

Routing Protocols and Concepts

CCNA Exploration Labs and Study Guide

Instructor Edition

Allan Johnson

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Routing Protocols and Concepts

CCNA Exploration Labs and Study Guide

Instructor Edition

Allan Johnson

Copyright© 2008 Cisco Systems, Inc.

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

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

ISBN-13: 978-1-58705-575-1

ISBN-10: 1-58705-575-9

Warning and Disclaimer

This book is designed to provide information about Routing Protocols and Concepts of the Cisco Network Academy CCNA Exploration curriculum. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Trademark Acknowledgments

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

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

Publisher

Paul Boger

Associate Publisher

Dave Dusthimer

Cisco Representative

Anthony Wolfenden

Cisco Press Program Manager

Jeff Brady

Executive Editor

Mary Beth Ray

Production Manager

Patrick Kanouse

Senior Development Editor

Christopher Cleveland

Senior Project Editor

San Dee Phillips

Copy Editor

John Edwards

Technical Editor

Tony Chen

Editorial Assistant

Vanessa Evans

Book and Cover Designer

Louisa Adair

Composition

Louisa Adair

Multimedia Developer

Dan Scherf

Proofreader

Sheri Cain

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

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



Feedback Information

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

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

We greatly appreciate your assistance.



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0683

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.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ Logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

About the Author

Allan Johnson entered the academic world in 1999 after 10 years as a business owner/operator to dedicate his efforts to his passion for teaching. He holds both an M.B.A. and an M.Ed. in occupational training and development. He is an information technology instructor at Del Mar College in Corpus Christi, Texas. In 2003, Allan began to commit much of his time and energy to the CCNA Instructional Support Team, providing services to Networking Academy instructors worldwide and creating training materials. He now works full time for the Academy in Learning Systems Development.

About the Technical Reviewer

Tony Chen, CCNP and CCAI, manages Cisco Networking Academy for the College of DuPage in Glen Ellyn, Illinois, and teaches CCNA and CCNP classes at the college. As a manager for regional academy, he also trains and supports local Cisco networking academies. He also manages the computer network for the Ball Foundation. The Ball Foundation's motto is to discover and develop human potential. Tony Chen has a understanding wife, Joanne, and one wonderful daughter, Kylie.

Dedications

For my wife, Becky. Without the sacrifices you made during the project, this work would not have come to fruition. Thank you providing me the comfort and resting place only you can give.

—Allan Johnson

Acknowledgments

As technical editor, Tony Chen served admirably as my second pair of eyes, finding and correcting technical inaccuracies as well as grammatical errors. Tony's meticulous attention to detail helped to make this project a first-class production.

Mary Beth Ray, executive editor, you amaze me with your ability to juggle multiple projects at once, steering each from beginning to end. I can always count on you to make the tough decisions.

This is my third project with Christopher Cleveland as development editor. His dedication to perfection pays dividends in countless, unseen ways. Thank you again, Chris, for providing me with much-needed guidance and support. This book could not be a reality without your persistence.

Last, I cannot forget to thank all my students—past and present—who have helped me over the years to create engaging and exciting activities and labs. There is no better way to test the effectiveness of an activity or lab than to give it to a team of dedicated students. They excel at finding the obscurest of errors! I could have never done this without all your support.

Contents at a Glance

Introduction	xxv
Chapter 1	Introduction to Routing and Packet Forwarding 1
Chapter 2	Static Routing 69
Chapter 3	Introduction to Dynamic Routing Protocols 139
Chapter 4	Distance Vector Routing Protocols 169
Chapter 5	RIP Version 1 189
Chapter 6	VLSM and CIDR 245
Chapter 7	RIPv2 307
Chapter 8	The Routing Table: A Closer Look 357
Chapter 9	EIGRP 393
Chapter 10	Link-State Routing Protocols 474
Chapter 11	OSPF 495

Contents

	Introduction	xxv
Chapter 1	Introduction to Routing and Packet Forwarding	1
	Study Guide	2
	Inside the Router	2
	Vocabulary Exercise: Matching	2
	Vocabulary Exercise: Completion	4
	Label the External Components of a Router Exercise	6
	Label the Internal Components of a Router Exercise	7
	Describe the Internal Components of a Router Exercise	8
	Router Bootup Process Exercise	10
	Interpreting the show version Command Exercise	10
	CLI Configuration and Addressing	11
	Implementing Basic Addressing Schemes Exercise	11
	Basic Router Configuration Exercise	12
	Packet Tracer Exercise 1-1: Basic Router Configuration	15
	Task 1: Add Devices and Connect Cables	15
	Task 2: Configure PCs	15
	Task 3: Configure R1	16
	Task 4: Configure R2	16
	Task 5: Save the Packet Tracer File	17
	Building the Routing Table	17
	Vocabulary Exercise: Completion	17
	Routing Table Principles Exercise	19
	Path Determination and Switching Functions	20
	Internet Protocol (IP) Packet Format Exercise	20
	MAC Layer Frame Format Exercise	20
	Best Path and Metrics: Completion and Short Answer Exercise	21
	Path Determination and Switching Function Exercise	21
	Labs and Activities	25
	Command Reference	25
	Lab 1-1: Cabling a Network and Basic Router Configuration (1.5.1)	26
	Task 1: Cable the Ethernet Links of the Network	27
	Task 2: Cable the Serial Link Between the R1 and R2 Routers	28
	Task 3: Establish a Console Connection to the R1 Router	29
	Task 4: Erase and Reload the Routers	29
	Task 5: Understand Command-Line Basics	30
	Task 6: Perform Basic Configuration of Router R1	33
	Task 7: Perform Basic Configuration of Router R2	35
	Task 8: Configure IP Addressing on the Host PCs	36
	Task 9: Examine Router show Commands	37

Task 10: Use the ping Command	41
Task 11: Use the traceroute Command	42
Task 12: Create a start.txt File	43
Task 13: Load the start.txt File onto the R1 Router	45
Packet Tracer Companion	46
Appendix 1A: Installing and Configuring Tera Term for Use in Windows XP	47
Appendix 1B: Configuring Tera Term as the Default Telnet Client in Windows XP	48
Appendix 1C: Accessing and Configuring HyperTerminal	51

Lab 1-2: Basic Router Configuration (1.5.2) 52

Task 1: Cable the Network	53
Task 2: Erase and Reload the Routers	54
Task 3: Perform Basic Configuration of Router R1	55
Task 4: Perform Basic Configuration of Router R2	57
Task 5: Configure IP Addressing on the Host PCs	58
Task 6: Verify and Test the Configurations	58
Task 7: Reflection	60
Task 8: Documentation	61
Task 9: Clean Up	61
Packet Tracer Companion	61

Lab 1-3: Challenge Router Configuration (1.5.3) 61

Task 1: Subnet the Address Space	62
Task 2: Determine Interface Addresses	62
Task 3: Prepare the Network	63
Task 4: Perform Basic Router Configurations	63
Task 5: Configure and Activate Serial and Ethernet Addresses	63
Task 6: Verify the Configurations	64
Task 7: Reflection	64
Task 8: Document the Router Configurations	64
Packet Tracer Companion	65

Packet Tracer Skills Integration Challenge 65

Task 1: Design and Document an Addressing Scheme	66
Task 2: Cable Devices	66
Task 3: Apply a Basic Configuration	67
Task 4: Identify Layer 2 and Layer 3 Addresses Used to Switch Packets	67
Reflection	67

End Notes 68

Chapter 2 Static Routing 69

Study Guide 70

Routers and the Network 70

Document the Addressing Scheme	70
Packet Tracer Exercise 2-1	71

Router Configuration Review	72
show Commands Matching Exercise	72
Configuring and Verifying Interfaces Exercise	73
Exploring Directly Connected Networks	75
Directly Connected Networks Exercise	75
Packet Tracer Exercise 2-1: Task 3—Basic Router Configuration	78
Cisco Discovery Protocol Exercise	78
Packet Tracer Exercise 2-1: Task 4—Configure CDP	80
Static Routes with Next-Hop Addresses	80
Static Route Command Syntax Exercise	81
Static Routes with Next-Hop Address Exercise	81
Packet Tracer Exercise 2-1	83
Configuring a Static Route with an Exit Interface	84
Static Routes with an Exit Interface Exercise	84
Packet Tracer Exercise 2-2	85
Summary and Default Static Routes	86
Calculating Summary Route Exercises	86
Combining Static Routes into Summary Routes Exercise	91
Packet Tracer Exercise 2-3: Summary Route Configuration	93
Configuring Default Static Routes Exercise	94
Packet Tracer Exercise 2-4: Default Route Configuration	95
Managing and Troubleshooting Static Routes	96
Troubleshooting a Missing Route	96
Labs and Activities	97
Command Reference	97
Lab 2-1: Basic Static Route Configuration (2.8.1)	98
Task 1: Cable, Erase, and Reload the Routers	99
Task 2: Perform Basic Router Configuration	99
Task 3: Interpreting Debug Output	101
Task 4: Finish Configuring Router Interfaces	106
Task 5: Configure IP Addressing on the Host PCs	106
Task 6: Test and Verify the Configurations	106
Task 7: Gather Information	107
Task 8: Configure a Static Route Using a Next-Hop Address	109
Task 9: Configure a Static Route Using an Exit Interface	111
Task 10: Configure a Default Static Route	113
Task 11: Configure a Summary Static Route	114
Task 12: Summary, Reflection, and Documentation	116
Task 13: Clean Up	117
Task 14: Challenge	117
Packet Tracer Companion: Basic Static Route Configuration (2.8.1)	118

	Lab 2-2: Challenge Static Route Configuration (2.8.2)	118
	Task 1: Subnet the Address Space	119
	Task 2: Determine Interface Addresses	120
	Task 3: Prepare the Network	121
	Task 4: Perform Basic Router Configurations	121
	Task 5: Configure and Activate Serial and Ethernet Addresses	121
	Task 6: Verify Connectivity to Next-Hop Device	121
	Task 7: Configure Static Routing on BRANCH	122
	Task 8: Configure Static Routing on HQ	123
	Task 9: Configure Static Routing on ISP	124
	Task 10: Verify the Configurations	124
	Task 11: Reflection	125
	Task 12: Document the Router Configurations	125
	Task 13: Clean Up	125
	Packet Tracer Companion: Challenge Static Route Configuration (2.8.2)	125
	Lab 2-3: Troubleshooting Static Routes (2.8.3)	125
	Task 1: Cable, Erase, and Reload the Routers	127
	Task 2: Load Routers with the Supplied Scripts	127
	Task 3: Troubleshoot the BRANCH Router	131
	Task 4: Troubleshoot the HQ Router	133
	Task 5: Troubleshoot the ISP Router	134
	Task 6: Reflection	135
	Task 7: Documentation	135
	Packet Tracer Companion: Troubleshooting Static Routes (2.8.3)	136
	Packet Tracer Skills Integration Challenge	136
	Introduction	136
	Task 1: Cable the Devices	137
	Task 2: Apply a Basic Configuration	137
	Task 3: Configure Static and Default Routing	137
	Task 4: Test Connectivity and Examine the Configuration	137
	End Notes	137
Chapter 3	Introduction to Dynamic Routing Protocols	139
	Study Guide	140
	Introduction and Advantages	140
	Routing Protocols Evolution and Classification Exercise	140
	Vocabulary Exercise: Matching (Key Words)	141
	Dynamic Routing Protocol Concepts Exercise	142
	Dynamic Versus Static Routing Exercise	143
	Classifying Dynamic Routing Protocols	143
	Dynamic Routing Protocols Classification Chart	144
	Dynamic Routing Protocols Classification Exercise	144

	Metrics	146
	Metric Parameters Exercise	146
	Administrative Distances	147
	Concept of Administrative Distance Exercise	147
	Routing Sources and Administrative Distance Exercise	148
	Identifying Elements of the Routing Table Exercise	148
	Labs and Activities	150
	Command Reference	150
	Lab 3-1: Subnetting Scenario 1 (3.5.2)	150
	Task 1: Examine the Network Requirements	152
	Task 2: Design an IP Addressing Scheme	152
	Task 3: Assign IP Addresses to the Network Devices	153
	Task 4: Test the Network Design	153
	Task 5: Reflection	154
	Lab 3-2: Subnetting Scenario 2 (3.5.3)	154
	Task 1: Examine the Network Requirements	157
	Task 2: Design an IP Addressing Scheme	157
	Task 3: Assign IP Addresses to the Network Devices	158
	Task 4: Test the Network Design	160
	Task 5: Reflection	160
	Lab 3-3: Subnetting Scenario 3 (3.5.4)	161
	Task 1: Examine the Network Requirements	163
	Task 2: Design an IP Addressing Scheme	163
	Task 3: Reflection	163
	Packet Tracer Skills Integration Challenge	164
	Introduction	164
	Task 1: Design and Document an Addressing Scheme	165
	Task 2: Apply a Basic Configuration	166
	Task 3: Configure Static and Default Routing	166
	Task 4: Test Connectivity and Examine the Configuration	166
Chapter 4	Distance Vector Routing Protocols	169
	Study Guide	170
	Introduction to Distance Vector Routing Protocols	170
	Distance Vector Protocols Concepts Exercise	170
	Routing Protocols Characteristics Exercise	171
	Comparing Routing Protocol Characteristics Exercise	172
	Network Discovery	172
	Network Discovery Exercise	172
	Routing Table Maintenance	174
	Distance Vector Table Maintenance Techniques Exercise	174
	Routing Loops	176
	Routing Loop Concepts Exercise	176

Distance Vector Routing Protocols Today 178

Comparing Distance Vector Routing Protocols 178

Labs and Activities 179

Lab 4-1: Routing Table Interpretation (4.6.1) 179

Task 1: Examine the Router Output 179

Task 2: Create a Diagram of the Network Based on the Router Output 181

Task 3: Create the Network 182

Task 4: Configure the Routing Protocol for Each Router 182

Task 5: Document the Router Configurations 183

Task 6: Clean Up 183

Packet Tracer Companion: Routing Table Interpretation (4.6.1) 183

Packet Tracer Skills Integration Challenge 183

Introduction 183

Task 1: Design and Document an Addressing Scheme 184

Task 2: Apply a Basic Configuration 187

Task 3: Configure Static and Default Routing 187

Task 4: Test Connectivity and Examine the Configuration 187

Chapter 5 RIP Version 1 189

Study Guide 190

RIPv1: Distance Vector, Classful Routing Protocol 190

RIP Concepts Exercise 190

Basic RIPv1 Configuration 192

Document the Addressing Scheme 192

Packet Tracer Exercise 5-1 193

Configuring RIP as the Routing Protocol 194

Packet Tracer Exercise 5-1 (Continued) 195

Verification and Troubleshooting 195

show ip route Command 195

Interpreting show ip route Output 196

show ip protocols Command 196

debug ip rip Command 197

Passive Interfaces 198

Packet Tracer Exercise 5-1 (Continued) 198

Automatic Summarization 199

Automatic Summarization Concepts 199

Automatic Summarization Example 200

Default Routes and RIPv1 201

Default Routing Exercise 201

Packet Tracer Exercise 5-2 202

Labs and Activities 204

Command Reference 204**Lab 5-1: Basic RIP Configuration (5.6.1) 204**

- Scenario A: Running RIPv1 on Classful Networks 205
- Packet Tracer Companion: Basic RIP Configuration (5.6.1a) 210
- Scenario B: Running RIPv1 with Subnets and Between Classful Networks 210
- Packet Tracer Companion: Basic RIP Configuration (5.6.1b) 214
- Scenario C: Running RIPv1 on a Stub Network 215
- Packet Tracer Companion: Basic RIP Configuration (5.6.1c) 218

Lab 5-2: Challenge RIP Configuration (5.6.2) 219

- Task 1: Subnet the Address Space 220
- Task 2: Determine Interface Addresses 221
- Task 3: Prepare the Network 221
- Task 4: Perform Basic Router Configurations 221
- Task 5: Configure and Activate Serial and Ethernet Addresses 222
- Task 6: Verify Connectivity to Next-Hop Device 222
- Task 7: Configure RIP Routing on the BRANCH Router 222
- Task 8: Configure RIP and Static Routing on the HQ Router 223
- Task 9: Configure Static Routing on the ISP Router 223
- Task 10: Verify the Configurations 223
- Task 11: Reflection 224
- Task 12: Document the Router Configurations 224
- Task 13: Clean Up 225
- Packet Tracer Companion: Challenge RIP Configuration (5.6.2) 225

Lab 5-3: RIP Troubleshooting (5.6.3) 225

- Task 1: Cable, Erase, and Reload the Routers 227
- Task 2: Load Routers with the Supplied Scripts 227
- Task 3: Troubleshoot the BRANCH Router 231
- Task 4: Troubleshoot the HQ Router 233
- Task 5: Troubleshoot the ISP Router 235
- Task 6: Reflection 236
- Task 7: Documentation 236
- Task 8: Clean Up 237
- Packet Tracer Companion: RIP Troubleshooting (5.6.3) 237

Packet Tracer Skills Integration Challenge 237

- Introduction 237
- Task 1: Design and Document an Addressing Scheme 240
- Task 3: Apply a Basic Configuration 242
- Task 4: Configure Static Routing Between ISP Routers 242
- Task 5: Configure RIPv1 Routing in Region 1 and Region 2 242
- Task 6: Disable RIP Updates on Appropriate Interfaces 243
- Task 7: Configure Default Routes and Redistribute Through RIP 243
- Task 8: Verify Full Connectivity Between All Devices in the Topology 243

Chapter 6	VLSM and CIDR	245
	Study Guide	246
	Classful and Classless Addressing	246
	Move from Classful to Classless Addressing Exercise	246
	VLSM	248
	VLSM Addressing Design Exercises	248
	VLSM Addressing Design Scenarios	251
	CIDR	259
	Calculating a Summary Route Exercises	259
	Labs and Activities	262
	Activity 6-1: Basic VLSM Calculation and Addressing Design (6.4.1)	262
	Task 1: Examine the Network Requirements	263
	Task 2: Design an IP Addressing Scheme	263
	Task 3: Assign IP Addresses to the Network Devices	266
	Packet Tracer Companion: Basic VLSM Calculation and Addressing Design (6.4.1)	268
	Activity 6-2: Challenge VLSM Calculation and Addressing Design (6.4.2)	268
	Task 1: Examine the Network Requirements	270
	Task 2: Divide the Network into Three Subnetworks	270
	Task 3: Design an IP Addressing Scheme for the Central Network	271
	Task 4: Design an IP Addressing Scheme for the West Network	272
	Task 5: Design an IP Addressing Scheme for the East Network	275
	Packet Tracer Companion: Challenge VLSM Calculation and Addressing Design (6.4.2)	280
	Activity 6-3: Troubleshooting a VLSM Addressing Design (6.4.3)	280
	Task 1: Examine the Addressing for the HQ LANs	281
	Task 2: Examine the Addressing for the Branch1 LANs	282
	Task 3: Examine the Addressing for the Branch2 LANs	283
	Task 4: Examine the Addressing for the Links Between Routers	283
	Task 5: Document the Corrected Addressing Information	284
	Packet Tracer Companion: Troubleshooting a VLSM Addressing Design (6.4.3)	285
	Activity 6-4: Basic Route Summarization (6.4.4)	285
	Task 1: Determine the Summary Route for the HQ LANs	286
	Task 2: Determine the Summary Route for the EAST LANs	286
	Task 3: Determine the Summary Route for the WEST LANs	287
	Task 4: Determine the Summary Route for the HQ, EAST, and WEST LANs	287
	Packet Tracer Companion: Basic Route Summarization (6.4.4)	287
	Activity 6-5: Challenge Route Summarization (6.4.5)	288
	Task 1: Determine the Summary Route for the S-WEST LANs	290
	Task 2: Determine the Summary Route for the NW-BR1 LANs	290
	Task 3: Determine the Summary Route for the NW-BR2 LANs	290
	Task 4: Determine the Summary Route for the Northwest Portion of the Network	291

Task 5: Determine the Summary Route for the West Portion of the Network	291
Task 6: Determine the Summary Route for the Central Portion of the Network	292
Task 7: Determine the Summary Route for the N-EAST LANs	292
Task 8: Determine the Summary Route for the SE-BR1 LANs	292
Task 9: Determine the Summary Route for the SE-BR2 LANs	293
Task 10: Determine the Summary Route for the SE-ST1 LANs	293
Task 11: Determine the Summary Route for the SE-ST2 LANs	293
Task 12: Determine the Summary Route for the Southeast Portion of the Network	294
Task 13: Determine the Summary Route for the East Portion of the Network	294
Task 14: Determine the Summary Route for the Entire Network	295
Packet Tracer Companion: Challenge Route Summarization (6.4.5)	295

Activity 6-6: Troubleshooting Route Summarization (6.4.6) 295

Task 1: Examine the Summary Routes on the HQ Router	296
Task 2: Examine the Summary Routes on the WEST Router	297
Task 3: Examine the Summary Routes on the EAST Router	297
Task 4: Examine the Summary Route on the ISP Router	297
Task 5: Document the Corrected Summary Routes	297
Packet Tracer Companion: Troubleshooting Route Summarization (6.4.6)	298

Packet Tracer Skills Integration Challenge: VLSM and CIDR 298

Task 1: Design and Document an Addressing Scheme	301
Task 3: Apply a Basic Configuration	304
Task 4: Configure Static Routing Between ISP Routers	304
Task 5: Configure RIPv2 Routing in Region 1 and Static Routing in Region 2	304
Task 6: Disable RIP Updates on Appropriate Interfaces	304
Task 7: Configure Default Routes and Redistribute Through RIP	304
Task 8: Verify Full Connectivity Between All Devices in the Topology	305

Chapter 7 RIPv2 307

Study Guide 308

RIPv1 Limitations 308

Documenting the Addressing Scheme	308
Packet Tracer Exercise 7-1	310
Dynamic and Static Routing Configuration	311
Packet Tracer Exercise 7-1	312
Concept Questions	312

Configuring RIPv2 314

RIPv2 Message Format	314
RIPv2 Configurations	315
Packet Tracer Exercise 7-1	316

VLSM and CIDR 316

RIPv2 and VLSM 316

RIPv2 and CIDR 317

Verifying and Troubleshooting RIPv2 317

Verification and Troubleshooting Commands 317

Common RIPv2 Issues 318

Authentication 318

Labs and Activities 319**Command Reference 319****Lab 7-1: RIPv2 Basic Configuration (7.5.1) 319**

Task 1: Cable, Erase, and Reload the Routers 320

Task 2: Load Routers with the Supplied Scripts 321

Task 3: Examine the Current Status of the Network 323

Task 4: Configure RIP Version 2 325

Task 5: Examine the Automatic Summarization of Routes 326

Task 6: Disable Automatic Summarization 328

Task 7: Examine the Routing Tables 328

Task 8: Verify Network Connectivity 329

Task 9: Documentation 330

Task 10: Clean Up 330

Packet Tracer Companion: RIPv2 Basic Configuration (7.5.1) 330

Lab 7-2: RIPv2 Challenge Configuration (7.5.2) 331

Task 1: Subnet the Address Space 331

Task 2: Determine Interface Addresses 332

Task 3: Prepare the Network 334

Task 4: Perform Basic Router Configurations 334

Task 5: Configure and Activate Serial and Ethernet Addresses 334

Task 6: Verify Connectivity to the Next-Hop Device 334

Task 7: Configure RIPv2 Routing on the BRANCH Router 335

Task 8: Configure RIPv2 and Static Routing on HQ 335

Task 9: Configure Static Routing on the ISP Router 336

Task 10: Verify the Configurations 336

Task 11: Reflection 337

Task 12: Document the Router Configurations 337

Task 13: Clean Up 337

Packet Tracer Companion: RIPv2 Challenge Configuration (7.5.2) 338

Lab 7-3: RIPv2 Troubleshooting (7.5.3) 338

Task 1: Cable, Erase, and Reload the Routers 340

Task 2: Load Routers with the Supplied Scripts 340

Task 3: Troubleshoot the BRANCH1 Router 345

Task 4: Troubleshoot HQ 347

Task 5: Troubleshoot BRANCH2 349

Task 6: Reflection 352

- Task 7: Documentation 352
- Task 8: Clean Up 352
- Packet Tracer Companion: Troubleshooting RIPv2 Configuration (7.5.3) 352

Packet Tracer Skills Integration Challenge: Configuring and Troubleshooting RIPv2 352

- Task 1: Design and Document an Addressing Scheme 354
- Task 2: Select Equipment and Cable Devices 355
- Task 3: Apply a Basic Configuration 355
- Task 4: Test Connectivity 355
- Task 5: Configure and Verify RIPv2 Routing 355
- Task 6: Configure Static and Default Routing 355
- Task 7: Test Connectivity and Examine the Configuration 355

Chapter 8 The Routing Table: A Closer Look 357

Study Guide 358

Routing Table Structure 358

- Level 1 and Level 2 Routes 358
- Parent and Child Routes 359

Routing Table Lookup Process 361

- Complete the Chart 361
- Routing Table Lookup Exercise 361

Routing Behavior 363

- Classful and Classless Routing Behavior 363
- Determine the Route 364
- Determine the Topology 365

Labs and Activities 370

Command Reference 370

Lab 8-1: Investigating the Routing Table Lookup Process (8.4.1) 370

- Scenario A: Level 1 and Level 2 Routes 371
- Packet Tracer Companion: Investigating the Routing Table Lookup Process (8.4.1) 375
- Scenario B: Classful and Classless Routing Behavior 375

Lab 8-2: show ip route Challenge (8.4.2) 378

- Task 1: Examine the Router Outputs 378
- Task 2: Create a Diagram of the Network Based on the show ip route Output on Routers R1–R5 381
- Task 3: Build and Configure the Diagram Using Packet Tracer 382
- Task 4: Identify Routing Processes 383
- Packet Tracer Companion: show ip route Challenge Lab (8.4.2) 384

Packet Tracer Skills Integration Challenge 385

- Introduction 385
- Task 1: Design and Document an Addressing Scheme 388
- Task 2: Apply a Basic Configuration 391

Task 3: Configure Static Routing Between ISP Routers	391
Task 4: Configure RIPv2 Routing in Both Regions	391
Task 5: Disable RIP Updates on Appropriate Interfaces	391
Task 6: Configure Default Routes and Redistribute Through RIP	391
Task 7: Verify Full Connectivity Between All Devices in the Topology	391

Chapter 9 EIGRP 393

Study Guide 394

Introduction to EIGRP 394

Vocabulary Exercise: Matching	395
EIGRP Concepts Exercise	396

Basic EIGRP Configuration 400

Documenting the Addressing Scheme	401
Packet Tracer Exercise 9-1	404
Configuring EIGRP as the Routing Protocol	404
Verifying EIGRP	405
Packet Tracer Exercise 9-1 (Continued)	407

EIGRP Metric Calculation 407

EIGRP Metric Concepts	407
Modifying the Bandwidth	408
Packet Tracer Exercise 9-1 (Continued)	409

DUAL 409

DUAL Concepts Exercise	409
DUAL FSM Completion Exercise	412

More EIGRP Configurations 413

Manual Summarization Exercise	413
EIGRP Default Route Exercise	414
Fine-Tuning EIGRP Exercise	414
Packet Tracer Exercise 9-1 (Continued)	415

Labs and Activities 417

Command Reference 417

Lab 9-1: Basic EIGRP Configuration (9.6.1) 417

Task 1: Prepare the Network	419
Task 2: Perform Basic Router Configurations	419
Task 3: Configure and Activate Serial and Ethernet Addresses	419
Task 4: Configure EIGRP on the R1 Router	420
Task 5: Configure EIGRP on the R2 and R3 Routers	421
Task 6: Verify EIGRP Operation	422
Task 7: Examine EIGRP Routes in the Routing Tables	423
Task 8: Configure EIGRP Metrics	424
Task 9: Examine Successors and Feasible Distances	426
Task 10: Determine Whether R1 Is a Feasible Successor for the Route from R2 to the 192.168.1.0 Network	427

Task 11: Examine the EIGRP Topology Table	428
Task 12: Disable EIGRP Automatic Summarization	429
Task 13: Configure Manual Summarization	430
Task 14: Configure and Distribute a Static Default Route	432
Task 15: Documentation	433
Task 16: Clean Up	433
Packet Tracer Companion: Basic EIGRP Configuration (9.6.1)	433
Lab 9-2: Comprehensive EIGRP Configuration	433
Task 1: Cable the Topology and Basic Configurations	434
Task 2: Configure Interfaces and EIGRP Routing	435
Task 3: Configure Bandwidth and Automatic Summarization	436
Task 4: Configure Manual Summarization	437
Lab 9-3: Challenge EIGRP Configuration (9.6.2)	438
Task 1: Subnet the Address Space	439
Task 2: Determine Interface Addresses	440
Task 3: Prepare the Network	441
Task 4: Perform Basic Router Configurations	441
Task 5: Configure and Activate Serial and Ethernet Addresses	442
Task 6: Verify Connectivity to the Next-Hop Device	442
Task 7: Configure EIGRP Routing on the BRANCH1 Router	442
Task 8: Configure EIGRP and Static Routing on the HQ Router	443
Task 9: Configure EIGRP Routing on the BRANCH2 Router	444
Task 10: Verify the Configurations	444
Task 11: Reflection	445
Task 12: Document the Router Configurations	445
Task 13: Clean Up	445
Packet Tracer Companion: Challenge EIGRP Configuration (9.6.2)	446
Challenge Lab 9-4: EIGRP Design and Configuration	446
Task 1: Design the Addressing Scheme	446
Task 2: Cable the Topology and Basic Configuration	448
Task 3: Configure EIGRP Routing and Default Routing	448
Task 4: Manual Summarization	448
Task 5: Verification and Documentation	449
Lab 9-5: EIGRP Troubleshooting (9.6.3)	456
Task 1: Cable, Erase, and Reload the Routers	457
Task 2: Load Routers with the Supplied Scripts	458
Task 3: Troubleshoot the BRANCH1 Router	463
Task 4: Troubleshoot the HQ Router	465
Task 5: Troubleshoot the BRANCH2 Router	467
Task 6: Reflection	470
Task 7: Documentation	470
Task 8: Clean Up	471
Packet Tracer Companion: EIGRP Troubleshooting (9.6.3)	471

