2. Examples 3-3 and 3-4 show the configuration added during the lab.

Example 3-3 Configuration on Sw1 Added During This Lab

```
enable secret cisco
!
interface FastEthernet 0/23
 duplex full
 speed 100
!
interface vlan 1
 ip address 172.30.1.101 255.255.255.0
!
ip default-gateway 172.30.1.251
!
```

Example 3-4 Configuration on Sw2 Added During This Lab

```
interface FastEthernet 0/24
 duplex full
 speed 100

!
interface vlan 1
 ip address 172.30.1.102 255.255.255.0
!
ip default-gateway 172.30.1.251
```

Video Presentation Reference

This video presents several figures and a table that support the concepts covered in the lab. This section simply lists these figures for reference. Because the video is organized into two separate steps, the reference materials have been organized into two separate sections.

Step 1 Reference

Figure 3-1 Completed MAC Address Tables After Learning All PC MAC Addresses

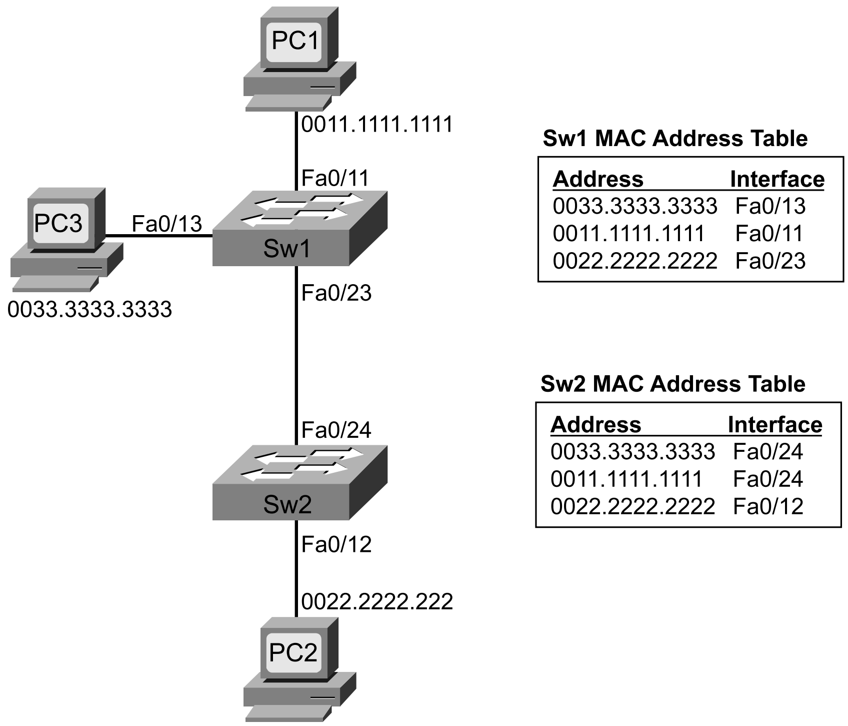


Figure 3-2 Forwarding Path and MAC Address Table Entries Used for Frames from PC3 to PC1

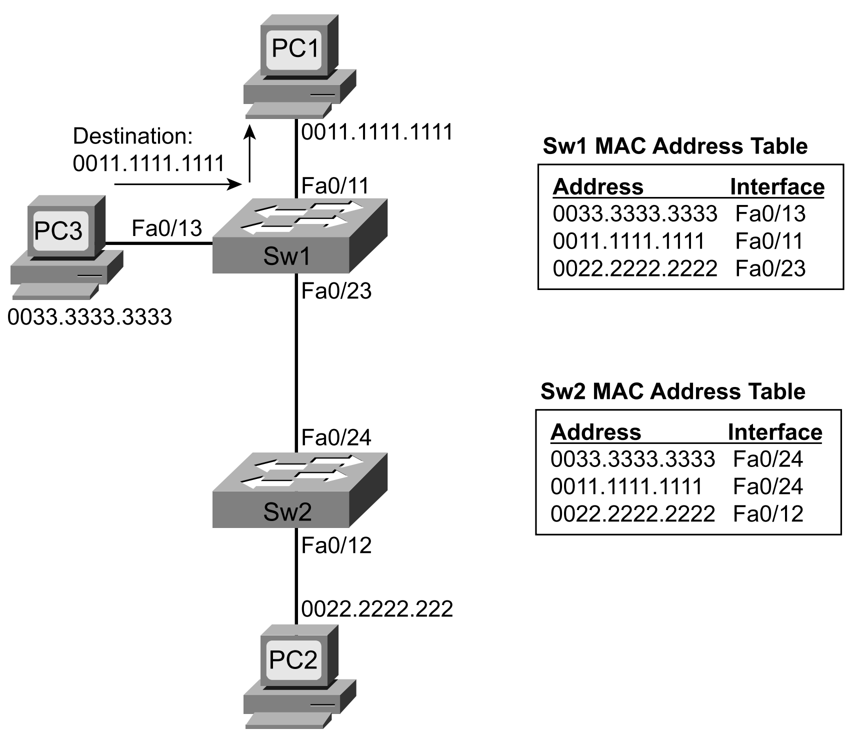
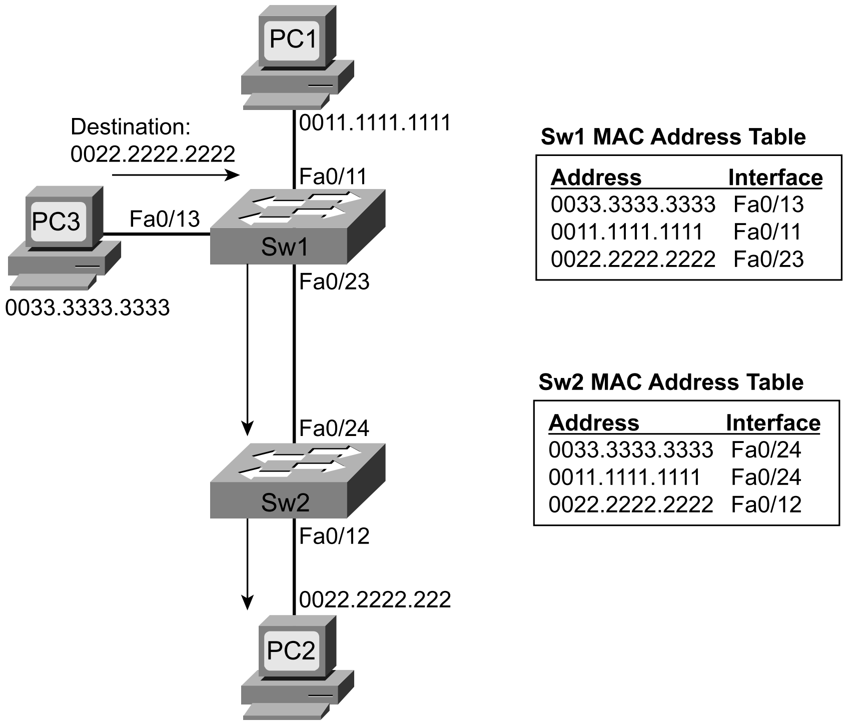


Figure 3-3 Forwarding Path and MAC Address Table Entries Used for Frames from PC3 to PC2

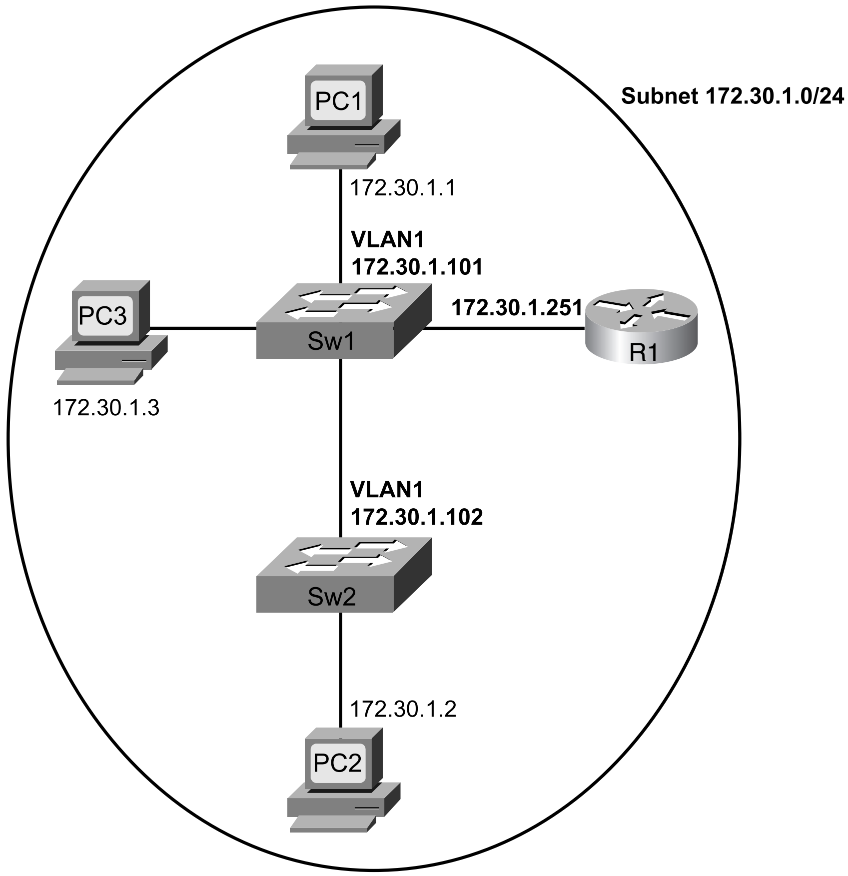


Step 2 Reference

Table 3-1 Switch Configuration Command Reference

Command	Purpose
interface fastethernet *x/y*	Moves the user into interface configuration mode
speed {**10** | **100**}	Manually sets the speed of the interface
duplex {**half** | **full**}	Manually sets the duplex of an interface
interface vlan 1	Moves the user to VLAN 1 configuration mode
ip address *address mask*	Allows the configuration of a management IP address on the switch
ip default-gateway *address*	Defines the switch's default gateway IP address

Figure 3-4 IP Address Reference



Lab 4

Finding the Subnet Number

This *CCNA Video Mentor* (CVM) lab explains how to find the subnet number in which an IP address resides. In particular, it shows you how to find the subnet number in which 128.200.100.100, mask 255.255.224.0, resides.

The objectives of this lab are as follows:

- To help you understand how to use a particular process (found in the Cisco Press *CCENT/CCNA ICND1 Official Exam Certification Guide*) to find an address's resident subnet
- To help you understand how to find the answers to this kind of question quickly, accurately, and with confidence

Scenario

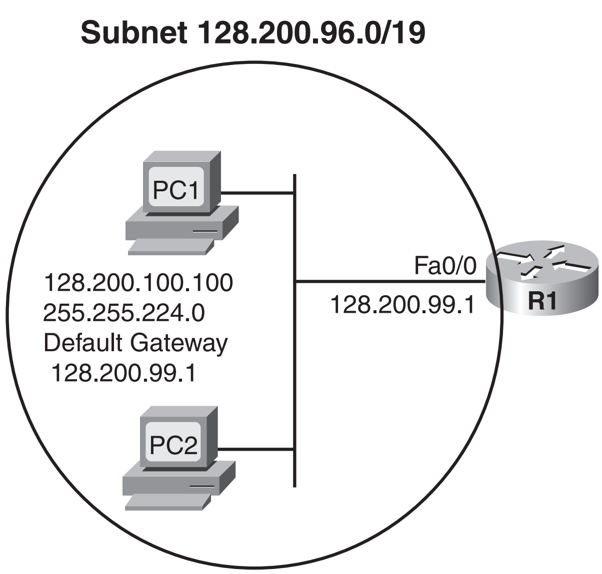
This lab contains a single step, focusing on the process by which to find the subnet number (128.200.96.0/19) in which IP address 128.200.100.100/19 resides.

Video Presentation Reference

The video presents figures, tables, and text with short lectures before showing the command-line interface (CLI) of the router. This section simply lists these figures and tables for reference.

Figure 4-1 shows the part of an internetwork in which IP address 128.200.100.100/19 resides.

Figure 4-1 Location of Host 128.200.100.100/19



Subnet	Next-Hop	Int.
128.200.96.0/19	(Connected)	Fa0/0

The following list describes the process demonstrated in the video:

1. Write down the mask and IP address in a table, in dotted-decimal format.
2. Find the interesting octet of the mask—the octet that is neither 255 nor 0—and draw a rectangle around that column of the table.
3. Write down values for three octets of the subnet number, as follows:

   a) For octets to the left of the rectangle, copy the IP address's value.

   b) For octets to the right of the rectangle, write down 0s.
4. For the interesting octet's value:

   a) Calculate the magic number (256 minus the mask's value in the interesting octet).

   b) Calculate the integer multiples of the magic number, starting at 0, through 256.

   c) Find the multiple that is closest to the IP address's value in the interesting octet, but not bigger than the IP address's value. Write this multiple down as the subnet number's value in the interesting octet.

Figure 4-2 shows work in progress with the process shown in this video, after the completion of Step 3.

Figure 4-2 Work in Progress Through Step 3

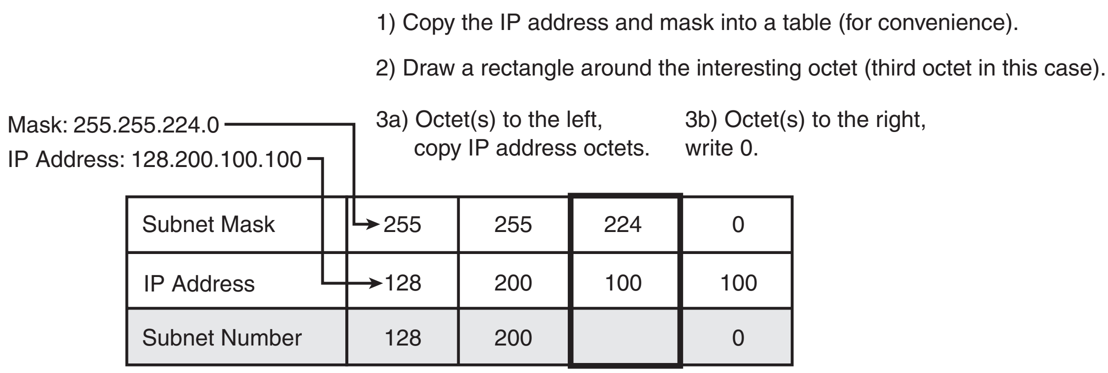
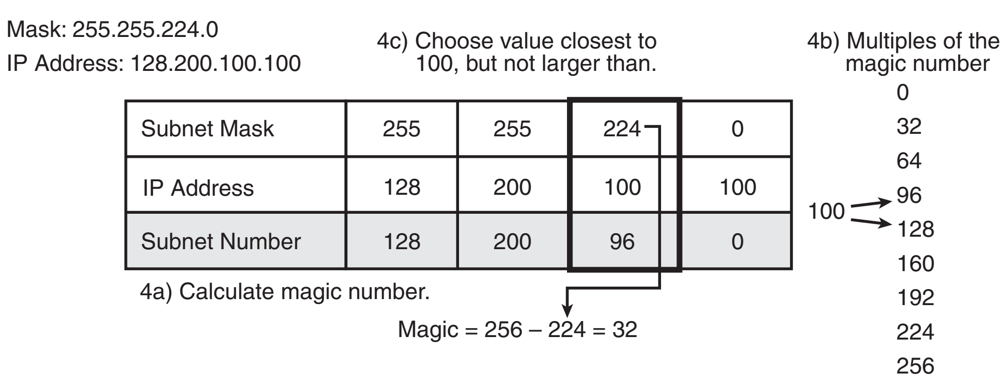


Figure 4-3 shows some of the final work to finish the process and identify the resident subnet.

Figure 4-3 Work in Progress, Through Completion



Lab 5

Finding the Broadcast Address and Range of Addresses in a Subnet

This *CCNA Video Mentor* (CVM) lab explains how to find a subnet's broadcast address, which then enables you to find the range of addresses in the subnet that can be assigned to hosts in that subnet. In particular, it shows you how to find the broadcast address and range of addresses for subnet 128.200.96.0, mask 255.255.224.0.

Note that Lab 4, "Finding the Subnet Number," shows you how to find this particular subnet number, given an IP address in the subnet—address 128.200.100.100 is used in Lab 4. You should watch Lab 4 before watching this video.

The objectives of this lab are as follows:

- To help you understand how to use a particular process (found in the Cisco Press *CCENT/CCNA ICND1 Official Exam Certification Guide*) to find a subnet's broadcast address and the range of usable addresses in the subnet
- To help you understand how to find the answers to this kind of question quickly, accurately, and with confidence

Scenario

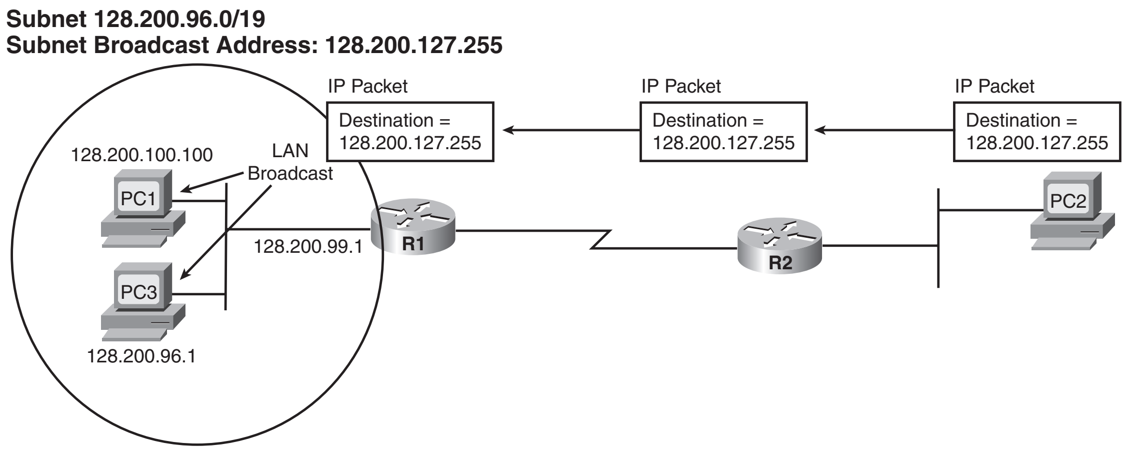
This lab contains a single step, focusing on the process by which to find the broadcast address (128.200.127.255) of a given subnet (128.200.96.0/19).

Video Presentation Reference

The video presents figures, tables, and text with short lectures before showing the CLI of the router. This section simply lists these figures and tables for reference.

Figure 5-1 shows a figure used in the video to demonstrate the original purpose of the subnet broadcast address.

Figure 5-1 Flow of a Packet Sent to a Subnet Broadcast Address



This video demonstrates Steps 5, 6, and 7 from the following process. Steps 1 through 4 were demonstrated in Lab 4 and are listed here for convenient reference:

1. Write down the mask and IP address in a table, in dotted-decimal format.
2. Find the interesting octet of the mask—the octet that is neither 255 nor 0—and draw a rectangle around that column of the table.
3. Write down values for three octets of the subnet number, as follows:

   a) For octets to the left of the rectangle, copy the IP address's value.

   b) For octets to the right of the rectangle, write down 0s.
4. For the interesting octet's value:

   a) Calculate the magic number (256 minus the mask's value in the interesting octet).

   b) Calculate the integer multiples of the magic number, starting at 0, through 256.

   c) Find the multiple that is closest to the IP address's value in the interesting octet, but not bigger than the IP address's value. Write this multiple down as the subnet number's value in the interesting octet.
5. To find the subnet broadcast address:

   a) For octets to the left of the rectangle, copy the subnet number or IP address's value.

   b) For octets to the right of the rectangle, write down 255s.

   c) In the interesting octet, add the subnet number's value to the magic number and subtract 1.
6. For the first IP address in the range of addresses, copy the subnet number but add 1 to the fourth octet.
7. For the last IP address in the range of addresses, copy the subnet broadcast address but subtract 1 from the fourth octet.

Figure 5-2 shows work in progress after Steps 5A and 5B.

Figure 5-2 Work in Progress Through Step 5B

Mask: 255.255.224.0
IP Address: 128.200.100.100

Interesting Octet

Subnet Mask	255	255	224	0
IP Address	128	200	100	100
Subnet Number	128	200	96	0
First IP Address				
Last IP Address				
Broadcast Address	128	200		255

5b) For mask octets to the right of the rectangle, write down 255.

5a) For mask octets to the left of the rectangle, copy subnet number's octets.

Figure 5-3 shows some of the work required at Step 5C, the trickiest part of the process.

Figure 5-3 Work in Progress, Step 5C

Mask: 255.255.224.0
IP Address: 128.200.100.100

Interesting Octet

Subnet Mask	255	255	224	0
IP Address	128	200	100	100
Subnet Number	128			0
First IP Address				
Last IP Address				
Broadcast Address	128			255

Subnet's Interesting Octet	96
Add Magic	+ 32
Minus 1	– 1
Broadcast Value in Interesting Octet	127

5c) For the interesting octet…

Magic = 256 – 224 = 32

Lab 6

Finding All Subnets of a Network with Less Than 8 Subnet Bits

This *CCNA Video Mentor* (CVM) lab explains how to find all subnets of a single classful IP network, assuming that a single mask is used throughout the network and that the mask implies fewer than eight subnet bits. The process shown in this lab, like Labs 4 and 5, is the same process described in the Cisco Press *CCENT/CCNA ICND1 Official Exam Certification Guide*. As such, it is best to view this video after viewing Labs 4 and 5.

This video shows you how to find all subnets of Class B network 128.200.0.0, with mask 255.255.224.0.