Packet Tracer Skills Integration Challenge: EIGRP Configuration 471

Task 1: Design and Document an Addressing Scheme 474

Task 2: Apply a Basic Configuration 474

Task 3: Test Connectivity 474

Task 4: Configure and Verify EIGRP Routing 475

Task 5: Fine-Tune EIGRP 475

Task 6: Configure Static and Default Routing 475

Task 7: Test Connectivity and Examine the Configuration 475

Chapter 10 Link-State Routing Protocols 477

Study Guide 478

Link-State Routing 478

Link-State Routing Concepts Exercise 478

Implementing Link-State Routing Protocols 484

Advantages of a Link-State Routing Protocol Exercise 485

Requirements of a Link-State Routing Protocol Exercise 485

Labs and Activities 487

Packet Tracer Skills Integration Challenge: EIGRP and RIPv2 Configuration 487

Task 1: Design and Document an Addressing Scheme 490

Task 2: Apply a Basic Configuration 493

Task 3: Configure Static Routing Between ISP Routers 493

Task 4: Configure EIGRP Routing in Region 1 and RIPv2 Routing Region 2 493

Task 5: Disable Routing Updates on Appropriate Interfaces 493

Task 6: Configure and Redistribute Default Routes 493

Task 7: Verify Full Connectivity Between All Devices in the Topology 494

Chapter 11 OSPF 495

Study Guide 496

Introduction to OSPF 496

Vocabulary Exercise: Matching 497

OSPF Concepts Exercise 498

Basic OSPF Configuration 500

Learn the OSPF Commands Exercise 500

Verify OSPF Configuration Exercise 502

OSPF Metric 503

Calculating the Cost Metric Exercise 503

Modifying the Cost Metric Exercise 504

OSPF and Multiaccess Networks 504

OSPF and Multiaccess Networks Completion Exercise 504

DR/BDR Election Exercise 506

More OSPF Configuration 508

Redistributing an OSPF Default Route Exercise 508

Fine-Tuning OSPF Exercise 509

Labs and Activities 510**Command Reference 510****Lab 11-1: Basic OSPF Configuration (11.6.1) 511**

- Scenario A: Basic OSPF Configuration 511
 - Task 1: Prepare the Network 512
 - Task 2: Perform Basic Router Configurations 513
 - Task 3: Configure and Activate Serial and Ethernet Addresses 513
 - Task 4: Configure OSPF on the R1 Router 513
 - Task 5: Configure OSPF on the R2 and R3 Routers 514
 - Task 6: Configure OSPF Router IDs 515
 - Task 7: Verify OSPF Operation 518
 - Task 8: Examine OSPF Routes in the Routing Tables 519
 - Task 9: Configure OSPF Cost 519
 - Task 10: Redistribute an OSPF Default Route 522
 - Task 11: Configure Additional OSPF Features 523
 - Task 12: Document the Router Configurations 525
 - Task 13: Clean Up 525
- Packet Tracer Companion: Basic OSPF Configuration (11.6.2) 525
- Scenario B: Configure OSPF on a Multiaccess Network 525
 - Task 1: Prepare the Network 526
 - Task 2: Perform Basic Router Configurations 526
 - Task 3: Configure and Activate Ethernet and Loopback Addresses 527
 - Task 4: Configure OSPF on the DR Router 527
 - Task 5: Configure OSPF on the BDR 528
 - Task 6: Configure OSPF on the DROther Router 529
 - Task 7: Use the OSPF Priority to Determine the DR and BDR 530
 - Task 8: Document the Router Configurations 532
 - Task 9: Clean Up 532
- Packet Tracer Companion: Basic OSPF Configuration (11.6.1) 533

Lab 11-2: Challenge OSPF Configuration (11.6.2) 533

- Task 1: Subnet the Address Space 534
- Task 2: Determine Interface Addresses 535
- Task 3: Prepare the Network 536
- Task 4: Perform Basic Router Configurations 536
- Task 5: Configure and Activate Serial and Ethernet Addresses 536
- Task 6: Verify Connectivity to the Next-Hop Device 537
- Task 7: Configure OSPF Routing on the Branch1 Router 537
- Task 8: Configure OSPF and Static Routing on the HQ Router 538
- Task 9: Configure OSPF Routing on the Branch2 Router 539
- Task 10: Verify the Configurations 539
- Task 11: Reflection 540
- Task 12: Documentation 540

Task 13: Clean Up 541

Packet Tracer Companion: Challenge OSPF Configuration (11.6.2) 541

Lab 11-3: OSPF Troubleshooting Lab (11.6.3) 541

Task 1: Cable, Erase, and Reload the Routers 543

Task 2: Load Routers with the Supplied Scripts 543

Task 3: Troubleshoot the Branch1 Router 548

Task 4: Troubleshoot the HQ Router 550

Task 5: Troubleshoot the Branch2 Router 552

Task 6: Reflection 554

Task 7: Documentation 555

Task 8: Clean Up 555

Packet Tracer Companion: OSPF Troubleshooting (11.6.3) 555

Packet Tracer Skills Integration Challenge: OSPF Configuration 555

Task 1: Design and Document an Addressing Scheme 557

Task 2: Apply a Basic Configuration 557

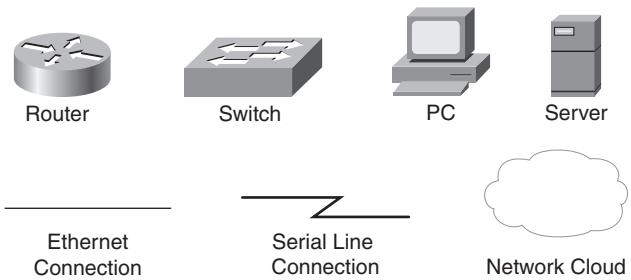
Task 3: Configure OSPF Routing 557

Task 4: Fine-Tuning OSPF 557

Task 5: Configure a Loopback 558

Task 6: View OSPF Updates 558

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

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

- Basic Routing and Packet-Forwarding Concepts
- Understanding and Configuring Static and Default Routes
- Distance Vector Routing Protocol Concepts
- RIPv1, RIPv2, and EIGRP Concepts and Configuration
- IP Addressing with VLSM
- Classful and Classless Routing
- Link-State Routing Protocol Concepts
- OSPF Concepts and Configuration
- Troubleshooting Routing Issues

Labs and Study Guides similar to this one are also available for the other three courses: *Network Fundamentals, CCNA Exploration Labs and Study Guide*; *LAN Switching and Wireless, CCNA Exploration Labs and Study Guide*; and *Accessing the WAN, CCNA Exploration Labs and Study Guide*.

A Word About Packet Tracer

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

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

Goals and Methods

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

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

The Routing Protocols and Concepts course focuses on the third and fourth bullets.

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

- Vocabulary Matching and Completion
- Skill-Building Activities and Scenarios
- Configuration Scenarios
- Concept Questions
- Journal Entries
- Internet Research

Packet Tracer
 Activity

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

The Labs and Activities sections include a Command Reference table, all the online Curriculum Labs, and a Packet Tracer Skills Integration Challenge Activity. The Curriculum Labs are divided into three categories:

- **Basic:** The Basic Labs are procedural in nature and assume that you have no experience configuring the technologies that are the topic of the lab.
- **Challenge:** The Challenge Labs are implementation in nature and assume that you have a firm enough grasp on the technologies to "go it alone." These labs often only give you a general requirement that you must implement fully without the details of each small step. In other

words, you must use the knowledge and skills you gained in the chapter text, activities, and Basic Lab to successfully complete the Challenge Labs. Avoid the temptation to work through the Challenge Lab by flipping back through the Basic Lab when you are not sure of a command. Do not try to short-circuit your CCNA training. You need a deep understanding of CCNA knowledge and skills to ultimately be successful on the CCNA exam.

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

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

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

Audience for This Book

This book's main audience is anyone taking the CCNA Exploration Routing Protocols and Concepts course of the Cisco Networking Academy curriculum. Many Academies use this textbook as a required tool in the course, while other Academies recommend the Companion Guides as an additional source of study and practice materials.

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

How This Book Is Organized

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

The book covers the major topic headings in the same sequence as the online curriculum for the CCNA Exploration Routing Protocols and Concepts course. This book has 11 chapters, with the same numbers and similar names as the online course chapters.

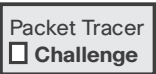
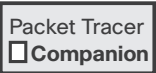
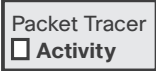
Each routing protocol chapter and the static routing chapter begin with a single topology that is used throughout the chapter. The single topology per chapter allows better continuity and easier understanding of routing commands, operations, and outputs. However, the topology is different than the one used in the online curriculum and the Companion Guide. A different topology affords you the opportunity to practice your knowledge and skills without just simply recording the information you find in the text.

- **Chapter 1, “Introduction to Routing and Packet Forwarding”:** This chapter begins with several exercises devoted to reinforcing your understanding of the basic hardware and software components of a router as well as testing your knowledge of basic routing and packet forwarding. Then you will practice the basic addressing and configuration skills that are crucial to all future chapters. The Study Guide portion of the chapter ends with a review of routing principles

as well as explains how a router determines the path and switches the packet. The Lab portion includes two versions of the Basic Lab, a Challenge Lab, and the Packet Tracer Skills Integration Challenge Activity.

- **Chapter 2, “Static Routing”:** The exercises in the first part of this chapter will help you understand basic router configuration and verification as well as the concept of directly connected networks. Then the exercises cover, in detail, static routes, summary routes, and default routes. The Lab portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge Activity.
- **Chapter 3, “Introduction to Dynamic Routing Protocols”:** The exercises in this chapter focus on the concepts of dynamic routing, including basic concepts and advantages, classification, metrics, administrative distance, and routing table elements. The Lab section includes six subnetting scenarios to help you hone your IP addressing design skills. The Lab section also includes a Packet Tracer Skills Integration Challenge Activity.
- **Chapter 4, “Distance Vector Routing Protocols”:** This chapter’s exercises are devoted to the concepts of distance vector routing protocols, including their characteristics, how they maintain the routing table, and how they guard against routing loops. The Lab section includes a routing table interpretation activity and a Packet Tracer Skills Integration Challenge Activity.
- **Chapter 5, “RIP Version 1”:** Exercises in this chapter focus on RIPv1 concepts, basic configuration, verification, troubleshooting, automatic summarization, and RIP default route propagation. The Lab portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge Activity.
- **Chapter 6, “VLSM and CIDR”:** This chapter is a transition from classful routing to classless routing. Therefore, exercises focus on the concepts and skills necessary for implementing VLSM addressing schemes and CIDR. The Lab section includes three VLSM design scenarios and three route summarization scenarios. The Lab section also includes a Packet Tracer Skills Integration Challenge Activity.
- **Chapter 7, “RIPv2”:** The exercises in this chapter cover the concepts and configurations of the classless version of RIPv2. First, you explore how RIPv2 addresses the limitations of RIPv1. Then you configure, verify, and troubleshoot RIPv2. The Lab portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge Activity.
- **Chapter 8, “The Routing Table: A Closer Look”:** This chapter represents a pivotal point in your studies of routing protocols and concepts as you delve into exercises that take you deep into the structure of the routing table. Understanding exactly how the routing table is constructed and then used by the IOS provides a valuable tool in verifying and troubleshooting networks. The Lab portion of the chapter includes two routing table labs and a Packet Tracer Skills Integration Challenge Activity.
- **Chapter 9, “EIGRP”:** Exercises in this chapter focus on EIGRP concepts, basic configuration, verification, troubleshooting, metric calculation, and DUAL operation as well as some more advanced EIGRP configurations. The Lab portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge Activity.
- **Chapter 10, “Link-State Routing Protocols”:** The exercises in this chapter help you transition from distance vector routing protocols to link-state routing protocols. There are no labs for this chapter. However, there is a Packet Tracer Skills Integration Challenge Activity.

- **Chapter 11, “OSPF”:** This chapter concludes your studies of routing protocols with exercises focusing on basic OSPF concepts and configurations, including the OSPF metric calculation, OSPF multiaccess networks, and some advanced OSPF configurations for single-area OSPF implementations. The Lab portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge Activity.



About the CD-ROM

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

Updates to these files can be obtained from the website for this book, <http://www.ciscopress.com/title/1587132044>. The files will be updated to cover any subsequent releases of Packet Tracer.

About the Cisco Press Website for This Book

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

To register this book, go to <http://www.ciscopress.com/bookstore/register.asp> and enter the book's ISBN, which is located on its back cover. You'll then be prompted to log in or join [ciscopress.com](http://www.ciscopress.com) to continue registration.

After you register the book, a link to any additional content will be listed on your My Registered Books page.

Introduction to Routing and Packet Forwarding

The Study Guide portion of this chapter uses a combination of matching, fill-in-the-blank, multiple-choice, and open-ended question exercises to test your knowledge and skills of basic router concepts and configuration. The Lab Exercises portion of this chapter includes all the online curriculum labs to ensure that you have mastered the hands-on skills needed to understand basic IP addressing and router configuration.

As you work through this chapter, use Chapter 1 in *Routing Protocols and Concepts, CCNA Exploration Companion Guide* or use the corresponding Chapter 1 in the Exploration Routing Protocols and Concepts online curriculum for assistance.

Study Guide

Inside the Router

A router is a computer and has many of the common hardware components found on other types of computers. A router also includes an operating system. The exercises in this section will reinforce your understanding of the basic hardware and software components of a router. You will also gain a better understanding of the routing and packet-forwarding process.

Vocabulary Exercise: Matching

Match the definition on the left with a term on the right. This exercise is not necessarily a one-to-one matching. Some definitions might be used more than once, and some terms might have multiple definitions.

Definitions

- a. Because routers do not necessarily have the same information in their routing tables, packets can traverse the network in one direction, using one path, and return through another path.
- b. Routing protocols use _____ to evaluate what path will be the best for a packet to travel to a destination network.
- c. Routing that depends on manually entered routes in the routing table.
- d. A management port on the router.
- e. A company that provides WAN technologies to connect the customer's local networks to the Internet and other remote networks.
- f. Most common LAN technology.
- g. Table of IP address-to-MAC address mappings used by routers that have Ethernet interfaces.
- h. The fastest route to a certain destination, which is based on the routing protocol's metric.
- i. A data link layer technology often used for WAN links.
- j. A dynamic routing protocol used by routers to determine the best path for IP packets.
- k. Port on the router that can be attached to a modem for remote management access.
- l. A series of questions prompting the user for basic configuration information because the router did not locate a startup configuration file.
- m. A form of permanent storage used by Cisco devices to store the bootstrap instructions, basic diagnostic software, and a scaled-down version of IOS.
- n. A router's ability to use multiple paths to the same destination because the paths have the same metric value.
- o. Identifies how many routers can be traversed by the datagram before being dropped.
- p. Stores the instructions and data needed to be executed by the CPU.
- q. An end device or node on the network that implies a computer system.
- r. This router mode allows the user to make configuration changes. The router prompt will change from a ">" to a "#."
- s. A router's ability to send packets over multiple networks, even when the metric is not the same.
- t. Common process that occurs on most every computer during bootup to test the router hardware.
- u. Used by the Cisco IOS as permanent storage for the startup configuration file.
- v. Nonvolatile computer memory that is used as permanent storage for the operating system, Cisco IOS.
- w. Port used to initially configure a router.
- x. Used by the router to determine the best path to forward the packet.
- y. Used by routers to automatically learn about remote networks and build their routing tables.

Terms

- g ARP cache
- a asymmetric routing
- i Asynchronous Transfer Mode
- d, k auxiliary port
- h best path
- j BGP
- d, w console port
- y dynamic routing protocols
- j EIGRP
- n equal-cost load balancing
- f Ethernet
- v flash
- i Frame Relay
- q hosts
- j IGRP
- e Internet service provider (ISP)
- j IS-IS
- b metric
- u NVRAM
- j OSPF
- t power-on self test (POST)
- i Point-to-Point Protocol (PPP)
- r privileged EXEC
- p RAM
- j RIP
- m ROM
- x routing table
- l setup mode
- c static routing
- o Time to Live (TTL)
- s unequal-cost load balancing

Vocabulary Exercise: Completion

Complete the paragraphs that follow by filling in the appropriate words and phrases.

Routers Are Computers

A router is a computer, just like any other computer including a PC. Routers have many of the same hardware and software components that are found in other computers including

- CPU
- RAM
- ROM
- Operating system

Each network that a router connects to typically requires a separate interface. These interfaces are used to connect a combination of both local-area networks (LAN) and wide-area networks (WAN). LANs are commonly Ethernet networks that contain devices such as PCs, printers, and servers. WANs are used to connect networks over a large geographical area and are commonly used to connect a LAN to the Internet service provider's (ISP) network.

The router's primary responsibility is to forward packets destined for local and remote networks by

- Determining the best path to send packets
- Forwarding packets toward their destination

The router uses its routing table to determine the best path to forward the packet. When a match is found, the router encapsulates the IP packet into the data-link frame of the outgoing or exit interface, and the packet is then forwarded towards its destination.

It is likely that a router will receive a packet encapsulated in one type of data-link frame, such as an Ethernet frame, and when forwarding the packet, encapsulate it in a different type of data-link frame.

Static routes and dynamic routing protocols are used by routers to learn about remote networks and build their routing tables.

Router CPU and Memory

Like a PC, the CPU in a router executes operating system instructions, such as system initialization, routing functions, and network interface control.

Similar to other computers, RAM stores the instructions and data needed to be executed by the CPU. It is volatile memory that loses its content when the router is powered down or restarted. For this reason, the router also contains permanent storage areas such as ROM, flash, and NVRAM.

ROM is a form of permanent storage. On Cisco devices, it stores

- The bootstrap instructions
- Basic diagnostic software
- Scaled-down version of IOS

In most models of Cisco routers, the IOS is permanently stored in flash memory and copied into RAM during the bootup process.

NVRAM is nonvolatile random-access memory that does not lose its information when power is turned off. NVRAM is used by the Cisco IOS as permanent storage for the startup configuration file.

Internetwork Operating System (IOS)

Like any operating system on any other computer, Cisco IOS is responsible for managing the hardware and software resources of the router. Although the Cisco IOS might appear to be the same on many routers, there are many different IOS [images](#): a file that contains the entire IOS for that router.

Although some routers provide a GUI ([graphical user interface](#)), the CLI ([command-line interface](#)) is a much more common method of configuring Cisco routers.

Upon bootup, the startup-config file in [NVRAM](#) is copied into [RAM](#) and stored as the [running-config](#) file. Any changes entered by the network administrator are stored in the [running-config](#) file and immediately implemented by the [IOS](#).

Router Bootup Process

Like all computers, a router uses a systematic process to boot up. The four phases are

1. [POST](#): Testing the router hardware
2. Loading the [bootstrap](#) program
3. Locating and loading the [IOS](#)
4. Locating and loading the [startup](#) configuration file or entering [setup mode](#)

[Power-on self test](#) (POST) is a common process that occurs on most every computer during bootup. The POST process is used to [test](#) the router [hardware](#).

After the POST, the [bootstrap](#) program is copied from ROM into RAM. Its job is to locate the Cisco IOS and load it into RAM.

After the IOS is loaded, it searches for the [startup-config](#) file. If this file is located, it is copied into RAM as the [running-config](#) file. The IOS executes the commands in the file one line at a time.

If the startup configuration file cannot be located, the router will prompt the user to enter [setup mode](#), a series of questions prompting the user for basic configuration information. Setup mode will not be used in this course.

After the normal loading process is completed and the prompt is displayed, the router is now running the IOS with the current running configuration file. The network administrator can now begin using IOS commands on this router.

The [show version](#) command can be used to help verify and troubleshoot some of the basic hardware and software components of the router.

Router Ports and Interfaces

Routers have [management](#) ports, which are physical connectors used by the administrator to configure the router and are not used for packet forwarding. The most common of the management ports is the [console](#) port. It must be used during initial configuration of the router. Another management port is the [auxiliary](#) port, which can also be used to attach a modem.

The term *interface* on Cisco routers refers to a physical connector on the router whose main purpose is to receive and forward [packets](#). Routers have multiple interfaces used to connect to multiple networks.

Every interface on the router is a member, a host on a different IP [network](#). A router's [Ethernet](#) interface usually uses an RJ-45 jack that supports unshielded twisted-pair (UTP) cabling. When a router is connected to a switch, a [straight-through](#) cable is used. When a PC's network interface card (NIC) is

connected directly to a router's Ethernet interface, a [crossover](#) cable is used.

Similar to LAN interfaces, each WAN interface has its own IP [address](#) and [subnet](#) mask, making it a member of a specific [network](#). Remember, MAC addresses are used only on [Ethernet](#) interfaces and are not on WAN interfaces.

Routers and the Network Layer

Key to understanding the role of a router in the network is to understand that a router is a Layer [3](#) device responsible for forwarding packets. However, a router also operates at Layers 1 and 2.

The main purpose of a router is to connect multiple networks and forward packets destined for its own networks or other networks. A router is considered a Layer 3 device because its primary forwarding decision is based on the information in the Layer [3](#) [IP packet](#), specifically the destination IP [address](#). This is known as [routing](#).

When a router receives a packet, it examines the [destination](#) IP address. If the packet does not belong to any of the router's directly connected networks, the router must [forward](#) this packet to another [router](#) or drop the packet.

When forwarding a packet, the router will encapsulate the Layer [3](#) IP packet into the data portion of a Layer [2](#) data-link [frame](#) appropriate for the exit interface. The Layer [2](#) [frame](#) will then be encoded into the Layer [1](#) physical signals used to represent these bits over the physical link.

Label the External Components of a Router Exercise

Choose the correct label description for each number shown in Figure 1-1.

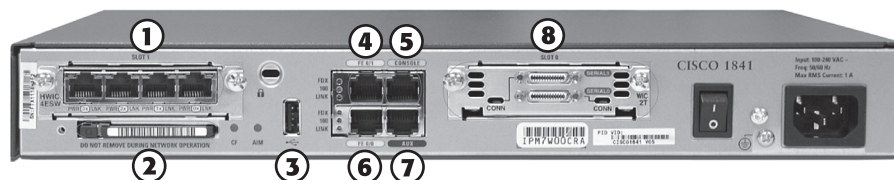


Figure 1-1 Rear View of an 1841 Cisco Router

Figure 1-1 Label Description:

- [7](#) Alternative management port that can support remote access through a modem
- [3](#) Single-slot USB port
- [1](#) 4-port Cisco EtherSwitch 10BASE-T/100BASE-TX autosensing high-speed WAN interface card
- [6](#) FastEthernet port 0/0
- [8](#) High-speed WAN interface card with two serial interfaces
- [2](#) Compact flash module
- [5](#) Management port used for local access to the device; must be used for initial configuration
- [4](#) FastEthernet port 0/1

Label the Internal Components of a Router Exercise

Choose the correct label description for each number shown in Figure 1-2.

Figure 1-2 Logical Diagram of the Internal Components of an 1841 Cisco Router

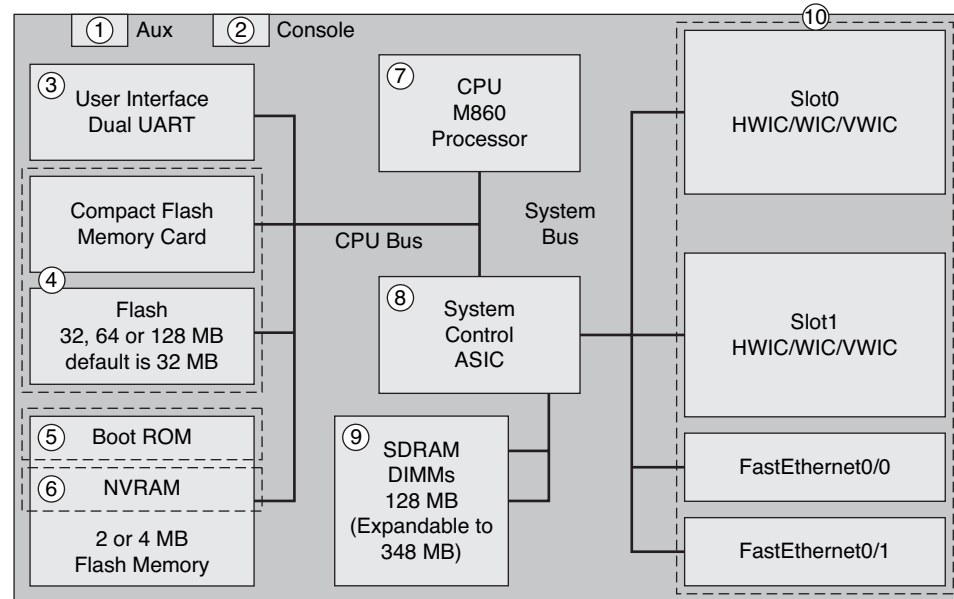


Figure 1-2 Label Description:

- 3 Universal asynchronous receiver/transmitter, which controls the dual access through the console and auxiliary ports
- 5 Holds the bootstrap program, ROM monitor, and possibly a scaled-down version of IOS software
- 10 Includes two modular slots and two built-in LAN interfaces
- 9 Holds running configuration, routing tables, and other data structures
- 6 Holds startup configuration
- 1 Management port used for remote configuration through a modem; not all routers have one of these
- 7 Loads instructions defined in Cisco IOS Software from the main processor memory and executes them
- 8 Controls the flow of data among memory, interfaces, and the CPU
- 2 Management port used for local configuration of the device
- 4 Stores the Cisco IOS Software image

Describe the Internal Components of a Router Exercise

Knowing the functions of the main internal components of a router is more important than knowing the locations of the physical components inside a particular model. Therefore, in your own words, provide a sufficiently detailed description of each component.

Component	Description
CPU	The central processing unit (CPU) executes the instructions of the operating system. Among these functions are system initialization, routing functions, and network interface control.
RAM	RAM is used for storing the IOS and for the working memory needed by the IOS. This includes the routing table, running configurations, and packet queues, which hold packets until the interface can be used to forward the packet. The contents of RAM are lost when the router loses power.
Flash	Flash memory is used for storage of a full Cisco IOS Software image. In most routers, a copy of the IOS is transferred to RAM from flash during the bootup process. Physically, flash memory consists of single in-line memory modules (SIMM) or PCMCIA cards, which can be upgraded to increase the amount of flash. Flash memory does not lose its contents when the router loses power.
NVRAM	NVRAM is used to store the startup configuration. As described in Chapter 2, "Static Routing," a router will copy the startup configuration from NVRAM into RAM when the router is initialized, and use the running configuration in RAM for normal router operation. NVRAM retains its contents when the router loses power.
Buses	Buses provide a physical means for the router to move bits between the different components of the router. Most routers contain a system bus and a CPU bus. The system bus is used to communicate between the CPU and the interfaces. For example, this bus transfers the packets to and from the interfaces. The CPU bus is used by the CPU for accessing router storage devices, like NVRAM and flash memory.
ROM	ROM holds the bootstrap program, the ROM Monitor software, and optionally a scaled-down version of the IOS. (Chapter 2 covers these types of software.) ROMs are not erasable and can only be upgraded by replacing the ROM chips, but ROM does retain its contents when the router loses power.
Power supply	The power supply converts the voltage and current of a standard power source to the voltage and current required by the devices in the router. The power supplies can be internal or external to the router chassis (the chassis is the metal box that holds the components of the router), and some routers have multiple power supplies for redundancy.

Another way to learn the internal components of a router is by listing the components' functions. For each component from the following list, indicate in the table that follows which component performs the listed function:

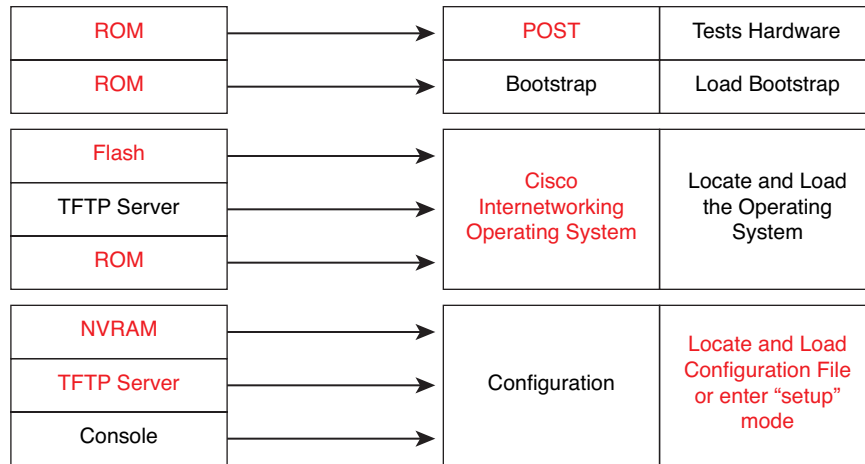
- A. RAM
- B. NVRAM
- C. Flash
- D. ROM
- E. Interfaces

Answer	Function
<u>A</u>	Provides temporary memory for the configuration file of the router while the router is powered on
<u>C</u>	Allows software to be updated without removing and replacing chips on the processor
<u>A</u>	Stores routing tables
<u>D</u>	Maintains instructions for power-on self test (POST) diagnostics
<u>E</u>	Connects the router to the network for frame entry and exit
<u>E</u>	Can be on the motherboard or on a separate module
<u>C</u>	Is a type of electronically erasable programmable ROM (EEPROM)
<u>B</u>	Retains content when router is powered down or restarted
<u>D</u>	Stores bootstrap program and basic operating system software
<u>A</u>	Holds ARP cache
<u>A</u>	Loses content when router is powered down or restarted
<u>B</u>	Retains content when router is powered down or restarted
<u>C</u>	Holds the operating system image (IOS)
<u>B</u>	Provides storage for the startup configuration file
<u>C</u>	Can store multiple versions of IOS software

Router Bootup Process Exercise

Figure 1-3 displays an incomplete diagram of the default boot sequence of a router. Provide detail where information is missing.

Figure 1-3 Diagram of the Router Boot Sequence



Interpreting the show version Command Exercise

Figure 1-4 displays the output from the **show version** command with parts of the output numbered. Choose the correct label description for each number shown in the figure.

Figure 1-4 show version Command

```

Router#show version
Cisco Internetwork Operating System Software
① IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Image text-base: 0x8000808C, data-base: 0x80A1FECC

② ROM: System Bootstrap, Version 12.1 (3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
ROM: C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

System returned to ROM by reload
System image file is "flash:c2600-i-mz.122-28.bin"

③ cisco 2621 (MPC860) processor (revision 0x200) with ④ 60416K/5120K bytes of memory
.

Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.

⑤ 2 FastEthernet/IEEE 802.3 interface(s)
⑥ 2 Low-speed serial(sync/async) network interface(s)
⑦ 32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

Router#
    
```


Figure 1-4 Label Description:

- 2 Bootstrap version
- 5 Number and type of interfaces
- 7 Amount of flash
- 3 Model and CPU
- 4 Amount of RAM
- 6 Amount of NVRAM
- 1 IOS version

CLI Configuration and Addressing

The basic addressing and configuration of Cisco devices were covered in a previous course. However, we will spend some time reviewing these topics as well as prepare you for the hands-on lab experience in this course.

Implementing Basic Addressing Schemes Exercise

When designing a new network or mapping an existing network, it is important to document the network. At a minimum, the documentation should include a topology map of the network and an addressing table that lists the following information:

- Device names
- Interface
- IP address and subnet mask
- Default gateway address for end devices such as PCs

Refer to the topology shown in Figure 1-5 and Table 1-1 that follows it. Using the following guidelines, fill in the addressing table with the correct information:

- The routers use the first address in each network for the LANs.
- R1 uses the first address and R2 uses the second address for the WAN.
- The PCs use the tenth address.

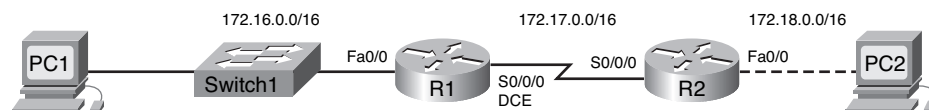
Figure 1-5 Chapter 1 Study Guide Topology

Table 1-1 Addressing Table for Chapter 1 Topology

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.16.0.1	255.255.0.0	—
	S0/0/0	172.17.0.1	255.255.0.0	—
R2	Fa0/0	172.18.0.1	255.255.0.0	—
	S0/0/0	172.17.0.2	255.255.0.0	—
PC1	NIC	172.16.0.10	255.255.0.0	172.16.0.1
PC2	NIC	172.18.0.10	255.255.0.0	172.18.0.1

Basic Router Configuration Exercise

When configuring a router, there are certain basic tasks that are performed, including

- Naming the router
- Setting passwords
- Configuring interfaces
- Configuring a banner
- Saving changes on a router
- Verifying basic configuration and router operations

The first prompt is at **user** mode and will allow you to view the state of the router. What major limitation does this mode have?

User mode will not allow you to modify the router configuration.

What is the router prompt for this mode?

Router>

The **enable** command is used to enter the **privileged** mode. What is the major difference between this mode and the previous mode?

Privileged mode allows the user to make configuration changes on the router.

What is the router prompt for this mode?

Router#

Basic Configuration Tasks

Table 1-2 lists the basic router configuration tasks in the left column. Fill in the right column with the correct command syntax for each of the tasks.

Table 1-2 Basic Router Configuration Command Syntax

Configuration Task	Command Syntax
Naming the router	Router(config)# hostname name
Setting passwords	Router(config)# enable secret password
	Router(config)# line console 0
	Router(config-line)# password password
	Router(config-line)# login
	Router(config)# line vty 0 4
	Router(config-line)# password password
	Router(config-line)# login
Configuring a message-of-the-day banner	Router(config)# banner motd # message #
Configuring an interface	Router(config)# interface type number
	Router(config-if)# ip address address mask
	Router(config-if)# description description
	Router(config-if)# no shutdown
Saving changes on a router	Router# copy running-config startup-config
Examining the output of show commands	Router# show running-config
	Router# show ip route
	Router# show ip interface brief
	Router# show interfaces

Applying a Basic Configuration

The following exercise will walk you through a basic configuration.

First, enter global configuration mode.

```
Router# config t
```

Next, apply a unique host name to the router. Use R1 for this example.

```
Router(config)# hostname R1
```

Now, configure the password that is to be used to enter privileged EXEC mode. Use class as the password.

```
Router(config)# enable secret class
```

Next, configure the console and Telnet lines with the password cisco. The console commands follow:

```
R1(config)# line console 0
```

```
R1(config-line)# password cisco
```

```
R1(config-line)# login
```

The Telnet lines use similar commands:

```
R1(config)# line vty 0 4
```

```
R1(config-line)# password cisco
```

```
R1(config-line)# login
```

From global configuration mode, configure the message-of-the-day banner. Use the following text: **Authorized Access Only**. A delimiting character, such as a #, is used at the beginning and at the end of the message.

```
R1(config)# banner motd # Authorized Access Only #
```

What is the purpose of the message of the day?

At a minimum, a banner should warn against unauthorized access. Never configure a banner that “welcomes” an unauthorized user.

Refer to Figure 1-5 for the correct interface designations. What is the command to enter interface configuration mode for R1’s serial interface?

```
R1(config)# interface Serial10/0/0
```

Enter the command to configure the IP address using the address you specified in Table 1-1.

```
R1(config-if)# ip address 172.17.0.1 255.255.255.0
```

Describe the interface with the following text: **Link to R2**.

```
R1(config-if)# description Link to R2
```

Because R1 is on the data communications equipment (DCE) side, set the clocking signal to **64000**.

```
R1(config-if)# clock rate 64000
```

Activate the interface.

```
Router(config-if)# no shutdown
```

Now enter the commands to configure and activate the Fast Ethernet interface on R1. Use the following description text: **R1 LAN**.

```
R1(config)# interface FastEthernet0/0
```

```
R1(config-if)# ip address 172.16.0.1 255.255.255.0
```

```
R1(config-if)# description R1 LAN
```

```
R1(config-if)# no shutdown
```

What command will save the current configuration?

```
Router# copy running-config startup-config
```

Verifying Basic Router Configuration

Basic configurations can be verified using four basic **show** commands. In Table 1-3, list the command in the left column that fits the description in the right column.

Table 1-3 Basic Router Configuration Verification Commands

Command	Description
show running-config	Displays the current running configuration that is stored in RAM
show startup-config	Displays the startup configuration file stored in NVRAM
show ip route	Displays the routing table that the IOS is currently using to choose the best path to its destination networks

Command	Description
show interfaces	Displays all the interface configuration parameters and statistics
show ip interface brief	Displays abbreviated interface configuration information, including IP address and interface status

Packet Tracer
 Activity

Packet Tracer Exercise 1-1: Basic Router Configuration

Now you are ready to use Packet Tracer to apply your documented addressing scheme. Open file LSG02-0101.pka on the CD-ROM that accompanies this book to perform this exercise using Packet Tracer.

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

Learning Objectives

- Add Devices and Connect Cables
- Configure PCs
- Configure R1
- Configure R2
- Save the Packet Tracer file

Scenario

In this exercise, you will practice configuring the Chapter 1 Study Guide Topology (Figure 1-1). Use the Addressing Table (Table 1-1) you completed in the section “Implementing Basic Addressing Schemes Exercise.”

Task 1: Add Devices and Connect Cables

- Step 1.** Add two PCs: PC1 and PC2. Make sure that you name both PCs. Attach PC1 to S1 and PC2 to R2.
- Step 2.** Connect the devices. Attach R1 to S1. Attach R1 to R2. Make sure that R1 is the DCE side of the connection.
- Step 3.** Your completion percentage should be 11%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure PCs

- Step 1.** Configure PC1 and PC2 according to the addressing table you filled out in the section “Implementing Basic Addressing Schemes Exercise.” If you have not completed that exercise, do so now.
- Step 2.** Check results. Both PCs should now be configured. Your completion percentage should be 21%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure R1

- Step 1.** Configure the host name, banner, enable secret password, console and Telnet lines according to the following guidelines:
- To avoid incorrect grading, make sure that all names and text strings are case sensitive, with no spacing before or after the name or text string.
 - Use the host name **R1**.
 - Use the following text for the banner: **Authorized Access Only**.
 - For the secret password, use **class**. (Note: The activity does not grade this configuration.)
 - For the console and Telnet lines, configure login access with the password **cisco**.
 - Your completion percentage should be 46%. If not, click **Check Results** to see which required components are not yet completed.
- Step 2.** Configure the Fast Ethernet interface.
- Use the IP address and subnet mask according to the addressing table in the section “Implementing Basic Addressing Schemes Exercise.”
 - Describe the link as **R1 LAN**.
 - Activate the interface.
 - Your completion percentage should be 53%. If not, click **Check Results** to see which required components are not yet completed.
- Step 3.** Configure the serial interface.
- Use the IP address and subnet mask according to the addressing table in the section “Implementing Basic Addressing Schemes Exercise.”
 - Describe the link as **Link to R2**.
 - R1 provides clocking at 64,000 bps.
 - Activate the interface.
 - R1 is now configured. Your completion percentage should be 61%. If not, click **Check Results** to see which required components are not yet completed.
- Step 4.** Save the configuration to R1.

Task 4: Configure R2

- Step 1.** Configure the host name, banner, enable secret password, and console and Telnet lines according to the following guidelines:
- To avoid incorrect grading, make sure that all names and text strings are case sensitive, with no spacing before or after the name or text string.
 - Use the host name **R2**.
 - Use the following text for the banner: **Authorized Access Only**.
 - For the secret password, use **class**. (Note: The activity does not grade this configuration.)

- For the console and Telnet lines, configure login access with the password **cisco**.
- Your completion percentage should be 86%. If not, click **Check Results** to see which required components are not yet completed.

Step 2. Configure the Fast Ethernet interface.

- Use the IP address and subnet mask according to the addressing table in the section “Implementing Basic Addressing Schemes Exercise.”
- Describe the link as **R2 LAN**.
- Activate the interface.
- Your completion percentage should be 93%. If not, click **Check Results** to see which required components are not yet completed.

Step 3. Configure the serial interface.

- Use the IP address and subnet mask according to the addressing table in the section “Implementing Basic Addressing Schemes Exercise.”
- Describe the link as **Link to R1**.
- Activate the interface.
- R1 is now configured. Your completion percentage should be 100%. All the connectivity tests should show a status of “successful.” If not, click **Check Results** to see which required components are not yet completed.

Step 4. Save the configuration to R2.

Task 5: Save the Packet Tracer File

Save your Packet Tracer file as LSG02-0101-end.pka. You will use this file to complete some of the remaining exercises in this chapter.

Building the Routing Table

The primary function of a router is to forward packets toward the destination network, the destination IP address of the packet. To do this, a router needs to search the routing information stored in its routing table. In this section, you will learn how a router builds the routing table. Then, you will learn the three basic routing principles.

Vocabulary Exercise: Completion

Complete the paragraphs that follow by filling in appropriate words and phrases.

Introducing the Routing Table

A routing table is a data file stored in **RAM** that is used to store route information about directly connected and remote networks.

There are two major types of routes in the routing table:

- A **directly connected** network: When a router’s interface is configured with an **IP address** and **subnet mask**, the interface becomes a host on that attached network.

- A **remote** network: This is a network that can only be reached by sending the packet to another router. These networks are added to the routing table by using a **dynamic routing protocol** or by configuring **static routes**. **Dynamic** routes are routes to remote networks that were learned automatically by the router. **Static** routes are routes to networks that a network administrator manually configured.

show ip route Command

Describe the meaning of each part of the following route entry:

```
C    172.16.0.0/16 is directly connected, FastEthernet0/0
```

- **C:** The information in this column denotes the source of the route information, directly connected network, static route, or a dynamic routing protocol. The C represents a directly connected route.
- **172.16.0.0/24:** This is the network address and subnet mask of the directly connected or remote network.
- **FastEthernet 0/0:** The information at the end of the route entry represents the exit interface and/or the IP address of the next-hop router. In this example, both FastEthernet 0/0 and Serial 0/0/0 are the exit interfaces used to reach these networks.

Static Routing

When the IOS learns about a remote network and the interface it will use to reach that network, it adds that route to the **routing table**, as long as the **exit interface** is enabled.

Static routes are denoted with the code **S** in the routing table.

List and describe three situations in which static routes should be used.

- **A network consists of only a few routers. Using a dynamic routing protocol in such a case does not present any substantial benefit. On the contrary, dynamic routing can add more administrative overhead.**
- **A network is connected to the Internet only through a single ISP. There is no need to use a dynamic routing protocol across this link because the ISP represents the only exit point to the Internet.**
- **A large network is configured in a hub-and-spoke topology. A hub-and-spoke topology consists of a central location (the hub) and multiple branch locations (spokes), with each spoke having only one connection to the hub. Using a dynamic routing protocol would be unnecessary because each branch only has one path to a given destination—through the central location.**

Dynamic Routing

Dynamic routing protocols are used by routers to share information about the reachability and status of remote networks. Dynamic routing protocols perform several activities, including

- **Network discovery**, which is a routing protocol's ability to share information about the networks it knows about with other routers that are also using the same routing protocol
- **Maintain** routing tables, which is a routing protocol's ability to compensate for any topology changes without involving the network administrator

IP Routing Protocols

List the acronym and full name of the dynamic routing protocols for IP.

- [RIP \(Routing Information Protocol\)](#)
- [IGRP \(Interior Gateway Routing Protocol\)](#)
- [EIGRP \(Enhanced Interior Gateway Routing Protocol\)](#)
- [OSPF \(Open Shortest Path First\)](#)
- [IS-IS \(Intermediate System-to-Intermediate System\)](#)
- [BGP \(Border Gateway Protocol\)](#)

Routing Table Principles Exercise

In your own words, describe the three routing table principles according to Alex Zinin in his book *Cisco IP Routing*.¹

Instructor note: The student should restate the principles. The following answers are examples.

Principle #1: [Each router makes a routing decision solely based on information in its own routing table.](#)

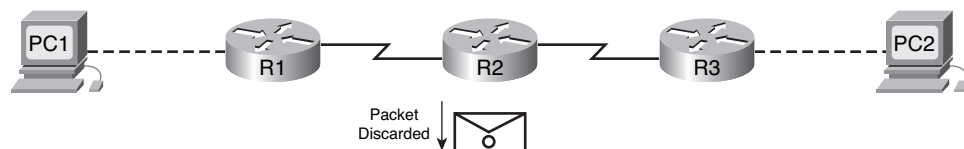
Principle #2: [Just because the local router has a route in its table does not mean that other routers have the same route.](#)

Principle #3: [Even though a router can route to the destination does not mean that the same router can route a response back to the originating source.](#)

Refer to Figure 1-6. R2 received a packet from R1 destined for PC2. R2 did not have a route for the network that PC2 belongs to, so R2 discarded the packet. Which routing principle does this illustrate?

[Routing Principle #2](#)

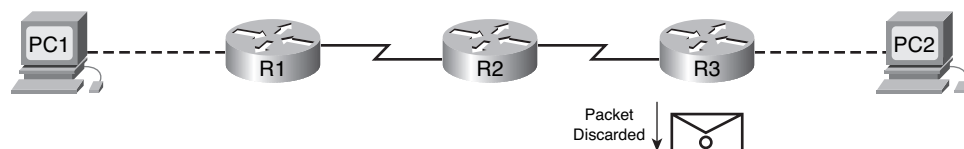
Figure 1-6 Routing Principles: Example 1



Refer to Figure 1-7. R3 received a packet from R2 destined for PC2. R3 sent the packet on to R2. But when R2 sent a response to PC1, R3 discarded the packet. Which routing principle does this illustrate?

[Routing Principle #3](#)

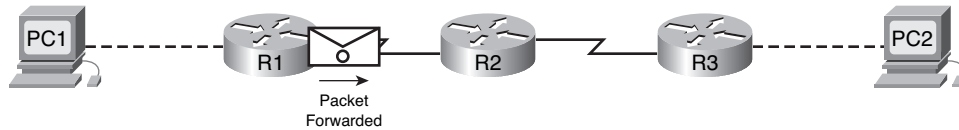
Figure 1-7 Routing Principles: Example 2



Refer to Figure 1-8. R1 received a packet from PC1 destined for PC2. R1 forwarded the packet to R2. Which routing principle does this illustrate?

Routing Principle #1

Figure 1-8 Routing Principles: Example 3



Path Determination and Switching Functions

The following sections use exercises to focus your attention on exactly what happens to data as it moves from source to destination. First, we review the packet and frame field specifications. Then, we discuss in detail how the frame fields change from hop to hop, whereas the packet fields remain unchanged.

Internet Protocol (IP) Packet Format Exercise

Figure 1-9 shows the structure of fields for the packet header. Fill in the missing field names.

Figure 1-9 Field Specification for the IP Header

Byte 1		Byte 2		Byte 3		Byte 4	
Version	IHL	Type of Service		Packet Length			
Identification				Flags	Fragment Offset		
Time to Live		Protocol		Header Checksum			
Source IP Address							
Destination IP Address							
Options						Padding	

MAC Layer Frame Format Exercise

Figure 1-10 shows the two compatible version of Ethernet. Fill in the missing field names.

Figure 1-10 Field Specification for Ethernet Frames

Ethernet						
Field Length in Bytes						
8	6	6	2	46-1500	4	
Preamble	Destination Address	Source Address	Type	Data	FCS	

IEEE 802.3						
Field Length in Bytes						
7	1	6	6	2	46-1500	4
Preamble	S O F	Destination Address	Source Address	Length	802.2 Header and Data	FCS

Best Path and Metrics: Completion and Short Answer Exercise

Complete the paragraphs that follow by filling in appropriate words and phrases.

Best Path

The best path is selected by a routing protocol based on the value or **metric** it uses to determine the distance to reach a network. Some routing protocols, such as RIP, use simple **hop count**, which is simply the number of routers between a router and the destination network. Other routing protocols, such as OSPF, determine the shortest path by examining the **bandwidth** of the links.

A **metric** is the quantitative value used to measure the distance to a given route. The best path to a network is the path with the **lowest metric**.

The primary objective of the routing protocol is to determine the **best paths** for each route to include in the routing table. The routing **algorithm** generates a value, a **metric** for each path through the network. The smaller the value of the **metric**, the better the path.

Provide a short answer for the following questions.

Comparing Hop Count and Bandwidth

When hop count is used as the metric, the resulting path can sometimes be suboptimal. Explain why this might happen.

Answers can vary but should include the following concept: Hop count does not consider the bandwidth or speed on the links between source and destination, nor does it consider the current load on a link. Hop count will choose a path that only has two hops as opposed to a path that has three hops—even though the three-hop path might be faster.

Equal-Cost Load Balancing

What happens if a routing table has two or more paths with the same metric to the same destination network?

The router will perform equal-cost load balancing using both paths (or multiple paths) to route to the same destination. The routing table will contain the single destination network but will have multiple exit interfaces, one for each equal-cost path.

Path Determination and Switching Function Exercise

Can you describe the exact details of what happens to a packet at Layer 2 and Layer 3 as it travels from source to destination? Use the topology and Figure 1-11, the addressing table in Table 1-4, and the routing tables in Example 1-1 to fill in the blanks in the steps that follow.

Figure 1-11 Path Determination and Switching Function Topology

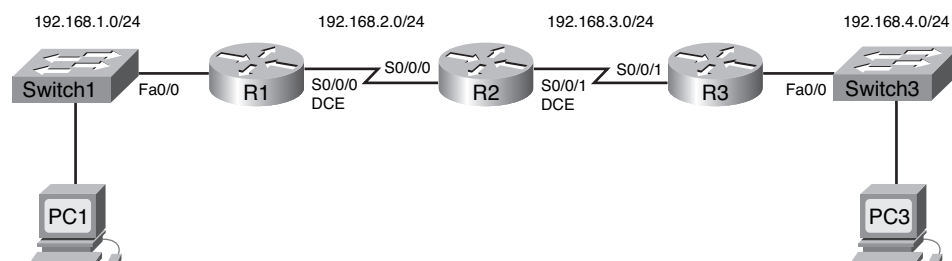


Table 1-4 Addressing Table for Figure 1-11

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	—
	S0/0/0	192.168.2.1	255.255.255.0	—
R2	S0/0/0	192.168.2.2	255.255.255.0	—
	S0/0/1	192.168.3.1	255.255.255.0	—
R3	S0/0/1	192.168.3.2	255.255.255.0	—
	Fa0/0	192.168.4.1	255.255.255.0	—
PC1	NIC	192.168.1.10	255.255.255.0	192.168.1.1
PC3	NIC	192.168.4.10	255.255.255.0	192.168.4.1

Example 1-1 Routing Tables for Figure 1-11

```
R1# show ip route
```

```
<output omitted>
```

```
Gateway of last resort is not set
```

```
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

```
C    192.168.2.0/24 is directly connected, Serial0/0/0
```

```
R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:04, Serial0/0/0
```

```
R    192.168.4.0/24 [120/2] via 192.168.2.2, 00:00:04, Serial0/0/0
```

```
R2# show ip route
```

```
<output omitted>
```

```
Gateway of last resort is not set
```

```
R    192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:06, Serial0/0/0
```