The objectives of this lab are as follows:

- To help you understand how to use a particular process (found in the Cisco Press *CCENT/CCNA ICND1 Official Exam Certification Guide*) to find all subnets of a single IP network
- To show how to identify the zero and broadcast subnets
- To help you understand how to find the answers to this kind of question quickly and with confidence

Scenario

This lab contains a single step that shows how to find all the subnets of a single classful network.

Video Presentation Reference

The video presents figures, tables, and text with short lectures before showing the CLI of the router. This section simply lists these figures and tables for reference.

The process demonstrated in this video is summarized in the following list:

1. Write down the mask in a table, in dotted-decimal format.
2. Find the interesting octet of the mask—the octet that is neither 255 nor 0—and draw a rectangle around that column of the table.
3. Calculate the magic number (256 minus the mask's value in the interesting octet).
4. Write down the classful network number in the row labeled Zero Subnet.
5. To find each successive subnet number:

   a) Copy the previous subnet number's three boring octets.

   b) For the interesting octet, add the magic number to the previous subnet's interesting octet value.

6. When Step 5b's sum is 256, stop. The subnet found before the sum of 256 is the last subnet, namely the broadcast subnet.

Figure 6-1 shows work in progress through Step 4.

Figure 6-1 Work in Progress Through Step 4

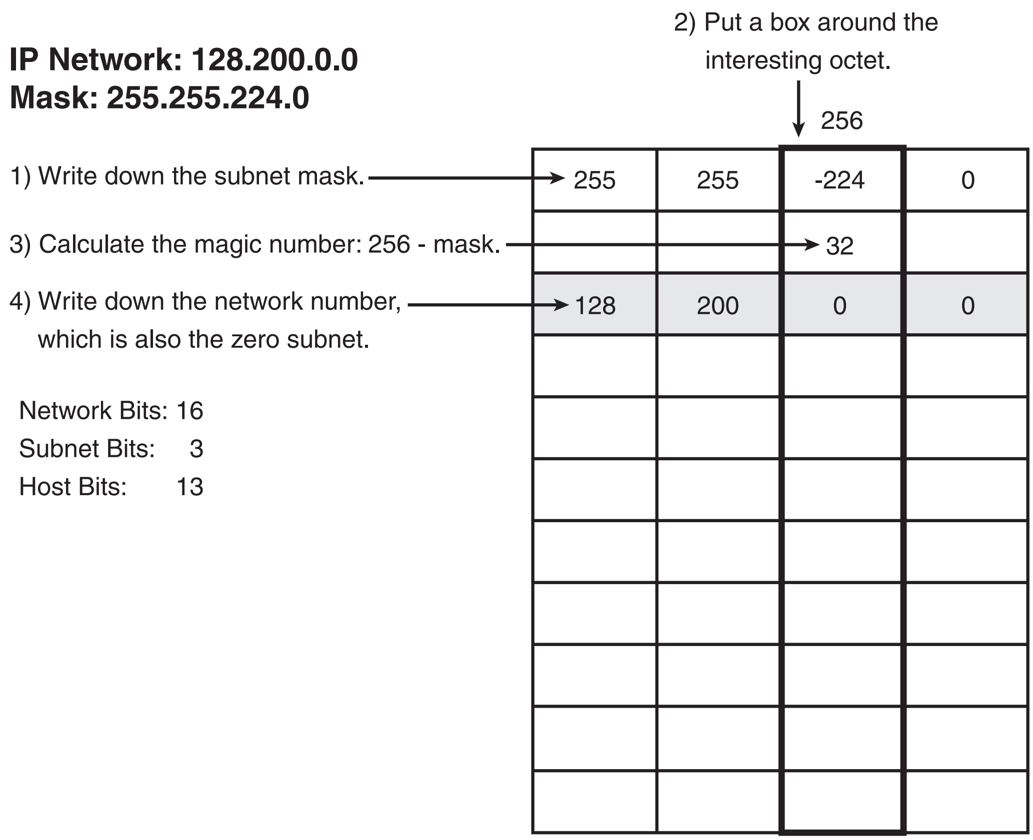


Figure 6-2 shows work in progress after the first pass through Step 5.

Figure 6-2 Work in Progress After First Pass Through Step 5

Mask	255	255	224	0
Magic Number			32	
Network Number/Zero Subnet	128	200	+ 0	0
5a) Copy previous subnet's three uninteresting octets.	128	200	32	0
5b) Add the magic number to the previous subnet's interesting octet.				

Figure 6-3 shows work in progress after the second pass through Step 5.

Figure 6-3 Work in Progress After Second Pass Through Step 5

Mask	255	255	224	0
Magic Number			32	
Network Number/Zero Subnet	128	200	0	0
	128	200	32	0
5a) Copy the previous subnet's three uninteresting octets.	128	200	+ 32 64	0
5b) Add the magic number to the previous subnet's interesting octet.				

Figure 6-4 shows work in progress after Step 6, which tells you when to stop the process.

Figure 6-4 Work in Progress After Step 6

Mask	255	255	224	0
Magic Number			32	
Network Number/Zero Subnet	128	200	0	0
	128	200	32	0
	128	200	64	0
	128	200	96	0
	128	200	128	0
	128	200	160	0
	128	200	192	0
Broadcast Subnet	128	200	224	0
6) 256 is out of range – this is not a valid subnet number.			~~256~~	

Figure 6-5 shows the list of eight subnets, as well as the zero subnet and broadcast subnet.

Figure 6-5 Answer: A List of Subnets

Zero Subnet	128	200	0	0
	128	200	32	0
	128	200	64	0
	128	200	96	0
	128	200	128	0
	128	200	160	0
	128	200	192	0
Broadcast Subnet	128	200	224	0

Lab 7

IP Subnet Design and Implementation

This *CCNA Video Mentor* (CVM) lab explains how to find all subnets of a single classful IP network, assuming that a single mask is used throughout the network and that the mask implies fewer than eight subnet bits. The process shown in this lab, like Labs 4 and 5, is the same process described in the Cisco Press *CCENT/CCNA ICND1 Official Exam Certification Guide*. As such, it is best to view this video after viewing Labs 4 and 5.

This video shows you how to find all subnets of class B network 128.200.0.0, with mask 255.255.224.0.

The objectives of this lab are as follows:

- Identify the location of the subnets required for a given network topology.
- Be more familiar with the process of finding all subnets of a network, using a static-length subnet mask.
- Review the process of finding the range of IP addresses in each subnet.

Scenario

This lab contains three steps, as follows:

1. Examine an internetwork design, identifying the number of required subnets and the location of each subnet.
2. Calculate the possible subnet numbers and choose the (numerically) smallest subnets.
3. Assign IP addresses to each router, switch, and host.

Video Presentation Reference

The video presents figures and animation with short lectures. This section simply lists these figures and other information for reference.

Step 1 Reference

Figure 7-1 Topology Reference

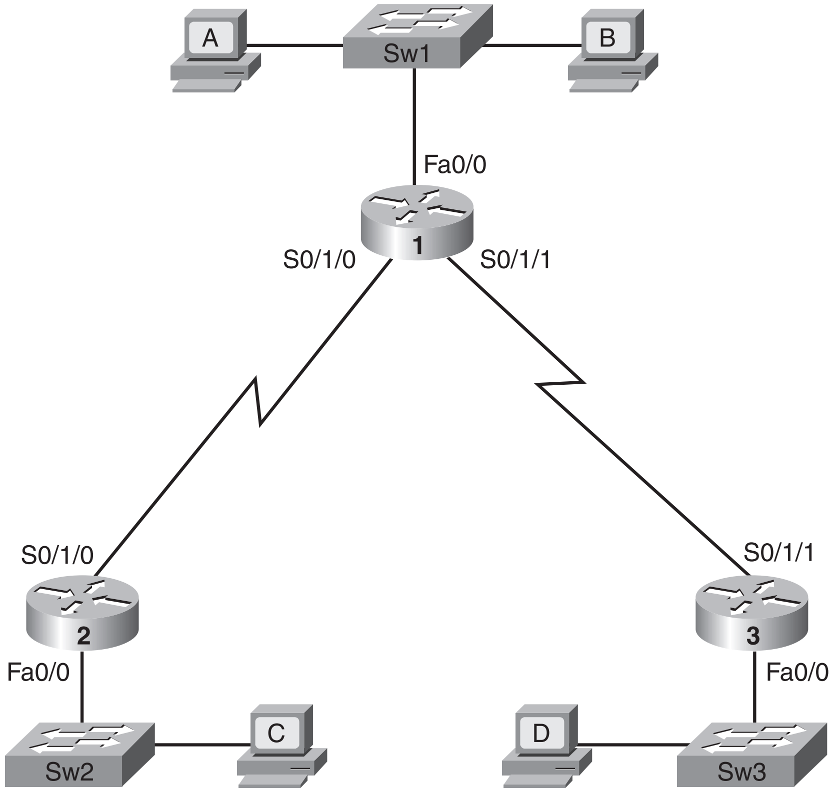


Figure 7-2 Location of the Required Subnets

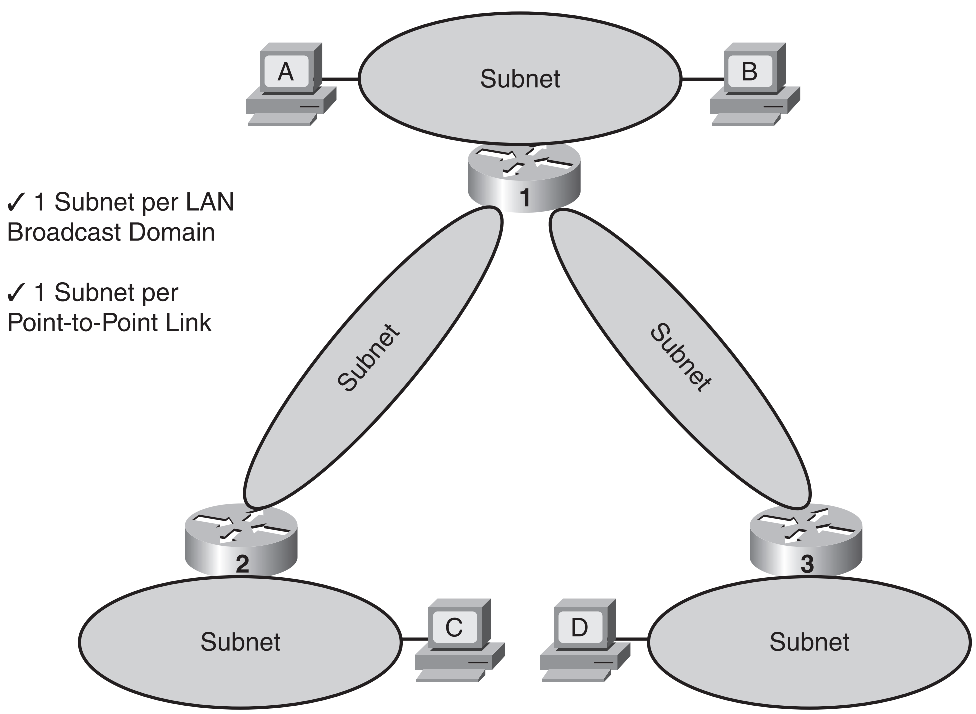
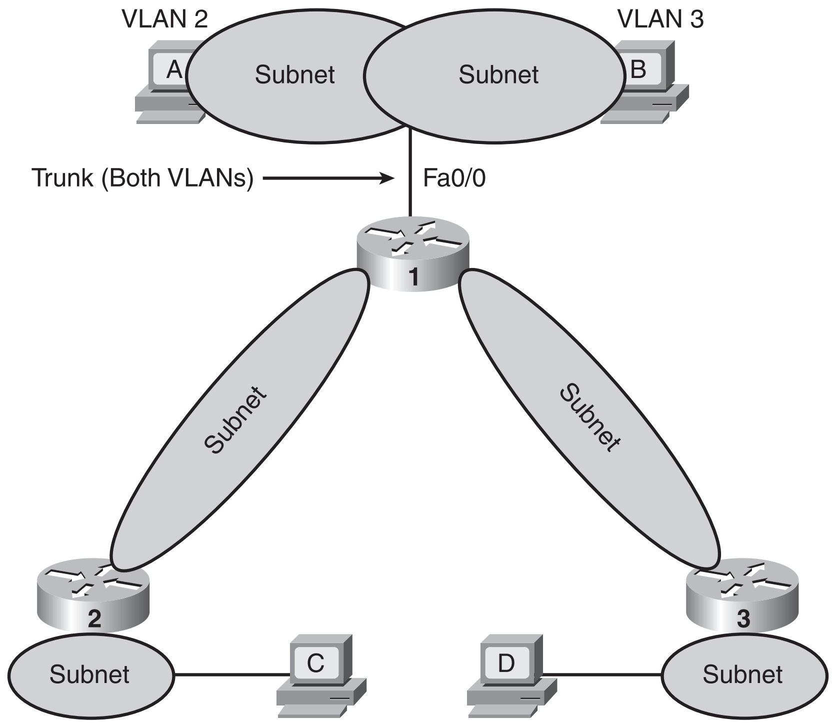


Figure 7-3 Additional Subnets when Using VLANs



Step 2 Reference

This step shows another example of the process shown in Lab 6, which explains how to find all subnets of a classful network. The generic process used to find these subnets, which is also found in Lab 6, is as follows:

1. Write down the mask in a table, in dotted-decimal format.
2. Find the interesting octet of the mask—the octet that is neither 255 nor 0—and draw a rectangle around that column of the table.
3. Calculate the magic number (256 minus the mask's value in the interesting octet).
4. Write down the classful network number in the row labeled Zero Subnet.
5. To find each successive subnet number:

   a) Copy the previous subnet number's three boring octets.

   b) For the interesting octet, add the magic number to the previous subnet's interesting octet value.
6. When Step 5b's sum is 256, stop. The subnet found before the sum of 256 is the last subnet, namely the broadcast subnet.

Figure 7-4 shows work in progress through Step 4.

Figure 7-4 Work in Progress Through Step 4

IP Network: 172.20.0.0
Mask: 255.255.255.0

2) Put a box around the interesting octet.

1) Write down the subnet mask.

3) Calculate the magic number: 256 - mask.

4) Write down the network number, which is also the zero subnet.

Use Smallest Numeric Subnet Numbers

Network Bits: 16
Subnet Bits: 8
Host Bits: 8

		256	
255	255	-255	0
		1	
172	20	0	0

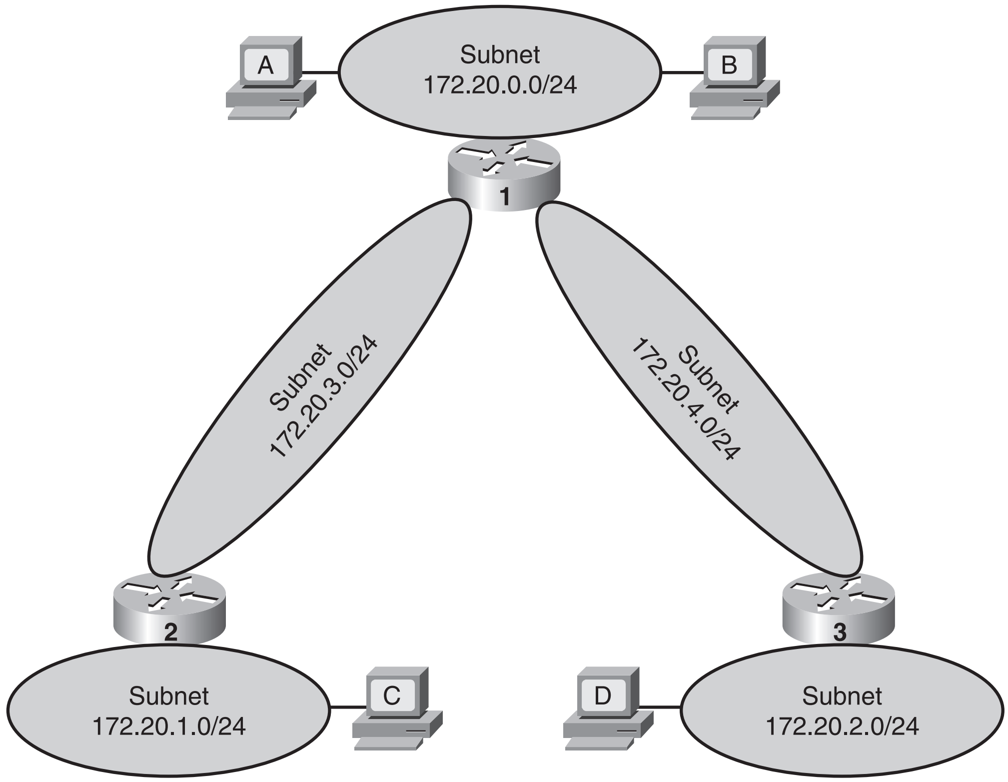
Figure 7-5 shows work in progress after completing all passes and finding all subnet numbers.

Figure 7-5 List of All Subnets

Mask	255	255	255	0
Magic Number			1	
Network Number/Zero Subnet	172	20	+ 0	0
5a) Copy the previous subnet's three uninteresting octets.			1	
	172	20	2	0
	172	20	3	0
	172	20	4	0
	172	20	5	0
5b) Add the magic number to the previous subnet's interesting octet.	172	20	6	0
			…	
	172	20	255	0

Figure 7-6 shows the subnets chosen from the list of subnets and the locations for each subnet.

Figure 7-6 Subnets and Locations in This Video



Step 3 Reference

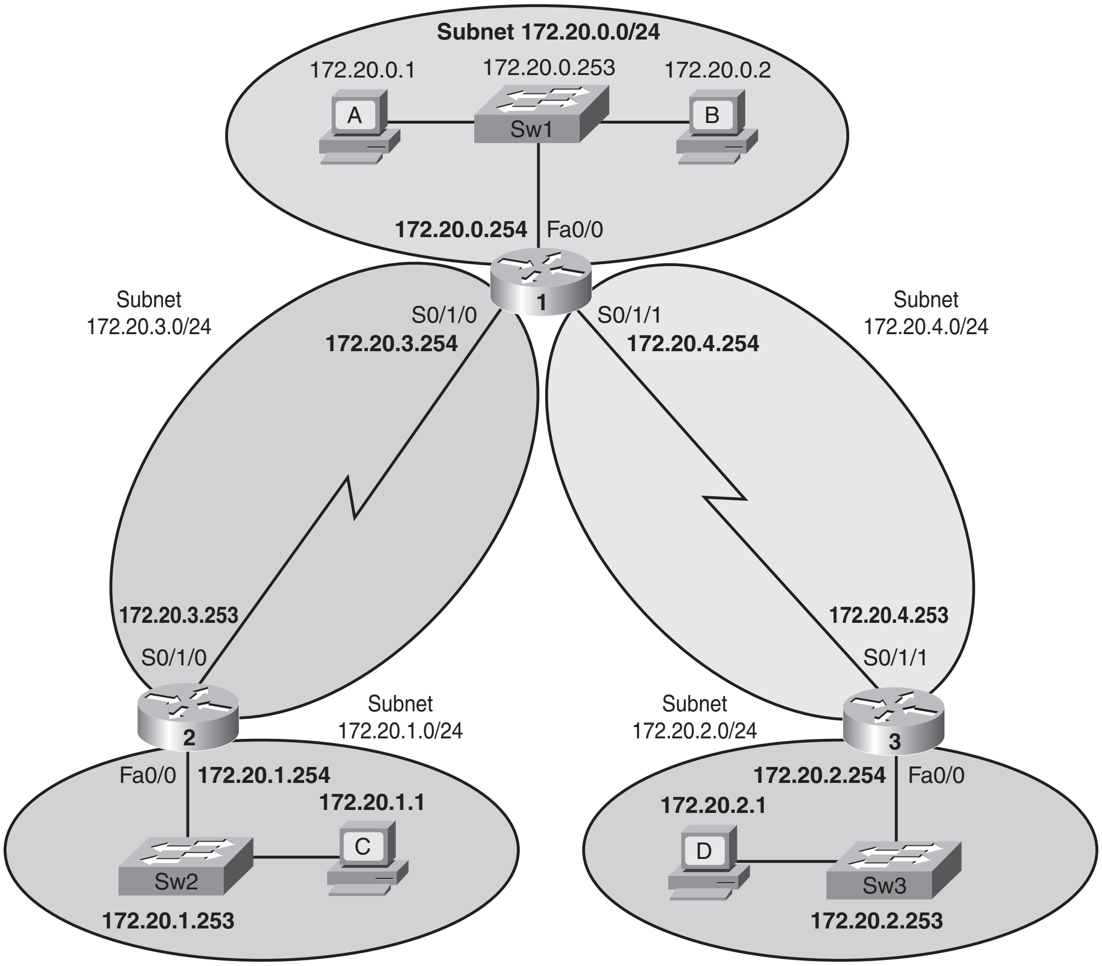
Table 7-1 lists the six numerically smallest subnet numbers for this video, along with the range of IP addresses and subnet broadcast address for each subnet.

Table 7-1 Numerically Smallest Subnet Numbers, IP Address Range, and Broadcast Address

Subnet Number	Smallest Usable Address	Largest Usable Address	Broadcast Address
172.20.0.0	172.20.0.1	172.20.0.254	172.20.0.255
172.20.1.0	172.20.1.1	172.20.1.254	172.20.1.255
172.20.2.0	172.20.2.1	172.20.2.254	172.20.2.255
172.20.3.0	172.20.3.1	172.20.3.254	172.20.3.255
172.20.4.0	172.20.4.1	172.20.4.254	172.20.4.255
172.20.5.0	172.20.5.1	172.20.5.254	172.20.5.255

Figure 7-7 shows the individual IP addresses chosen to meet the requirements of the network manager—highest IP addresses for the routers, next highest for the switches, and smallest for the hosts.