```
C    192.168.2.0/24 is directly connected, Serial0/0/0
```

```
C    192.168.3.0/24 is directly connected, Serial0/0/1
```

```
R    192.168.4.0/24 [120/1] via 192.168.3.2, 00:00:06, Serial0/0/1
```

```
R3# show ip route
```

```
<output omitted>
```

```
Gateway of last resort is not set
```

```
R    192.168.1.0/24 [120/2] via 192.168.3.1, 00:00:07, Serial0/0/1
```

```
R    192.168.2.0/24 [120/1] via 192.168.3.1, 00:00:07, Serial0/0/1
```

```
C    192.168.3.0/24 is directly connected, Serial0/0/1
```

```
C    192.168.4.0/24 is directly connected, FastEthernet0/0
```

1. The Internet Control Message Protocol (ICMP) process on PC1 formulates a ping request to PC3 and sends the reply to the IP process.
2. The IP process on PC1 encapsulates the ping packet with a source IP address of [192.168.1.10](#) and destination IP address of [192.168.4.10](#).
3. PC1 then frames the packet with the source MAC address of (indicate device name) [PC1](#) and the destination MAC address of (indicate device name) [R1](#).
4. Next, PC1 sends the frame out on the media as an encoded stream of [bits](#).
5. R1 receives the bit stream on its [FastEthernet 0/0](#) interface. Because the destination MAC address matches the receiving interface's MAC address, R1 strips off the Ethernet header.
6. R1 looks up the destination network address [192.168.4.0/24](#) in its routing table. This destination has a next-hop IP address of [192.168.2.2](#). The next-hop IP address is reachable out interface [Serial 0/0/0](#).
7. R1 encapsulates the packet in a High-Level Data Link Control (HDLC) frame and forwards the frame out the correct interface. (Because this is a point-to-point link, no address is needed. However, the address field in the HDLC packet contains the value 0x8F.)
8. R2 receives the frame on the [Serial 0/0/0](#) interface. Because the frame is HDLC, R2 strips off the header and looks up the network address [192.168.4.0/24](#) in its routing table. This destination has a next-hop IP address of [192.168.3.2](#). The next-hop IP address is reachable out interface [Serial 0/0/1](#).
9. R2 encapsulates the packet in an HDLC frame and forwards the frame out the correct interface.
10. R3 receives the frame on the [Serial 0/0/1](#) interface. R3 strips off the header and looks up the network address [192.168.4.0/24](#) in its routing table. This destination address is directly connected to the [FastEthernet 0/0](#) interface.
11. R3 encapsulates the ping request in a frame with the source MAC address of (indicated device name) [R3](#) and the destination MAC address of (indicate device name) [PC3](#).
12. R3 then sends the frame out on the media as an encoded bit stream.
13. PC3 receives the bit stream on its [Fast Ethernet](#) interface. Because the destination MAC address matches the MAC address of PC3, PC3 strips off the Ethernet header.
14. The IP process on PC3 examines the [192.168.4.10](#) IP address to make sure that it matches its own IP address. Then PC3 passes the data to the ICMP process.
15. The ICMP process on PC3 formulates a ping reply to PC1 and sends the reply to the IP process.
16. The IP process on PC3 encapsulates the ping packet with a source IP address of [192.168.4.10](#) and destination IP address of [192.168.1.10](#).
17. PC3 then frames the packet with the source MAC address of (indicate device name) [PC3](#) and the destination MAC address of (indicate device name) [R3](#).
18. PC3 then sends the frame out on the media as an encoded bit stream.
19. R3 receives the bit stream on its [FastEthernet 0/0](#) interface. Because the destination MAC address matches the receiving interface's MAC address, R3 strips off the Ethernet header.
20. R3 looks up the destination network address [192.168.1.0/24](#) in its routing table. This destination has a next-hop IP address of [192.168.3.1](#). The next-hop IP address is reachable out interface [Serial 0/0/1](#).

21. R3 encapsulates the packet in an HDLC frame and forwards the frame out the correct interface.
22. R2 receives the frame on the [Serial 0/0/1](#) interface. R2 strips off the header and looks up the network address [192.168.1.0/24](#) in its routing table. This destination has a next-hop IP address of [192.168.2.1](#). The next-hop IP address is reachable out interface [Serial 0/0/0](#).
23. R2 encapsulates the packet in an HDLC frame and forwards the frame out the correct interface.
24. R1 receives the frame on the [Serial 0/0/0](#) interface. R1 strips off the header and looks up the destination network address [192.168.1.0/24](#) in its routing table. This destination address is directly connected to the [FastEthernet 0/0](#) interface.
25. R1 encapsulates the ping request in a frame with the source MAC address of (indicated device name) [R1](#) and the destination MAC address of (indicate device name) [PC1](#).
26. R1 then sends the frame out on the media as an encoded bit stream.
27. PC1 receives the bit stream on its [Ethernet \(NIC\)](#) interface. Because the destination MAC address matches the MAC address of PC1, PC1 strips off the Ethernet header.
28. The IP process on PC1 examines the [192.168.1.10](#) IP address to make sure that it matches its own IP address. Then PC1 passes the data to the ICMP process.
29. ICMP sends a “success” message to the requesting application.

Labs and Activities

Command Reference

In Table 1-5, record the command, *including the correct router prompt*, that fits the description. Fill in any blanks with the appropriate missing information.

Table 1-5 Commands for Basic Router Configuration

Command	Description
Router# configure terminal	Moves into global configuration mode
Router(config)# hostname CISCO	Names the router with the name CISCO ; name can be anything you want
Router(config)# enable secret class	Sets the enable password to class and encrypts it
Router(config)# banner motd #Authorized Access Only#	Configures a message-of-the-day banner that uses # as the delimiting character and displays the following when users attempt to log in: Authorized Access Only
Router(config)# line console 0	Enters console line configuration mode
Router(config-line)# password cisco	Sets the console password to cisco
Router(config-line)# login	Enables password checking when users log in
Router(config)# line vty 0 4	Enters vty line configuration mode for five vty lines
Router(config)# interface fa 0/0	Enters interface configuration mode for Fa0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0	Sets an interface address as 192.168.1.1/24
Router(config-if)# description Link to ISP	Configures an interface with the text Link to ISP , which is used to describe the purpose of the link
Router(config-if)# clock rate 64000	Configures the DCE side of the link to clock bits at 64,000 bps
Router(config-if)# no shutdown	Activates an interface
Router# show interfaces	Displays detailed information and statistics about all interfaces
Router# show ip interface brief	Displays a summary of all interfaces, including status and IP address assigned
Router# show ip route	Displays the routing table
Router# show version	Displays the version of the software currently running on the router

continues

Table 1-5 Commands for Basic Router Configuration *continued*

Command	Description
Router# copy running-config startup-config	Saves the current configuration to NVRAM
Router# show running-config	Displays the current configuration in RAM
Router# show startup-config	Displays the configuration saved in NVRAM



Lab 1-1: Cabling a Network and Basic Router Configuration (1.5.1)

Upon completion of this lab, you will be able to

- Cable devices and establish console connections
- Erase and reload the routers
- Perform basic IOS command-line interface operations
- Perform basic router configuration
- Verify and test configurations using **show** commands, ping, and traceroute
- Create a startup configuration file
- Reload a startup configuration file
- Install a terminal emulation program

Scenario

Instructor Note: This lab replaces “Lab 1-2: Basic Router Configuration (1.5.2)” and should be used if the student needs extensive review of prior skills.

In this lab activity, you will review previously learned skills, including cabling devices, establishing a console connection, and executing basic IOS command-line interface operation and configuration commands. You will also learn to save configuration files and capture your configurations to a text file. The skills presented in this lab are essential to completing the rest of the labs in this course. However, you can substitute the shorter version, “Lab 1-2: Basic Router Configuration (1.5.2),” if your instructor determines that you are proficient in the essential skills reviewed in this lab.

Figure 1-12 shows the topology for this lab, and Table 1-6 shows the IP addressing, subnet, and default gateway information for the devices in the topology.

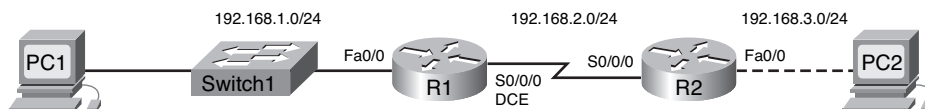
Figure 1-12 Topology Diagram for Lab 1-1

Table 1-6 Addressing Table for Lab 1-1

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	—
	S0/0/0	192.168.2.1	255.255.255.0	—
R2	Fa0/0	192.168.3.1	255.255.255.0	—
	S0/0/0	192.168.2.2	255.255.255.0	—
PC1	NIC	192.168.1.10	255.255.255.0	192.168.1.1
PC2	NIC	192.168.3.10	255.255.255.0	192.168.3.1

Task 1: Cable the Ethernet Links of the Network

Cable the Ethernet links for a network that is similar to the one in the topology diagram. The output used in this lab is from Cisco 1841 routers. However, you can use any current router in your lab as long as it has the required interfaces as shown in the topology. A simple way to identify the available interfaces on a router is by entering the **show ip interface brief** command.

Which of the devices in the topology diagram require an Ethernet cable between them?

[PC1 to S1, S1 to R1, and R2 to PC2](#)

Step 1. Connect the R1 router to the S1 switch.

Use a straight-through Ethernet cable to connect the FastEthernet 0/0 interface of the R1 router to the FastEthernet 0/1 interface on the S1 switch.

What color is the link status light next to the FastEthernet 0/0 interface on R1? [green](#)

What color is the link status light next to the FastEthernet 0/1 interface on S1? [green](#)

Step 2. Connect PC1 to the S1 switch.

Use a straight-through Ethernet cable to connect the NIC of PC1 to the FastEthernet 0/2 interface of the S1 switch.

What color is the link status light next to the NIC interface on PC1? [green](#)

What color is the link status light next to the FastEthernet 0/2 interface on S1? [green](#)

If the link status lights are not green, wait a few moments for the link between the two devices to become established. If the lights do not turn green after a few moments, check that you are using a straight-through Ethernet cable and that the power is on for the S1 switch and PC1.

Step 3. Connect PC2 to the R2 router.

Use a crossover Ethernet cable to connect the FastEthernet 0/0 interface of the R2 router to the NIC of PC2. Because there is no switch between PC2 and the R2 router, a crossover cable is required for a direct link between the PC and the router.

What color is the link status light next to the NIC interface on PC2? [green](#)

What color is the link status light next to the FastEthernet 0/0 interface on R2? [green](#)

Task 2: Cable the Serial Link Between the R1 and R2 Routers

In a real-world WAN connection, the customer premises equipment (CPE), which is often a router, is the data terminal equipment (DTE). This equipment is connected to the service provider through a data communications equipment (DCE) device, which is commonly a modem or channel service unit (CSU)/data service unit (DSU). This device is used to convert the data from the DTE into a form acceptable to the WAN service provider.

Unlike the cables in the academy lab setup, the serial cables in the real world are not connected back to back. In a real-world situation, one router might be in New York, while another router might be in Sydney, Australia. An administrator located in Sydney would have to connect to the router in New York through the WAN cloud to troubleshoot the New York router.

In the academy labs, devices that make up the WAN cloud are simulated by the connection between the back-to-back DTE-DCE cables. The connection from one router serial interface to another router serial interface simulates the entire WAN cloud.

Step 1. Create a null serial cable to connect the R1 router to the R2 router.

In the academy labs, the WAN connection between routers uses one DCE cable and one DTE cable. The DCE-DTE connection between routers is referred to as a null serial cable. The labs will use one V.35 DCE cable and one V.35 DTE cable to simulate the WAN connection. The V.35 DCE connector is usually a female V.35 (34-pin) connector. The DTE cable has a male V.35 connector. The cables are also labeled as DCE or DTE on the router end of the cable.

The DTE and DCE V.35 cables must be joined. Holding one of the V.35 ends in each hand, examine the pins and sockets as well as the threaded connectors. Note that there is only one proper way for the cables to fit together. Align the pins on the male cable with the sockets on the female cable and gently couple them. Very little effort should be required to accomplish this. When they are joined, turn the thumbscrews clockwise and secure the connectors.

Step 2. Connect the DCE end of the null serial cable to the Serial 0/0/0 interface of the R1 router, and the DTE end of the null serial cable to the Serial 0/0/0 interface of the R2 router.

Review the following information before making these connections.

Before making the connection to one of the routers, examine the connector on the router and the cable. Note that the connectors are tapered to help prevent improper connection. Holding the connector in one hand, orient the cable and router connectors so that the tapers match. Now push the cable connector partially into the router connector. It probably will not go in all the way because the threaded connectors need to be tightened for the cable to be inserted completely. While holding the cable in one hand and gently pushing the cable toward the router, turn one of the thumbscrews clockwise, 3 or 4 rounds, to start the screws. Now turn the other thumbscrew clockwise, 3 or 4 rounds, to get it started. At this point, the cable should be attached sufficiently to free both hands to advance each thumbscrew at the same rate until the cable is fully inserted. Do not overtighten these connectors.

Task 3: Establish a Console Connection to the R1 Router

The console port is a management port used to provide out-of-band access to a router. It is used to set up the initial configuration of a router and to monitor it.

A rollover cable and an RJ-45-to-DB-9 adapter are used to connect a PC to the console port. As you know from your previous studies, terminal emulation software is used to configure the router over the console connection. The Cisco Networking Academy Program recommends using Tera Term. However, you can also use HyperTerminal, which is part of the Windows operating system.

At the end of this lab, the following three appendices are available for your reference concerning these two terminal emulation programs:

- Appendix 1A: Installing and Configuring Tera Term for Use in Windows XP
- Appendix 1B: Configuring Tera Term as the Default Telnet Client in Windows XP
- Appendix 1C: Accessing and Configuring HyperTerminal

Step 1. Examine the router and locate the RJ-45 connector labeled Console.

Step 2. Examine PC1 and locate a 9-pin male connector serial port.
It might—or might not—be labeled as COM1 or COM2.

Step 3. Locate the console cable.

Some console cables have an RJ-45-to-DB-9 adapter built into one end. Others do not. Locate either a console cable with a built-in adapter or a console cable with a separate RJ-45-to-DB-9 adapter attached to one end.

Step 4. Connect the console cable to the router and PC.

First, connect the console cable to the router console port, an RJ-45 connector. Next, connect the DB-9 end of the console cable to the serial port of PC1.

Step 5. Test router connection:

- a. Open your terminal emulation software (HyperTerminal, Tera Term, or other software specified by your instructor).
- b. Configure the software parameters specific to your applications (see the appendices for help).
- c. When the terminal window is open, press **Enter**. There should be a response from the router. If there is, the connection has been successfully completed. If there is no connection, troubleshoot as necessary. For example, verify that the router has power. Check the connection to the serial port on the PC and the console port on the router.

Task 4: Erase and Reload the Routers

Step 1. Using the HyperTerminal session established in Task 3, enter privileged EXEC mode on R1.

```
Router> enable
Router#
```

Step 2. Erase the configuration.

To clear the configuration, issue the **erase startup-config** command. Press **Enter** when prompted to [**confirm**] that you really do want to erase the configuration currently stored in NVRAM. The result should look something like this:

```
Router# erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

Step 3. Reload the configuration.

When the prompt returns, issue the **reload** command. Answer **no** if asked to save changes. After the router finishes the boot process, choose not to use the AutoInstall facility, as shown:

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Would you like to terminate autoinstall? [yes]:
Press Enter to accept default.
Press RETURN to get started!
```

Step 4. Establish a HyperTerminal session to R2.

Repeat Steps 1 through 3 to remove any startup configuration files that might be present.

Task 5: Understand Command-Line Basics

Step 1. Establish a HyperTerminal session to router R1.

Step 2. Enter privileged EXEC mode.

```
Router> enable
Router#
```

Step 3. Enter an incorrect command and observe the router response.

```
Router# configure terminal
      ^
% Invalid input detected at '^' marker.

Router#
```

Command-line errors occur primarily from typing mistakes. If a command keyword is incorrectly typed, the user interface uses the caret symbol (^) to identify and isolate the error. The ^ appears at or near the point in the command string where an incorrect command, keyword, or argument was entered.

Step 4. Correct the previous command.

If a command is entered incorrectly, and the **Enter** key is pressed, the **Up Arrow** key can be pressed to repeat the last command. Use the **Right Arrow** and **Left Arrow** keys to move the cursor to the location where the mistake was made. Then make the correction. If something needs to be deleted, use the **Backspace** key. Use the directional keys and the **Backspace** key to correct the command to **configure terminal**, and then press **Enter**:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Step 5. Return to privileged EXEC mode with the **exit** command.

```
Router(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
Router#
```

Step 6. Examine the commands that are available for privileged EXEC mode.

A question mark (?) can be entered at the prompt to display a list of available commands:

```
Router# ?
Exec commands:
 <1-99>      Session number to resume
 clear       Reset functions
 clock       Manage the system clock
 configure   Enter configuration mode
 connect     Open a terminal connection
 copy        Copy from one file to another
 debug       Debugging functions (see also 'undebug')
 delete      Delete a file
 dir         List files on a filesystem
 disable     Turn off privileged commands
 disconnect  Disconnect an existing network connection
 enable      Turn on privileged commands
 erase       Erase a filesystem
 exit        Exit from the EXEC
 logout      Exit from the EXEC
 no          Disable debugging informations
 ping        Send echo messages
 reload      Halt and perform a cold restart
 resume      Resume an active network connection
 setup       Run the SETUP command facility
 show        Show running system information
--More--
```

Notice the **--More--** at the bottom of the command output. The **--More--** prompt indicates that there are multiple screens of output. When a **--More--** prompt appears, press the **Spacebar** to view the next available screen. To display only the next line, press **Enter**. Press any other key to return to the prompt.

Step 7. View the output.

View the rest of the command output by pressing the **Spacebar**. The remainder of the output will appear where the **--More--** prompt appeared previously:

```
telnet       Open a telnet connection
traceroute   Trace route to destination
```

undebg	Disable debugging functions (see also 'debug')
vlan	Configure VLAN parameters
write	Write running configuration to memory, network, or terminal

Step 8. Exit privileged EXEC mode with the **exit** command.

```
Router# exit
```

The following output should be displayed:

```
Router con0 is now available
```

Press RETURN to get started.

Step 9. Press **Enter** to enter user EXEC mode.

The Router> prompt should be visible.

Step 10. Type an abbreviated IOS command.

IOS commands can be abbreviated, as long as enough characters are typed for the IOS to recognize the unique command.

Enter only the character **e** at the command prompt and observe the results:

```
Router> e
% Ambiguous command: "e"
Router>
```

Enter **en** at the command prompt and observe the results:

```
Router> en
Router#
```

The abbreviated command **en** contains enough characters for the IOS to distinguish the **enable** command from the **exit** command.

Step 11. Press **Tab** after an abbreviated command to use autocomplete.

Typing an abbreviated command, such as **conf**, followed by the **Tab** key completes a partial command name. This functionality of the IOS is called *autocomplete*. Type the abbreviated command **conf**, press the **Tab** key, and observe the results:

```
Router# conf
Router# configure
```

This autocomplete feature can be used as long as enough characters are typed for the IOS to recognize the unique command.

Step 12. Enter IOS commands in the correct mode.

IOS commands must be entered in the correct mode. For example, configuration changes cannot be made while in privileged EXEC mode. Attempt to enter the command **hostname R1** at the privileged EXEC prompt and observe the results:

```
Router# hostname R1
^
% Invalid input detected at '^' marker.
Router#
```

Task 6: Perform Basic Configuration of Router R1

Step 1. Establish a HyperTerminal session to router R1.

Step 2. Enter privileged EXEC mode.

```
Router> enable
Router#
```

Step 3. Enter global configuration mode.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Step 4. Configure the router name as R1.

Enter the command **hostname R1** at the prompt:

```
Router(config)# hostname R1
R1(config)#
```

Step 5. Disable DNS lookup with the **no ip domain-lookup** command.

```
R1(config)# no ip domain-lookup
R1(config)#
```

Why would you want to disable DNS lookup in a lab environment?

So that the router does not attempt to look up a DNS entry for a name that is really only a typing error.

What would happen if you disabled DNS lookup in a production environment?

A router would not be able to resolve names, causing potential problems when the router needs an IP address to address a packet.

Step 6. Configure an EXEC mode password.

Configure an EXEC mode password using the **enable secret password** command. Use **class** for the *password* argument:

```
R1(config)# enable secret class
R1(config)#
```

The **enable secret** command is used to provide an additional layer of security over the **enable password** command. The **enable secret** command provides better security by storing the **enable secret** password using a nonreversible cryptographic function. The added layer of security encryption is useful in environments where the password crosses the network or is stored on a TFTP server. When both the **enable password** and **enable secret** passwords are configured, the **enable password** is overridden by **enable secret** and therefore has no meaning in the configuration. To avoid confusion, simply avoid using **enable password** when **enable secret** is used.

Step 7. Remove the **enable password**.

Because the **enable secret** is configured, the **enable password** is no longer necessary. IOS commands can be removed from the configuration using the **no** form of the command:

```
R1(config)# no enable password
R1(config)#
```

Step 8. Configure a message-of-the-day banner using the **banner motd** command.

```
R1(config)# banner motd &
Enter TEXT message. End with the character '&'.
*****
!!!AUTHORIZED ACCESS ONLY!!!
*****
&
R1(config)#
```

When does this banner display?

When a user logs in to the router either through Telnet or the console connection.

Why should every router have a message-of-the-day banner?

To provide a warning against intentional or unintentional unauthorized access.

Step 9. Configure the console password on the router.

Use **cisco** as the password. When you are finished, exit from line configuration mode:

```
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
```

Step 10. Configure the password for the virtual terminal lines.

Use **cisco** as the password. When you are finished, exit from line configuration mode:

```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
```

Step 11. Configure the FastEthernet 0/0 interface with the IP address 192.168.1.1/24.

```
R1(config)# interface fastethernet 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
R1(config-if)#
```


Step 12. Use the **description** command to provide a description for this interface.

```
R1(config-if)# description R1 LAN
R1(config-if)#
```

Step 13. Configure the Serial 0/0/0 interface with the IP address 192.168.2.1/24.

Set the clock rate to 64,000.

Note: Because the routers in the labs will not be connected to a live leased line, one of the routers will need to provide the clocking for the circuit. This is normally provided to each of the routers by the service provider. To provide this clocking signal in the lab, one of the routers will need to act as the DCE on the connection. This function is achieved by applying the **clock rate 64,000** command on the Serial 0/0/0 interface, where the DCE end of the null modem cable has been connected. The purpose of the **clock rate** command is discussed further in Chapter 2, “Static Routing.”

```
R1(config-if)# interface serial 0/0/0
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# clock rate 64000
R1(config-if)# no shutdown
R1(config-if)#
```

Note: The interface will not be activated until the serial interface on R2 is configured and activated.

Step 14. Use the **description** command to provide a description for this interface.

```
R1(config-if)# description Link to R2
R1(config-if)#
```

Step 15. Use the **end** command to return to privileged EXEC mode.

```
R1(config-if)# end
R1#
```

Step 16. Save the R1 configuration.

Save the R1 configuration using the **copy running-config startup-config** command:

```
R1# copy running-config startup-config
Building configuration...
[OK]
R1#
```

Task 7: Perform Basic Configuration of Router R2

Step 1. For R2, repeat Steps 1 through 10 from Task 6.

Step 2. Configure the Serial 0/0/0 interface with the IP address 192.168.2.2/24.

```
R2(config)# interface serial 0/0/0
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# no shutdown
```

```
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
R2(config-if)#
```

Step 3. Use the **description** command to provide a description for this interface.

```
R1(config-if)# description Link to R1  
R1(config-if)#
```

Step 4. Configure the FastEthernet 0/0 interface with the IP address 192.168.3.1/24.

```
R2(config-if)# interface fastethernet 0/0  
R2(config-if)# ip address 192.168.3.1 255.255.255.0  
R2(config-if)# no shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed  
state to up  
R2(config-if)#
```

Step 5. Use the **description** command to provide a description for this interface.

```
R1(config-if)# description R2 LAN  
R1(config-if)#
```

Step 6. Use the **end** command to return to privileged EXEC mode.

```
R2(config-if)# end  
R2#
```

Step 7. Save the R2 configuration.

Save the R2 configuration using the **copy running-config startup-config** command:

```
R2# copy running-config startup-config  
Building configuration...  
[OK]  
R2#
```

Task 8: Configure IP Addressing on the Host PCs

Step 1. Configure the host PC1.

Configure the host PC1 that is attached to R1 with an IP address of 192.168.1.10/24 and a default gateway of 192.168.1.1.

Step 2. Configure the host PC2.

Configure the host PC2 that is attached to R2 with an IP address of 192.168.3.10/24 and a default gateway of 192.168.3.1.

Task 9: Examine Router show Commands

There are many **show** commands that you can use to examine the operation of the router. In both privileged EXEC and user EXEC modes, the command **show ?** provides a list of available **show** commands. The list is considerably longer in privileged EXEC mode than it is in user EXEC mode.

Step 1. Examine the **show running-config** command.

The **show running-config** command is used to display the contents of the currently running configuration file. From privileged EXEC mode on the R1 router, examine the output of the **show running-config** command. If the **--More--** prompt appears, press the **Spacebar** to view the remainder of the command output:

```
R1# show running-config
!
version 12.3
!
hostname R1
!
!
enable secret 5 $1$AFDd$0HCi0iYHkEWR4cegQdTQu/
!
no ip domain-lookup
!
interface FastEthernet0/0
  description R1 LAN
  mac-address 0007.eca7.1511
  ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/1
  mac-address 0001.42dd.a220
  no ip address
  duplex auto
  speed auto
  shutdown
!
interface Serial0/0/0
  description Link to R2
  ip address 192.168.2.1 255.255.255.0
  clock rate 64000
!
interface Serial0/0/1
  no ip address
```

```
shutdown
!  
interface Vlan1  
no ip address  
shutdown  
!  
ip classless  
!  
!  
!  
!  
line con 0  
password cisco  
login  
line vty 0 4  
password cisco  
login  
!  
end
```

Step 2. Examine the **show startup-config** command.

The **show startup-config** command displays the startup configuration file contained in NVRAM. From privileged EXEC mode on the R1 router, examine the output of the **show startup-config** command. If the **--More--** prompt appears, press the **Spacebar** to view the remainder of the command output:

```
R1# show startup-config  
Using 583 bytes  
!  
version 12.3  
!  
hostname R1  
!  
!  
no ip domain-lookup  
!  
interface FastEthernet0/0  
description R1 LAN  
mac-address 0007.eca7.1511  
ip address 192.168.1.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
mac-address 0001.42dd.a220  
no ip address  
duplex auto  
speed auto  
shutdown
```

```

!
interface Serial0/0/0
description Link to R2
 ip address 192.168.2.1 255.255.255.0
 clock rate 64000
!
interface Serial0/0/1
no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
!
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end

```

Step 3. Examine the **show interfaces** command.

The **show interfaces** command displays statistics for all interfaces configured on the router. A specific interface can be added to the end of this command to display the statistics for only that interface. From privileged EXEC mode on the R1 router, examine the output of the **show interfaces fastEthernet0/0** command. If the **--More--** prompt appears, press the **Spacebar** to view the remainder of the command output:

```

R1# show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0007.eca7.1511 (bia 0002.1625.1bea)
  Description: R1 LAN
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec

```

```
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
R1#
```

Step 4. Examine the **show version** command.

The **show version** command displays information about the currently loaded software version along with hardware and device information. From privileged EXEC mode on the R1 router, examine the output of the **show version** command. If the **--More--** prompt appears, press the **Spacebar** to view the remainder of the command output:

```
R1# show version
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.3(14)T7,
  RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 15-May-06 14:54 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-ipbase-mz.123-14.T7.bin"
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E

```

M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
191K bytes of NVRAM.
31360K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102

```

```
R1#
```

Step 5. Examine the **show ip interface brief** command.

The **show ip interface brief** command displays a summary of the usability status information for each interface. From privileged EXEC mode on the R1 router, examine the output of the **show ip interface brief** command.

```

R1# show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.1.1	YES	manual	up	up
FastEthernet0/1	unassigned	YES	manual	administratively down	down
Serial0/0/0	192.168.2.1	YES	manual	up	up
Serial0/0/1	unassigned	YES	manual	administratively down	down
Vlan1	unassigned	YES	manual	administratively down	down

Task 10: Use the ping Command

The **ping** command is a useful tool for troubleshooting Layers 1 through 3 of the OSI model and diagnosing basic network connectivity. This operation can be performed at either the user or privileged EXEC modes. Using **ping** sends an ICMP packet to the specified device and then waits for a reply. Pings can be sent from a router or a host PC.

Step 1. Use the **ping** command to test connectivity between the R1 router and PC1.

```
R1# ping 192.168.1.10
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
```

```
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 72/79/91 ms
```

Each exclamation point (!) indicates a successful echo. Each period (.) on the display indicates that the application on the router timed out while it waited for a packet echo from a target. The first ping packet failed because the router did not have an ARP table entry for the destination address of the IP packet. Because there is no ARP table entry, the packet is dropped. The router then sends an ARP request, receives a response, and adds the MAC address to the ARP table. When the next ping packet arrives, it will be forwarded and be successful.

Step 2. Repeat the **ping** command from R1 to PC1.

```
R1# ping 192.168.1.10
```

Type escape sequence to abort.

```
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/83/93 ms
```

```
R1#
```

All the pings are successful this time because the router has an entry for the destination IP address in the ARP table.

Step 3. Send an extended ping from R1 to PC1.

To accomplish this, type **ping** at the privileged EXEC prompt and press **Enter**. Fill out the rest of the prompts as shown:

```
R1# ping
```

```
Protocol [ip]:
```

```
Target IP address: 192.168.1.10
```

```
Repeat count [5]: 10
```

```
Datagram size [100]:
```

```
Timeout in seconds [2]:
```

```
Extended commands [n]:
```

```
Sweep range of sizes [n]:
```

Type escape sequence to abort.

```
Sending 10, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
```

```
!!!!!!!!!!!!
```

```
Success rate is 100 percent (10/10), round-trip min/avg/max = 53/77/94 ms
```

```
R1#
```

Step 4. Send a ping from PC1 to R1.

In Windows, choose **Start > Programs > Accessories > Command Prompt**. In the Command Prompt window that opens, ping R1 by issuing the following command:

```
C:\> ping 192.168.1.1
```

The ping should respond with successful results.

Step 5. Send an extended ping from PC1 to R1.

To accomplish this, enter the following command at the Windows command prompt:

```
C:\> ping 192.168.1.1 -n 10
```

There should be ten successful responses from the command.

Task 11: Use the traceroute Command

The **traceroute** command is an excellent utility for troubleshooting the path that a packet takes through an internetwork of routers. It can help to isolate problem links and routers along the way. The **traceroute** command uses ICMP packets and the error message generated by routers when the packet

exceeds its Time to Live (TTL). This operation can be performed at either the user or privileged EXEC modes. The Windows version of this command is **tracert**.

Step 1. Use the **traceroute** command at the R1 privileged EXEC prompt to discover the path that a packet will take from the R1 router to PC1.

```
R1# traceroute 192.168.1.10

Type escape sequence to abort.
Tracing the route to 192.168.1.10
  1  192.168.1.10    103 msec  81 msec   70 msec
R1#
```

Step 2. Use the **tracert** command at the Windows command prompt to discover the path that a packet will take from the R1 router to PC1.

```
C:\> tracert 192.168.1.1

Tracing route to 192.168.1.1 over a maximum of 30 hops:

  1  71 ms   70 ms   73 ms   192.168.1.1

Trace complete.

C:\>
```

Task 12: Create a start.txt File

Router configurations can be captured to a text (.txt) file and saved for later use. The configuration can be copied back to the router so that the commands do not have to be entered one at a time.

Step 1. View the running configuration of the router using the **show running-config** command.

```
R1# show running-config

!
version 12.3
!
hostname R1
!
enable secret 5 $1$J.hq$Ds72Qz86tvpcuW2X3FqBS.
!
no ip domain-lookup
!
interface FastEthernet0/0
  description R1 LAN
  mac-address 0007.eca7.1511
  ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/1
```

```
mac-address 0001.42dd.a220
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
description Link to R2
ip address 192.168.2.1 255.255.255.0
clock rate 64000
!
interface Serial0/0/1
no ip address
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
!
!
!
!
line con 0
password cisco
login
line vty 0 4
password cisco
login
!
end

R1#
```

Step 2. Copy the command output.

Select the command output. From the HyperTerminal Edit menu, choose the **Copy** command.

Step 3. Paste the output in Notepad.

Open Notepad. Notepad is typically found on the **Start** menu under **Programs > Accessories**. From the Notepad Edit menu, choose **Paste**.

Step 4. Edit commands.

Some commands will have to be edited or added before the startup script can be applied to a router. Some of these changes are as follows:

- Adding a **no shutdown** command to Fast Ethernet and serial interfaces that are being used
- Replacing the encrypted text in the **enable secret** command with the appropriate password

- Removing the **mac-address** command from the interfaces
- Removing the **ip classless** command
- Removing unused interfaces

Edit the text in the Notepad file as follows:

```
hostname R1
!
!
enable secret class
!
no ip domain-lookup
!
interface FastEthernet0/0
  description R1 LAN
  ip address 192.168.1.1 255.255.255.0
  no shutdown
  duplex auto
  speed auto
!
interface Serial0/0/0
  description Link to R2
  ip address 192.168.2.1 255.255.255.0
  clock rate 64000
  no shutdown
!
!
!
!
line con 0
  password cisco
  login
line vty 0 4
  password cisco
  login
!
end
```

Step 5. Save the open file in Notepad to start.txt.

Task 13: Load the start.txt File onto the R1 Router

Step 1. Erase the current startup configuration of R1.

To clear the configuration, issue the **erase startup-config** command. Press **Enter** when prompted to **[confirm]** that you really do want to erase the configuration currently stored in NVRAM. The result should look something like this:

```
R1# erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

Step 2. When the prompt returns, issue the **reload** command.