Figure 7-7 Figure with Actual IP Addresses Listed



Lab 8

Static and Connected Routes

This *CCNA Video Mentor* (CVM) lab shows how to configure static routes in a simple internetwork. In particular, the objectives of this lab are the following:

- Explain the concept of connected routes
- List the requirements for a router to create a connected route
- Configure an **ip route** command using two different styles:
  - Using a next-hop IP address
  - Using an outgoing interface
- Describe the parts of an individual route

Scenario

This lab contains three main steps, as follows:

Step 1. Show how two routers, when configured with IP addresses on working interfaces, add connected routes to their routing tables.

Step 2. Explain the need for a static route on router R1 to forward packets from left-to-right in the network used in this lab and see how to configure and verify that static route.

Step 3. Explain the need for a static route on router R2 to forward packets from right-to-left in the network used in this lab. Then see how to configure and verify that static route, this time using the outgoing interface option in the **ip route** command.

Initial Configurations

Examples 8-1 and 8-2 show the pertinent configurations of routers R1 and R2 for this lab. As usual, the parts of the configurations not relevant to this lab have been omitted.

Example 8-1 Initial Configuration for R1

```
hostname R1
!
interface FastEthernet 0/0
 ip address 172.22.11.1 255.255.255.0
!
interface Serial 0/1/0
 ip address 172.22.112.1 255.255.255.0
```

Example 8-1 Initial Configuration for R1 *continued*

```
!
interface Serial 0/1/1
 ip address 172.22.113.1 255.255.255.0
 shutdown
```

Example 8-2 Initial Configuration for R2

```
hostname R2
!
interface FastEthernet 0/0
 ip address 172.22.12.2 255.255.255.0
!
interface Serial 0/1/0
 ip address 172.22.112.2 255.255.255.0
```

Ending Configurations

None of the initial configuration is changed. However, Examples 8-3 and 8-4 show the configuration added to R1 and R2, respectively, by the end of the lab video.

Example 8-3 Configuration Added to R1 During the Lab Video

```
ip route 172.22.12.0 255.255.255.0 172.22.112.2
```

Example 8-4 Configuration Added to R2 During the Lab Video

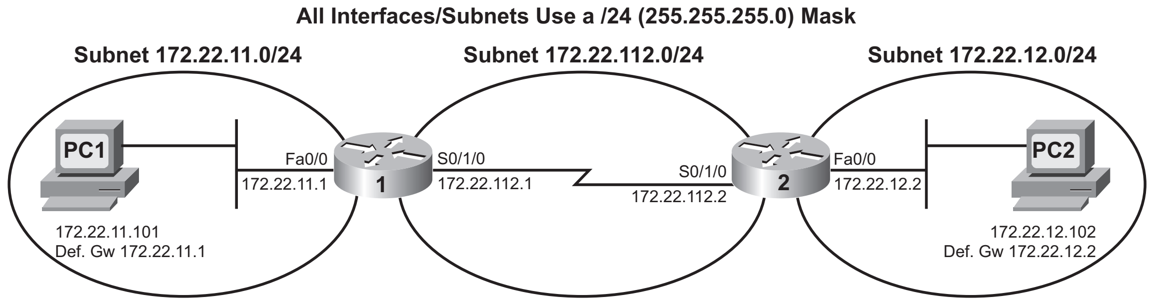
```
ip route 172.22.11.0 255.255.255.0 S0/1/0
```

Video Presentation Reference

This video presents several figures that describe the internetwork and the need for additional routes on the routers. This section simply lists these figures for reference.

Figure 8-1 shows a diagram of the network used in this example.

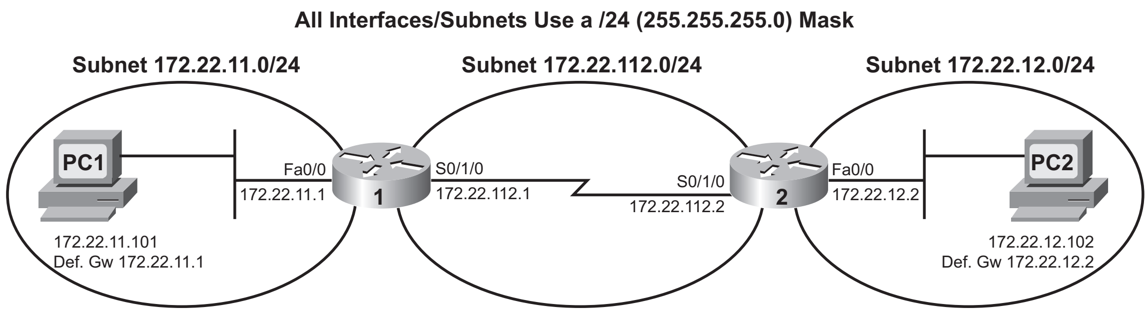
Figure 8-1 Lab 5 Network Topology



Because the video is organized into three separate steps, the reference materials have been organized into three separate sections.

Step 1 Reference

Figure 8-2 Analysis of Connected Routes



R1 Routing Table

Subnet	Next-Hop	Int.
172.22.11.0/24	(Connected)	Fa0/0
172.22.112.0/24	(Connected)	S0/1/0

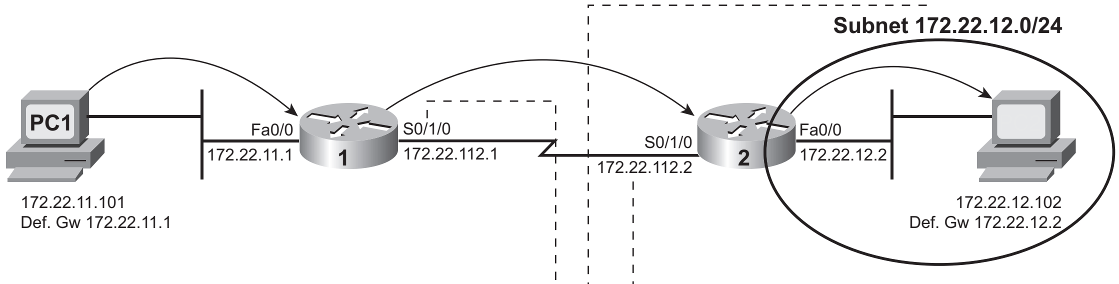
R2 Routing Table

Subnet	Next-Hop	Int.
172.22.112.0/24	(Connected)	S0/1/0
172.22.12.0/24	(Connected)	Fa0/0

Requirements to Add a Connected Route:
1) IP address is configured on the interface.
2) Interface is “UP and UP.”

Step 2 Reference

Figure 8-3 Need for a Static Route to 172.22.12.0/24



R1 Routing Table

Subnet	Next-Hop	Int.
172.22.11.0/24	(Connected)	Fa0/0
172.22.112.0/24	(Connected)	S0/1/0
172.22.12.0/24	**172.22.112.2**	**S0/1/0**

R2 Routing Table

Subnet	Next-Hop	Int.
172.22.112.0/24	(Connected)	S0/1/0
172.22.12.0/24	(Connected)	Fa0/0

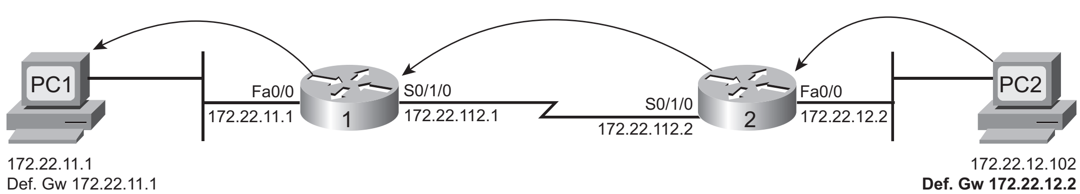
Figure 8-4 ip route Command with Next-hop

ip route *subnet-number subnet-mask* *next-hop-ip-address*

172.22.12.0 255.255.255.0 172.22.112.2 (R2)

Step 3 Reference

Figure 8-5 Need for a Static Route to 172.22.11.0/24



R1 Routing Table

Subnet	Next-Hop	Int.
172.22.11.0/24	(Connected)	Fa0/0
172.22.112.0/24	(Connected)	S0/1/0
172.22.12.0/24	**172.22.112.2**	**S0/1/0**

R2 Routing Table

Subnet	Next-Hop	Int.
172.22.112.0/24	(Connected)	S0/1/0
172.22.12.0/24	(Connected)	Fa0/0
172.22.11.0/24	**172.22.112.1**	**S0/1/0**

Figure 8-6 ip route Command with Outgoing Interface

ip route *subnet-number subnet-mask* *outgoing-interface*

172.22.11.0 255.255.255.0 S0/1/0

Lab 9

RIP Configuration

This *CCNA Video Mentor* lab shows how to configure RIP Version 1 (V1) in an internetwork that uses two alternative IP addressing schemes. The objectives of this lab are as follows:

- Configure the RIP **network** command.
- Describe how a router interprets the RIP **network** command.
- Describe some of the key information in the output of the **show ip protocols** command.
- Compare the default RIP version behavior to a router that has been configured to use only RIP version 2.

Scenario

This lab contains two main steps, as follows:

Step 1. Configure RIP in a network that uses only subnets of Class B network 172.22.0.0, with default version settings.

Step 2. See the effects of mismatched versions, and migrate to Version 2.

Initial Configurations

Examples 9-1 through 9-3 show the pertinent initial configurations of Routers R1, R2, and R3 in the lab video. Note that this lab begins with these three routers having the correct IP addresses configured, along with the initial RIP configuration on Router R3, to match the topology illustrated later in the chapter in Figure 9-1. As usual, the parts of the configurations not relevant to this lab have been omitted.

Example 9-1 Initial Configuration for R1

```
hostname R1
!
interface FastEthernet 0/0
 ip address 172.22.11.1 255.255.255.0
!
interface serial 0/1/0
 ip address 172.22.112.1 255.255.255.0
 clock rate 1536000
!
interface serial 0/1/1
 ip address 172.22.113.1 255.255.255.0
 clock rate 1536000
```

Example 9-2 Initial Configuration for R2

```
hostname R2
!
interface FastEthernet 0/0
 ip address 172.22.12.2 255.255.255.0
!
interface serial 0/1/0
 ip address 172.22.112.2 255.255.255.0
!
interface serial 0/1/1
 ip address 172.22.123.2 255.255.255.0
 clock rate 1536000
```

Example 9-3 Initial Configuration for R3

```
hostname R3
!
interface FastEthernet 0/0
 ip address 172.22.13.3 255.255.255.0
!
interface serial 0/1/0
 ip address 172.22.123.3 255.255.255.0
!
interface serial 0/1/1
 ip address 172.22.113.3 255.255.255.0
!
router rip
 version 2
 network 172.22.0.0
```

Configuration After Lab Step 1

This lab adds configuration at both Step 1 and Step 2. Example 9-4 shows the configuration added to R1 during Step 1. Example 9-5 shows the configuration added to R2 at Step 1.

Example 9-4 Configuration Added to R1 During Step 1

```
router rip
 network 172.22.0.0
```

Example 9-5 Configuration Added to R2 During Step 1

```
router rip
 network 172.22.0.0
```

Ending Configurations

This lab adds the RIP **version 2** command to both R1's and R2's RIP configuration as part of Step 2. Example 9-6, 9-7, and 9-8 list the ending RIP configuration on Routers R1, R2, and R3, for easy reference.

Example 9-6 Ending RIP Configuration on R1

```
router rip
 version 2
 network 192.22.0.0
```

Example 9-7 Ending Configuration on R2

```
router rip
 version 2
 network 192.22.0.0
```

Example 9-8 Ending Configuration on R3

```
router rip
 version 2
 network 192.22.0.0
```

Video Presentation Reference

This video includes several figures that contain the same images used in the lab video. Because the video is organized into two separate steps, the reference materials have been organized into two separate sections. Each section simply lists these figures and tables for reference.

Step 1 Reference

Figure 9-1 Three Routers, Six Subnets of Class B Network 172.22.0.0

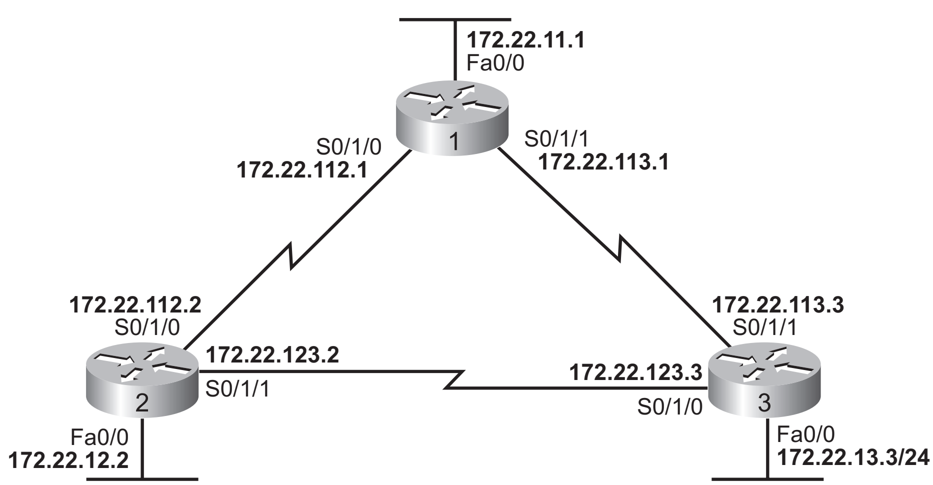


Figure 9-2 **Subnet Reference for Step 1**

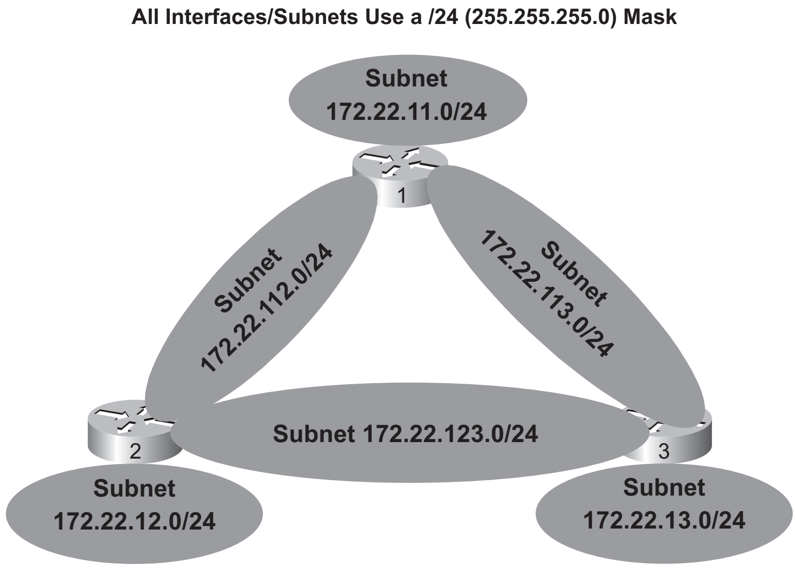


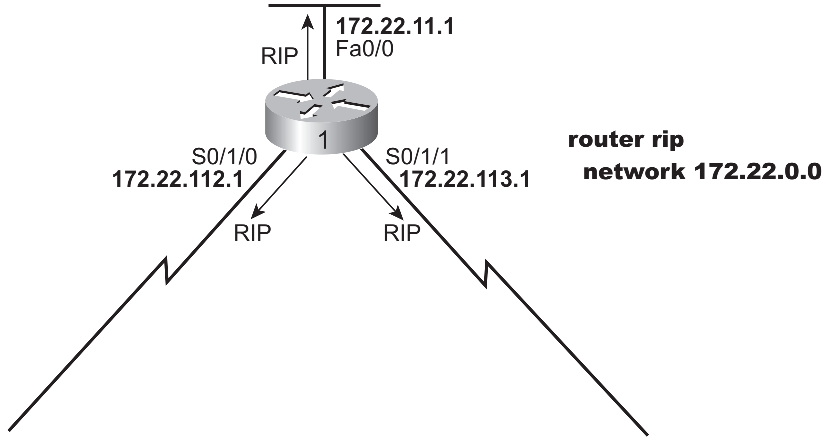
Figure 9-3 **Format of the RIP network Command**

network *network-number*

The **network** command

- ✓ Class A, B, or C network number
- ✓ Tells router to "do RIP" on all interfaces in that network
- ✓ "Doing RIP" on an interface means:
  1. Send RIP updates
  2. Listen for RIP updates
  3. Advertise about the subnet connected to the interface

Figure 9-4 Impact of the RIP network Command: R1, Step 1



Step 2 Reference

Figure 9-5 Effect of Version 2 Updates Sent to R1 and R2

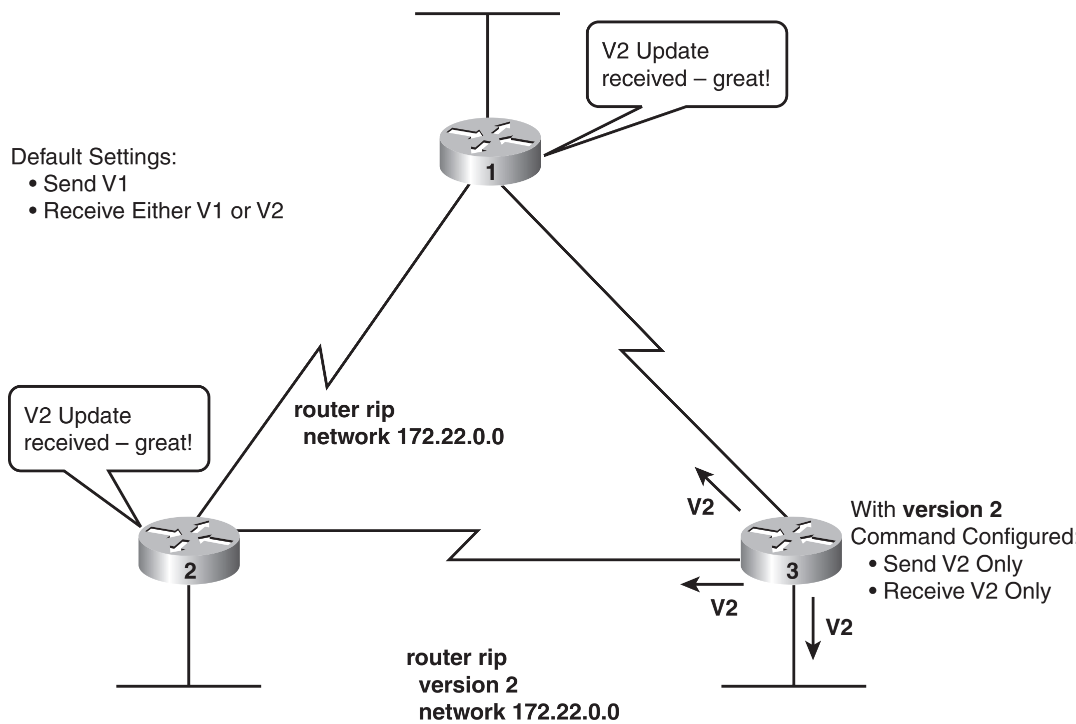
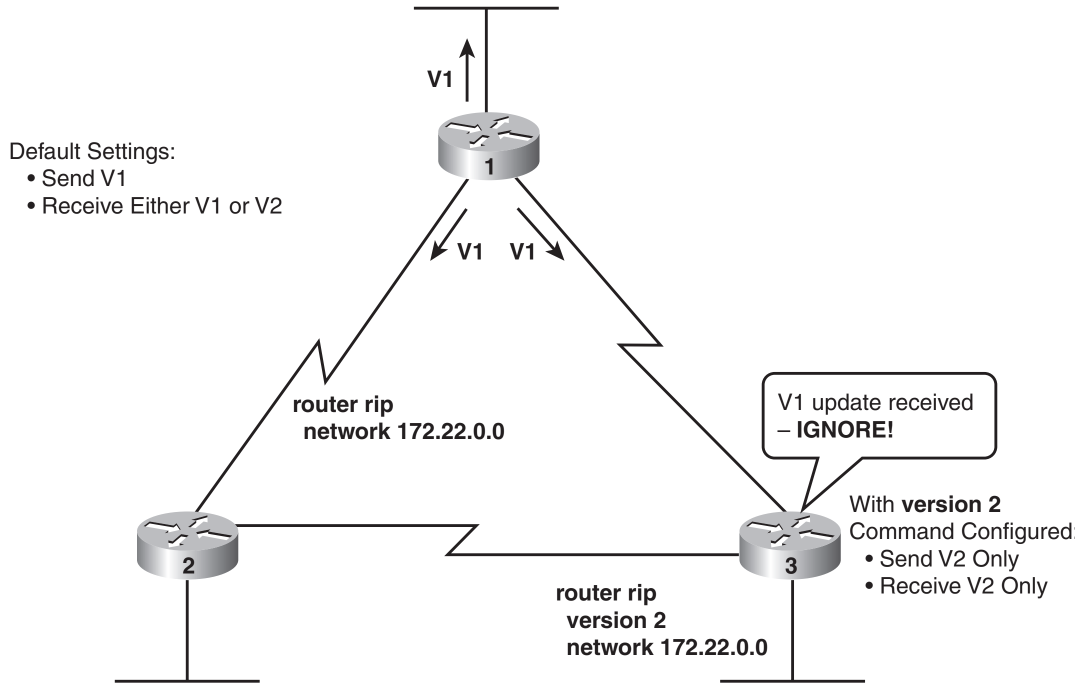


Figure 9-6 Effect of Version 1 Updates Sent to R3



ICND2 Labs

The CCNA certification can be achieved through two different paths: by taking the single CCNA (640-802) exam or by taking both the ICND1 (640-822) and ICND2 (640-816) exams. This product separates the video labs into two sections, with labs focusing on the ICND2 exam in this section and labs focusing on the ICND1 exam in the other section. The labs in both sections apply to the CCNA exam.

Lab 1

Configuring VLANs

This *CCNA Video Mentor* lab shows how to use the commands required to configure virtual LANs (VLANs) on Cisco IOS Software-based switches, in addition to a few of the commands used to examine VLAN operations. In particular, the objectives of this lab are as follows:

- Configure VLANs on Cisco switches
- Configure the VTP mode on Cisco switches
- Determine the status of VLAN trunks
- Configure 802.1Q trunking between two Cisco switches

Scenario

This lab contains two main steps, as follows:

Step 1. Use a *three-step process* to create the first VLAN on a switch:

Configure VTP mode

Create a VLAN

Add interfaces to that VLAN

Step 2. Examine and configure *802.1Q trunking* between two switches

Initial Configurations

The two switches in this lab begin with some basic configuration. First, host switches have their host-names configured. Second, the switch ports connected to the PCs have been configured to use the **spanning-tree portfast** command, which causes these end-user ports not to wait on Spanning Tree Protocol (STP) timers when the ports are administratively enabled. However, all VLAN configurations has been removed before this lab begins. Examples 1-1 and 1-2 show the basic initial configurations for both switches in this lab.

Example 1-1 Initial Configuration for Sw1

```
hostname Sw1
!
interface FastEthernet 0/11
 spanning-tree portfast
!
interface FastEthernet 0/13
```

Example 1-1 Initial Configuration for Sw1 *continued*

```
 spanning-tree portfast
!
interface vlan 1
 ip address 172.30.1.101 255.255.255.0
 no shutdown
!
ip default-gateway 172.30.1.251
```

Example 1-2 Initial Configuration for Sw2

```
hostname Sw2
!
interface FastEthernet 0/12
 spanning-tree portfast
!
interface vlan 1
 ip address 172.30.1.102 255.255.255.0
 no shutdown
!
ip default-gateway 172.30.1.251
```

Ending Configurations

This lab adds some configuration commands to both Sw1 and Sw2; however, it does not change any of the earlier configurations. Examples 1-3 and 1-4 show the configuration added during the lab.

Example 1-3 Configuration on Sw1 Added During this Lab

```
vtp transparent
!
vlan 11
 name thisisvlan11
!
interface FastEthernet 0/11
 switchport access vlan 11
!
interface FastEthernet 0/13
 switchport access vlan 11
!
interface FastEthernet 0/23
 switchport mode trunk
```

Example 1-4 Configuration on Sw2 Added During this Lab

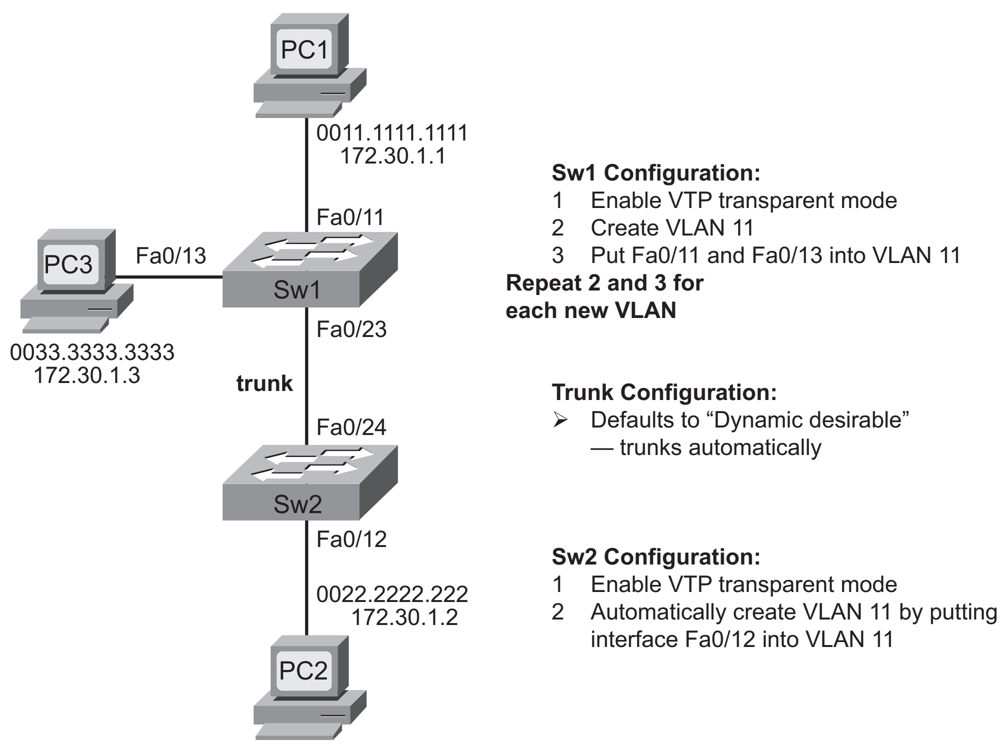
```
vtp transparent
!
vlan 11
!
interface FastEthernet 0/12
 switchport access vlan 11
```

Video Presentation Reference

This video presents several figures and a table that support the concepts covered in the lab. This section simply lists these figures for reference. Because the video is organized into three separate steps, the reference materials have been organized into three separate sections.

Step 1 Reference

Figure 1-1 Step 1 Topology and Configuration Steps



Step 2 Reference

Table 1-1 The Meaning of the *type* Option of the switchport mode Command

Value of the *type* Keyword	Meaning of the *type* Keyword
access	Always do *not* trunk
trunk	Always trunk
dynamic desirable	Negotiate whether to trunk or not and initiate the process
dynamic auto	Negotiate whether to trunk or not but do not initiate the process

Table 1-2 Trunk Configuration Options for Making Two LAN Switches Trunk

SW1 Configuration for Trunking Mode	Required Setting on SW2 to Trunk
access	None—cannot trunk
trunk	Trunk, dynamic desirable, or dynamic auto
dynamic desirable	Trunk, dynamic desirable, or dynamic auto
dynamic auto	Trunk or dynamic desirable

Lab 2

VTP Servers and Clients

This *CCNA Video Mentor* lab explains how to configure VTP servers and clients, lists the requirements that must be met for those switches to exchange VLAN information, and explains how to use **show** commands to confirm that the switches have learned about new VLANs. In particular, the objectives of this lab are as follows:

- Configure VTP on Cisco switches.
- Verify whether the switches meet the required conditions that enable VTP to work between two switches.
- Verify that a VTP client has learned VLAN information from a VTP peer.

Scenario

This lab contains three main steps, as follows:

Step 1. Configure one switch as a VTP server and another as a VTP client.

Step 2. Complete all VTP requirements by configuring trunking between two switches.

Step 3. Configure VLANs on the VTP server and confirm that the VTP client has learned about the VLANs.

Initial Configurations

The two 2960 switches in this lab begin with some basic configuration, but with all default settings related to VTP and the VLAN database. Both switches have their hostnames configured, and each has an IP address assigned to its respective VLAN 1 interface. Example 2-1 and Example 2-2 show the basic initial configurations for both switches in this lab.

Example 2-1 Initial Configuration for Sw1

```
hostname Sw1
!
interface vlan 1
 ip address 172.30.1.101 255.255.255.0
 no shutdown
```

Example 2-2 Initial Configuration for Sw2

```
hostname Sw2
!
interface vlan 1
 ip address 172.30.1.102 255.255.255.0
 no shutdown
```

Ending Configurations

This lab adds some configuration commands to both Sw1 and Sw2; however, it does not change any of the earlier configurations. Example 2-3 and Example 2-4 show the configuration added during the lab.

Example 2-3 Configuration on Sw1 Added During This Lab

```
vtp domain Fred
vtp password Barney
!
vlan 2
 name Wilma
!
interface gigabitEthernet 0/1
 switchport mode trunk
!
interface fastethernet 0/1
 switchport access vlan 2
```

Example 2-4 shows the ending configuration on Sw2; however, note that the video shows the configuration of the **vtp domain fred** command, which is later replaced with the **vtp domain Fred** command.

Example 2-4 Configuration on Sw2 Added During This Lab

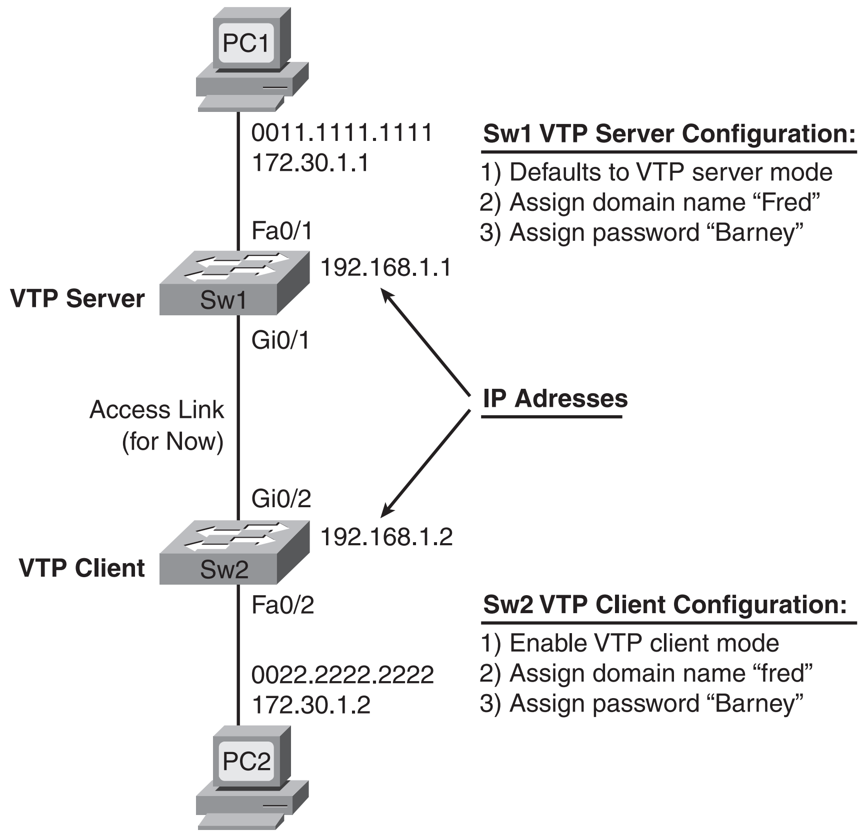
```
vtp mode client
vtp domain Fred
vtp password Barney
!
interface fastethernet 0/2
 switchport access vlan 2
```

Video Presentation Reference

This video presents several figures and a table that support the concepts covered in the lab. This section simply lists these figures for reference. Because the video is organized into three separate steps, the reference materials have been organized into three separate sections.

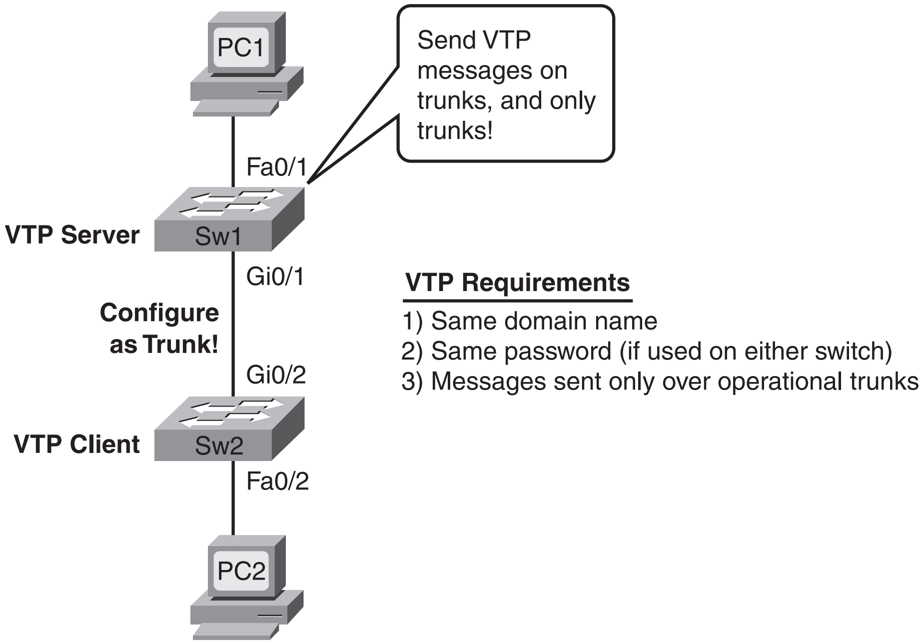
Step 1 Reference

Figure 2-1 Step 1 Topology and Configuration



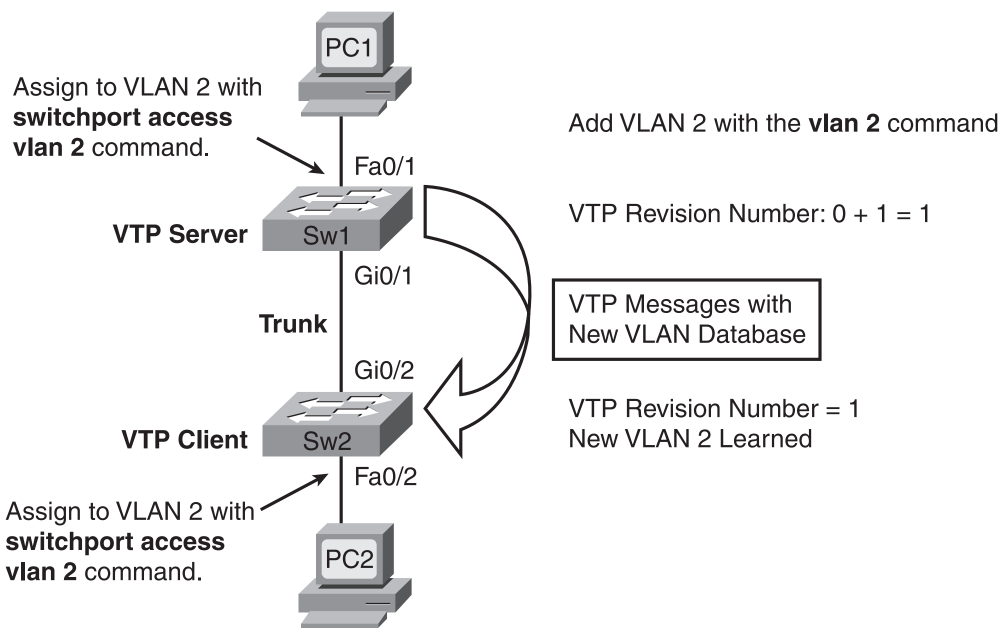
Step 2 Reference

Figure 2-2 **Requirements for VTP to Work Properly**



Step 3 Reference

Figure 2-3 **VLAN Configuration Process Shown in This Video**



Lab 3

RIP V1 with Split Horizon, Route Poisoning, and Poison Reverse

This *CCNA Video Mentor* lab helps you build a deeper understanding of RIP operations, particularly of the effect of distance vector loop-avoidance mechanisms. The lab begins with a small working internetwork using RIP. Then the lab explains how RIP works when all links are up and working and how RIP works when a link fails. In particular, this lab covers the following:

- Interpret the contents of the routing table using the **show ip route** command
- Determine which RIP update sources continue to send periodic updates using the **show ip protocols** command
- Interpret debug messages that show the effects of
  - Split horizon
  - Route poisoning
  - Poison reverse
  - Triggered updates

Scenario

This lab contains three main steps, as follows:

Step 1. A description of an internetwork topology—including descriptions of the routes learned by each router—and ways to confirm that RIP continues to send periodic routing updates.

Step 2. A description of split horizon, with router **debug** messages showing the effects of split horizon on the internetwork

Step 3. A description of triggered updates, poison routes, and poison reverse routes, followed by router **debug** command output that shows all of these features.

Initial Configurations

Example 3-1 shows the initial configuration of router R2 at the beginning of the lab. Note that only the pertinent configuration is shown. Similarly, Example 3-2 shows the initial configuration of R3. As usual, the parts of the configurations that are not relevant to this lab have been omitted.

Example 3-1 Initial Configuration for R2

```
interface fastethernet0/0
 ip address 192.168.2.2 255.255.255.0
!
interface serial 0/1/1
 ip address 192.168.4.9 255.255.255.252
 clock rate 1536000
!
interface serial 0/1/0
 description link connected to router R1 - not used in this lab
 shutdown
!
router rip
 network 192.168.2.0
 network 192.168.4.0
```

Example 3-2 Initial Configuration for R3

```
interface fastethernet0/0
 ip address 192.168.3.3 255.255.255.0
!
interface fastethernet0/1
 ip address 192.168.33.3 255.255.255.0
!
interface serial 0/1/0
 ip address 192.168.4.10 255.255.255.252
!
interface serial 0/1/1
! description link connected to router R1 – not used in this lab
 shutdown
!
router rip
 network 192.168.3.0
 network 192.168.33.0
 network 192.168.4.0
```

Ending Configurations

This lab does not change the routers' configurations, other than to shut down the fa0/1 interface on R3 to demonstrate what happens with RIP.

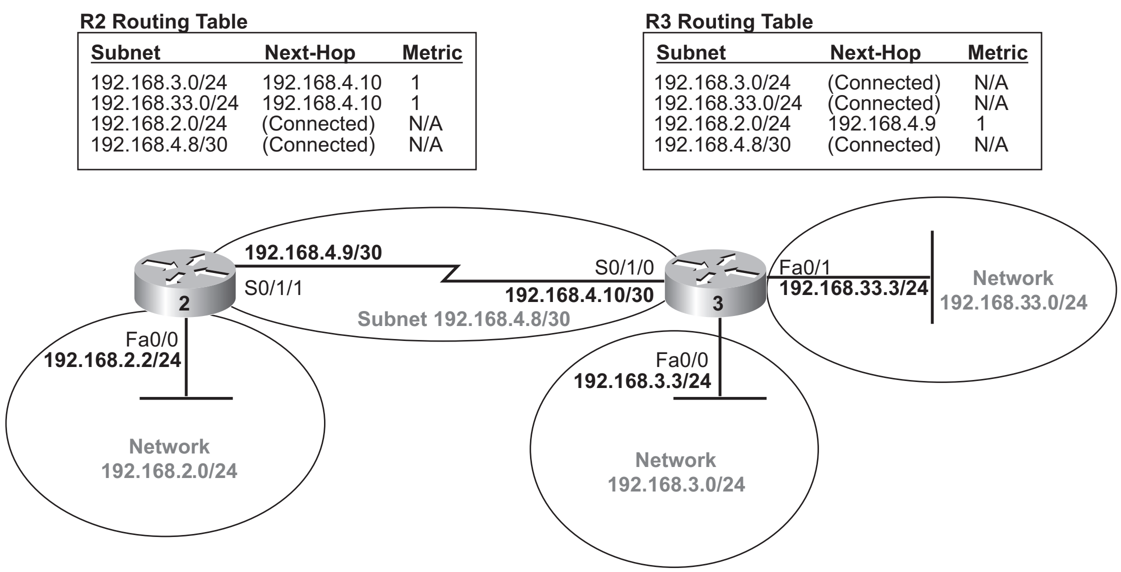
Video Presentation Reference

This video presents several figures that describe the internetwork and the need for additional routes on the routers. This section simply lists these figures for reference.

Because the video is organized into three separate steps, the reference materials have been organized into three separate sections.