Answer **no** if asked to save changes. After the router finishes the boot process, choose not to use the AutoInstall facility, as shown:

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Would you like to terminate autoinstall? [yes]:
Press Enter to accept default.
Press RETURN to get started!
```

Step 3. Enter global configuration mode.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Step 4. Copy the commands.

In the start.txt file that was created in Notepad, select all the lines, and then choose **Edit > Copy**.

Step 5. From the HyperTerminal Edit menu, choose **Paste to Host**.

Step 6. Verify the running configuration.

After all the pasted commands have been applied, use the **show running-config** command to verify that the running configuration appears as expected.

Step 7. Save the running configuration.

Save the running configuration to NVRAM using the **copy running-config startup-config** command:

```
R1# copy running-config startup-config
Building configuration...
[OK]
R1#
```



Packet Tracer Companion

You can now open the file LSG02-Lab151.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity. Use the Lab PDF for more details.

Appendix 1A: Installing and Configuring Tera Term for Use in Windows XP

Tera Term is a free terminal emulation program for Windows. It can be used in the lab environment in place of Windows HyperTerminal. Tera Term can be obtained at the following URL:

<http://hp.vector.co.jp/authors/VA002416/teraterm.html>

Download the ttermp23.zip file, unzip it, and install Tera Term.

Step 1. Open the Tera Terminal program.

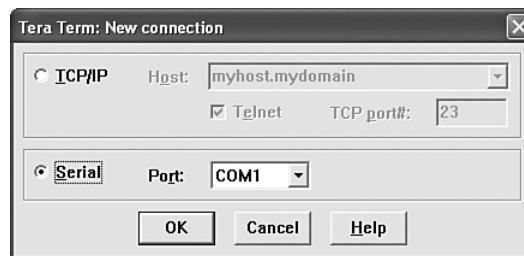
Step 2. Assign the serial port.

To use Tera Term to connect to the router console, open the **New Connection** dialog box and select the **Serial** port.

Step 3. Set serial port parameters.

Set appropriate parameters for **Port** in the **Serial** section of the **Tera Term: New Connection** dialog box, as shown in Figure 1-13. Normally, your connection is through COM1. If you are unsure what port to use, ask your instructor for assistance.

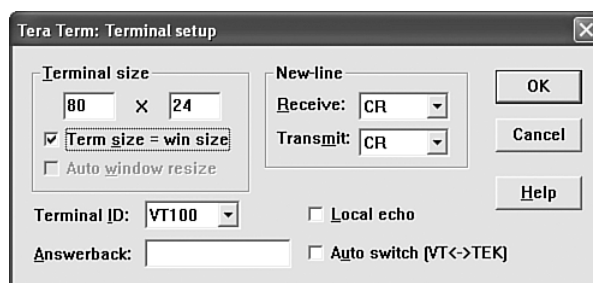
Figure 1-13 Tera Term: New Connection Dialog Box



Step 4. Configure settings.

Tera Term has some settings that can be changed to make it more convenient to use. From the **Setup > Terminal** menu, select the **Term size = win size** check box, as shown in Figure 1-14. This setting allows command output to remain visible when the Tera Term window is resized.

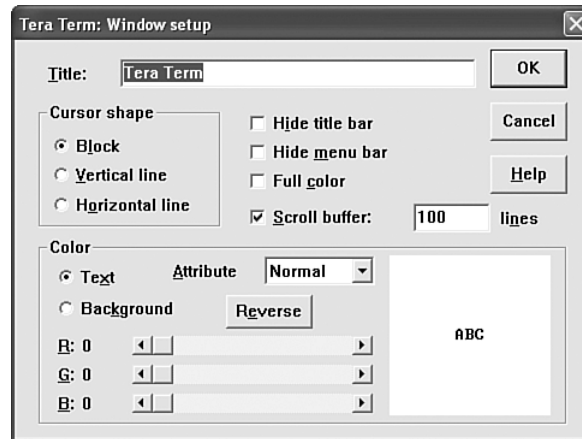
Figure 1-14 Tera Term: Terminal Setup Dialog Box



Step 5. Change scroll buffer number.

From the **Setup > Window** menu, as shown in Figure 1-15, change the scroll buffer number to a number higher than 100. This setting allows you to scroll up and view previous commands and outputs. If there are only 100 lines available in the buffer, only the last 100 lines of output are visible. For example, set the scroll buffer to 1000 lines.

Figure 1-15 Tera Term: Window Setup Dialog Box



Appendix 1B: Configuring Tera Term as the Default Telnet Client in Windows XP

By default, Windows can be set to use HyperTerminal as the Telnet client. Windows can also be set to use the DOS version of Telnet. In the NetLab environment, you can change the Telnet client to **Local Telnet Client**, which means that NetLab will open the current Windows default Telnet client. This can be set to HyperTerminal or to the DOS-like version of Telnet embedded in the Windows operating system.

Complete the following steps to change your default Telnet client to Tera Term (or any other Telnet client):

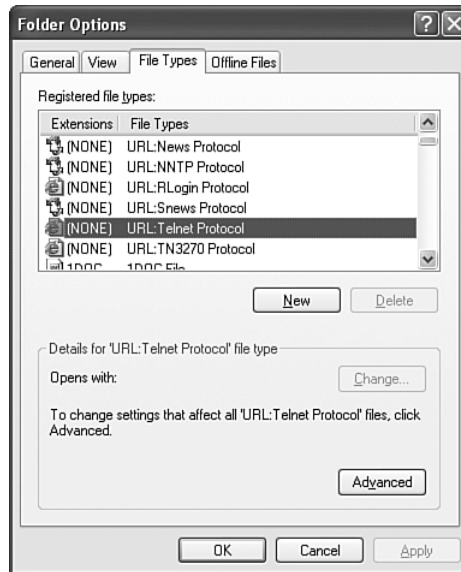
Step 1. Go to Folder Options.

Double-click **My Computer**, and then choose **Tools > Folder Options**.

Step 2. Go to (NONE) URL:Telnet Protocol.

Click the **File Types** tab and scroll down in the list of **Registered file types:** until you find the **(NONE) URL:Telnet Protocol** entry, as shown in Figure 1-16. Select it and then click the **Advanced** button.

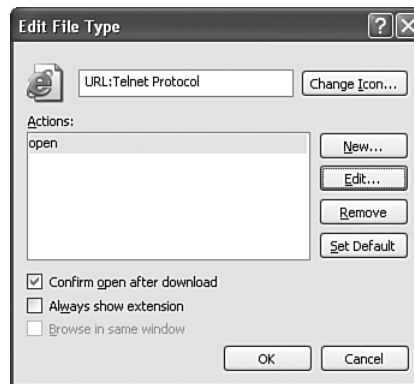
Figure 1-16 Folder Options Dialog Box



Step 3. Edit the open action.

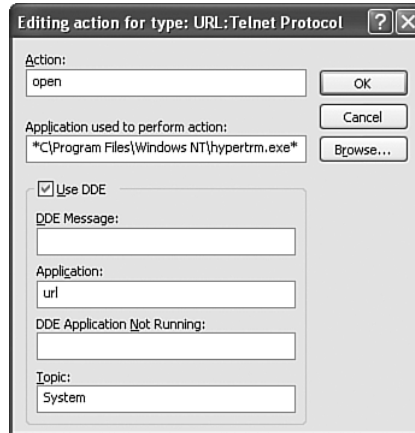
In the **Edit File Type** dialog box, click **Edit** to edit the **open** action, as shown in Figure 1-17.

Figure 1-17 Edit File Type Dialog Box



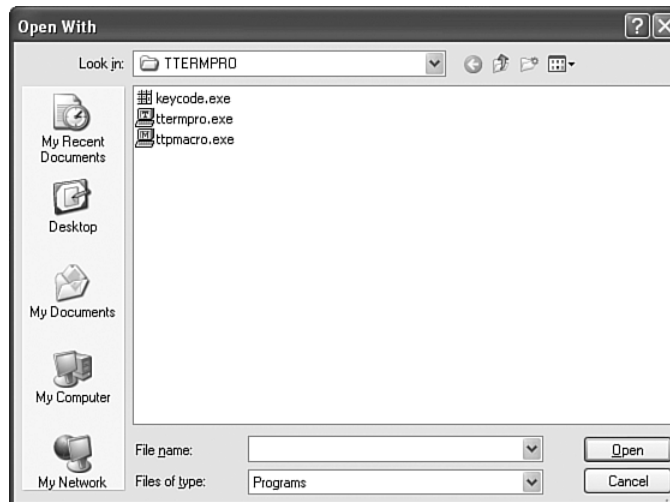
Step 4. Change the application.

In the **Editing action for type: URL: Telnet Protocol** dialog box, the **Application used to perform action** is currently set to HyperTerminal, as shown in Figure 1-18. Click **Browse** to change the application.

Figure 1-18 Editing Action for Type Dialog Box

Step 5. Open ttermpro.exe.

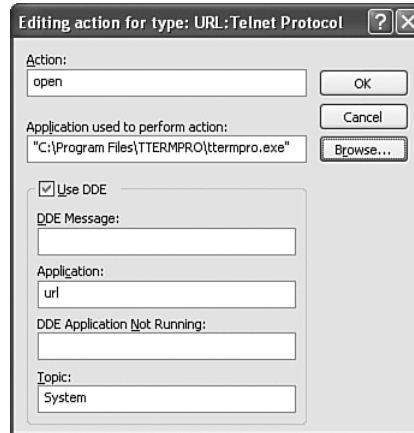
Browse to the Tera Term installation folder shown in Figure 1-19. Click the **ttermpro.exe** file to specify this program for the **open** action, and then click **Open**.

Figure 1-19 Open With Dialog Box

Step 6. Confirm ttermpro.exe and close.

From the window shown in Figure 1-20, click **OK** twice and then **Close** to close the **Folder Options** dialog box. The Windows default Telnet client is now set to Tera Term.

Figure 1-20 Editing Action for Type Dialog Box



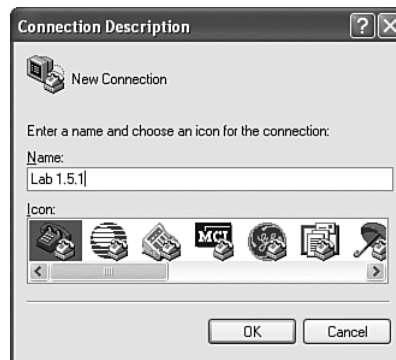
Appendix 1C: Accessing and Configuring HyperTerminal

In most versions of Windows, HyperTerminal can be found by choosing **Start > Programs > Accessories > Communications > HyperTerminal**.

Step 1. Create a new connection.

Open HyperTerminal to create a new connection to the router. Enter an appropriate description in the **Connection Description** dialog box shown in Figure 1-21 and then click **OK**.

Figure 1-21 Connection Description Dialog Box



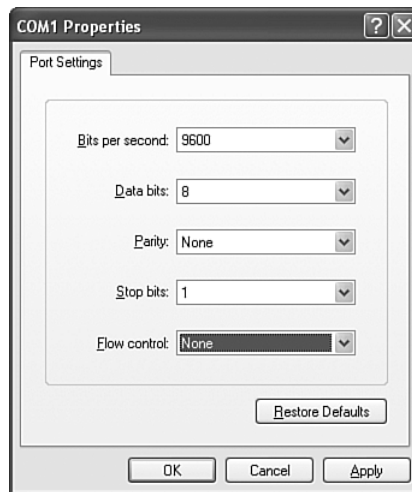
Step 2. Assign COM1 port.

In the **Connect To** dialog box, shown in Figure 1-22, make sure that the correct serial port is selected in the **Connect using** field. Some PCs have more than one COM port. Click **OK**.

Figure 1-22 Connect To Dialog Box

Step 3. Set COM1 properties.

In the **COM1 Properties** dialog box under **Port Setting**, clicking **Restore Defaults** normally sets the correct properties. If not, set the properties to the values shown in Figure 1-23, and then click **OK**.

Figure 1-23 COM1 Properties Dialog Box

Step 4. Verify connection.

You should now have a console connection to the router. Press **Enter** to get a router prompt.



Lab 1-2: Basic Router Configuration (1.5.2)

Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Perform basic configuration tasks on a router
- Configure and activate Ethernet interfaces

- Test and verify configurations
- Reflect upon and document the network implementation

Scenario

Instructor note: Skip this lab if the student is required to complete “Lab 1-1: Cabling a Network and Basic Router Configuration (1.5.1).”

In this lab activity, you will create a network that is similar to the one shown in the topology diagram in Figure 1-24. Begin by cabling the network as shown in Figure 1-24. You will then perform the initial router configurations required for connectivity. Use the IP addresses that are provided in the topology diagram to apply an addressing scheme to the network devices. When the network configuration is complete, examine the routing tables to verify that the network is operating properly. This lab is a shorter version of “Lab 1-1: Cabling a Network and Basic Router Configuration (1.5.1)” and assumes that you are proficient in basic cabling and configuration file management.

Table 1-7 shows the IP addressing, subnet, and default gateway information for the devices in the topology.

Figure 1-24 Topology Diagram for Lab 1-2

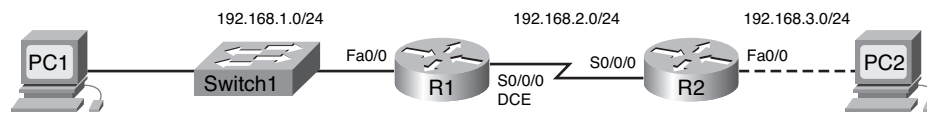


Table 1-7 Addressing Table for Lab 1-2

Device	Interface	IP Address	Subnet Mask	Def. Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	—
	S0/0/0	192.168.2.1	255.255.255.0	—
R2	Fa0/0	192.168.3.1	255.255.255.0	—
	S0/0/0	192.168.2.2	255.255.255.0	—
PC1	N/A	192.168.1.10	255.255.255.0	192.168.1.1
PC2	N/A	192.168.3.10	255.255.255.0	192.168.3.1

Task 1: Cable the Network

Cable a network that is similar to the one in Figure 1-24. The output used in this lab is from Cisco 1841 routers. You can use any current router in your lab as long as it has the required interfaces as shown in the topology. Be sure to use the appropriate type of Ethernet cable to connect from host to switch, switch to router, and host to router. Refer to “Lab 1-1: Cabling a Network and Basic Router Configuration (1.5.1),” if you have any trouble connecting the devices. Be sure to connect the serial DCE cable to router R1 and the serial DTE cable to router R2.

Answer the following questions:

What type of cable is used to connect the Ethernet interface on a host PC to the Ethernet interface on a switch? [Straight-through \(patch\) cable](#)

What type of cable is used to connect the Ethernet interface on a switch to the Ethernet interface on a router? [Straight-through \(patch\) cable](#)

What type of cable is used to connect the Ethernet interface on a router to the Ethernet interface on a host PC? [Crossover cable](#)

Task 2: Erase and Reload the Routers

Step 1. Establish a terminal session to router R1.

Refer to Lab 1-1 for a review of terminal emulation and connecting to a router.

Step 2. Enter privileged EXEC mode:

```
Router> enable
Router#
```

Step 3. Clear the configuration.

To clear the configuration, issue the **erase startup-config** command. Press **Enter** when prompted to **[confirm]** that you really do want to erase the configuration currently stored in NVRAM:

```
Router# erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

Step 4. Reload the configuration.

When the prompt returns, issue the **reload** command. Answer **no** if asked to save changes.

What would happen if you answered **yes** to the question, “System configuration has been modified. Save?”

[The current running configuration would be saved to NVRAM, negating the entire purpose of erasing the startup configuration. The router would boot up with a configuration.](#)

The result should look something like this:

```
Router# reload

System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]
```

Press **Enter** when prompted to **[confirm]** that you really do want to reload the router. After the router finishes the boot process, choose not to use the AutoInstall facility, as shown:

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Would you like to terminate autoinstall? [yes]: [Press Return]
Press Enter to accept default.
Press RETURN to get started!
```

- Step 5.** Repeat Steps 1 through 4 on router R2 to remove any startup configuration file that might be present.

Task 3: Perform Basic Configuration of Router R1

- Step 1.** Establish a HyperTerminal session to router R1.

- Step 2.** Enter privileged EXEC mode.

```
Router> enable
Router#
```

- Step 3.** Enter global configuration mode.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

- Step 4.** Configure the router name as R1.

Enter the command **hostname R1** at the prompt:

```
Router(config)# hostname R1
R1(config)#
```

- Step 5.** Disable DNS lookup.

Disable DNS lookup with the **no ip domain-lookup** command:

```
R1(config)# no ip domain-lookup
R1(config)#
```

Why would you want to disable DNS lookup in a lab environment?

So that the router does not attempt to look up a DNS entry for a name that is really only a typing error.

What would happen if you disabled DNS lookup in a production environment?

A router would not be able to resolve names, causing potential problems when the router needs an IP address to address a packet.

- Step 6.** Configure the EXEC mode password.

Configure the EXEC mode password using the **enable secret password** command. Use **class** for the **password**:

```
R1(config)# enable secret class
R1(config)#
```

Why is it not necessary to use the **enable password password** command?

Although both passwords are listed in the configuration, the **enable secret** command overrides the **enable password** command.

Step 7. Configure a message-of-the-day banner.

Configure a message-of-the-day banner using the **banner motd** command:

```
R1(config)# banner motd &  
Enter TEXT message. End with the character '&'.  
*****  
    !!!AUTHORIZED ACCESS ONLY!!!  
*****  
&  
R1(config)#
```

When does this banner display?

When a user logs in to the router either through Telnet or the console connection.

Why should every router have a message-of-the-day banner?

To provide a warning against intentional or unintentional unauthorized access.

Step 8. Configure the console password on the router.

Use **cisco** as the password. When you are finished, exit from line configuration mode:

```
R1(config)# line console 0  
R1(config-line)# password cisco  
R1(config-line)# login  
R1(config-line)# exit  
R1(config)#
```

Step 9. Configure the password for the virtual terminal lines.

Use **cisco** as the password. When you are finished, exit from line configuration mode.

```
R1(config)# line vty 0 4  
R1(config-line)# password cisco  
R1(config-line)# login  
R1(config-line)# exit  
R1(config)#
```

Step 10. Configure the FastEthernet 0/0 interface.

Configure the FastEthernet 0/0 interface with the IP address 192.168.1.1/24:

```
R1(config)# interface fastethernet 0/0  
R1(config-if)# ip address 192.168.1.1 255.255.255.0  
R1(config-if)# no shutdown  
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed  
state to up  
R1(config-if)#
```

Step 11. Configure the Serial 0/0/0 interface.

Configure the Serial 0/0/0 interface with the IP address 192.168.2.1/24. Set the clock rate to 64,000:

Note: The purpose of the **clock rate** command is explained in Chapter 2.

```
R1(config-if)# interface serial 0/0/0
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# clock rate 64000
R1(config-if)# no shutdown
R1(config-if)#
```

Note: The interface will be not activated until the serial interface on R2 is configured and activated.

Step 12. Return to privileged EXEC mode.

Use the **end** command to return to privileged EXEC mode:

```
R1(config-if)# end
R1#
```

Step 13. Save the R1 configuration.

Save the R1 configuration using the **copy running-config startup-config** command:

```
R1# copy running-config startup-config
Building configuration...
[OK]
R1#
```

What is a shorter version of this command? [**copy run start**](#)

Task 4: Perform Basic Configuration of Router R2

Step 1. For R2, repeat Steps 1 through 9 from Task 3.

Step 2. Configure the Serial 0/0/0 interface.

Configure the Serial 0/0/0 interface with the IP address 192.168.2.2/24:

```
R2(config)# interface serial 0/0/0
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# no shutdown
```

```
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
R2(config-if)#
```

Step 3. Configure the FastEthernet 0/0 interface.

Configure the FastEthernet 0/0 interface with the IP address 192.168.3.1/24:

```
R2(config-if)# interface fastethernet 0/0
R2(config-if)# ip address 192.168.3.1 255.255.255.0
R2(config-if)# no shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
R2(config-if)#
```

Step 4. Return to privileged EXEC mode.

Use the **end** command to return to privileged EXEC mode:

```
R2(config-if)# end
R2#
```

Step 5. **Save the R2 configuration.**

Save the R2 configuration using the **copy running-config startup-config** command:

```
R2# copy running-config startup-config
Building configuration...
[OK]
R2#
```

Task 5: Configure IP Addressing on the Host PCs

Step 1. Configure the host PC1.

Configure the host PC1 that is attached to R1 with an IP address of 192.168.1.10/24 and a default gateway of 192.168.1.1.

Step 2. Configure the host PC2.

Configure the host PC2 that is attached to R2 with an IP address of 192.168.3.10/24 and a default gateway of 192.168.3.1.

Task 6: Verify and Test the Configurations

Step 1. Verify that routing tables have the following routes using the **show ip route** command.

The **show ip route** command and output will be thoroughly explored in upcoming chapters. For now, you are interested in seeing that both R1 and R2 have two routes. Both routes are designated with a **C**. These are the directly connected networks that were activated when you configured the interfaces on each router. If you do not see two routes for each router as shown in the following output, proceed to Step 2:

```
R1# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
       level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
       route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set
```



```

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
R1#
-----
R2# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
       level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
       route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
R2#

```

Step 2. Verify interface configurations.

Another common problem is router interfaces that are not configured correctly or not activated. Use the **show ip interface brief** command to quickly verify the configuration of each router's interfaces. Your output should look similar to the following:

```

R1# show ip interface brief
Interface      IP-Address      OK? Method Status          Protocol
FastEthernet0/0 192.168.1.1    YES manual up             up
FastEthernet0/1 unassigned      YES unset  administratively down  down
Serial0/0/0     192.168.2.1    YES manual up             up
Serial0/0/1     unassigned      YES unset  administratively down  down
Vlan1           unassigned      YES manual administratively down  down
-----
R2# show ip interface brief
Interface      IP-Address      OK? Method Status          Protocol
FastEthernet0/0 192.168.3.1    YES manual up             up
FastEthernet0/1 unassigned      YES unset  administratively down  down
Serial0/0/0     192.168.2.2    YES manual up             up
Serial0/0/1     unassigned      YES unset  down              down
Vlan1           unassigned      YES manual administratively down  down

```

If both interfaces are up and up, both routes will be in the routing table. Verify this again by using the **show ip route** command.

Step 3. Test connectivity.

Test connectivity by pinging from each host to the default gateway that has been configured for that host.

From the host attached to R1, is it possible to ping the default gateway? **Yes**

From the host attached to R2, is it possible to ping the default gateway? **Yes**

If the answer is **no** for either of the preceding questions, troubleshoot the configurations to find the error using the following systematic process:

1. Check the PCs.

Are they physically connected to the correct router? (Connection could be through a switch or directly.) [Yes](#)

Are link lights blinking on all relevant ports? [Yes](#)

2. Check the PC configurations.

Do they match the topology diagram? [Yes](#)

3. Check the router interfaces using the **show ip interface brief** command.

Are the interfaces up and up? [Yes](#)

If your answer to all three steps is **yes**, you should be able to successfully ping the default gateway.

- Step 4.** Test connectivity between router R1 and R2.

From router R1, is it possible to ping R2 using the **ping 192.168.2.2** command? [Yes](#)

From router R2, is it possible to ping R1 using the **ping 192.168.2.1** command? [Yes](#)

If the answer is **no** for either of the preceding questions, troubleshoot the configurations to find the error using the following systematic process:

1. Check the cabling.

Are the routers physically connected? [Yes](#)

Are link lights blinking on all relevant ports? [Yes](#)

2. Check the router configurations.

Do they match the topology diagram? [Yes](#)

Did you configure the **clock rate** command on the DCE side of the link? [Yes](#)

3. Check the router interfaces using the **show ip interface brief** command.

Are the interfaces up and up? [Yes](#)

If your answer to all three steps is **yes**, you should be able to successfully ping from R2 to R1 and from R2 to R3.

Task 7: Reflection

- Step 1.** Attempt to ping from the host connected to R1 to the host connected to R2.

This ping should be unsuccessful.

- Step 2.** Attempt to ping from the host connected to R1 to router R2.

This ping should be unsuccessful.

- Step 3.** Attempt to ping from the host connected to R2 to router R1.

This ping should be unsuccessful.

What is missing from the network that is preventing communication between these devices?

After reading the chapter text, the student should be able to state that this network is missing either static or dynamic routing (or both!).

Task 8: Documentation

On each router, capture the command output from the following commands to a text (.txt) file and save for future reference.

```
show running-config
```

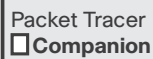
```
show ip route
```