Step 1 Reference

Figure 3-1 Lab 7 Topology



Step 2 Reference

Figure 3-2 Split Horizon on R2

R2 Routing Table

Subnet	Next-Hop	Out. Int.	Metric
192.168.2.0/24	(Connected)	Fa0/0	N/A
192.168.33.0/24	192.168.4.10	S0/1/1	1
192.168.3.0/24	192.168.4.10	S0/1/1	1
192.168.4.8/30	(Connected)	S0/1/1	N/A

Split Horizon:

For an update sent out **S0/1/1,** do not advertise routes whose outgoing interface is **S0/1/1**

RIP V1 Update – Sent out S0/1/1

Subnet	Metric
192.168.2.0	1

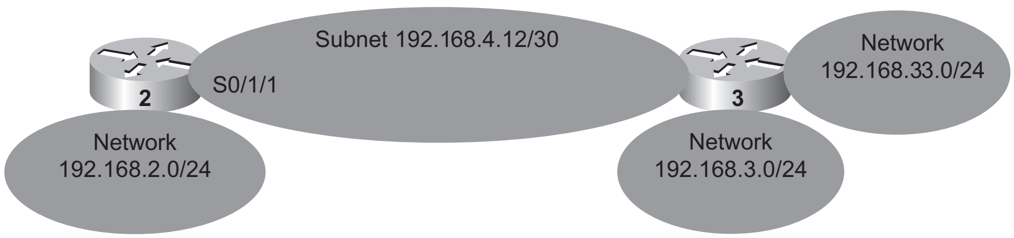


Figure 3-3 Split Horizon on R3

Split Horizon:

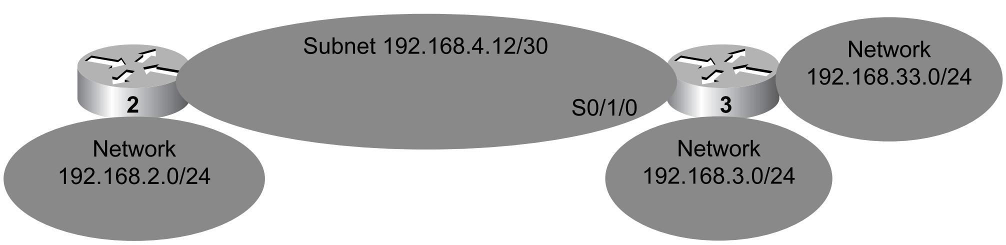
For an update sent out **S0/1/0**, do not advertise routes whose outgoing interface is **S0/1/0**

R3 Routing Table

Subnet	Next-Hop	Out. Int.	Metric
192.168.3.0/24	(Connected)	Fa0/0	N/A
192.168.33.0/24	(Connected)	Fa0/1	N/A
192.168.2.0/24	192.168.4.9	S0/1/0	1
192.168.4.8/30	(Connected)	S0/1/0	N/A

RIP V1 Update – Sent out S0/1/0

Subnet	Metric
192.168.3.0	1
192.168.33.0	1



Step 3 Reference

Figure 3-4 Triggered Updates and Route Poisoning

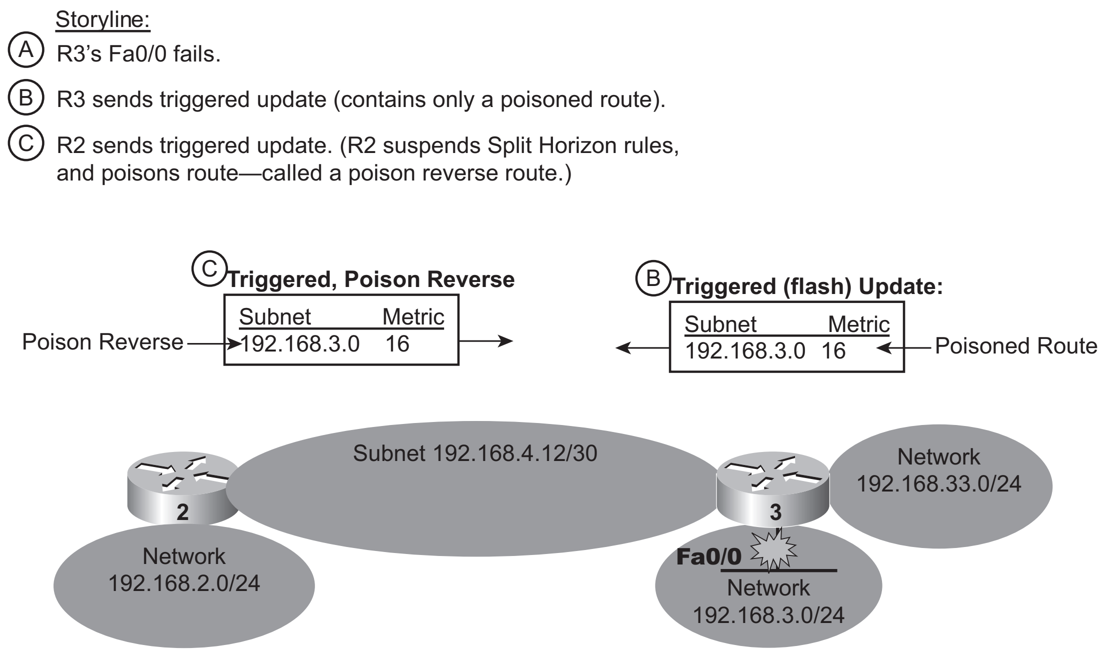
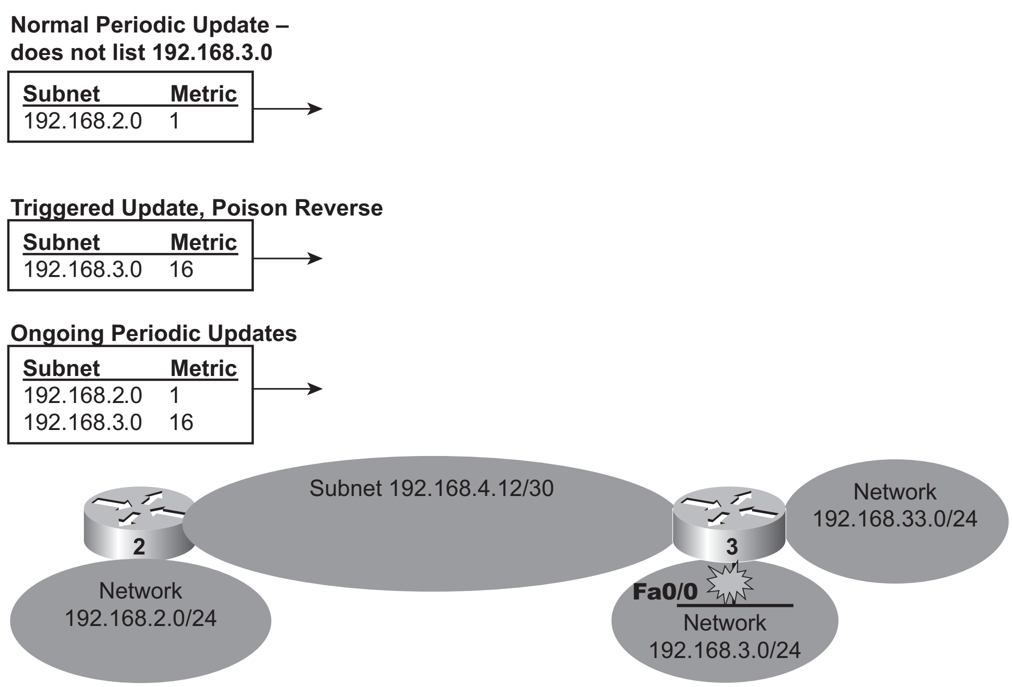


Figure 3-5 Split Horizon with Poison Reverse



Lab 4

Single Area and Multi-area OSPF Configuration

This *CCNA Video Mentor* lab shows how to configure OSPF using several different styles of OSPF **network** commands, both for a single area and for multiple areas. In particular, the objectives of this lab are the following:

- Configure the OSPF **network** command to correctly match an interface and place it into the correct area
- Describe generally how the wildcard mask controls how the OSPF **network** command works
- Configure an Area Border Router (ABR) by placing different interfaces in different areas
- Distinguish between intra-area and interarea OSPF-learned routes
- Describe how a router picks its router ID (RID)

Scenario

This lab contains three main steps, as follows:

Step 1. Examine the single-area OSPF configuration on three routers (R1, R2, and R3)

Step 2. Configure an Area Border Router (ABR) to be connected to multiple OSPF areas

Step 3. Analyze how a router chooses its OSPF RID and verify the RID chosen by a router

Initial Configurations: Lab Step 1

Examples 4-1 through 4-3 show the pertinent initial configurations of routers R1, R2, and R3. All routers begin with all pertinent IP addresses configured, all necessary links up, and OSPF configured to put all links into area 0, as illustrated in Figure 4-1. As usual, the parts of the configurations not relevant to this lab have been omitted.

Example 4-1 Initial Configuration for R1

```
hostname R1
!
interface FastEthernet 0/0
 ip address 172.22.11.1 255.255.255.0
!
interface FastEthernet 0/1
 ip address 172.22.10.1 255.255.255.0
!
interface loopback 1
 ip address 11.11.11.11 255.255.255.0
!
interface loopback 2
 ip address 1.1.1.1 255.255.255.0
!
router ospf 1
 network 172.22.11.1 0.0.0.0 area 0
 network 172.22.10.1 0.0.0.0 area 0
```

Example 4-2 Initial Configuration for R2

```
interface FastEthernet 0/0
 ip address 172.22.12.2 255.255.255.0
!
interface FastEthernet 0/1
 ip address 172.22.10.2 255.255.255.0
!
interface loopback 1
 ip address 2.2.2.2 255.255.255.0
!
router ospf 1
 network 0.0.0.0 255.255.255.255 area 0
```

Example 4-3 Initial Configuration for R3

```
interface FastEthernet 0/0
 ip address 172.22.13.3 255.255.255.0
!
interface FastEthernet 0/1
 ip address 172.22.10.3 255.255.255.0
!
router ospf 2
 network 172.22.0.0  0.0.255.255 area 0
```

Initial Configurations: Lab Step 2

Lab 4's second step adds routers R5 and R6 to the network topology. Examples 4-4 and 4-5 show the initial configurations on these routers needed to begin Step 2. Both routers begin with all pertinent IP addresses configured and all necessary links up, but OSPF is configured on R6 only. The OSPF configuration matches the design shown in Figure 4-1.

Example 4-4 R5 Initial Configuration Needed to Begin Step 2

```
hostname R5
!
interface Serial0/0
 ip address 172.22.115.5 255.255.255.0
!
interface FastEthernet0/0
 ip address 172.22.15.5 255.255.255.0
```

Example 4-6 R6 Initial Configuration Needed to Begin Step 2

```
hostname R6
!
interface Serial0/0
 ip address 172.22.116.6 255.255.255.0
!
interface FastEthernet0/0
 ip address 172.22.16.6 255.255.255.0
!
router ospf 1
 network 0.0.0.0 255.255.255.255 area 6
```

Ending Configurations

This lab video ends with R1 having added configuration to support areas 5 and 6 and with OSPF configuration having been added to router R5. Example 4-6 shows the configuration added to R1, with Example 4-7 showing all pertinent configuration of R5.

Example 4-6 Configuration Added to R1 During the Video

```
interface Serial0/1/0
 ip address 172.22.115.1 255.255.255.0
 clock rate 1536000
 no shutdown
!
```

Example 4-6 Configuration Added to R1 During the Video *continued*

```
interface Serial0/1/1
 ip address 172.22.116.1 255.255.255.0
 clock rate 1536000
 no shutdown
!
router ospf 1
 network 172.22.115.1 0.0.0.0 area 5
 network 172.22.116.1 0.0.0.0 area 6
```

Example 4-7 Configuration Added to R5 During the Video

```
router ospf 1
 network 0.0.0.0 255.255.255.255 area 5
```

Video Presentation Reference

This video includes several figures and one table that both help explain the scenario in the lab and list important reference information.

Because the video is organized into three separate steps, the reference materials have been organized into three separate sections. Each section simply lists these figures and tables for reference.

Step 1 Reference

Figure 4-1 Three Routers and Four LAN Subnets Used in Step 1

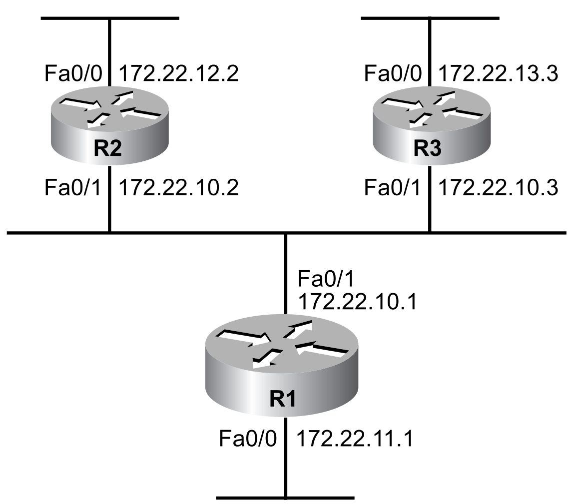


Figure 4-2 Subnets and OSPF Areas Used in Step 1

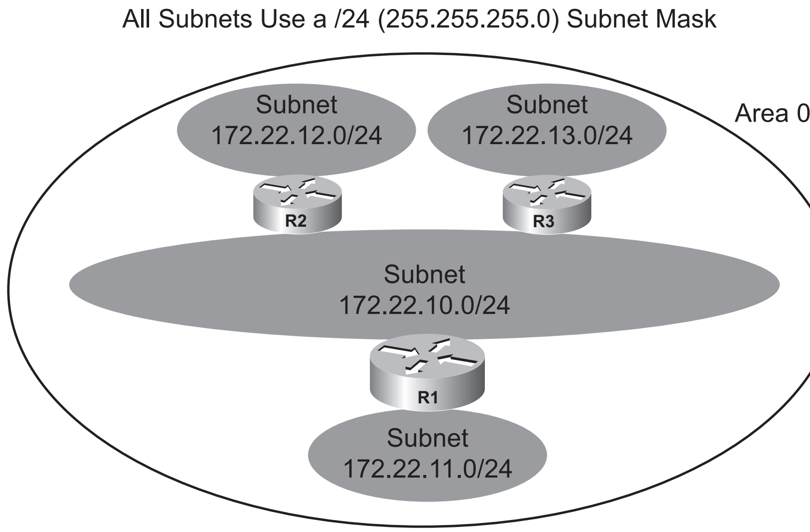


Figure 4-3 Format of the OSPF network Command

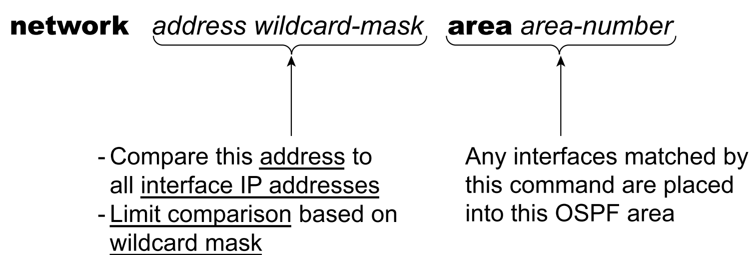


Table 4-1 Sample OSPF network Command Wildcard Masks and Their Meanings

Wildcard Mask	Meaning
0.0.0.0	Compare the entire address
0.0.0.255	Compare the first 3 octets only
0.0.255.255	Compare the first 2 octets only
0.255.255.255	Compare the first octet only
255.255.255.255	No need to compare anything—all addresses are considered to match

Step 2 Reference

Figure 4-4 Expanded Topology for Step 2

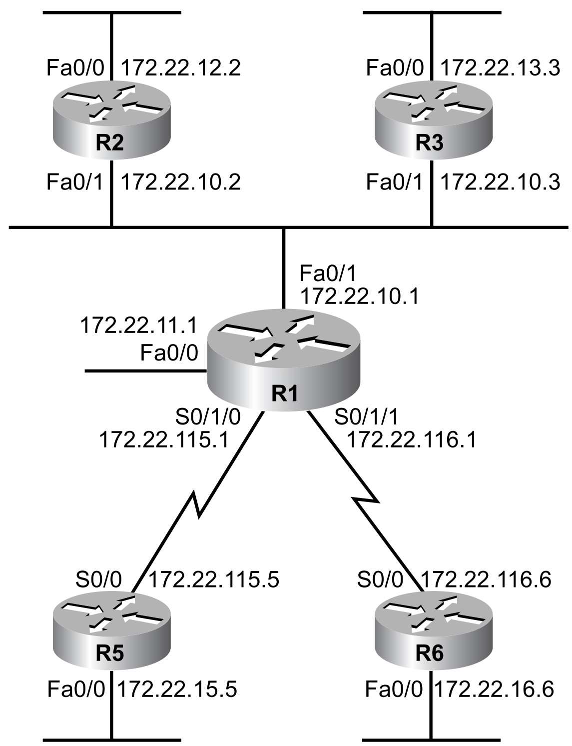


Figure 4-5 Subnet Numbers in Step 2

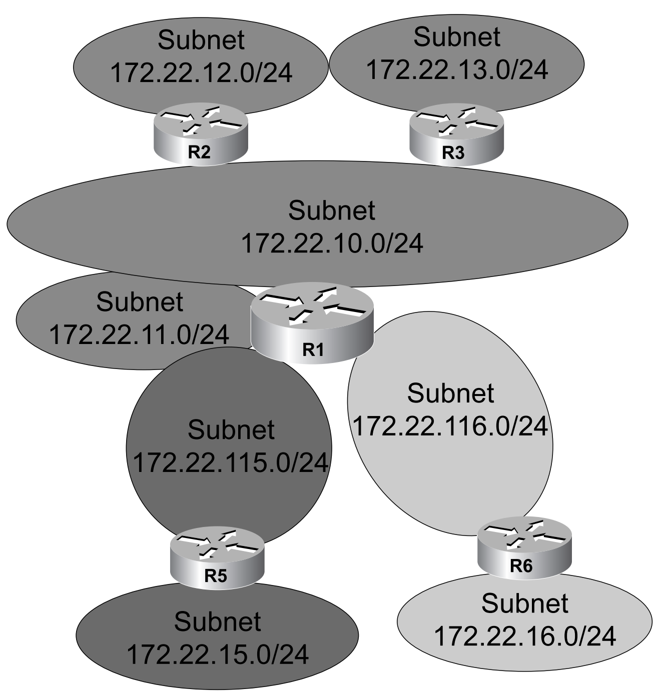
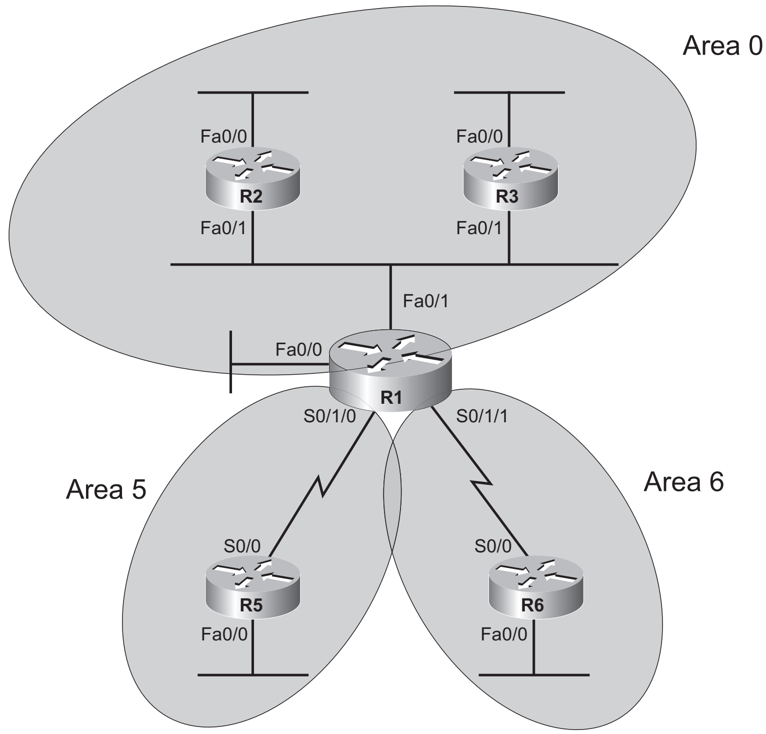


Figure 4-6 Area Design for Expanded Topology

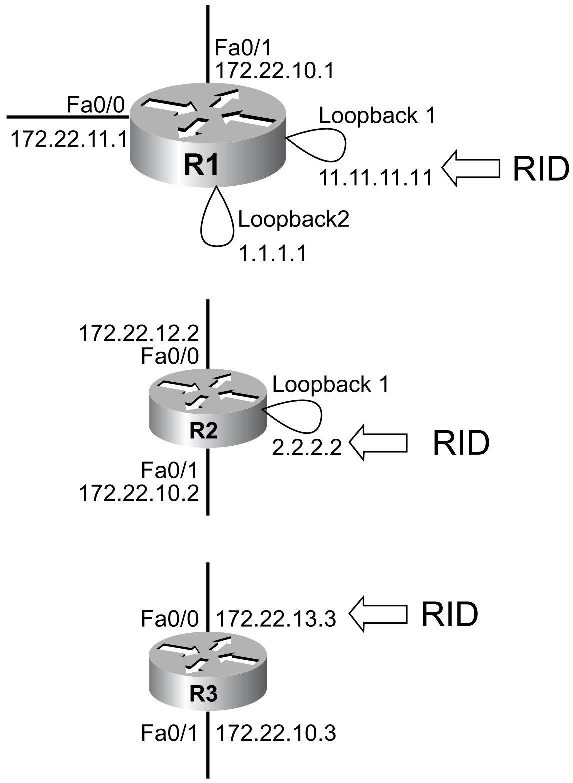


Step 3 Reference

OSPF chooses its router ID using the following sequence of choices:

1. As configured with the OSPF **router-id** command (as configured under the **router ospf** command).
2. If the **router-id** command is not configured, the router uses the highest IP address of all "up/up" loopback interfaces.
3. If steps 1 and 2 do not define the OSPF RID, the router uses the highest IP address of all "up/up" non-loopback interfaces.

Figure 4-7 Examples of OSPF Router ID Choices



Lab 5

EIGRP Configuration and Operation

This *CCNA Video Mentor* lab shows how to configure EIGRP in an internetwork having one Class B network that uses variable-length subnet masks (VLSM). The objectives of this lab are as follows:

- Configure the EIGRP **network** command
- Confirm on which interfaces a router has enabled EIGRP
- Interpret the **show ip route** command output when VLSM are used

Scenario

This lab contains two main steps, as follows:

Step 1. Configure EIGRP in a network that uses only subnets of the Class B network 172.22.0.0

Step 2. Discover the impact when a router does not enable EIGRP on an interface

Initial Configurations

Examples 5-1 through 5-3 show the pertinent initial configurations of routers R1, R2, and R3 in the lab video. Note that this lab begins with these three routers having the correct IP addresses configured, but only router R2 has been configured for EIGRP. As usual, the parts of the configurations not relevant to this lab have been omitted.

Example 5-1 Initial Configuration for R1

```
hostname R1
!
interface FastEthernet 0/0
 ip address 172.22.11.1 255.255.255.128
!
interface serial 0/1/0
 ip address 172.22.112.101 255.255.255.252
 clock rate 1536000
!
interface serial 0/1/1
 ip address 172.22.113.209 255.255.255.252
 clock rate 1536000
```

Example 5-2 Initial Configuration for R2

```
hostname R2
!
interface FastEthernet 0/0
 ip address 172.22.12.202 255.255.255.192
!
interface serial 0/1/0
 ip address 172.22.112.102 255.255.255.252
!
interface serial 0/1/1
 ip address 172.22.123.97 255.255.255.252
!
router eigrp 1
 network 172.22.0.0
```

Example 5-3 Initial Configuration for R3

```
hostname R3
!
interface FastEthernet 0/0
 ip address 172.22.13.103 255.255.255.224
!
interface serial 0/1/0
 ip address 172.22.123.98 255.255.255.252
 clock rate 1536000
!
interface serial 0/1/1
 ip address 172.22.113.210 255.255.255.252
```

Ending Configurations

This lab does not change any of the initial configurations in routers R1, R2, or R3. However, it does add to the configurations of R1 and R3, as shown in Examples 5-4 and 5-5.