```
show ip interface brief
```

If you need to review the procedures for capturing command output, refer to “Lab 1-1: Cabling a Network and Basic Router Configuration (1.5.1).”

Task 9: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.



Packet Tracer Companion

You can now open the file LSG02-Lab152.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity. Use the Lab PDF for more details.



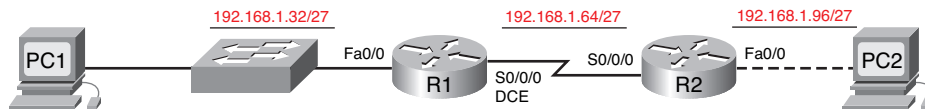
Lab 1-3: Challenge Router Configuration (1.5.3)

Upon completion of this lab, you will be able to

- Subnet an address space given requirements
- Assign appropriate addresses to interfaces and document
- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Perform basic configuration tasks on a router
- Configure and activate serial and Ethernet interfaces
- Test and verify configurations
- Reflect on and document the network implementation

Scenario

In this lab activity, you will design and apply an IP addressing scheme for the topology shown in the topology diagram in Figure 1-25. You will be given one Class C address that you must subnet to provide a logical addressing scheme for the network. You must first cable the network as shown before the configuration can begin. When the network is cabled, configure each device with the appropriate basic configuration commands. The routers will then be ready for interface address configuration according to your IP addressing scheme. When the configuration is complete, use the appropriate IOS commands to verify that the network is working properly.

Figure 1-25 Topology Diagram for Lab 1-3 (Answer)

Task 1: Subnet the Address Space

Step 1. Examine the network requirements.

You have been given the 192.168.1.0/24 address space to use in your network design. The network consists of the following segments:

- The network connected to router R1 will require enough IP addresses to support 20 hosts.
- The network connected to router R2 will require enough IP addresses to support 20 hosts.
- The link between router R1 and router R2 will require IP addresses at each end of the link.

Step 2. Consider the following questions when creating your network design:

How many subnets are needed for this network? 3

What is the subnet mask for this network in dotted decimal format? 255.255.255.224

What is the subnet mask for the network in slash format? /27

How many usable hosts are there per subnet? 30

Step 3. Assign subnetwork addresses to the topology diagram.

- a. Assign subnet 1 to the network attached to R1.
- b. Assign subnet 2 to the link between R1 and R2.
- c. Assign subnet 3 to the network attached to R2.

Task 2: Determine Interface Addresses

Step 1. Assign appropriate addresses to the device interfaces.

- a. Assign the first valid host address in subnet 1 to the LAN interface on R1.
- b. Assign the last valid host address in subnet 1 to PC1.
- c. Assign the first valid host address in subnet 2 to the WAN interface on R1.
- d. Assign the last valid host address in subnet 2 to the WAN interface on R2.
- e. Assign the first valid host address in subnet 3 to the LAN interface of R2.
- f. Assign the last valid host address in subnet 3 to PC2.

Step 2. Document the addresses to be used in Table 1-8.

Table 1-8 Addressing Table for Lab 1-3

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.33	255.255.255.224	—
	S0/0/0	192.168.1.65	255.255.255.224	—
R2	Fa0/0	192.168.1.97	255.255.255.224	—
	S0/0/0	192.168.1.94	255.255.255.224	—
PC1	NIC	192.168.1.62	255.255.255.224	192.168.1.33
PC2	NIC	192.168.1.126	255.255.255.224	192.168.1.97

Task 3: Prepare the Network

Step 1. Cable a network that is similar to the one in the topology diagram.

You can use any current router in your lab as long as it has the required interfaces as shown in the topology.

Step 2. Clear any existing configurations on the routers.

Task 4: Perform Basic Router Configurations

Perform basic configuration of the R1 and R2 routers according to the following guidelines:

1. Configure the router host name.
2. Disable DNS lookup.
3. Configure an EXEC mode password.
4. Configure a message-of-the-day banner.
5. Configure a password for console connections.
6. Configure a password for vty connections.

Task 5: Configure and Activate Serial and Ethernet Addresses

Step 1. Configure the router interfaces.

Configure the interfaces on the R1 and R2 routers with the IP addresses from your network design. When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 2. Configure the PC interfaces.

Configure the Ethernet interfaces of PC1 and PC2 with the IP addresses and default gateways from your network design.

Task 6: Verify the Configurations

Answer the following questions to verify that the network is operating as expected.

From the host attached to R1, is it possible to ping the default gateway? Yes

From the host attached to R2, is it possible to ping the default gateway? Yes

From router R1, is it possible to ping the Serial 0/0/0 interface of R2? Yes

From router R2, is it possible to ping the Serial 0/0/0 interface of R1? Yes

The answer to the above questions should be **yes**. If any of the above pings failed, check your physical connections and configurations. If necessary, refer to “Lab 1-2: Basic Router Configuration (1.5.2).”

What is the status of the FastEthernet 0/0 interface of R1? up and up

What is the status of the Serial 0/0/0 interface of R1? up and up

What is the status of the FastEthernet 0/0 interface of R2? up and up

What is the status of the Serial 0/0/0 interface of R2? up and up

What routes are present in the routing table of R1?

C 192.168.1.64 is directly connected, Serial0/1/0

C 192.168.1.32 is directly connected, FastEthernet0/0

What routes are present in the routing table of R2?

C 192.168.1.96 is directly connected, FastEthernet0/0

C 192.168.1.64 is directly connected, Serial0/0/0

Task 7: Reflection

Are there any devices on the network that cannot ping each other?

R1 cannot ping the Fast Ethernet interface on R2. R2 cannot ping the Fast Ethernet interface on R1. PC1 cannot ping PC2. PC2 cannot ping PC1.

What is missing from the network that is preventing communication between these devices?

After reading the chapter text, the student should be able to state that this network is missing either static or dynamic routing (or both!).

Task 8: Document the Router Configurations

On each router, capture the following command output to a text (.txt) file and save for future reference:

- Running configuration
- Routing table
- Summary of status information for each interface

Packet Tracer
Companion

Packet Tracer Companion

You can now open the file LSG02-Lab153.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity. Use the Lab PDF for more details.

Packet Tracer
Challenge

Packet Tracer Skills Integration Challenge

This activity integrates all the knowledge and skills you acquired in previous courses and the first chapter of this course. You build a network from the ground up. Starting with an addressing space and network requirements, you must implement a network design that satisfies the specifications. You are responsible for configuring the routers with basic configurations and assigning IP addresses to all devices. Routing has already been configured, so you can verify full connectivity between all devices. Finally, you investigate the Layer 2 and Layer 3 addresses used as a ping packet traverses the network you built. Open the file LSG02-PTskills1.pka on the CD-ROM that accompanies this book. Use the topology in Figure 1-26 and the addressing tables in Table 1-9 to document your design.

Upon completion of this challenge activity, you will be able to

- Design and document an addressing scheme based on requirements
- Select appropriate equipment and cable the devices
- Apply a basic configuration to the devices
- Verify full connectivity between all devices in the topology
- Identify Layer 2 and Layer 3 addresses used to switch packets

Open the file LSG02-PTskills1.pka on the CD-ROM that accompanies this book. You will use the topology in Figure 1-26 and the addressing table in Table 1-9 to document your design.

Figure 1-26 Topology Diagram Packet Tracer Challenge (Answer)

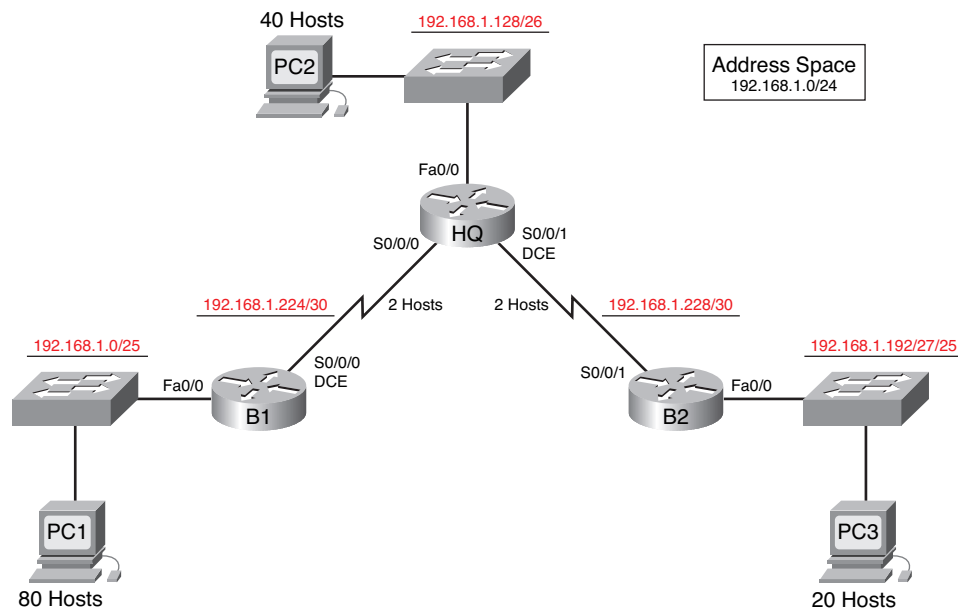


Table 1-9 Addressing Table for Packet Tracer Challenge

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	Fa0/0	192.168.1.129	255.255.255.192	—
	S0/0/0	192.168.1.225	255.255.255.252	—
	S0/0/1	192.168.1.229	255.255.255.252	—
B1	Fa0/0	192.168.1.1	255.255.255.128	—
	S0/0/0	192.168.1.226	255.255.255.252	—
B2	Fa0/0	192.168.1.193	255.255.255.224	—
	S0/0/1	192.168.1.230	255.255.255.252	—
PC1	NIC	192.168.1.126	255.255.255.128	192.168.1.1
PC2	NIC	192.168.1.190	255.255.255.192	192.168.1.129
PC3	NIC	192.168.1.222	255.255.255.224	192.168.1.193

Task 1: Design and Document an Addressing Scheme

Step 1. Design an addressing scheme.

Based on the network requirements shown in the topology, design an appropriate addressing scheme given block 192.168.1.0/24:

- Starting with the largest LAN, determine the size of subnet you will need for the given host requirement. Then, assign subnets starting with the largest LAN moving to the smallest.
- After the LAN subnets are determined, assign the first available address space to the WAN link between B1 and HQ.
- Assign the second available address space to the WAN link between HQ and B2.

Step 2. Document the addressing scheme.

- Record the network addresses in dotted-decimal/slash format.
- Document the IP addresses, subnet masks, and default gateway addresses.
 - For the LANs, assign the first IP address to the router interface. Assign the last IP address to the PC.
 - For the WAN links, assign the first IP address to HQ.

Task 2: Cable Devices

Step 1. Cable the networks according to the topology.

- B1 S0/0/0 (DCE) to HQ S0/0/0 (DTE)
- HQ S0/0/1 (DCE) to B2 S0/0/1 (DTE)
- B1 Fa0/0 to S1 Fa0/1
- S1 Fa0/2 to PC1

- HQ Fa0/0 to S2 Fa0/1
- S2 Fa0/2 to PC2
- B2 Fa0/0 to S3 Fa0/1
- S3 Fa0/2 to PC3

Task 3: Apply a Basic Configuration

Step 1. Configure the routers.

Using your documentation, configure the routers with basic configurations including addressing. Use **cisco** as the line passwords and **class** as the secret password. Use **64000** as the clock rate.

Step 2. Configure the PCs.

Using your documentation, configure the PCs with an IP address, subnet mask, and default gateway.

Task 4: Identify Layer 2 and Layer 3 Addresses Used to Switch Packets

Step 1. Create a PDU ping packet.

RIP routing has already been configured for you. Therefore, you should have end-to-end connectivity.

- Enter Simulation Mode.
- Use the Add Simple PDU button to create a ping from PC1 to PC3.
- Change Edit Filters so that only ICMP is simulated.
- Record the Layer 2 and Layer 3 addresses for the packet at PC1.
- Record the Layer 2 and Layer 3 addresses for the packet at B1.
- Record the Layer 2 and Layer 3 addresses for the packet at HQ.
- Record the Layer 2 and Layer 3 addresses for the packet at B2

Reflection

Which addresses changed as the packet progressed through the network? Which addresses did not? Why?

Static Routing

The Study Guide portion of this chapter uses a combination of matching, fill-in-the-blank, multiple-choice, and open-ended question exercises to test your knowledge and skills of basic router configuration, including static, summary, and default routes.

The Labs and Activities portion of this chapter includes the online curriculum lab to ensure that you have mastered routing table interpretation skills.

As you work through this chapter, use Chapter 2 in *Routing Protocols and Concepts, CCNA Exploration Companion Guide* or use the corresponding Chapter 2 in the Exploration Routing Protocols and Concepts online curriculum for assistance.

Study Guide

Routers and the Network

Understanding a router's place in the network is a prerequisite to moving ahead in your studies of routing and routing protocols. You studied routers extensively in Chapter 1, "Introduction to Routing and Packet Forwarding." The following sections review some of the basic skills you need to progress to the next step: static routing.

Document the Addressing Scheme

Refer to the topology shown in Figure 2-1. Use Table 2-1 to document the IP addresses for all the interfaces. Use the following guidelines to ensure that your addresses will work with the Packet Tracer Exercise 2-1.

1. Assign the first IP address for all LANs to the router interface.
2. Assign HQ the first IP address for all WAN links to Branch routers.
3. In the Packet Tracer Exercise, you will configure the PCs to use the .10 address for the respective LAN.

Figure 2-1 Static Routing Study Guide Topology

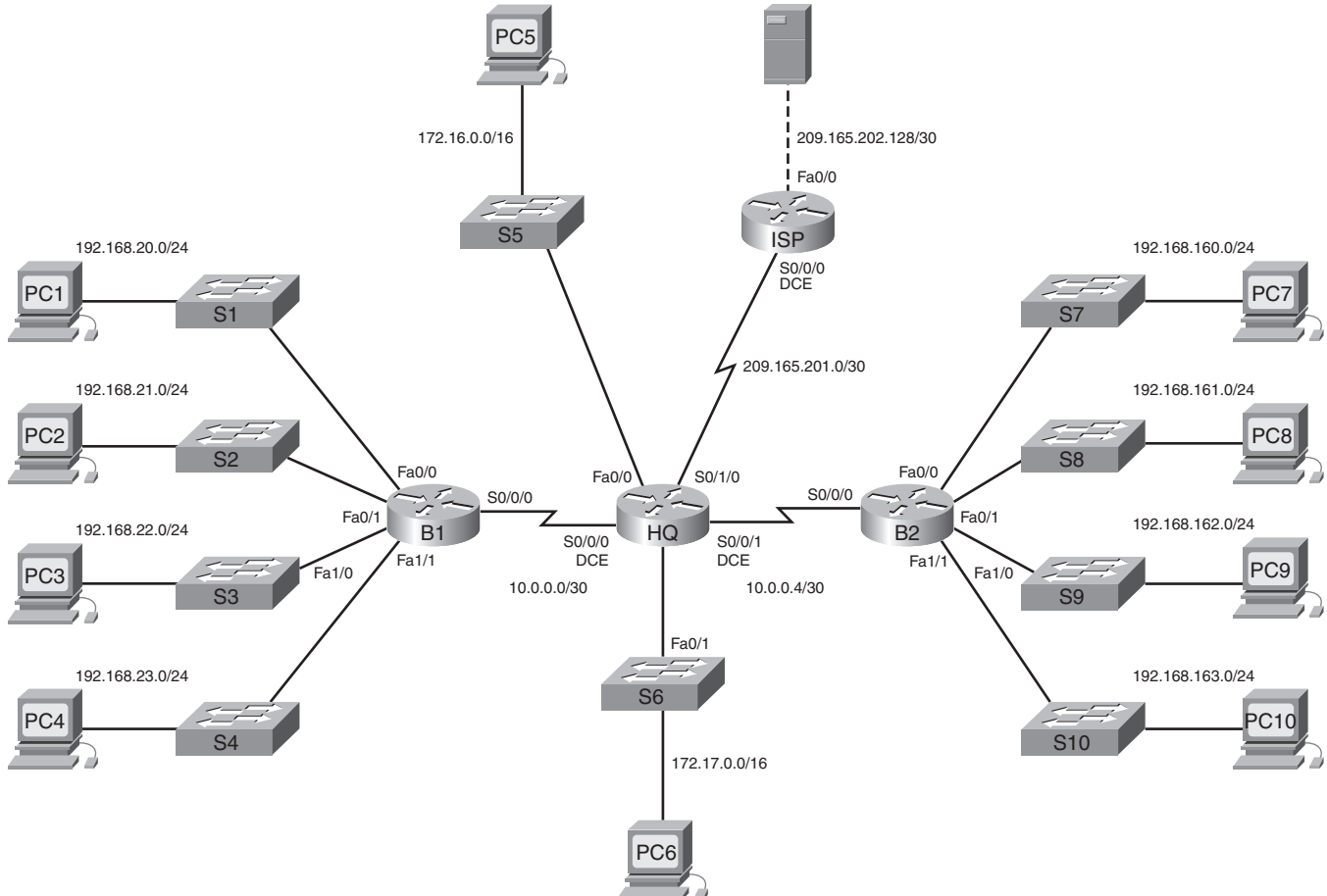


Table 2-1 Addressing Table for Static Routing Study Guide Topology

Device	Interface	IP Address	Subnet Mask
HQ	Fa0/0	172.16.0.1	255.255.0.0
	Fa0/1	172.17.0.1	255.255.0.0
	S0/0/0	10.0.0.1	255.255.255.252
	S0/0/1	10.0.0.5	255.255.255.252
	S0/1/0	209.165.201.2	255.255.255.252
B1	Fa0/0	192.168.20.1	255.255.255.0
	Fa0/1	192.168.21.1	255.255.255.0
	Fa1/0	192.168.22.1	255.255.255.0
	Fa1/1	192.168.23.1	255.255.255.0
	S0/0/0	10.0.0.2	255.255.255.252
B2	Fa0/0	192.168.160.1	255.255.255.0
	Fa0/1	192.168.161.1	255.255.255.0
	Fa1/0	192.168.162.1	255.255.255.0
	Fa1/1	192.168.163.1	255.255.255.0
	S0/0/0	10.0.0.6	255.255.255.252
ISP	Fa0/0	209.165.202.129	255.255.255.252
	S0/0/0	209.165.201.1	255.255.255.252
Web Server	NIC	209.165.202.130	255.255.255.252



Packet Tracer Exercise 2-1

Now you are ready to use Packet Tracer to apply your documented addressing scheme. Open file LSG02-0201.pka on the CD-ROM that accompanies this book to perform this exercise using Packet Tracer.

Task 1: Build the Chapter Topology

- Step 1.** Connect the devices according to Figure 2-1. Be sure to connect cable to the correct interface if an interface designation is shown.
- Step 2.** Your completion percentage should be 14%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure PCs

- Step 1.** Use the .10 address to configure each of the PCs with an address from the LAN it is attached to. Each PC should also have connectivity with its respective default gateway.

Step 2. Your completion percentage should be 39%. If not, click **Check Results** to see which required components are not yet completed.

After completing this task, save your Packet Tracer file to use again in the next section. Save the file as LSG02-0201-task2.pkt.

Router Configuration Review

To configure static routing and dynamic routing protocols, you need to know only the basic IOS commands. You should already be familiar with these commands. The following sections are only meant as a review. For more detailed explanations, refer to Chapter 1 and the Network Fundamentals course.

show Commands Matching Exercise

Using only the partial output shown, indicate which command displayed this output.

R1# show running-config or show startup-config

<output omitted>

!

hostname R1

!

!

enable secret 5 \$1\$.3R0\$VLU0dBF20qNBn0EjQBvR./

<output omitted>

R1# show interfaces or show interface [any fastethernet interface]

<output omitted>

Hardware is AmdFE, address is 000c.3010.9260 (bia 000c.3010.9260)

MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,

reliability 255/255, txload 1/255, rxload 1/255

<output omitted>

R1# show ip interface brief

<output omitted>

FastEthernet0/0 unassigned YES manual administratively down down

<output omitted>

R1# show ip route

<output omitted>

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

<output omitted>

Configuring and Verifying Interfaces Exercise

In this exercise, you will review the basic interface configuration for the HQ router shown earlier in Figure 2-1.

HQ does not yet have any routes. You should add two routes by configuring the Fast Ethernet interfaces for HQ. By default, all router interfaces are **shut down**, or turned off. To enable this interface, use the **no shutdown** command, which changes the interface from administratively down to up.

What commands will configure the Fast Ethernet interfaces with IP addresses and activate the interfaces?

```
HQ(config)# interface fastethernet 0/0
HQ(config-if)# ip address 172.16.0.1 255.255.0.0
HQ(config-if)# no shutdown
UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 01:16:09.214: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
  changed state to up
HQ(config-if)# interface fastethernet 0/1
HQ(config-if)# ip address 172.17.0.1 255.255.0.0
HQ(config-if)# no shutdown
UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar 1 01:16:09.214: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
  changed state to up
```

The IOS sends two messages to the console after you activate the interface. Both of these messages are important. The first **changed state to up** message indicates that the **physical** layer is up. If you do not get this first message, be sure that the interface is properly connected to a **switch** or a **hub**.

The second **changed state to up** message indicates that the **data link** layer is operational.

The IOS often sends **unsolicited** messages to the console while you are typing a command. To keep the **unsolicited** output separate from your input, enter line configuration mode for the console port and add the **logging synchronous** command.

After an interface is configured, it can be verified using various commands.

The **show interfaces fastethernet 0/0** command shows that the Fast Ethernet interface is up and the line protocol is up. The **no shutdown** command changed the interface from administratively down and down to up and up. This command also shows the MAC address for the interface:

```
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 000c.3010.9260 (bia 000c.3010.9260)
  Internet address is 172.16.0.1/24
  <output omitted>
```

The **show ip interface brief** command also verifies that an interface is up and up:

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	172.16.0.1	YES	manual	up	up
Serial0/0/0	unassigned	YES	unset	administratively down	down
FastEthernet0/1	72.17.0.1	YES	unset	up	up

Serial0/0/1	unassigned	YES	unset	administratively down	down
Serial0/1/0	209.165.201.2	YES	manual	up	up
Serial0/1/1	unassigned	YES	manual	administratively down	down
Vlan1	unassigned	YES	manual	administratively down	down

The following partial output is from the **show running-config** command. It also shows the current configuration of this interface. When the interface is disabled, this command displays **shutdown** under the interface; however, when the interface is enabled, **no shutdown** is not displayed:

```
<output omitted>
interface FastEthernet0/0
ip address 172.16.0.1 255.255.255.0
<output omitted>
```

As explained in Chapter 1, each interface must belong to a separate [subnet/network](#).

Next, configure the Serial 0/0/0 and Serial 0/0/1 interface on router HQ. The process to configure a serial interface is similar to the process to configure a Fast Ethernet interface. For the data communications equipment (DCE) side on the WAN link, you need to add the **clock rate** command. HQ will provide signaling to B1 and B2 at 64,000 kbps:

```
HQ(config)# interface serial 0/0/0
HQ(config-if)# ip address 10.0.0.1 255.255.255.252
HQ(config-if)# clock rate 64000
HQ(config-if)# no shutdown
%LINK-3-UPDOWN: Interface Serial0/0/0, changed state to down
HQ(config)# interface serial 0/0/1
HQ(config-if)# ip address 10.0.0.5 255.255.255.252
HQ(config-if)# clock rate 64000
HQ(config-if)# no shutdown

%LINK-3-UPDOWN: Interface Serial0/0/1, changed state to down
```

You can display the current state of Serial 0/0/0 using the **show interfaces serial 0/0/0** command:

```
HQ# show interfaces serial 0/0/0
Serial0/0/1 is down, line protocol is down
  Hardware is GT96K Serial
  Internet address is 10.0.0.5/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
```

Why is the link still down?

The link is down because we have not yet configured and enabled the other end of the serial link.

If a cable is connected between the two routers and neither end of the cable is labeled DCE or DTE, you can use the **show controllers** command to determine which end of the cable is attached to that interface:

```
HQ# show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, no clock
<output omitted>
```

Exploring Directly Connected Networks

Before a router can forward packets to a remote network, it must have active directly connected networks. Each directly connected network on the router is a member of a different network or subnet.

Directly Connected Networks Exercise

In this exercise, you will review the tools used to monitor and troubleshoot directly connected networks.

Monitoring Directly Connected Networks

To verify that directly connected networks are installed, use the **show ip route** command to view the routing table. Directly connected networks are listed with the code **C**.

In contrast to **show** commands, **debug** commands can be used to monitor router operations in real time. The **debug ip routing** command will let you see any changes that the router performs when adding or removing routes. In Task 3 of Packet Tracer Exercise 2-1, you will observe HQ adding a route using this monitoring command, as shown in Example 2-1.

Example 2-1 Monitoring a Route Added to the Table

```
HQ# debug ip routing
IP routing debugging is on
HQ# config t
Enter configuration commands, one per line. End with CNTL/Z.
HQ(config)# int fa0/0
HQ(config-if)# ip address 172.16.0.1 255.255.0.0
HQ(config-if)# no shut

is_up: 1 state: 4 sub state: 1 line: 1 has_route: True
RT: SET_LAST_RDB for 172.16.0.0/16
NEW rdb: is directly connected
```

continues

continued

```
RT: add 172.16.0.0/16 via 0.0.0.0, connected metric [0/0]
RT: NET-RED 172.16.0.0/16
RT: interface FastEthernet0/0 added to routing table

%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

The preceding output was organized for better readability, and the output that informed you that the route was added is highlighted. Often, IOS will mix the console messages with monitoring output, which can sometimes be confusing. Example 2-2 shows the output before it was better organized.

Example 2-2 Raw Output from Console and Monitoring Commands

```
HQ# debug ip routing
IP routing debugging is on
HQ# config t
Enter configuration commands, one per line. End with CNTL/Z.
HQ(config)# int fa0/0
HQ(config-if)# ip add 172.16.0.1 255.255.0.0
HQ(config-if)# no
is_up: 0 state: 6 sub state: 1 line: 1 has_route: False
is_up: 0 state: 6 sub state: 1 line: 1 has_route: False
HQ(config-if)# no shut
HQ(config-if)#
is_up: 1 state: 4 sub state: 1 line: 1 has_route: False
RT: SET_LAST_RDB for 172.16.0.0/16
    NEW rdb: is directly connected

RT: add 172.16.0.0/16 via 0.0.0.0, connected metric [0/0]
RT: NET-RED 172.16.0.0/16
RT: interface FastEthernet0/0 added to routing table
HQ(config-if)#
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
HQ(config-if)#
is_up: 1 state: 4 sub state: 1 line: 1 has_route: True
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
HQ(config-if)#
is_up: 1 state: 4 sub state: 1 line: 1 has_route: True
HQ(config-if)# end
```

```

HQ#
is_up: 0 state: 0 sub state: 1 line: 0 has_route: False
HQ#
%SYS-5-CONFIG_I: Configured from console by console
HQ#

```

You can disable the monitoring command, **debug ip routing**, by using the **undebug ip routing** command or the **undebug all** command.

How do you change an IP address or subnet mask for an interface?

Simply reconfigure the IP address and subnet mask for that interface. This change will overwrite the previous entry.

What two commands remove a directly connected network from a router? What does each command do?

Use these two commands: shutdown and no ip address. The shutdown command will disable the interface. The no ip address command will remove the IP address and subnet mask from the interface.

Accessing Devices on Directly Connected Networks

To return to the configuration of the devices in Figure 2-1, we will now assume that all directly connected networks are configured for HQ, B1, and B2. You will complete these configurations in Task 3 of Packet Tracer Exercise 2-1. Example 2-20 shows the rest of the configurations for routers R2 and R3.

What command is the quickest and most efficient way to verify that all the configured interfaces are up and up?

show ip interface brief

What command verifies that all directly connected networks are installed for routing?

show ip route

At this point in the configuration of HQ, B1, and B2, what devices and networks are reachable? Explain by listing the devices that HQ can reach.

When a router only has its interfaces configured, and the routing table contains the directly connected networks but no other routes, only devices on those directly connected networks are reachable. For example, HQ can reach B1, B2, ISP, PC5, and PC6.

What do these devices all have in common with HQ?

Each shares a directly connected network with HQ.

What are the IP addresses (excluding its own) that HQ can successfully ping?

172.16.0.10 (PC5)

172.17.0.10 (PC6)

10.0.0.2 (B1 S0/0/0)

[10.0.0.6 \(B2 S0/0/0\)](#)

[209.165.201.1 \(ISP S0/0/0\)](#)



Packet Tracer Exercise 2-1: Task 3—Basic Router Configuration

Open your LSG02-0201-task2.pka saved version of this Packet Tracer Exercise and complete the following steps.

- Step 1.** Use the following guidelines to configure the host name, banner, enable secret password, and lines for HQ, B1, and B2. Packet Tracer will grade only the host name configurations.
- To avoid incorrect grading, make sure that the router names are configured in ALL CAPS.
 - Use the following text for the banner: **Authorized Access Only**.
 - For the secret password, use **class**.
 - For the console and Telnet lines, configure login access with the password **cisco**.
- Step 2.** Configure the interfaces according to the following guidelines:
- To monitor routes as they are installed in the routing table, turn on the appropriate **debug** command.
 - Use the IP address and subnet mask according to what you filled in for Table 2-1 earlier.
 - Configure the description for each interface. (Packet Tracer will not grade this configuration.)
 - Configure clocking signals at 64,000 bps where necessary.
 - Activate the interfaces.
 - When finished, disable monitoring.
- Step 3.** Your completion percentage should be 66%. If not, click **Check Results** to see which required components are not yet completed.
- Step 4.** Save your configurations for HQ, B1, and B2.

After completing this task, save your Packet Tracer file to use again in the next section. Save the file as LSG02-0201-task3.pkt.

Cisco Discovery Protocol Exercise

Cisco Discovery Protocol (CDP) is a powerful network-monitoring and -troubleshooting tool. CDP is an information-gathering tool used by network administrators to get information about directly connected Cisco devices. CDP is a proprietary tool that enables you to access a summary of protocol and address information about Cisco devices that are directly connected.

In this exercise, you will review CDP features and operations. You will also list the commands used to configure and verify CDP.

Network Discovery with CDP

By default, each Cisco device sends periodic messages to directly connected Cisco devices. These messages are known as CDP advertisements. A Cisco device frequently has other Cisco devices on the network. These devices are known as its CDP neighbors. CDP can be used as a network discovery tool, helping you to build a logical topology of a network when such documentation is missing or lacking in detail.

Layer 3 Neighbors

At this point in the chapter's topology configuration, you only have directly connected neighbors. At Layer 3, routing protocols consider neighbors to be devices that share the same network address space.

In Figure 2-1, which routers are Layer 3 neighbors?

B1 and HQ

HQ and B2

HQ and ISP

Layer 2 Neighbors

CDP operates at Layer 2 only. Therefore, CDP neighbors are Cisco devices that are directly connected physically and share the same data link.

Assuming that all routers and switches are Cisco devices running CDP, list the CDP neighbors for the following devices.

HQ CDP Neighbors

B1, B2, ISP, S5, and S6

B1 CDP Neighbors

HQ, S1, S2, S3, and S4

B2 CDP Neighbors

HQ, S7, S8, S9, S10

ISP CDP Neighbors

HQ

How many CDP neighbors would each of the ten switches have?

Each switch only has one CDP neighbor—the directly connected router. Only Cisco devices can be CDP neighbors.

CDP show Commands

What **show** command will list a Cisco device's Layer 2 neighbors? List both versions of the command.

show cdp neighbors and show cdp neighbors detail

What important information that can be used for network discovery does the detailed version of this command show?

The IP address of the directly connected CDP neighbor (if it has one)

How is the information beneficial to network discovery?

For network discovery situations, knowing the IP address of the CDP neighbor is often all the information needed to telnet into that device. With an established Telnet session, information can be gathered about a neighbor's directly connected Cisco devices. In this fashion, you can telnet around a network and build a logical topology.

Disabling CDP

Why is CDP considered a security risk?

Because some IOS versions send out CDP advertisements by default, a packet sniffer can easily glean information about devices on the network.

What command disables CDP globally? Include the router prompt in your answer.

Router(config)# no cdp run

If you want to use CDP but need to stop CDP advertisements on a particular interface, what command would you use? Include the router prompt in your answer.

Router(config-if)# no cdp enable

In Task 4 for Packet Tracer Exercise 2-1, you will adjust the CDP settings so that only HQ, B1, and B2 are sending each other CDP advertisements.



Packet Tracer Exercise 2-1: Task 4—Configure CDP

Open your LSG02-0201-task3.pka saved version of this Packet Tracer Exercise and complete the following steps:

- Step 1.** CDP is not enabled for HQ, B1, or B2. Enter the commands to start CDP.
- Step 2.** Assume that network policy states that CDP advertisements should only be sent between directly connected, company-owned routers:
- Configure HQ, B1, and B2 to send CDP updates across the serial links to each other.
 - HQ should not send CDP advertisements to ISP.
 - HQ, B1, and B2 should not send CDP advertisements out LAN interfaces.
- Step 3.** Your completion percentage should be 81%. If not, click **Check Results** to see which required components are not yet completed.

After completing this task, save your Packet Tracer file to use again in the next section. Save the file as LSG02-0201-task4.pkt.

Static Routes with Next-Hop Addresses

As discussed previously, a router can learn about remote networks in one of two ways:

- Manually, from configured static routes
- Automatically, from a dynamic routing protocol

The rest of this chapter focuses on configuring static routes. In the following sections, you practice your knowledge and skills related to configuring static routes with a next-hop address.

Static Route Command Syntax Exercise

The command for configuring a static route is **ip route**. The complete syntax for configuring a static route is as follows:

```
ip route prefix mask {ip-address | interface-type interface-number [ip-address]}
[distance] [name] [permanent | track number] [tag tag]
```

What is the a simpler version of this command's syntax?

```
Router(config)# ip route network-address subnet-mask {ip-address | exit-interface}
```

Explain the parameters of the command.

- network-address: Destination network address of the remote network to be added to the routing table.
- subnet-mask: Subnet mask of the remote network to be added to the routing table. The subnet mask can be modified to summarize a group of networks.

One or both of the following parameters must also be used:

- ip-address: Commonly referred to as the next-hop router's IP address
- exit-interface: Outgoing interface that would be used in forwarding packets to the destination network

Static Routes with Next-Hop Address Exercise

Evaluating the Routing Table

Referring to Figure 2-1, neither static nor dynamic routing has yet been configured. However, all interfaces are in the up and up state.

By referring to the topology only, you should be able to list the details of the routes that are currently shown in each router's routing table. However, you can also refer to your saved version of Packet Tracer Exercise 2-1 (LSG02-0201-task4.pka).

HQ: Five directly connected routes coded with a "C" in the routing table: one for each of the LAN interfaces (172.16.0.0/16, 172.17.0.0/16) and three for each of the serial interfaces (10.0.0.0/30, 10.0.0.4/30, 209.165.201.0/30)

B1: Five directly connected routes code with a "C" in the routing table: four for each of the LAN interfaces (192.168.20.0/24, 192.168.21.0/24, 192.168.22.0/24, 192.168.23.0/24) and one for the S0/0/0 interface (10.0.0.0/30)

B2: Five directly connected routes code with a "C" in the routing table: four for each of the LAN interfaces (192.168.160.0/24, 192.168.161.0/24, 192.168.162.0/24, 192.168.163.0/24) and one for the S0/0/0 interface (10.0.0.4/30)

Each router needs to have a route pointing to the other remote networks. For this exercise, you will disregard the ISP router. You will add the ISP router in the section "Configuring Default Static Routes Exercise," later in the chapter.

Determining the Static Routing Needs

Not counting the WAN link to ISP and the Web Server LAN, how many total networks are there in the topology? (Hint: Don't forget the WAN links between HQ and B1 and B2.)

12 networks

What networks does HQ *not* have listed in its routing table?

All the LAN networks attached to B1 and B2—a total of eight networks.

Assuming that you will not summarize these networks, how many static routes need to be configured on HQ? 8

What networks does B1 *not* have listed in its routing table?

All the LAN networks attached to HQ and B2 as well as the WAN link between HQ and B2—a total of seven networks.

Assuming that you will not summarize these networks, how many static routes need to be configured on B1? 7

What networks does B2 *not* have listed in its routing table?

All the LAN networks attached to HQ and B1 as well as the WAN link between HQ and B1—a total of seven networks.

Assuming that you will not summarize these networks, how many static routes need to be configured on B2? 7

List the Static Route Commands

For each router, record the static route commands you would use to configure the static routes with the next-hop IP address specified.

Static routes with the next-hop address for HQ:

!Static routes to B1 LANs

ip route 192.168.20.0 255.255.255.0 10.0.0.2

ip route 192.168.21.0 255.255.255.0 10.0.0.2

ip route 192.168.22.0 255.255.255.0 10.0.0.2

ip route 192.168.23.0 255.255.255.0 10.0.0.2

!Static routes to B2 LANs

ip route 192.168.160.0 255.255.255.0 10.0.0.6

ip route 192.168.161.0 255.255.255.0 10.0.0.6

ip route 192.168.162.0 255.255.255.0 10.0.0.6

ip route 192.168.163.0 255.255.255.0 10.0.0.6

Static routes with the next-hop address for B1:

!Static routes to HQ LANs

ip route 172.16.0.0 255.255.0.0 10.0.0.1

ip route 172.17.0.0 255.255.0.0 10.0.0.1

!Static routes to B2 LANs

ip route 192.168.160.0 255.255.255.0 10.0.0.1

ip route 192.168.161.0 255.255.255.0 10.0.0.1

ip route 192.168.162.0 255.255.255.0 10.0.0.1


```
ip route 192.168.163.0 255.255.255.0 10.0.0.1
!Static route to the WAN link between HQ and B2
ip route 10.0.0.4 255.255.255.252 10.0.0.1
```

Static routes with the next-hop address for B2:

```
!Static routes to HQ LANs
ip route 172.16.0.0 255.255.0.0 10.0.0.5
ip route 172.17.0.0 255.255.0.0 10.0.0.5
!Static routes to B1 LANs
ip route 192.168.20.0 255.255.255.0 10.0.0.5
ip route 192.168.21.0 255.255.255.0 10.0.0.5
ip route 192.168.22.0 255.255.255.0 10.0.0.5
ip route 192.168.23.0 255.255.255.0 10.0.0.5
!Static route to the WAN link between HQ and B1
ip route 10.0.0.0 255.255.255.252 10.0.0.5
```

To test your answers, you will configure and test these static routes in Task 5 and Task 6 of Packet Tracer Exercise 2-1.



Packet Tracer Exercise 2-1

Open your LSG02-0201-task4.pka saved version of this Packet Tracer Exercise and complete Tasks 5–7.

Task 5: Static Route Configuration with Next-Hop Address

- Step 1.** Configure static routes for HQ according to your answers in the section “Static Routes with Next-Hop Address Exercise.”
- Your completion percentage should be 88%. If not, click **Check Results** to see which required components are not yet completed.
- Step 2.** Configure static routes for B1 according to your answers in the section “Static Routes with Next-Hop Address Exercise.”
- Your completion percentage should be 94%. If not, click **Check Results** to see which required components are not yet completed.
- Step 3.** Configure static routes for H3 according to your answers in the section “Static Routes with Next-Hop Address Exercise.”
- Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 6: Verify Connectivity

All PCs and routers should have end-to-end connectivity. Pinging from any source to any destination (with the exception of ISP and the web server) should be successful. You can also click **Check Results** and then click the **Connectivity Tests** tab to see whether all the connectivity tests are successful.

Task 7: Save the Packet Tracer File

Save your Packet Tracer file as LSG02-0201-end.pka.

Configuring a Static Route with an Exit Interface

In the previous sections, you saw how a static route can be configured with a next-hop address. Using a next-hop address is a correct method in configuring static routes. However, in some situations, using an exit interface can result in a more efficient route lookup process.

Static Routes with an Exit Interface Exercise

Explain in detail the difference between the next-hop address argument and the exit interface argument.

The next-hop argument requires a recursive route lookup, that is, the router still does not know the exit interface and will have to look up the next-hop IP address in the routing table to locate the exit interface. If the exit interface argument is used, no recursive lookup is necessary, and the router can immediately forward the packet to the outbound interface.

The network shown in Figure 2-1 already has static routes with next-hop addresses configured. Before configuring static routes with exit interfaces, you will need to remove the next-hop versions.

How do you remove a static route from the configuration?

Use the **no** form of the **ip route** command.

List the Static Route Commands

Assume that all the next-hop static routes have been removed. For each router in Figure 2-1, record the static route commands you would use to configure the static routes with an exit interface specified.

Static routes with an exit interface for HQ:

!Static routes to B1 LANs

ip route 192.168.20.0 255.255.255.0 Serial0/0/0

ip route 192.168.21.0 255.255.255.0 Serial0/0/0

ip route 192.168.22.0 255.255.255.0 Serial0/0/0

ip route 192.168.23.0 255.255.255.0 Serial0/0/0

!Static routes to B2 LANs

ip route 192.168.160.0 255.255.255.0 Serial0/0/1

ip route 192.168.161.0 255.255.255.0 Serial0/0/1

ip route 192.168.162.0 255.255.255.0 Serial0/0/1

ip route 192.168.163.0 255.255.255.0 Serial0/0/1

Static routes with an exit interface for B1:

!Static routes to HQ LANs

ip route 172.16.0.0 255.255.0.0 Serial0/0/0

ip route 172.17.0.0 255.255.0.0 Serial0/0/0

!Static routes to B2 LANs

ip route 192.168.160.0 255.255.255.0 Serial0/0/0

ip route 192.168.161.0 255.255.255.0 Serial0/0/0

ip route 192.168.162.0 255.255.255.0 Serial0/0/0

```
ip route 192.168.163.0 255.255.255.0 Serial0/0/0
!Static route to the WAN link between HQ and B2
ip route 10.0.0.4 255.255.255.252 Serial0/0/0
```

Static routes with an exit interface for B2:

```
!Static routes to HQ LANs
ip route 172.16.0.0 255.255.0.0 Serial0/0/0
ip route 172.17.0.0 255.255.0.0 Serial0/0/0
!Static routes to B1 LANs
ip route 192.168.20.0 255.255.255.0 Serial0/0/0
ip route 192.168.21.0 255.255.255.0 Serial0/0/0
ip route 192.168.22.0 255.255.255.0 Serial0/0/0
ip route 192.168.23.0 255.255.255.0 Serial0/0/0
!Static route to the WAN link between HQ and B1
ip route 10.0.0.0 255.255.255.252 Serial0/0/0
```



Packet Tracer Exercise 2-2

Now you are ready to test your answers to the “Static Routes with an Exit Interface Exercise” by configuring static routes in Packet Tracer. Open file LSG02-0202.pka on the CD-ROM that accompanies this book to perform this exercise using Packet Tracer.

Task 1: Remove Static Routes with Next-Hop Addresses

- Step 1.** Before configuring static routes with exit interfaces, remove the static routes that are using next-hop addresses.
- Step 2.** To verify that all the static routes are removed, view the routing tables on HQ, B1, and B2. Only directly connected networks should be listed.
- Your completion percentage should still be 0%. No commands are graded yet.

Task 2: Static Route Configuration with Exit Interface

- Step 1.** Configure static routes for HQ according to your answers in the section “Static Routes with an Exit Interface Exercise.”
- Your completion percentage should be 36%. If not, click **Check Results** to see which required components are not yet completed.
- Step 2.** Configure static routes for B1 according to your answers in the section “Static Routes with an Exit Interface Exercise.”
- Your completion percentage should be 68%. If not, click **Check Results** to see which required components are not yet completed.
- Step 3.** Configure static routes for H3 according to your answers in the section “Static Routes with an Exit Interface Exercise.”
- Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Verify Connectivity

All PCs and routers should have end-to-end connectivity. Pinging from any source to any destination (with the exception of ISP and the Web Server) should be successful. You can also click **Check Results** and then click the **Connectivity Tests** tab to see whether all the connectivity tests are successful.

Task 4: Save the Packet Tracer File

Save your Packet Tracer file as LSG02-0202-end.pka.

Summary and Default Static Routes

A router can have a specific route entry in its routing table for a destination network, or that same network can be part of a less specific route entry. The less specific route entry can be a summary route or a default route.

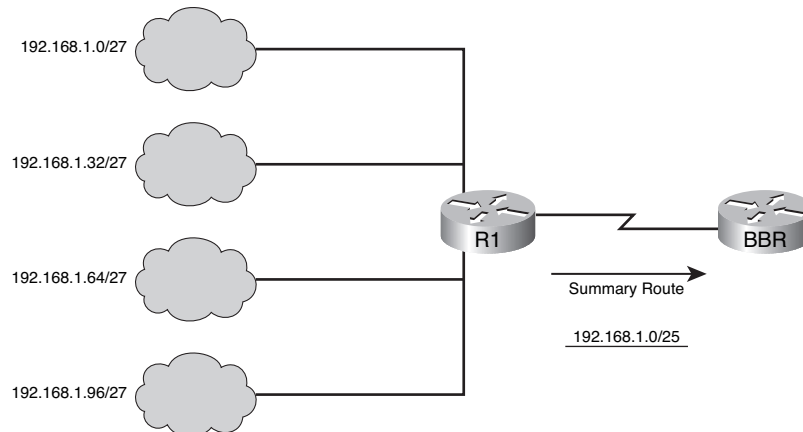
Calculating Summary Route Exercises

A summary route is a single route that can be used to represent multiple routes. Summary routes are generally a set of contiguous networks that have the same exit interface and/or next-hop IP address.

Use the following exercises to practice determining the summary route for a collection of subnets.

Referring to Figure 2-2, what summary route would R1 send to BBR (Backbone Router) for the four networks? Write your answer in the space provided.

Figure 2-2 Summary Route Example



Use the following steps to calculate a summary route:

1. Write out the networks that you want to summarize in binary, as shown following Step 4.
2. To find the subnet mask for summarization, start with the leftmost bit.
3. Work your way to the right, finding all the bits that match consecutively.

4. When you find a column of bits that do not match, stop. You are at the summary boundary.

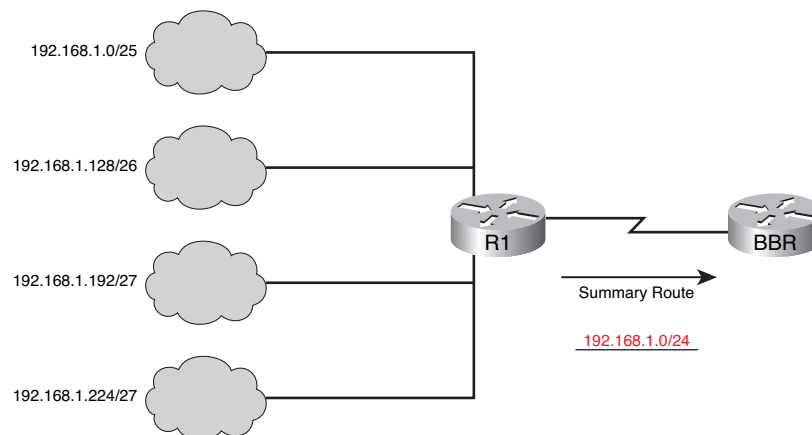
```
11000000.10101000.00000001.00000000
11000000.10101000.00000001.00100000
11000000.10101000.00000001.01000000
11000000.10101000.00000001.01100000
```

5. Count the number of leftmost matching bits, which in this example is 25. This number becomes your subnet mask for the summarized route, /25 or 255.255.255.128.
6. To find the network address for summarization, copy the matching 25 bits and add all 0 bits to the end to make 32 bits. In this example, the network address is 192.168.1.0.

Summary Route Exercise 1

Referring to Figure 2-3, what summary route would R1 send to BBR for the four networks? Write your answer in the space provided.

Figure 2-3 Summary Route Exercise 1 (Answer)



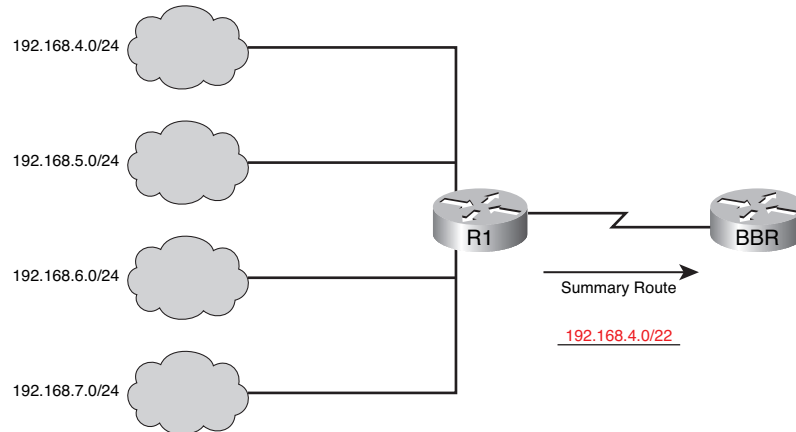
```
11000000.10101000.00000001.00000000
11000000.10101000.00000001.10000000
11000000.10101000.00000001.11000000
11000000.10101000.00000001.11100000
```

Summary Route: 192.168.1.0/24

Summary Route Exercise 2

Referring to Figure 2-4, what summary route would R1 send to BBR for the four networks? Write your answer in the space provided.

Figure 2-4 Summary Route Exercise 2 (Answer)



11000000.10101000.00000100.00000000

11000000.10101000.00000101.00000000

11000000.10101000.00000110.00000000

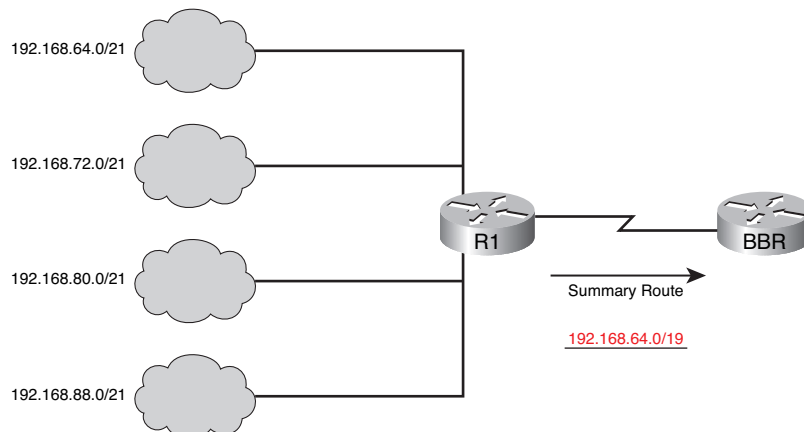
11000000.10101000.00000111.00000000

Summary Route: 192.168.4.0/22

Summary Route Exercise 3

Referring to Figure 2-5, what summary route would R1 send to BBR for the four networks? Write your answer in the space provided.

Figure 2-5 Summary Route Exercise 3 (Answer)



11000000.10101000.01000000.00000000

11000000.10101000.01001000.00000000

11000000.10101000.01010000.00000000

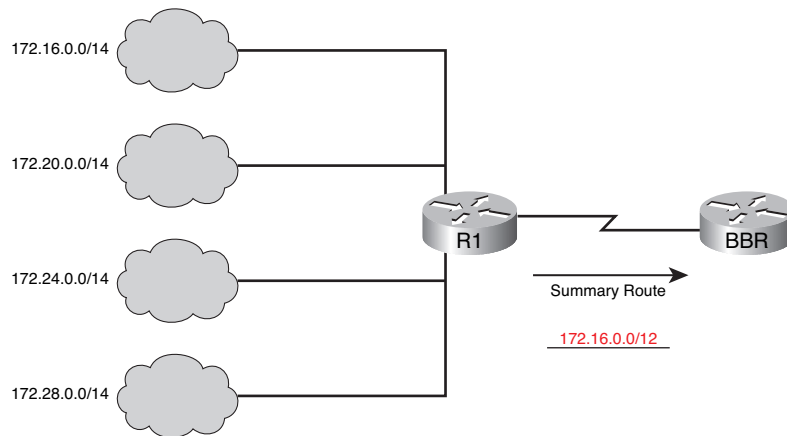
11000000.10101000.01011000.00000000

Summary Route: 192.168.64.0/19

Summary Route Exercise 4

Referring to Figure 2-6, what summary route would R1 send to BBR for the four networks?
Write your answer in the space provided.

Figure 2-6 Summary Route Exercise 4 (Answer)



10101100.00010000.00000000.00000000

10101100.00010100.00000000.00000000

10101100.00011000.00000000.00000000

10101100.00011100.00000000.00000000

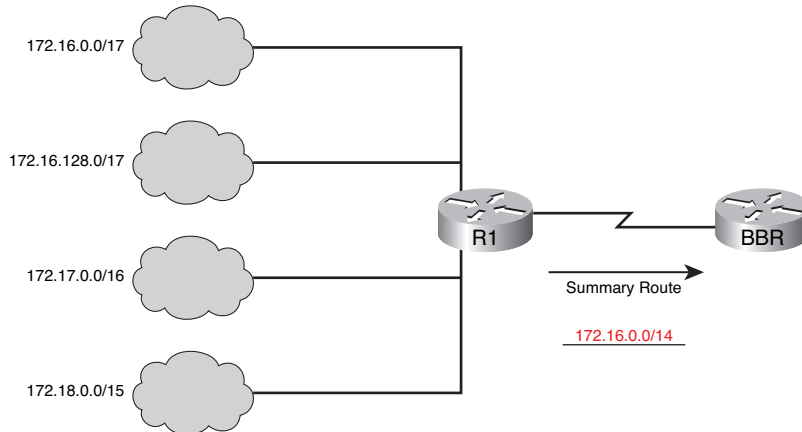
Summary Route: 172.16.0.0/12

Your students might be interested to know that the summary route 172.16.0.0/12 is also the entire range of Class B private IP addresses as defined by RFC 1918.

Summary Route Exercise 5

Referring to Figure 2-7, what summary route would R1 send to BBR for the four networks? Write your answer in the space provided.

Figure 2-7 Summary Route Exercise 5 (Answer)



```

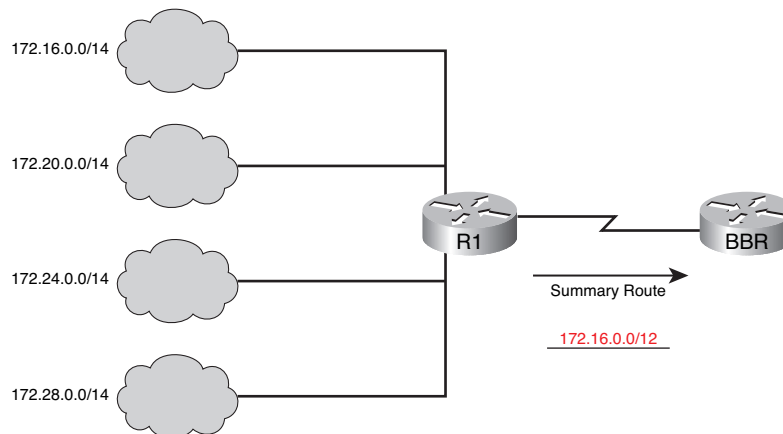
10101100.00010000.00000000.00000000
10101100.00010000.10000000.00000000
10101100.00010001.00000000.00000000
10101100.00010010.00000000.00000000
    
```

Summary Route: 172.16.0.0/14

Summary Route Exercise 6

Referring to Figure 2-8, what summary route would R1 send to BBR for the four networks? Write your answer in the space provided.

Figure 2-8 Summary Route Exercise 6 (Answer)




```
00001010.00001010.00000000.00000000
```

```
00001010.00001010.00001000.00000000
```

```
00001010.00001010.00010000.00000000
```

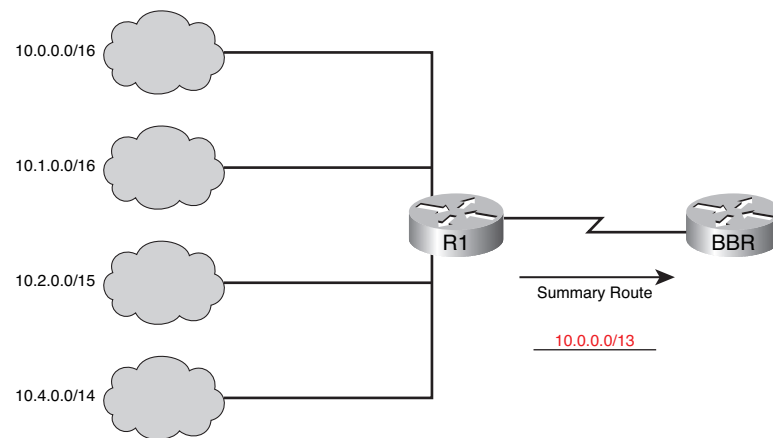
```
00001010.00001010.00011000.00000000
```

Summary Route: 10.10.0.0/19

Summary Route Exercise 7

Referring to Figure 2-9, what summary route would R1 send to BBR for the four networks? Write your answer in the space provided.

Figure 2-9 Summary Route Exercise 7 (Answer)



```
00001010.00000000.00000000.00000000
```

```
00001010.00000001.00000000.00000000
```

```
00001010.00000010.00000000.00000000
```

```
00001010.00000100.00000000.00000000
```

Summary Route: 10.0.0.0/13

Combining Static Routes into Summary Routes Exercise

The current configuration of the chapter topology (Figure 2-1) with static routes works fine. However, you can reduce the size of the routing tables by summarizing contiguous address space into one summary route.

HQ Summary Routes

HQ will need two summary routes: one for the LANs attached to B1 and one for the LANs attached to B2.

Calculate the summary route for the LANs attached to B1.

B1 LANs binary:

11000000.10101000.00010100.00000000

11000000.10101000.00010101.00000000

11000000.10101000.00010110.00000000

11000000.10101000.00010111.00000000

Summary: 192.168.20.0/22

Record the command that HQ will use to summarize the B1 LANs. Use the exit interface version of the static route command.

ip route 192.168.20.0 255.255.252.0 Serial0/0/0

Calculate the summary route for the LANs attached to B2.

B2 LANs in binary:

11000000.10101000.10100000.00000000

11000000.10101000.10100001.00000000

11000000.10101000.10100010.00000000

11000000.10101000.10100011.00000000

Summary: 192.168.160.0/22

Record the command HQ will use to summarize the B2 LANs. Use the exit interface version of the **static route** command.

ip route 192.168.160.0.0 255.255.252.0 Serial0/0/1

B1 Summary Routes

B1 will need two summary routes: one for the LANs attached to B2 and one for the LANs attached to HQ.

You already calculated the summary for the LANs attached to B2. Record the command that B1 will use to summarize the B2 LANs. Use the exit interface version of the **static route** command.

ip route 192.168.160.0.0 255.255.252.0 Serial0/0/0

Calculate the summary route for the LANs attached to HQ.

HQ LANs in binary:

10101100.00010000.00000000.00000000

10101100.00010001.00000000.00000000

Summary: 172.16.0.0/15

Record the command that B1 will use to summarize the HQ LANs. Use the exit interface version of the static route command.

ip route 172.16.0.0 255.254.0.0 Serial0/0/0

B2 Summary Routes

B2 will need two summary routes: one for the LANs attached to B1 and one for the LANs attached to HQ.

You already calculated the summary for both of the LANs attached to B1 and the LANs attached to HQ. Record the command that B2 will use to summarize the B1 LANs. Use the exit interface version of the static route command.

```
ip route 192.168.20.0 255.255.252.0 Serial0/0/0
```

Record the command that B2 will use to summarize the HQ LANs. Use the exit interface version of the static route command.

```
ip route 172.16.0.0 255.254.0.0 Serial0/0/0
```

Now you can test your answers to the preceding exercise by completing Packet Tracer Exercise 2-3: Summary Route Configuration.



Packet Tracer Exercise 2-3: Summary Route Configuration

Open file LSG02-0203.pka on the CD-ROM that accompanies this book to perform this exercise using Packet Tracer and complete Tasks 1–4.

Task 1: Remove Static Routes with Exit Interface

- Step 1.** Before configuring the summary routes, remove the individual static routes.
- Step 2.** To verify that all the static routes are removed, view the routing tables on HQ, B1, and B2. Only directly connected networks should be listed.
- Your completion percentage should still be 0%. No commands are graded yet.

Task 2: Configure Summary Routes

- Step 1.** Configure the summary routes for HQ according to your answers in the section “Combining Static Routes into Summary Routes Exercise.”
- Your completion percentage should be 33%. If not, click **Check Results** to see which required components are not yet completed.
- Step 2.** Configure the summary routes for B1 according to your answers in the section “Combining Static Routes into Summary Routes Exercise.”
- Your completion percentage should be 67%. If not, click **Check Results** to see which required components are not yet completed.
- Step 3.** Configure the summary routes for B2 according to your answers in the section “Combining Static Routes into Summary Routes Exercise.”
- Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Verify Connectivity

All PCs and routers should have end-to-end connectivity. Pinging from any source to any destination (with the exception of ISP and the web server) should be successful. You can also click **Check Results** and then click the **Connectivity Tests** tab to see whether all the connectivity tests are successful.

Task 4: Save the Packet Tracer File

Save your Packet Tracer file as LSG02-0203-end.pka.

Configuring Default Static Routes Exercise

What is the command syntax for a default static route?

Router(config)# ip route 0.0.0.0 0.0.0.0 [exit-interface | ip-address]

What is another name commonly used to refer to default static routes?

The quad-zero route.

Revisit the chapter topology from Figure 2-1. In this topology, which routers are stub routers?

B1 and B2 are stub routers.

Stub routers don't need specific routing information to reach networks beyond their gateway. A stub router can simply use a default route. For example, B1 does not need to know all the LANs attached to B2. B1 only needs to know to send all traffic not destined for a directly connected network to HQ. Currently, both B1 and B2 have two static summary routes. You can reduce the routing table further by removing the summary routes and configuring a default static route.

B1 and B2 Default Static Route

What command would you enter on both B1 and B2 to configure a default static route with an exit interface?

ip route 0.0.0.0 0.0.0.0 Serial0/0/0

HQ Default Static Route

HQ will also need a default static route to send traffic to the ISP router.

What command would you enter on HQ to configure a default static route with an exit interface?

ip route 0.0.0.0 0.0.0.0 Serial0/1/0

Just because a default static route is configured on HQ does not mean remove the static summary routes and expect HQ to still have connectivity to B1 and B2.

What would HQ do with traffic destined for a B1 or B2 LAN if the static summary routes are removed?

HQ would forward the traffic to ISP, its default route.

On HQ, you can leave the summary static routes.

ISP Static Summary Routes

To finish the configurations, ISP now needs to have four different static summary routes. You already calculated the summaries for the LANs attached to HQ, B1, and B2.

List the three static summary routes ISP will use for the LANs. Use the *exit-interface* argument.

ip route 172.16.0.0 255.254.0.0 Serial0/0/0

ip route 192.168.20.0 255.255.252.0 Serial0/0/0

ip route 192.168.160.0 255.255.252.0 Serial0/0/0

However, one summary route remains: the WAN links between HQ and B1 and HQ and B2.

Calculate the summary route for the WANs attached to HQ.

WANs in binary:

```
00001010.00000000.00000000.00000000
00001010.00000000.00000000.00000100
```

Summary: 10.0.0.0/29

Record the command that ISP will use to summarize the WANs. Use the exit interface version of the **static route** command.

```
ip route 10.0.0.0 255.255.255.248 Serial0/0/0
```

Now you can test your answers to the preceding exercise by completing Packet Tracer Exercise 2-4: Default Route Configuration.

Packet Tracer
 Activity

Packet Tracer Exercise 2-4: Default Route Configuration

Open file LSG02-0204.pka on the CD-ROM that accompanies this book to perform this exercise using Packet Tracer. Complete Tasks 1–5.

Task 1: Remove Static Routes on B1 and B2

- Step 1.** Before configuring the default routes, remove the summary routes on B1 and B2.
- Step 2.** To verify that all the static routes are removed from B1 and B2, view the routing tables. Only directly connected networks should be listed.
- Your completion percentage should still be 0%. No commands are graded yet.

Task 2: Configure Default Routes on B1, B2, and HQ

- Step 1.** Configure the default route on B1 according to your answers in the section “Configuring Default Static Routes Exercise.”
- Your completion percentage should be 14%. If not, click **Check Results** to see which required components are not yet completed.
- Step 2.** Configure the default route on B2 according to your answers in the section “Configuring Default Static Routes Exercise.”
- Your completion percentage should be 29%. If not, click **Check Results** to see which required components are not yet completed.
- Step 3.** Configure the default route on HQ according to your answers in the section “Configuring Default Static Routes Exercise.”
- Your completion percentage should be 43%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure Summary Routes on ISP

Configure the four summary routes on ISP according to your answers in the section “Configuring Default Static Routes Exercise.”

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

Task 4: Verify Connectivity

All PCs and routers should have end-to-end connectivity. Pinging from any source to any destination—including ISP and the Web Server—should be successful. You can also click **Check Results** and then click the **Connectivity Tests** tab to see whether all the connectivity tests are successful.

Task 5: Save the Packet Tracer File

Save your Packet Tracer file as LSG02-0204-end.pka.

Managing and Troubleshooting Static Routes

It is important to be able to properly manage and troubleshoot static routes. When a static route is no longer needed, that static route should be deleted from the running and startup configuration files.

Troubleshooting a Missing Route

Troubleshooting is a skill that develops as you gain more experience. It is always best to look for the most obvious and simplest issues first, such as an interface still in shutdown mode or an interface with the wrong IP address. After these items have been verified, begin looking for more complicated possibilities, like an error in the static route configuration.

List at least four commands that can help you troubleshoot a missing route.

[Answers will vary. Here are some possible answers.](#)

- [ping](#)
- [traceroute](#)
- [show ip route](#)
- [show ip interface brief](#)
- [show cdp neighbors detail](#)

Labs and Activities

Command Reference

In Table 2-2, record the command, *including the correct router prompt*, that fits the description. Fill in any blanks with the appropriate missing information.