Example 5-4 Configuration Added to R1 During the Lab

```
router eigrp 1
 network 172.22.0.0
```

Example 5-5 Configuration Added to R3 During the Lab

```
router eigrp 1
 network 172.22.113.0 0.0.0.255
 network 172.22.123.0 0.0.0.255
 network 172.22.13.0 0.0.0.255
```

Video Presentation Reference

This video includes several figures that contain the same images used in the lab video. Because the video is organized into two separate steps, the reference materials have been organized into two separate sections. Each section simply lists these figures and tables for reference.

Step 1 Reference

Figure 5-1 Three Routers, Six Subnets of Class B Network 172.22.0.0

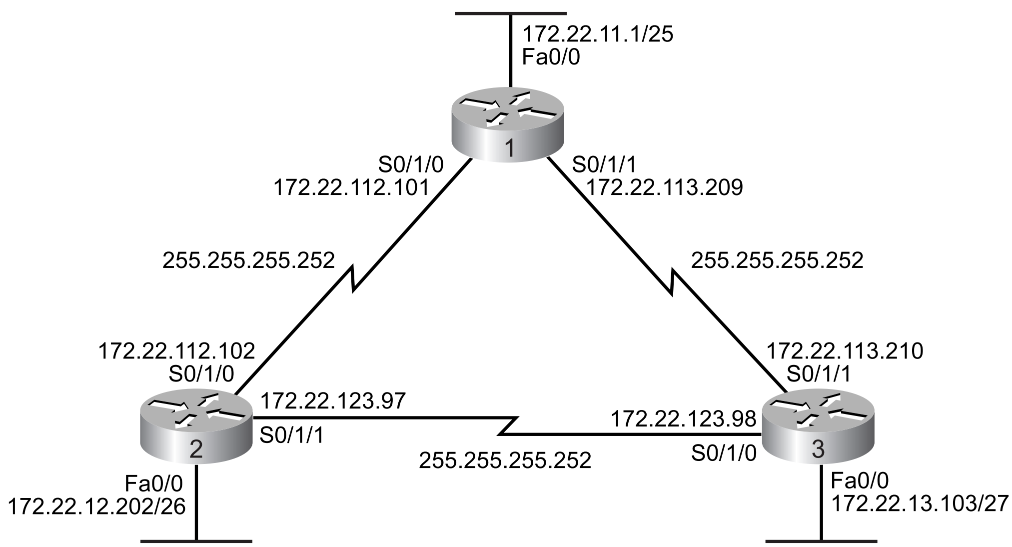


Table 5-1 lists the subnets shown in Figure 5-1.

Table 5-1 Four Key Internet Layer Protocols

Location	Subnet Number	Range of IP Addresses	Subnet Broadcast Address
R1 LAN	172.22.11.0/25	172.22.11.1–172.22.11.126	172.22.11.127
R2 LAN	172.22.12.192/26	172.22.12.193–172.22.12.254	172.22.12.255
R3 LAN	172.22.13.96/27	172.22.13.97–172.22.13.126	172.22.13.127
R1-R2 Serial	172.22.112.100/30	172.22.112.101–172.22.112.102	172.22.112.103
R1-R3 Serial	172.22.113.208/30	172.22.113.209–172.22.113.210	172.22.113.211
R2-R3 Serial	172.22.123.96/30	172.22.123.97–172.22.123.98	172.22.123.99

Figure 5-2 Subnet Reference for Step 1

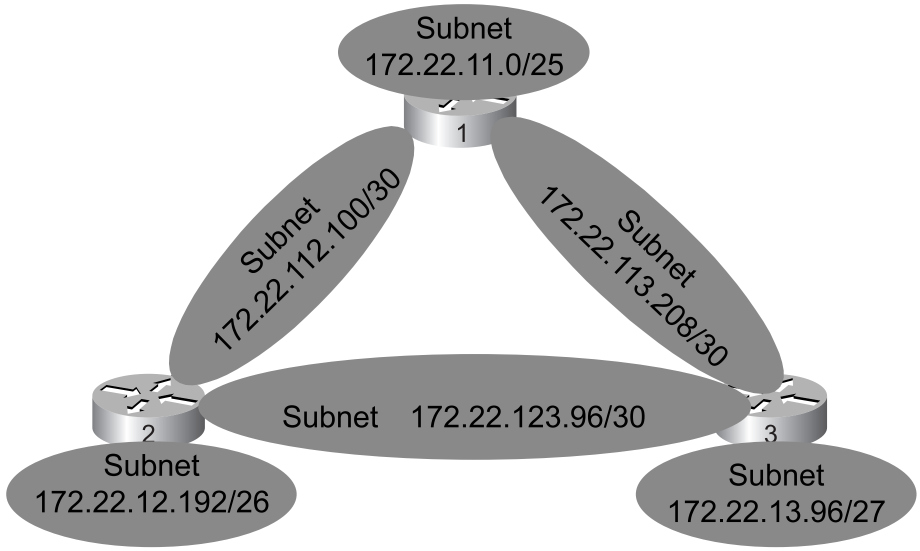


Figure 5-3 The Original Format of the EIGRP network Command

network *network-number*

The **network** command

- Class A, B, or C network number
- Tells router to "do EIGRP" on all interfaces in that network
- "Doing EIGRP" on an interface means:
  1. Send EIGRP messages
  2. Listen for EIGRP messages
  3. Advertise about the subnet connected to the interface

Figure 5-4 The Newer Format of the EIGRP network Command

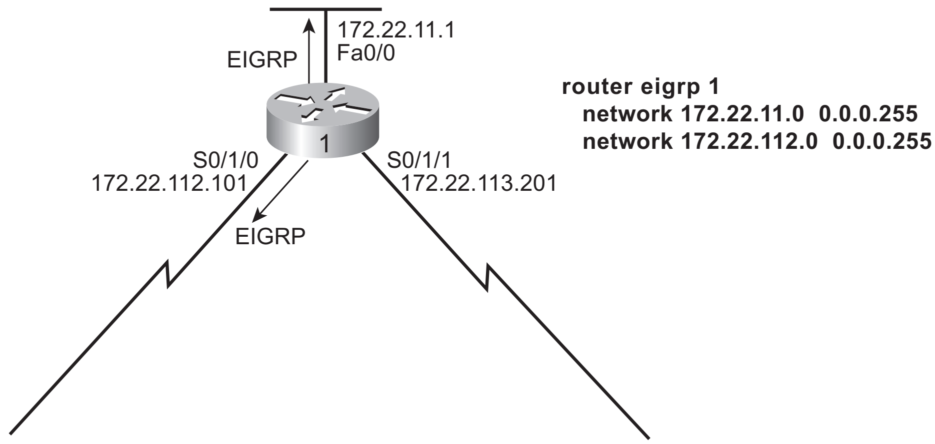
network *address* *wildcard-mask*

The **network** command

- Any dotted decimal number, typically an IP address or subnet number

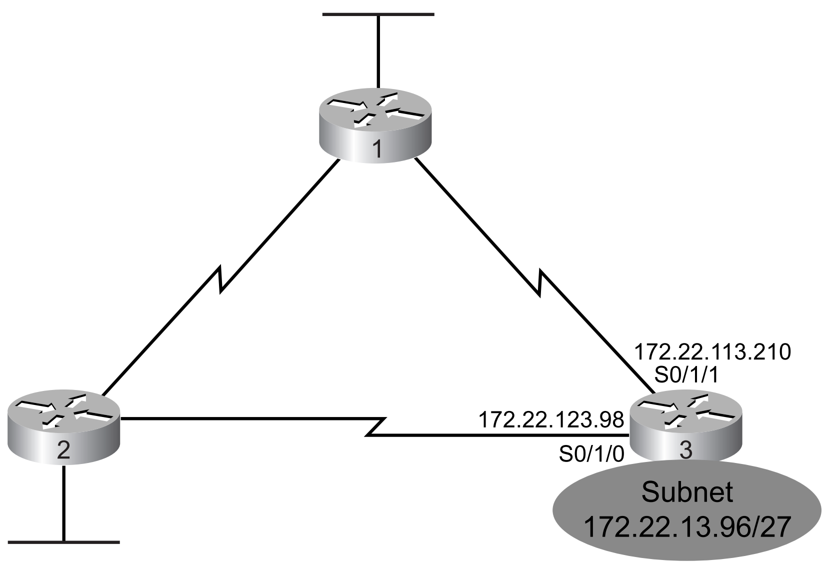
- Limits which parts of the network number must match an interface

Figure 5-5 **The Impact of the EIGRP network Command – R1, Step 1**



Step 2 Reference

Figure 5-6 **Problem of Not Advertising Subnet 172.22.13.96/27**



Lab 6

Understanding EIGRP Metric Calculations

This *CCNA Video Mentor* lab helps you understand the bandwidth and delay settings on router interfaces and how they impact the metric calculated by the EIGRP routing protocol. In particular, this lab covers the following:

- Determines which interface's bandwidth and delay settings impact EIGRP's metric calculation for a given route.
- Explains how EIGRP uses constraining (slowest) bandwidth but cumulative interface delay.
- Predicts the impact of changing an interface's bandwidth setting on the EIGRP metric calculation.

Scenario

This lab contains two main steps, as follows:

Step 1. Analyze the differences between the EIGRP metrics for two possible routes to reach a single subnet.

Step 2. Predict the change in EIGRP metrics based on a change to an interface's bandwidth setting.

Initial Configurations

Examples 6-1, 6-2, and 6-3 show the pertinent initial configurations of Routers R1, R2, and R3 in the lab video. Note that this lab begins with these three routers having the correct IP addresses configured, and with EIGRP configured and enabled on all interfaces—but with default bandwidth and delay settings. As usual, the parts of the configurations not relevant to this lab have been omitted.

Example 6-1 Initial Configuration for R1

```
hostname R1
!
interface FastEthernet 0/0
 ip address 172.22.11.1 255.255.255.128
!
interface serial 0/1/0
 ip address 172.22.112.101 255.255.255.252
 clock rate 1536000
!
interface serial 0/1/1
 ip address 172.22.113.209 255.255.255.252
 clock rate 1536000
!
router eigrp 1
 network 172.22.0.0
```

Example 6-2 Initial Configuration for R2

```
hostname R2
!
interface FastEthernet 0/0
 ip address 172.22.12.202 255.255.255.192
!
interface serial 0/1/0
 ip address 172.22.112.102 255.255.255.252
!
interface serial 0/1/1
 ip address 172.22.123.97 255.255.255.252
!
router eigrp 1
 network 172.22.0.0
```

Example 6-3 Initial Configuration for R3

```
hostname R3
!
interface FastEthernet 0/0
 ip address 172.22.13.103 255.255.255.224
!
interface serial 0/1/0
 ip address 172.22.123.98 255.255.255.252
 clock rate 1536000
!
interface serial 0/1/1
 ip address 172.22.113.210 255.255.255.252
```

```
!
router eigrp 1
 network 172.22.0.0
```

Ending Configurations

This lab does not change any of the initial configuration, but it does override the default bandwidth setting on R1's S0/1/0 interface. For easy reference, Example 6-4 lists the configuration added during the video.

Example 6-4 Configuration Added to R1 During the Video

```
interface serial 0/1/0
 bandwidth 64
```

Video Presentation Reference

This video presents several figures that describe the internetwork used in the video and how the bandwidth and delay settings impact EIGRP's choice of routes. This section simply lists these figures for reference. Because the video is organized into two separate steps, the reference materials have been organized into two separate sections.

Step 1 Reference

Figure 6-1 Lab 6 Topology and IP Addresses

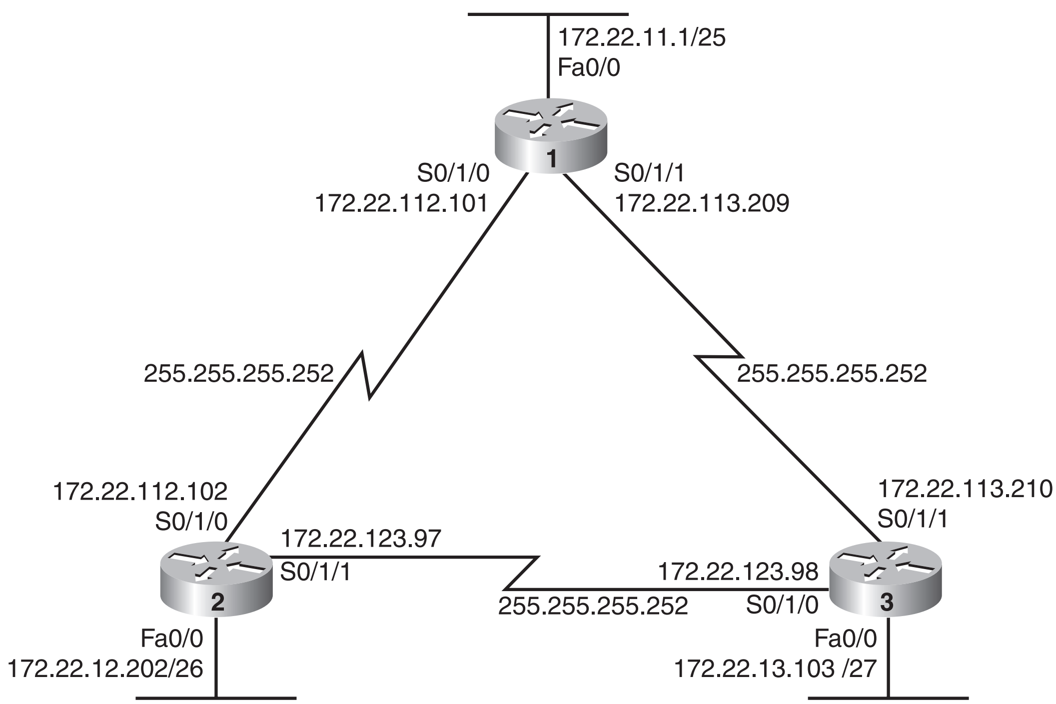


Figure 6-2 Lab 6 Subnet Number Reference

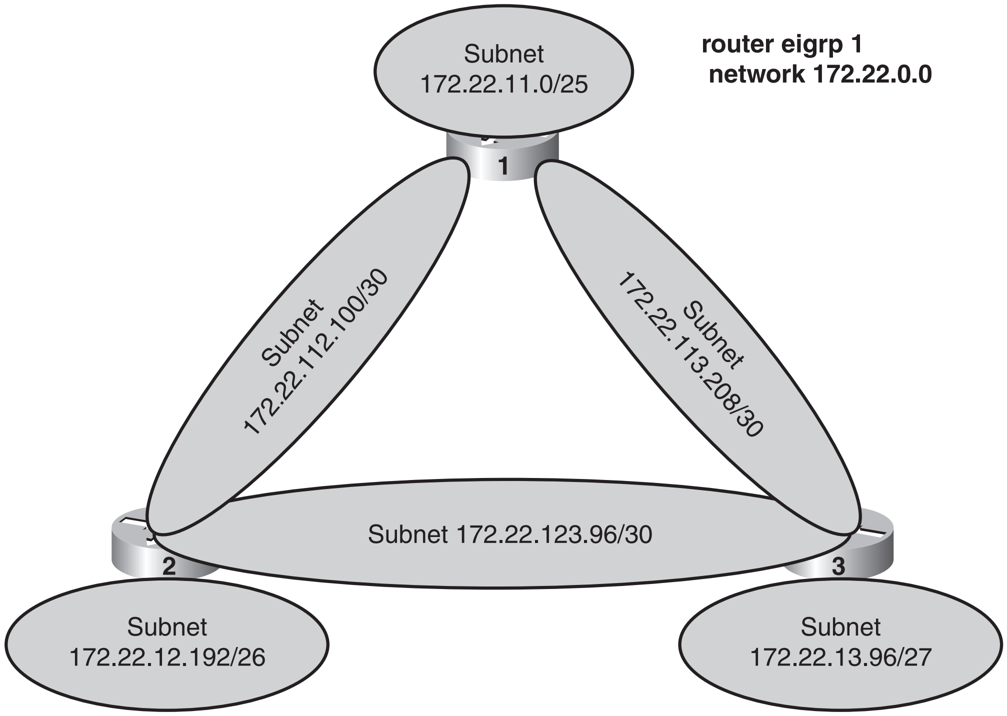


Figure 6-3 Bandwidth Settings That Impact R1's route to Subnet 172.22.12.192/26

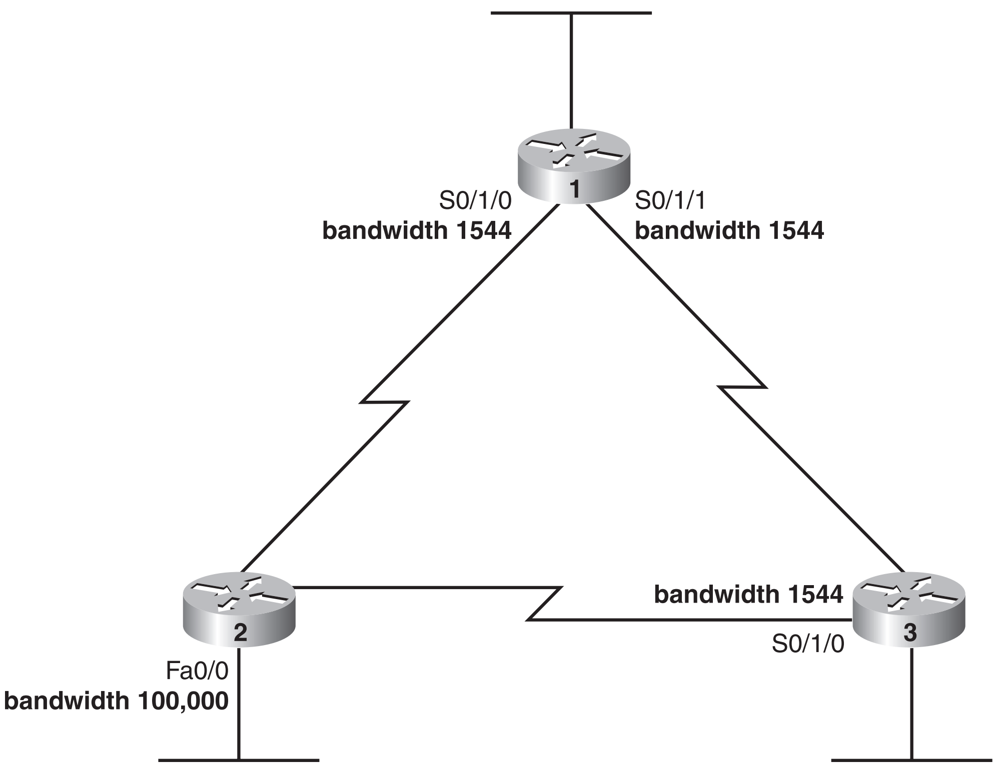


Figure 6-4 Bandwidth and Delay Inputs into R1's Two Competing Routes for 172.22.12.192/26

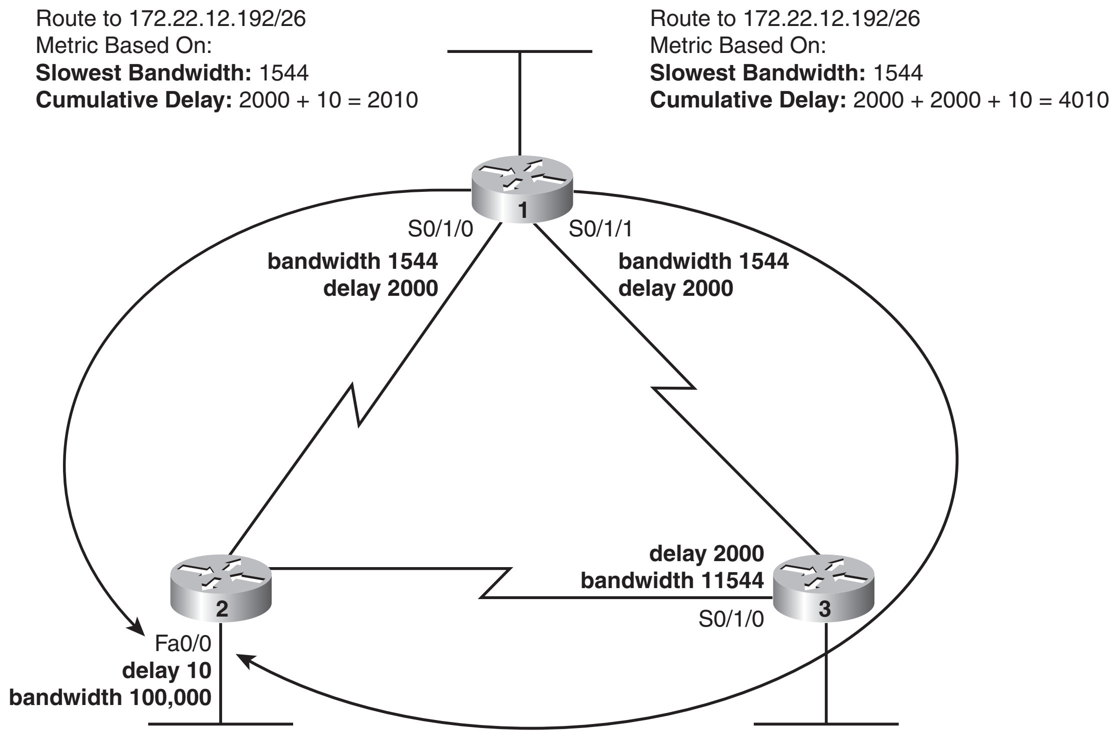
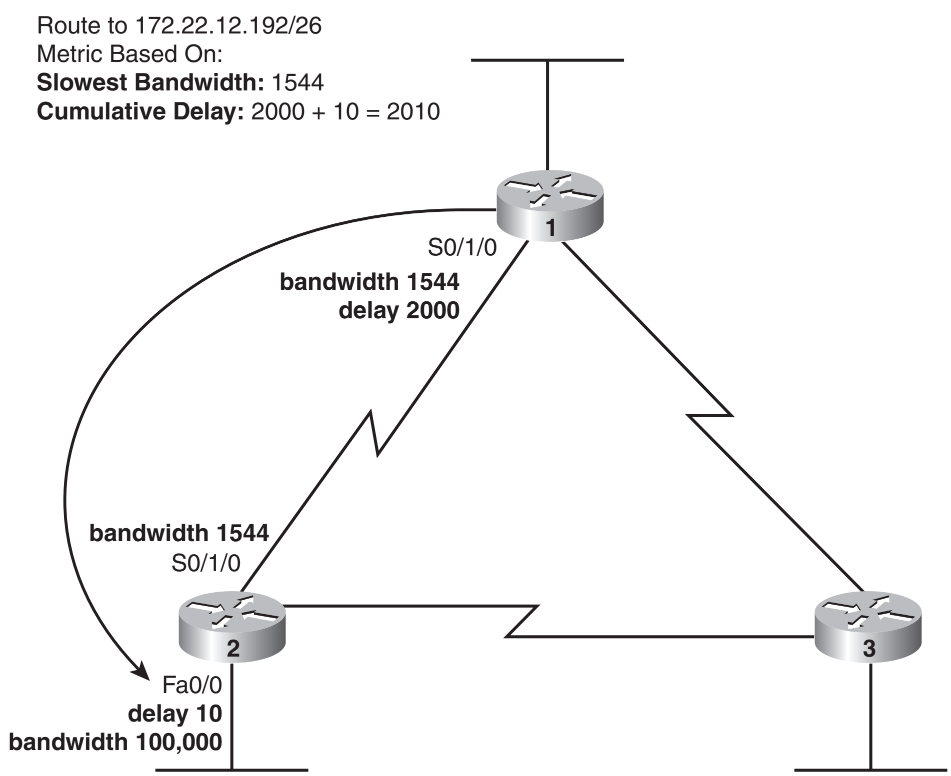


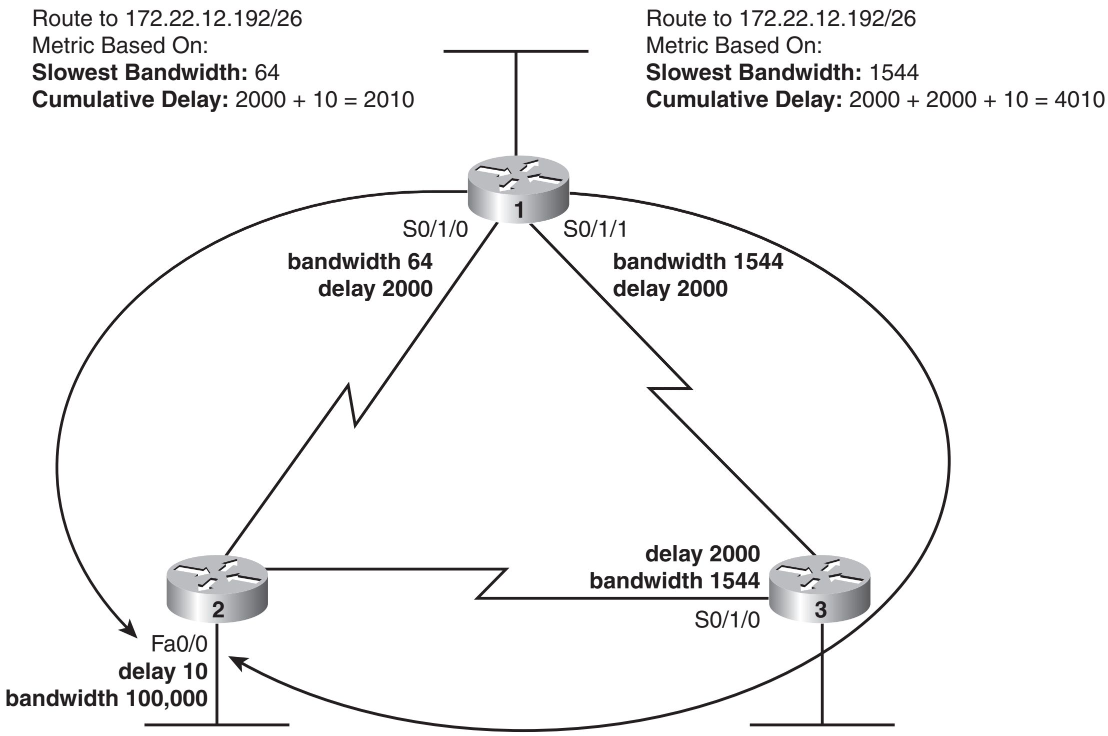
Figure 6-5 Metric Calculation Reference

Metric = 256 (10^7/bandwidth) + 256(delay) = 2,172,416



Step 2 Reference

Figure 6-6 Revised Bandwidth and Delay Inputs



Lab 7

NAT Overload (PAT)

This *CCNA Video Mentor* (CVM) lab shows how to configure Network Address Translation (NAT), specifically using the Port Address Translation (PAT) or overload feature. In particular, the objectives of this lab are as follows:

- Define the following NAT terms:
  - Inside, Outside, Inside Local, and Inside Global
- Describe how NAT changes the following:
  - IP addresses for Enterprise (Inside) hosts for a typical Internet connection
  - Port numbers to support thousands of connections using a single Inside Global IP address
- Configure NAT overload (PAT) using a single interface IP address for the Inside Global IP address

Scenario

This lab contains two main steps, as follows:

Step 1. Review the terms associated with the typical use of NAT and PAT with an Internet connection and see NAT working in a router.

Step 2. Review router NAT/PAT configuration using a single IP address on an interface (no NAT pool).

Initial Configurations

Example 7-1 shows the pertinent initial configuration of router R1 in the lab video. Note that this lab begins with R1 having a valid NAT/PAT overload configuration, using the Inside Global IP address of R1's S0/1/0 interface (100.1.1.2). As usual, the parts of the configurations not relevant to this lab have been omitted.

Example 7-1 Initial Configuration for R1

```
hostname R1
!
ip nat inside source list 3 interface serial 0/1/0 overload
!
interface FastEthernet 0/0
 ip address 172.22.11.1 255.255.255.0
 ip nat inside
!
```

Example 7-1 Initial Configuration for R1 *continued*

```
interface Serial 0/1/0
 ip address 100.1.1.2 255.255.255.248
 ip nat outside
!
access-list 3 permit 172.22.0.0 0.0.255.255
```

Ending Configurations

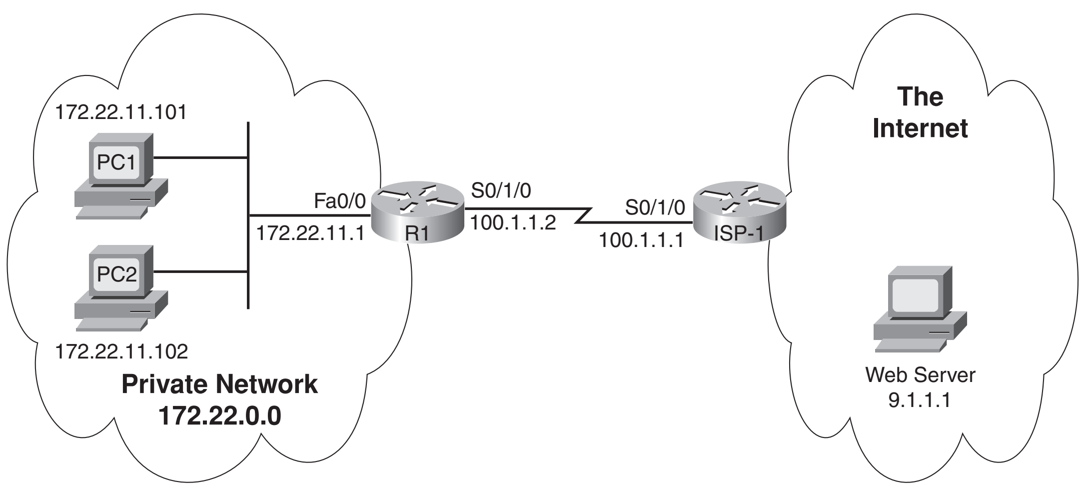
This lab video does not change the router configuration.

Video Presentation Reference

This video presents several figures that describe how NAT overload (PAT) works generally and how it works in the particular example shown in the lab video. This section simply lists these figures for reference.

Figure 7-1 shows a diagram of the network used in this example.

Figure 7-1 Lab 10 Scenario Topology



Because the video is organized into two separate steps, the reference materials have been organized into two separate sections.

Step 1 Reference

Figure 7-2 Concept of Inside and Outside with NAT

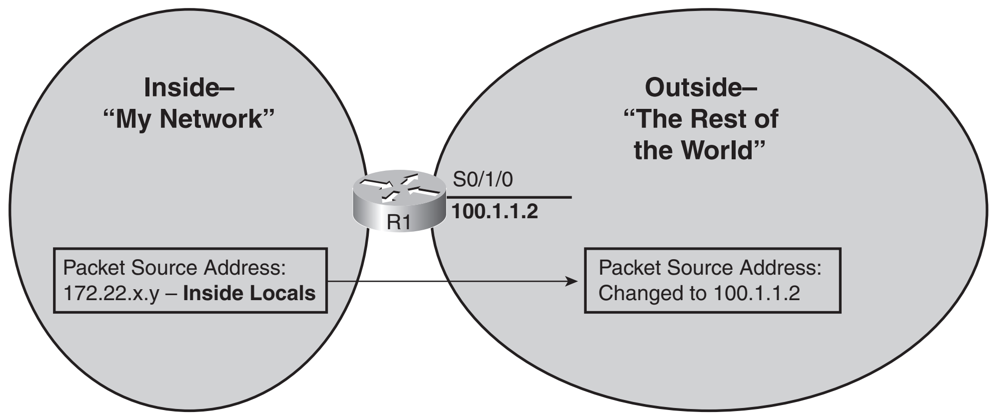


Figure 7-3 How NAT Overload Changes Inside Addresses and Ports

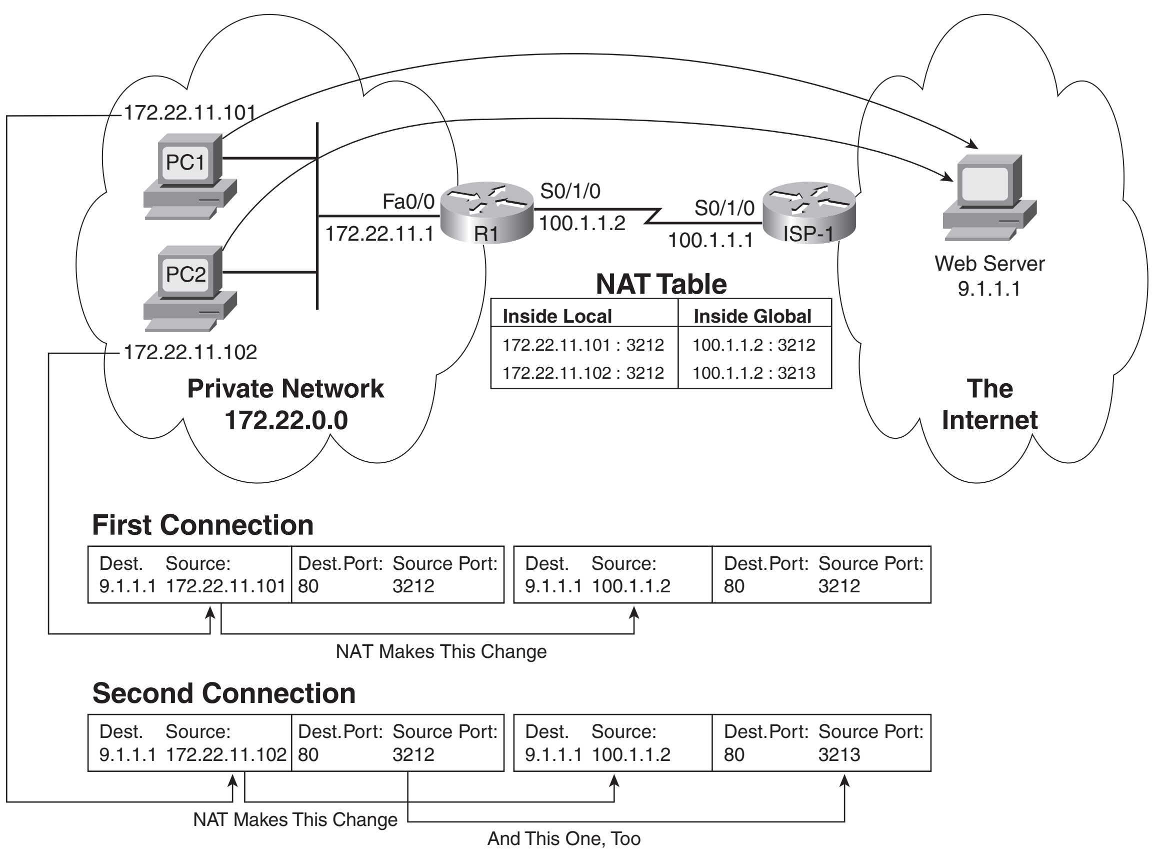
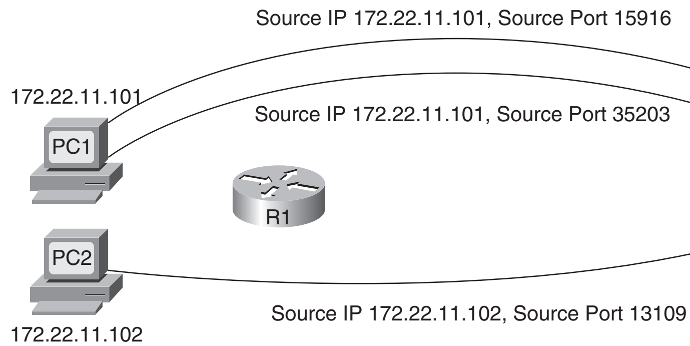


Figure 7-4 Three TCP Connections Created to Test NAT Overload



Step 2 Reference

Figure 7-5 Configuring Inside and Outside Interfaces

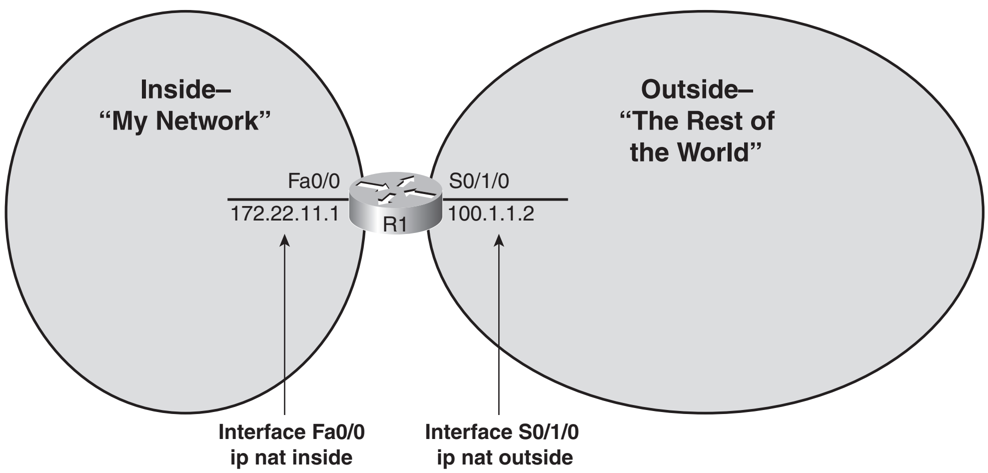
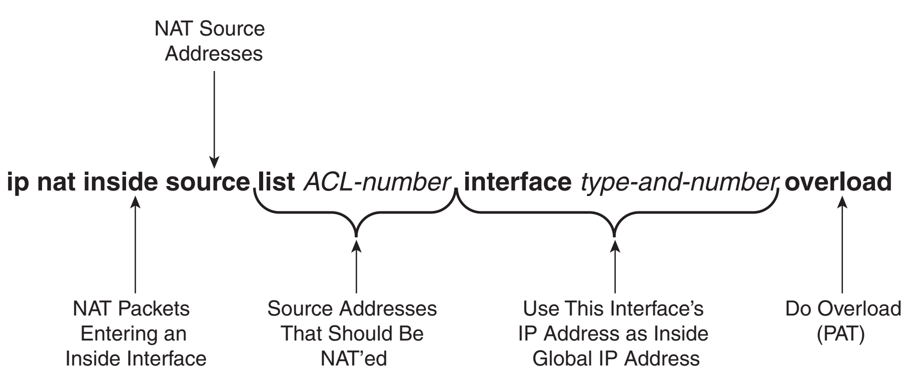


Figure 7-6 Configuring NAT Overload Using an Interface as Inside Global



Lab 8

IPv6 Subnetting and Address Configuration

This *CCNA Video Mentor* lab explains the format of one type of IP Version 6 (IPv6) address, compares the basic concepts of IPv4 and IPv6 subnetting, and shows how to configure IPv6 addresses on Cisco routers. In particular, the objectives of this lab are as follows:

- Describe the general format of IPv6 Global Unicast addresses.
- Describe the similarities between IPv4 and IPv6 subnetting.
- Configure IPv6 addresses on Cisco router interfaces.

Scenario

This lab contains two main steps, as follows:

Step 1. Compare IPv4 subnetting to IPv6 subnetting in a simple internetwork.

Step 2. Configure full 128-bit IPv6 addresses on a router.

Initial Configurations

The two routers used in this internetwork begin with IPv4 enabled. Example 8-1 and Example 8-2 list the pertinent IPv4 configuration on these two routers at the beginning of the video.

Example 8-1 Initial (Pertinent) Configuration for R1

```
hostname R1
!
interface Fastethernet 0/0
 ip address 128.107.11.1 255.255.255.0
!
interface Serial 0/1/0
 ip address 128.107.112.1 255.255.255.0
!
router eigrp 1
 network 128.107.0.0
```

Example 8-2 Initial (Pertinent) Configuration for R2

```
hostname R2
!
interface Fastethernet 0/0
```

```
 ip address 128.107.12.2 255.255.255.0
!
interface Serial 0/1/0
 ip address 128.107.112.2 255.255.255.0
!
router eigrp 1
 network 128.107.0.0
```

Ending Configurations

This lab adds a few commands to Router R1 to show the process of enabling IPv6 globally, and one option for how to configure IPv6 interface addresses. Example 8-3 shows the configuration added to R1 during the video.

Example 8-3 Configuration on Sw1 Added During This Lab

```
ipv6 unicast routing
!
interface Fastethernet 0/0
 ipv6 address 2233:0:2222:11::1/64
!
interface Serial 0/1/0
 ipv6 address 2233:0:2222:112::1/64
```

Video Presentation Reference

This video presents several figures that explain concepts and introduce configuration settings. Because the video is organized into two separate steps, the reference materials have been organized into two separate sections.

Step 1 Reference

Figure 8-1 Internetwork with Public IPv4 Addresses

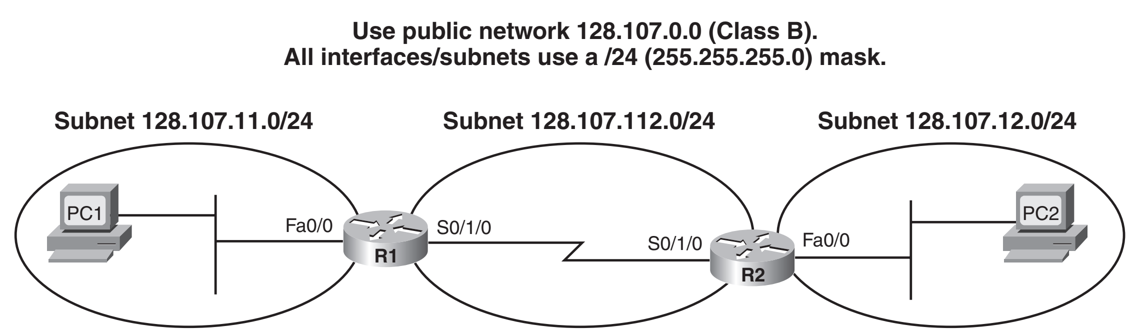


Figure 8-2 IPv4 Addresses: Network, Subnet, Host, and Prefix Length

Network Host

Subnet 128.107.11.0/24

Subnet Prefix Length

All **addresses in this internetwork** begin with 128.107

All **addresses on this LAN** begin with 128.107.11

The prefix length is the **length of network + subnet**

All addresses on this LAN need a different host ID; the **host ID is shown as 0s** in subnet number

Figure 8-3 IPv6 ISP Prefix

ISP Prefix

Subnet 2233:0000:2222:0011:0000:0000:0000:0000/64

All **addresses in this internetwork** begin with 2233:0000:2222

Figure 8-4 IPv6 Subnet

Subnet

Subnet 2233:0000:2222:0011:0000:0000:0000:0000/64

All **addresses in this internetwork** begin with 2233:0000:2222

All **addresses on this LAN** begin with 2233:0000:2222:0011

Figure 8-5 IPv6 Prefix Length

ISP Prefix Subnet Host (Interface ID) Prefix Length

Subnet 2233:0000:2222:0011:0000:0000:0000:0000/64

4 Quartets:
16 Hex Digits
64 Bits

All **addresses in this internetwork** begin with 2233:0000:2222

All **addresses on this LAN** begin with 2233:0000:2222:0011

The prefix length is the length of ISP prefix + subnet

All addresses on this LAN need a different interface ID; the **interface ID is shown as 0s** in subnet number

Figure 8-6 IPv6 Host (Interface) ID

ISP Prefix Subnet Host (Interface ID)

Subnet 2233:0000:2222:0011:0000:0000:0000:0000/64

All **addresses in this internetwork** begin with 2233:0000:2222

All **addresses on this LAN** begin with 2233:0000:2222:0011

The prefix length is the **length of ISP prefix + subnet**

All addresses on this LAN need a different interface ID; the **interface ID is shown as 0s** in subnet number

Figure 8-7 Abbreviating IPv6 Addresses and Subnet Numbers

Subnet 2233:0000:2222:0011:0000:0000:0000:0000/64

Subnet 2233:0000:2222:11:0000:0000:0000:0000/64

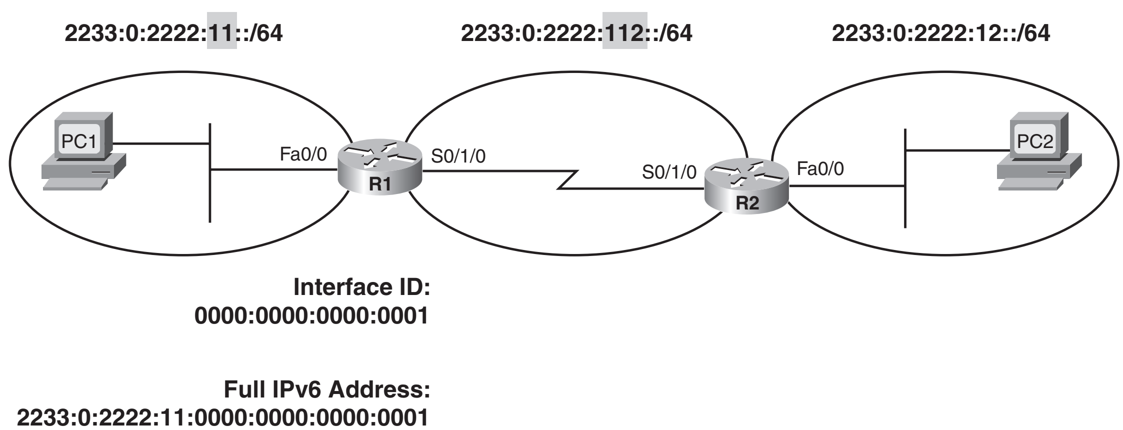
Subnet 2233:0:2222:11:0000:0000:0000:0000/64

Subnet 2233:0:2222:11::/64

1) Leading 0s in a quartet can always be omitted
2) A quartet of 0000 can be abbreviated as 0
3) One instance of multiple consecutive 0000 quartets can be abbreviated as ::

Step 2 Reference

Figure 8-8 IPv6 Subnets and Addresses Chosen for This Video



Lab 9

PPP and CHAP Configuration

This *CCNA Video Mentor* lab shows how to configure Point-to-Point Protocol (PPP) and Challenge Handshake Authentication Protocol (CHAP). The objectives of this lab are as follows:

- Configure PPP
- Describe the meaning of the two interface status codes
- Configure CHAP
- Explain how CHAP does not send the password over the link when performing authentication

Scenario

This lab contains two main steps, as follows:

Step 1. Migrate from HDLC to PPP

Step 2. Add CHAP authentication to a PPP link

Initial Configurations

Examples 9-1 and 9-2 show the pertinent initial configurations of routers R1 and R2 in the lab video. The lab begins with a working network, using the default of High-Level Data Link Control (HDLC) as the data link protocol on the serial link. As usual, the parts of the configurations not relevant to this lab have been omitted.

Example 9-1 Initial Configuration for R1

```
hostname R1
!
interface FastEthernet 0/0
 ip address 172.16.1.1 255.255.255.0
!
interface serial 0/1/0
 ip address 172.22.2.1 255.255.255.0
 clock rate 1536000
 shutdown
!
router rip
 network 172.16.0.0
```

Example 9-2 Initial Configuration for R2

```
hostname R2
!
interface FastEthernet 0/0
 ip address 172.16.3.2 255.255.255.0
!
interface serial 0/1/0
 ip address 172.16.2.2 255.255.255.0
!
router rip
 network 172.16.0.0
```

Ending Configurations

This lab ends with both routers having migrated to using PPP and CHAP. Examples 9-3 and 9-4 show the configurations added to R1 and R2 during the lab.

Example 9-3 Configuration Added to R1 During the Lab

```
username R2 password depth
!
interface serial 0/1/0
 no shutdown
 encapsulation ppp
 ppp authentication chap
```

Example 9-4 Configuration Added to R2 During the Lab

```
username R1 password depth
!
interface serial 0/1/0
 encapsulation ppp
 ppp authentication chap
```

Video Presentation Reference

This video includes several figures that contain the same images used in the lab video. Because the video is organized into two separate steps, the reference materials have been organized into two separate sections. Each section simply lists these figures and tables for reference.

Step 1 Reference

Figure 9-1 Two Routers Using a Point-to-Point Serial Link

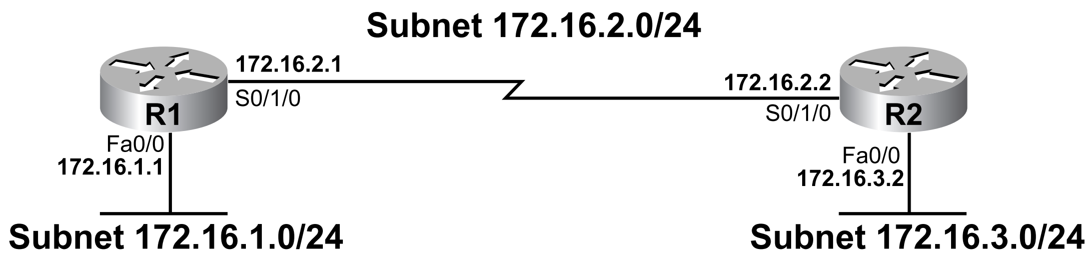


Table 9-1 lists the interface status code combinations and their meanings.

Table 9-1 Cisco Router Interface Status Code Combinations

First Interface Status Code	Second Interface Status Code	Most Likely Meaning
Administratively down	Down	Interface has been shut down
Down	Down	Layer 1 problem
Up	Down	Layer 2 problem
Up	Up	Interface is working

Step 2 Reference

Figure 9-2 Three-way CHAP Authentication Message Flow

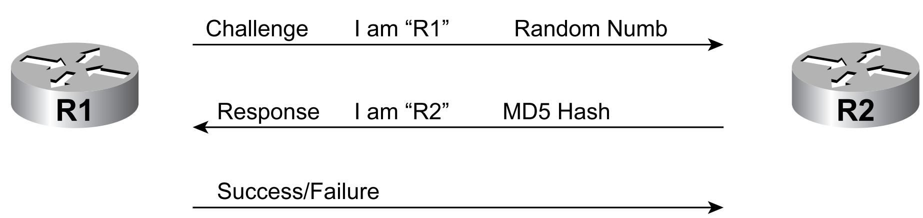
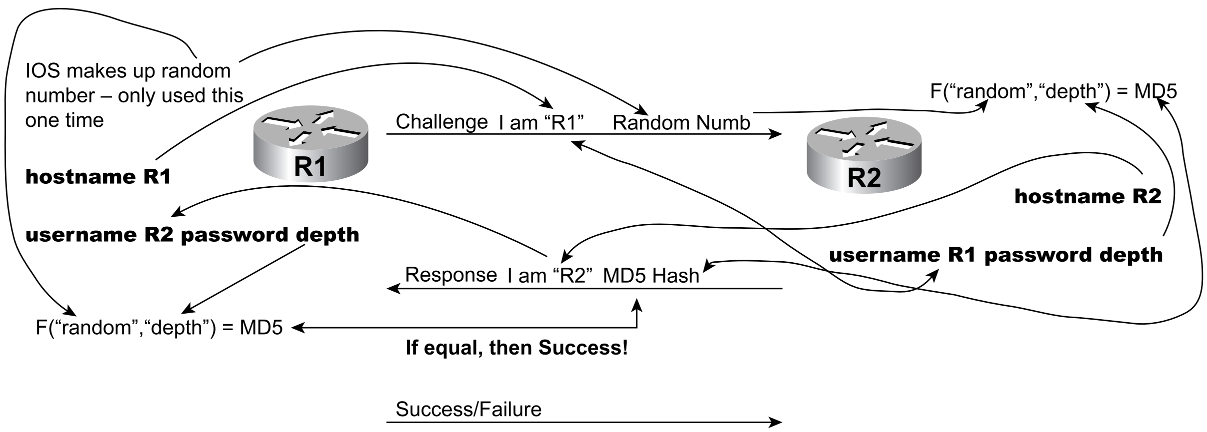


Figure 9-3 Comparing CHAP Configuration with CHAP Message Flow



Lab 10

Access Lists

This *CCNA Video Mentor* lab shows how to configure access control lists (ACLs), focusing on how ACLs can match applications based on TCP and UDP port numbers. The objectives of this lab are as follows:

- Configure extended IP ACLs
- Describe how to match both the source and destination port numbers with an IP ACL
- See counters for the number of packets that match each ACL statement

Scenario

This lab contains a single step, as follows:

Step 1. Filter packets going to a server farm

Initial Configurations

Examples 10-1 and 10-2 show the pertinent initial configurations of routers R1 and R2 in the lab video. The lab begins with a working network with IP addresses and the RIP routing protocol, but with no ACLs configured. As usual, the parts of the configurations not relevant to this lab have been omitted.

Example 10-1 Initial Configuration for R1

```
hostname R1
!
interface FastEthernet 0/0
 ip address 172.16.1.251 255.255.255.0
!
interface serial 0/1/0
 ip address 172.16.2.251 255.255.255.0
!
router rip
 network 172.16.0.0
```

Example 10-2 Initial Configuration for R2

```
hostname R2
!
interface FastEthernet 0/0
 ip address 172.16.3.252 255.255.255.0
!
interface serial 0/1/0
 ip address 172.16.2.252 255.255.255.0
!
router rip
 network 172.16.0.0
```

Ending Configurations

This lab ends with R1 having a new ACL configured and enabled. Example 10-3 shows the ending configuration for R1.

Example 10-3 Configuration for R1 at the End of the Lab

```
hostname R1
!
interface FastEthernet 0/0
 ip address 172.16.1.251 255.255.255.0
 ip access-group 101 in
!
interface serial 0/1/0
 ip address 172.16.2.251 255.255.255.0
!
router rip
 network 172.16.0.0
!
access-list 101 permit tcp host 172.16.1.1 172.16.3.0 0.0.0.255 eq www
access-list 101 permit tcp 172.16.1.0 0.0.0.255 gt 1023 172.16.3.0 0.0.0.255 eq
telnet
```

Video Presentation Reference

This video includes several figures that contain the same images used in the lab video. Because the video is organized into two separate steps, the reference materials have been organized into two separate sections. Each section simply lists these figures for reference.

Step 1 Reference

Figure 10-1 Lab 12 IP Address Reference

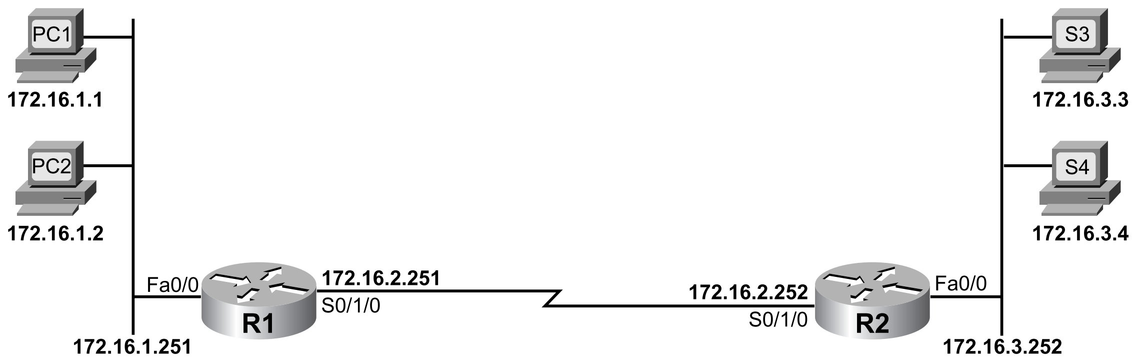


Figure 10-2 Lab 12 Subnet Reference

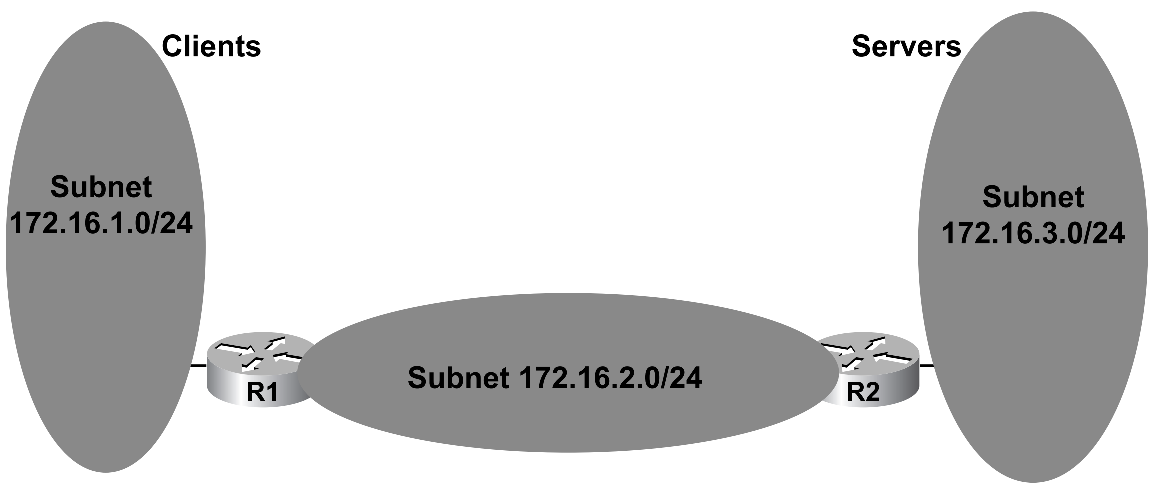
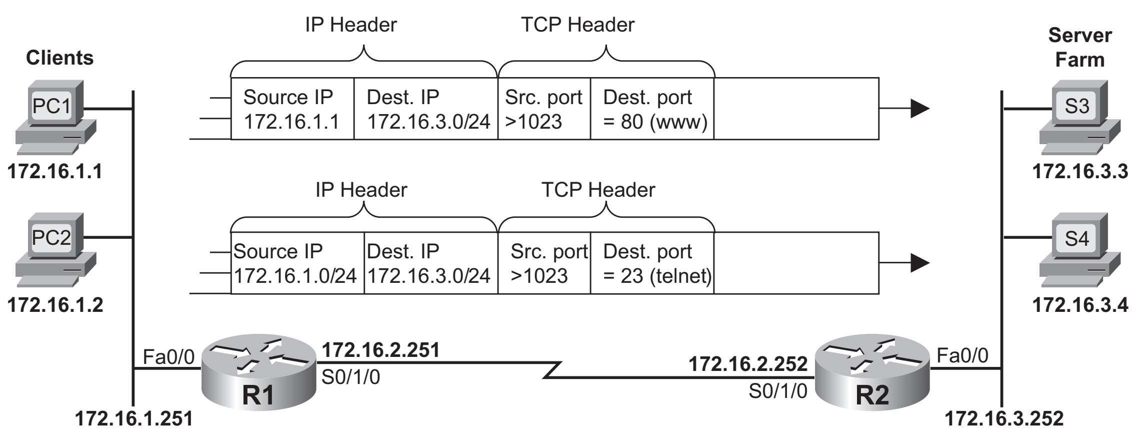


Figure 10-3 View of Packets That Should be Permitted by the ACL



Permit: from PC1 to web servers in subnet 172.16.3.0/24
Permit: from subnet 172.16.1.0/24 to Telnet servers in subnet 172.16.3.0/24
Deny: all else

Lab 11

Access Lists II

This *CCNA Video Mentor* lab shows how to configure access control lists (ACL), focusing on how ACLs can match applications based on TCP and UDP port numbers. The objectives of this lab are as follows:

- Explain how discarding packets sent by a server to a client prevents a client from talking to a server.
- Configure ACLs to match well-known ports as source ports.
- See counters for the number of packets that match each ACL statement.

Scenario

This lab contains a single step, as follows:

Step 1. Filter packets coming from a server farm.

Initial Configurations

Example 11-1 and Example 11-2 show the pertinent initial configurations of Routers R1 and R2 in the lab video. The lab begins with a working network with IP addresses and the RIP routing protocol, but with no ACLs configured. As usual, the parts of the configurations not relevant to this lab have been omitted.

Example 11-1 Initial Configuration for R1

```
hostname R1
!
interface FastEthernet 0/0
 ip address 172.16.1.251 255.255.255.0
!
interface serial 0/1/0
 ip address 172.16.2.251 255.255.255.0
!
router rip
 network 172.16.0.0
```

Example 11-2 Initial Configuration for R2

```
hostname R2
!
interface FastEthernet 0/0
 ip address 172.16.3.252 255.255.255.0
!
interface serial 0/1/0
 ip address 172.16.2.252 255.255.255.0
!
router rip
 network 172.16.0.0
```

Ending Configurations

This lab ends with R1 having a new configured and enabled ACL. Example 11-3 shows the ending configuration for R1.

Example 11-3 Configuration for R1 at the End of the Lab

```
hostname R1
!
interface FastEthernet 0/0
 ip address 172.16.1.251 255.255.255.0
 ip access-group 101 in
!
interface serial 0/1/0
 ip address 172.16.2.251 255.255.255.0
!
router rip
 network 172.16.0.0
!
access-list 101 permit tcp 172.16.3.0 0.0.0.255 eq www host 172.16.1.1 gt 1023
access-list 101 permit tcp 172.16.3.0 0.0.0.255 eq telnet 172.16.1.0 0.0.0.255 gt
 1023
access-list 101 deny ip any any
```

Video Presentation Reference

This video includes several figures that contain the same images used in the lab video. Because the video is organized into a single scenario step, the figures are listed in a single section for reference.

Figure 11-1 Lab 11 IP Address Reference

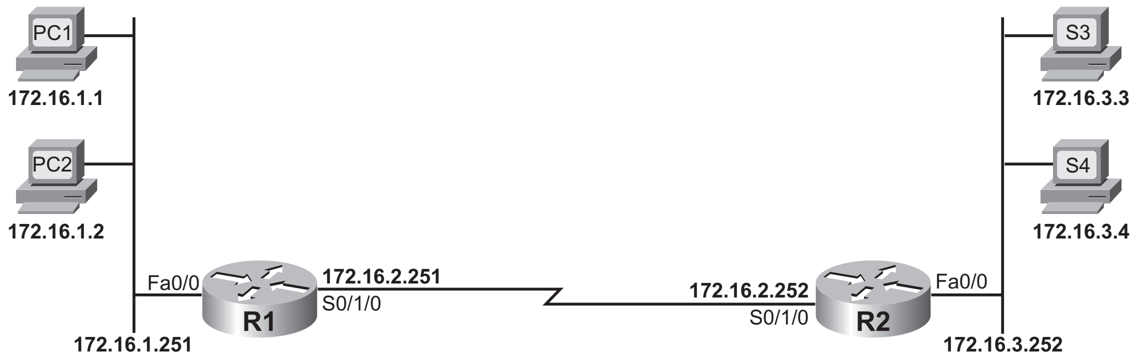


Figure 11-2 Lab 11 Subnet Reference

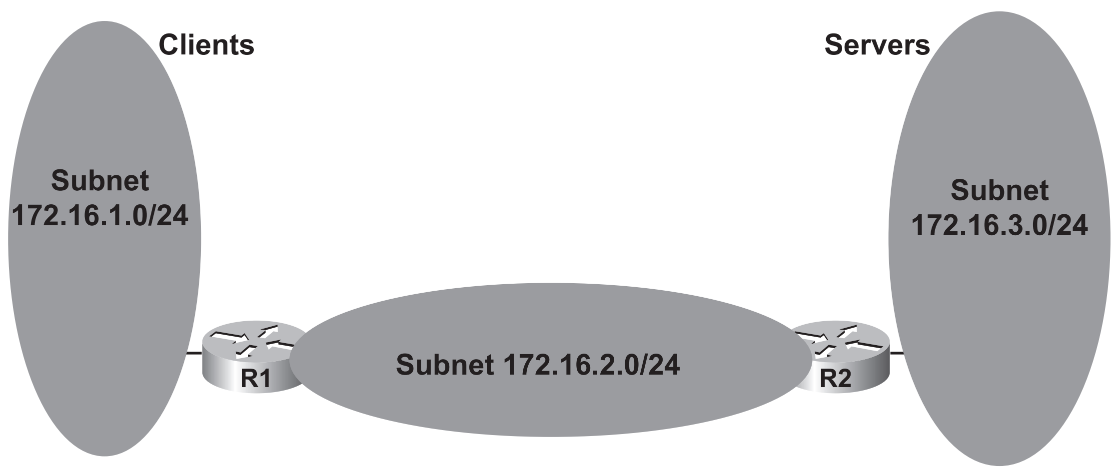


Figure 11-3 Lab 11 Filtering Reference