Table 2-2 Commands for Chapter 2, Static Routing

Command	Description
Router# show controllers serial 0/0/0	Displays which side of a cable is attached to the interface: DCE or DTE
Router# show cdp neighbors	Displays summary information about directly connected Layer 2 devices; uses a Cisco-proprietary protocol
Router# show cdp neighbors detail	Displays full information about directly connected Layer 2 devices; uses a Cisco-proprietary protocol
Router(config)# cdp run	Enables the Cisco Layer 2 protocol for the entire router
Router(config-if)# cdp enable	Enables the Cisco Layer 2 protocol for an interface
Router(config)# ip route 10.0.0.0 255.0.0.0 172.16.0.1	Configures a static route to 10.0.0.0/8 with a next hop of 172.16.0.1
Router(config)# ip route 10.0.0.0 255.0.0.0 Serial0/0/0	Configures a static route to 10.0.0.0/8 with an exit interface of Serial 0/0/0
Router(config)# ip route 172.16.0.0 255.240.0.0 Serial 0/0/0	Configures a summary static route for all addresses belonging to Class B networks 172.16.0.0/16 through 172.31.0.0/16; uses Serial 0/0/0 as the exit interface
Router(config)# ip route 0.0.0.0 0.0.0.0 Serial0/1/0	Configures a default static route with an exit interface of Serial 0/1/0



Lab 2-1: Basic Static Route Configuration (2.8.1)

Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Perform basic configuration tasks on a router
- Interpret **debug ip routing** output
- Configure and activate serial and Ethernet interfaces
- Test connectivity
- Gather information to discover causes for lack of connectivity between devices
- Configure a static route using an intermediate address
- Configure a static route using an exit interface
- Compare a static route with intermediate address to a static route with exit interface
- Configure a default static route
- Configure a summary static route
- Document the network implementation

Scenario

In this lab activity, you will create a network that is similar to the one shown in the topology diagram in Figure 2-10. Begin by cabling the network as shown in Figure 2-10. You will then perform the initial router configurations required for connectivity. Use the IP addresses provided in Table 2-3 to apply an addressing scheme to the network devices. After completing the basic configuration, test connectivity between the devices on the network. First test the connections between directly connected devices, and then test connectivity between devices that are not directly connected. Static routes must be configured on the routers for end-to-end communication to take place between the network hosts. You will configure the static routes that are needed to allow communication between the hosts. View the routing table after each static route is added to observe how the routing table has changed.

Figure 2-10 Topology Diagram for Lab 2-1

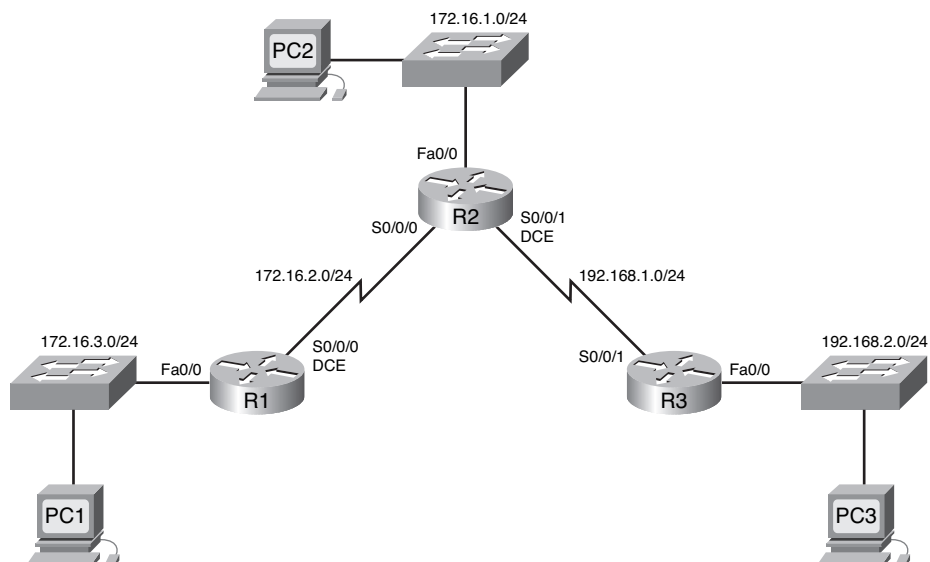


Table 2-3 Addressing Table for Lab 2-1

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.16.3.1	255.255.255.0	—
	S0/0/0	172.16.2.1	255.255.255.0	—
R2	Fa0/0	172.16.1.1	255.255.255.0	—
	S0/0/0	172.16.2.2	255.255.255.0	—
	S0/0/1	192.168.1.2	255.255.255.0	—
R3	FA0/0	192.168.2.1	255.255.255.0	—
	S0/0/1	192.168.1.1	255.255.255.0	—
PC1	NIC	172.16.3.10	255.255.255.0	172.16.3.1
PC2	NIC	172.16.1.10	255.255.255.0	172.16.1.1
PC3	NIC	192.168.2.10	255.255.255.0	192.168.2.1

Task 1: Cable, Erase, and Reload the Routers

Step 1. Cable a network that is similar to the one in the topology diagram shown in Figure 2-10.

Step 2. Clear the configuration on each router.

Clear the configuration on each of the routers using the **erase startup-config** command and then **reload** the routers. Answer **no** if asked to save changes.

Task 2: Perform Basic Router Configuration

Note: If you have difficulty with any of the commands in this task, see “Lab 1-1: Cabling a Network and Basic Router Configuration (1.5.1).”

Step 1. Use global configuration commands.

On the routers, enter global configuration mode and configure the basic global configuration commands, including the following:

```
hostname
no ip domain-lookup
enable secret
```

Step 2. Configure the console and virtual terminal line passwords on each of the routers:

```
password
login
```

Step 3. Add the **logging synchronous** command to the console and virtual terminal lines.

This command is helpful in both lab and production environments and uses the following syntax:

```
Router(config-line)# logging synchronous
```

To synchronize unsolicited messages and debug output with solicited Cisco IOS Software output and prompts for a specific console port line, auxiliary port line, or virtual terminal line, you can use the **logging synchronous** line configuration command. In other words, the **logging synchronous** command prevents IOS messages from being delivered to the console or Telnet lines from interrupting your keyboard input.

For example, you might have already experienced something similar to the following example:

Note: Do not configure R1 interfaces yet.

```
R1(config)# interface fastethernet 0/0
R1(config-if)# ip address 172.16.3.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# descri
*Mar 1 01:16:08.212: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed
state to up
*Mar 1 01:16:09.214: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
R1(config-if)#
```

IOS sends unsolicited messages to the console when you activate an interface with the **no shutdown** command. However, the next command you enter (in this case, **description**) is interrupted by these messages. The **logging synchronous** command solves this problem by copying the command entered up to that point down to the next router prompt.

```
R1(config)# interface fastethernet 0/0
R1(config-if)# ip address 172.16.3.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# description
*Mar 1 01:28:04.242: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed
state to up
*Mar 1 01:28:05.243: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
R1(config-if)# description <-- Keyboard input copied after message
```

R1 is shown here as an example. Add **logging synchronous** to the console and virtual terminal lines on all routers.

```
R1(config)# line console 0
R1(config-line)# logging synchronous
R1(config-line)# line vty 0 4
R1(config-line)# logging synchronous
```

Step 4. Add the **exec-timeout** command to the console and virtual terminal lines.

To set the interval that the EXEC command interpreter waits until user input is detected, you can use the **exec-timeout** line configuration command. This command allows you to control the amount of time a console or virtual terminal line can be idle before the session is terminated. The syntax is as follows:

```
Router(config-line)# exec-timeout minutes [seconds]
```

where the parameters are as follows:

- *minutes*: Integer that specifies the number of minutes
- *seconds* (optional): Additional time intervals in seconds

In a lab environment, you can specify “no timeout” by entering the **exec-timeout 0 0** command. This command is helpful because the default timeout for lines is 10 minutes. However, for security purposes, you would not normally set lines to “no timeout” in a production environment.

R1 is shown here as an example.

Add **exec-timeout 0 0** to console and virtual terminal lines on all routers:

```
R1(config)# line console 0
R1(config-line)# exec-timeout 0 0
R1(config-line)# line vty 0 4
R1(config-line)# exec-timeout 0 0
```

Task 3: Interpreting Debug Output

Note: If you already configured IP addressing on R1, please remove all **interface** commands now before proceeding. R1, R2, and R3 should be configured through the end of Task 2 without any interface configurations.

Step 1. On R1 from privileged EXEC mode, enter the **debug ip routing** command:

```
R1# debug ip routing
```

```
IP routing debugging is on
```

The **debug ip routing** command shows when routes are added, modified, and deleted from the routing table. For example, every time you successfully configure and activate an interface, Cisco IOS adds a route to the routing table. You can verify this by observing output from the **debug ip routing** command.

Step 2. Enter interface configuration mode for R1’s LAN interface.

```
R1# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R1(config)# interface fastethernet 0/0
```

Configure the IP address as specified in the topology diagram.

```
R1(config-if)# ip address 172.16.3.1 255.255.255.0
```

```
is_up: 0 state: 6 sub state: 1 line: 1 has_route: False
```

As soon as you press **Enter**, Cisco IOS debug output informs you that there is now a route, but its state is False. In other words, the route has not yet been added to the routing table. Why did this occur and what steps should be taken to ensure that the route is entered into the routing table?

The route cannot be entered into the routing table until the interface is activated with the **no shutdown** command.

Step 3. Enter the command necessary to install the route in the routing table.

If you are not sure what the correct command is, review the section “Configuring and Verifying Interfaces Exercise,” earlier in this chapter.

After you enter the correct command, you should see debug output. Your output might be slightly different from the following example:

```
is_up: 1 state: 4 sub state: 1 line: 1 has_route: False
RT: add 172.16.3.0/24 via 0.0.0.0, connected metric [0/0]
RT: NET-RED 172.16.3.0/24
RT: NET-RED queued, Queue size 1
RT: interface FastEthernet0/0 added to routing table
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
is_up: 1 state: 4 sub state: 1 line: 1 has_route: True
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
is_up: 1 state: 4 sub state: 1 line: 1 has_route: True
is_up: 1 state: 4 sub state: 1 line: 1 has_route: True
```

The new network you configured on the LAN interface is now added to the routing table, as shown in the highlighted output.

If you do not see the route added to the routing table, the interface did not come up. Use the following systematic process to troubleshoot your connection:

1. Check your physical connections to the LAN interface.

Is the correct interface attached? [yes](#)

Your router might have more than one LAN interface. Did you connect the correct LAN interface? [yes](#)

An interface will not come up unless it detects a carrier detect signal at the physical layer from another device. Is the interface connected to another device such as a hub, switch, or PC? [yes](#)

2. Check link lights. Are all link lights blinking? [yes](#)
3. Check the cabling. Are the correct cables connected to the devices? [yes](#)
4. Has the interface been activated or enabled? [yes](#)

If you can answer **yes** to all the proceeding questions, the interface should come up.

Step 4. Enter the command to verify that the new route is now in the routing table.

Your output should look similar to the following output. There should now be one route in the table for R1. What command did you use?

```
R1# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
172.16.0.0/24 is subnetted, 1 subnets
C 172.16.3.0 is directly connected, FastEthernet0/0
```

Step 5. Enter interface configuration mode for R1's WAN interface connected to R2.

```
R1# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R1(config)# interface Serial 0/0/0
```

Configure the IP address as specified in the topology diagram.

```
R1(config-if)# ip address 172.16.2.1 255.255.255.0
is_up: 0 state: 0 sub state: 1 line: 0 has_route: False
```

As soon as you press **Enter**, Cisco IOS debug output informs you that there is now a route, but its state is **False**. Because R1 is the DCE side of the lab environment, you must specify how fast the bits will be clocked between R1 and R2.

Step 6. Enter the **clock rate** command on R1.

You can specify any valid clocking speed. Use the **?** to find the valid rates. Here, we used 64,000 bps.

```
R1(config-if)# clock rate 64000
is_up: 0 state: 0 sub state: 1 line: 0 has_route: False
```

Some IOS versions display the output shown above every 30 seconds. Why is the state of the route still **False**? What step must you now take to make sure that the interface is fully configured?

The route cannot be entered into the routing table until the interface is activated with the **no shutdown** command.

Step 7. Enter the command necessary to ensure that the interface is fully configured.

If you are not sure what the correct command is, review the section “Configuring and Verifying Interfaces Exercise,” earlier in this chapter.

```
R1(config-if)# no shutdown
```

After you enter the correct command, you should see debug output similar to the following example:

```
is_up: 0 state: 0 sub state: 1 line: 0 has_route: False
%LINK-3-UPDOWN: Interface Serial0/0/0, changed state to down
```

Unlike configuring the LAN interface, fully configuring the WAN interface does not always guarantee that the route will be entered in the routing table, even if your cable connections are correct. The other side of the WAN link must also be configured.

- Step 8.** If possible, establish a separate terminal session by consoling into R2 from another workstation. Doing this allows you to observe the debug output on R1 when you make changes on R2. You can also use the **debug ip routing** command on R2.

```
R2# debug ip routing
IP routing debugging is on
```

Enter interface configuration mode for R2's WAN interface connected to R1.

```
R2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# interface serial 0/0/0
```

Configure the IP address as specified in the topology diagram.

```
R2(config-if)# ip address 172.16.2.2 255.255.255.0
is_up: 0 state: 6 sub state: 1 line: 0
```

- Step 9.** Enter the command necessary to ensure that the interface is fully configured.

If you are not sure what the correct command is, review the section “Configuring and Verifying Interfaces Exercise,” earlier in this chapter.

```
R2(config-if)# no shutdown
```

After you enter the correct command, you should see debug output similar to the following example:

```
is_up: 0 state: 4 sub state: 1 line: 0
%LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
is_up: 1 state: 4 sub state: 1 line: 0
RT: add 172.16.2.0/24 via 0.0.0.0, connected metric [0/0]
RT: interface Serial0/0/0 added to routing table
is_up: 1 state: 4 sub state: 1 line: 0
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
is_up: 1 state: 4 sub state: 1 line: 0
```

The new network that you configured on the WAN interface is now added to the routing table, as shown in the highlighted output.

If you do not see the route added to the routing table, the interface did not come up. Use the following systematic process to troubleshoot your connection:

1. Check your physical connections between the two WAN interfaces for R1 and R2.

Is the correct interface attached? [yes](#)

Your router has more than one WAN interface. Did you connect the correct WAN interface? [yes](#)

An interface will not come up unless it detects a link beat at the physical layer from another device. Is the interface connected to the other router's interface? [yes](#)

2. Check link lights. Are all link lights blinking? [yes](#)
3. Check the cabling. R1 must have the DCE side of the cable attached, and R2 must have the DTE side of the cable attached. Are the correct cables connected to the routers? [yes](#)
4. Has the interface been activated or enabled? [yes](#)

If you can answer **yes** to all the proceeding questions, the interface should come up.

- Step 10.** Enter the command to verify that the new route is now in the routing table for R1 and R2.

Your output should look similar to the following output. There should now be two routes in the routing table for R1 and one route in the table for R2. What command did you use?

R1# **show ip route**

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2

ia - IS-IS inter area, * - candidate default, U - per-user static
route

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 2 subnets

C 172.16.2.0 is directly connected, Serial0/0/0

C 172.16.3.0 is directly connected, FastEthernet0/0

R2# **show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.2.0 is directly connected, Serial0/0/0

- Step 11.** Turn off debugging on both routers using either the **no debug ip routing** or the **undebug all** command.

R1(config-if)# **end**

R1# **no debug ip routing**

IP routing debugging is off

Task 4: Finish Configuring Router Interfaces

Step 1. Configure the remaining R2 interfaces.

Finish configuring the remaining interfaces on R2 according to the topology diagram in Figure 2-10 and the addressing information in Table 2-3.

Step 2. Configure R3 interfaces.

Console into R3 and configure the necessary interfaces according to the topology diagram in Figure 2-10 and the addressing information in Table 2-3.

Task 5: Configure IP Addressing on the Host PCs

Step 1. Configure the host PC2.

Configure the host PC1 with an IP address of 172.16.3.10/24 and a default gateway of 172.16.3.1.

Step 2. Configure the host PC2.

Configure the host PC2 with an IP address of 172.16.1.10/24 and a default gateway of 172.16.1.1.

Step 3. Configure the host PC3.

Configure the host PC3 with an IP address of 192.168.2.10/24 and a default gateway of 192.168.2.1.

Task 6: Test and Verify the Configurations

Step 1. Test connectivity.

Test connectivity by pinging from each host to the default gateway that has been configured for that host.

From the host PC1, is it possible to ping the default gateway? yes

From the host PC2, is it possible to ping the default gateway? yes

From the host PC3, is it possible to ping the default gateway? yes

If the answer is **no** for any of these questions, troubleshoot the configurations to find the error using the following systematic process:

1. Check the cabling. (Connection could be through a switch or directly.) Are the PCs physically connected to the correct router? yes
Are link lights blinking on all relevant ports? yes
2. Check the PC configurations. Do they match the topology diagram? yes
3. Check the router interfaces using the **show ip interface brief** command. Are all relevant interfaces up and up? yes

If your answer to all three steps is **yes**, you should be able to successfully ping the default gateway.

Step 2. Use the **ping** command to test connectivity between directly connected routers.

From router R2, is it possible to ping R1 at 172.16.2.1? [yes](#)

From router R2, is it possible to ping R3 at 192.168.1.1? [yes](#)

If the answer is **no** for any of these questions, troubleshoot the configurations to find the error using the following systematic process:

1. Check the cabling.

Are the routers physically connected? [yes](#)

Are link lights blinking on all relevant ports? [yes](#)

2. Check the router configurations.

Do they match the topology diagram in Figure 2-10? [yes](#)

Did you configure the **clock rate** command on the DCE side of the link? [yes](#)

3. Has the interface been activated or enabled? [yes](#)

4. Check the router interfaces using the **show ip interface brief** command. Are the interfaces up and up? [yes](#)

If your answer to all three steps is **yes**, you should be able to successfully ping from R2 to R1 and from R2 to R3.

Step 3. Use the **ping** command to check connectivity between devices that are not directly connected.

From the host PC3, is it possible to ping the host PC1? [no](#)

From the host PC3, is it possible to ping the host PC2? [no](#)

From the host PC2, is it possible to ping the host PC1? [no](#)

From the router R1, is it possible to ping router R3? [no](#)

These pings should all fail. Why?

[At this point, routers only know about directly connected networks.](#)

Task 7: Gather Information

Step 1. Check the status of interfaces.

Check the status of the interfaces on each router with the **show ip interface brief** command. The following output is for R2:

```
R2# show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
FastEthernet0/0    172.16.1.1     YES manual up              up
FastEthernet0/1    unassigned     YES unset  administratively down  down
Serial0/0/0        172.16.2.2     YES manual up              up
Serial0/0/1        192.168.1.2    YES manual up              up
Vlan1              unassigned     YES manual administratively down  down
```

Are all the relevant interfaces on each router activated (that is, in the up and up state)? [yes](#)

How many interfaces are activated on R1 and R3? [2](#)

Why are there three activated interfaces on R2?

[R2 has two WAN links and a LAN link.](#)

Step 2. View the routing table information for all three routers using the correct command. Begin with R1.

R1# **show ip route**

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is not set

```
       172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
```

What networks are present in the topology diagram in Figure 2-10, but not in the routing table for R1?

[172.16.1.0/24, 192.168.1.0/24, 192.168.2.0/24](#)

R2# **show ip route**

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
       default
       U - per-user static route, o - ODR
```

Gateway of last resort is not set

```
       172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C       192.168.1.0/24 is directly connected, Serial0/0/1
```

What networks are present in the topology diagram but not in the routing table for R2?

[172.16.3.0/24, 192.168.2.0/24](#)

R3# **show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
 default
 U - per-user static route, o - ODR

Gateway of last resort is not set

```
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

What networks are present in the topology diagram but not in the routing table for R3?

[172.16.1.0/24, 172.16.2.0/24, 172.16.3.0/24](#)

Why are all the networks not in the routing tables for each of the routers?

[The routers are not configured with static or dynamic routing. Therefore, routers only know about the directly connected networks.](#)

What can be added to the network so that devices that are not directly connected can ping each other?

[Static routes.](#)

Task 8: Configure a Static Route Using a Next-Hop Address

Step 1. To configure static routes with a next-hop address specified, use the following syntax:

```
Router(config)# ip route network-address subnet-mask ip-address
```

where:

- *network-address* indicates the destination network address of the remote network to be added to the routing table.
- *subnet-mask* indicates the subnet mask of the remote network to be added to the routing table. The subnet mask can be modified to summarize a group of networks.
- *ip-address* indicates what is commonly referred to as the next-hop router's IP address.

On the R3 router, configure a static route to the 172.16.1.0 network using the Serial 0/0/1 interface of R2 as the next-hop address.

```
R3(config)# ip route 172.16.1.0 255.255.255.0 192.168.1.2
R3(config)#
```

Step 2. View the routing table to verify the new static route entry.

Notice that the route is coded with an **S**, which means that the route is a static route.

R3# **show ip route**

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
       default
       U - per-user static route, o - ODR
```

Gateway of last resort is not set

```
          172.16.0.0/24 is subnetted, 1 subnets
S          172.16.1.0 [1/0] via 192.168.1.2
C          192.168.1.0/24 is directly connected, Serial0/0/1
C          192.168.2.0/24 is directly connected, FastEthernet0/0
```

With this route entered in the routing table, any packet that matches the first 24 leftmost bits of 172.16.1.0/24 will be forwarded to the next-hop router at 192.168.1.2.

What interface will R3 use to forward packets to the 172.16.1.0/24 network? [Serial 0/0/1](#)

Assume that the following packets have arrived at R3 with the indicated destination addresses. Will R3 discard the packet or forward the packet? If R3 forwards the packet, with what interface will R3 send the packet?

Packet	Destination IP	Discard or Forward?	Interface
1	172.16.2.1	Discard	—
2	172.16.1.10	Forward	S0/0/1
3	192.168.1.2	Forward	S0/0/1
4	172.16.3.10	Discard	—
5	192.168.2.10	Forward	Fa0/0

Although R3 will forward packets to destinations for which there is a route, this does not mean that a packet will arrive safely at the final destination.

Step 3. Use **ping** to check connectivity between the host PC3 and the host PC2.

From the host PC3, is it possible to ping the host PC2? [no](#)

These pings should fail. The pings will arrive at PC2 if you have configured and verified all devices through Task 7, “Gather Information.” PC2 will send a ping reply to PC3. However, the ping reply will be discarded at R2 because R2 does not have a return route to the 192.168.2.0 network in the routing table.

Step 4. On the R2 router, configure a static route to reach the 192.168.2.0 network.

What is the next-hop address to which R2 would send a packet destined for the 192.168.2.0/24 network?

```
R2(config)# ip route 192.168.2.0 255.255.255.0 192.168.1.1
R2(config)#
```

Step 5. View the routing table to verify the new static route entry.

Notice that the route is coded with an **S**, which means the route is a static route.

```
R2# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
       default
       U - per-user static route, o - ODR
```

```
Gateway of last resort is not set
```

```
172.16.0.0/24 is subnetted, 2 subnets
C      172.16.1.0 is directly connected, FastEthernet0/0
C      172.16.2.0 is directly connected, Serial0/0/0
C      192.168.1.0/24 is directly connected, Serial0/0/1
S      192.168.2.0/24 [1/0] via 192.168.1.1
```

Step 6. Use **ping** to check connectivity between the host PC3 and the host PC2.

From the host PC3, is it possible to ping the host PC2? **yes**

This ping should be successful.

Task 9: Configure a Static Route Using an Exit Interface

To configure static routes with an exit interface specified, use the following syntax:

```
Router(config)# ip route network-address subnet-mask exit-interface
```

where:

- *network-address* indicates the destination network address of the remote network to be added to the routing table.
- *subnet-mask* indicates the subnet mask of the remote network to be added to the routing table. The subnet mask can be modified to summarize a group of networks.
- *exit-interface* indicates the outgoing interface that would be used in forwarding packets to the destination network.

Step 1. On the R3 router, configure a static route.

On the R3 router, configure a static route to the 172.16.2.0 network using the Serial 0/0/0 interface of the R3 router as the exit interface.

```
R3(config)# ip route 172.16.2.0 255.255.255.0 Serial0/0/1
R3(config)#
```

Step 2. View the routing table to verify the new static route entry.

```
R3# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
       default
       U - per-user static route, o - ODR
```

```
Gateway of last resort is not set
```

```

          172.16.0.0/24 is subnetted, 2 subnets
S          172.16.1.0 [1/0] via 192.168.1.2
S          172.16.2.0 is directly connected, Serial0/0/1
C          192.168.1.0/24 is directly connected, Serial0/0/1
C          192.168.2.0/24 is directly connected, FastEthernet0/0
```

Use the **show running-config** command to verify the static routes that are currently configured on R3.

```
R3# show running-config
```

```
Building configuration...
```

```
<output omitted>
```

```
!
hostname R3
!
interface FastEthernet0/0
ip address 192.168.2.1 255.255.255.0
!
interface Serial0/0/0
no ip address
shutdown
!
interface Serial0/0/1
ip address 192.168.1.1 255.255.255.0
!
ip route 172.16.1.0 255.255.255.0 192.168.1.2
ip route 172.16.2.0 255.255.255.0 Serial0/0/1
!
end
```

How would you remove either of these routes from the configuration?

Use the **no** form of the command. For example, **no ip route 172.16.2.0 255.255.255.0 S 0/0/1**.

Step 3. On the R2 router, configure a static route.

On the R2 router, configure a static route to the 172.16.3.0 network using the Serial 0/0/0 interface of the R2 router as the exit interface.

```
R2(config)# ip route 172.16.3.0 255.255.255.0 Serial0/0/0
R2(config)#
```

Step 4. View the routing table to verify the new static route entry.

```
R2# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
       default
       U - per-user static route, o - ODR
```

```
Gateway of last resort is not set
```

```
       172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
S       172.16.3.0 is directly connected, Serial0/0/0
C       192.168.1.0/24 is directly connected, Serial0/0/1
S       192.168.2.0/24 [1/0] via 192.168.1.1
```

At this point, R2 has a complete routing table with valid routes to all five networks shown in the topology diagram.

Does this mean that R2 can receive ping replies from all destinations shown in the topology diagram? no

Why or why not?

Although R2 can route to all networks in the topology, this does not guarantee that other routers can route back to R2.

Step 5. Use **ping** to check connectivity between the host PC2 and PC1.

This ping should fail because the R1 router does not have a return route to the 172.16.1.0 network in the routing table.

Task 10: Configure a Default Static Route

In the previous steps, you configured the router for specific destination routes. But could you do this for every route on the Internet? No. The router and you would be overwhelmed. To minimize the size of the routing tables, add a default static route. A router uses the default static route when there is not a better, more specific route to a destination.

Instead of filling the routing table of R1 with static routes, you could assume that R1 is a *stub router*. This means that R2 is the default gateway for R1. If R1 has packets to route that do not belong to any of R1's directly connected networks, R1 should send the packet to R2. However, you must explicitly configure R1 with a default route before it will send packets with unknown destinations to R2. Otherwise, R1 discards packets with unknown destinations.

To configure a default static route, use the following syntax:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 { ip-address | interface }
```

Step 1. Configure the R1 router with a default route.

Configure the R1 router with a default route using the Serial 0/0/0 interface of R1 as the next-hop interface.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 serial 0/0/0
```

Step 2. View the routing table to verify the new static route entry.

```
R1# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate
       default
       U - per-user static route, o - ODR
```

```
Gateway of last resort is 172.16.2.2 to network 0.0.0.0
```

```
172.16.0.0/24 is subnetted, 2 subnets
C      172.16.2.0 is directly connected, Serial0/0/0
C      172.16.3.0 is directly connected, FastEthernet0/0
S*    0.0.0.0/0 is directly connected, Serial0/0/0
```

Note that the R1 router now has a default route, the *gateway of last resort*, and will send all unknown traffic out Serial 0/0/0, which is connected to R2.

Step 3. Use **ping** to check connectivity between the host PC2 and PC1.

From the host PC2, is it possible to ping PC1? **yes**

The ping should be successful this time because the R1 router can return the packet using the default route.

From the host PC3, is it possible to ping the host PC1? **no**

Is there a route to the 172.16.3.0 network in the routing table on the R3 router? **no**

Task 11: Configure a Summary Static Route

You could configure another static route on R3 for the 172.16.3.0 network. However, you already have two static routes to 172.16.2.0/24 and 172.16.1.0/24. Because these networks are so close together, you can summarize them into one route. Again, doing this helps reduce the size of routing tables, which makes the route lookup process more efficient.

Looking at the three networks at the binary level, you can see a common boundary at the 22nd bit from the left.

```
172.16.1.0    10101100.00010000.00000001.00000000
172.16.2.0    10101100.00010000.00000010.00000000
172.16.3.0    10101100.00010000.00000011.00000000
```

The prefix portion will include 172.16.0.0, because this would be the prefix if you turned off all the bits to the right of the 22nd bit.

```
Prefix      172.16.0.0
```

To mask the first 22 leftmost bits, use a mask with 22 bits turned on from left to right:

```
Bit Mask    11111111.11111111.11111100.00000000
```

This mask, in dotted decimal format, is 255.255.252.0.

Step 1. Configure the summary static route on the R3 router.

The network to be used in the summary route is 172.16.0.0/22:

```
R3(config)# ip route 172.16.0.0 255.255.252.0 192.168.1.2
```

Step 2. Verify that the summary route is installed in the routing table.

```
R3# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
S      172.16.0.0/22 [1/0] via 192.168.1.2
S      172.16.1.0/24 [1/0] via 192.168.1.2
S      172.16.2.0/24 is directly connected, Serial0/0/1
C      192.168.1.0/24 is directly connected, Serial0/0/1
C      192.168.2.0/24 is directly connected, FastEthernet0/0
```

Configuring a summary route on R3 did not remove the static routes configured earlier because these routes are more specific routes. They both use the /24 mask, whereas the new summary will be using a /22 mask. To reduce the size of the routing table, you can now remove the more specific /24 routes.

Step 3. Remove static routes on R3.

Remove the two static routes that are currently configured on R3 by using the **no** form of the command.

```
R3(config)# no ip route 172.16.1.0 255.255.255.0 192.168.1.2
R3(config)# no ip route 172.16.2.0 255.255.255.0 Serial0/0/1
```

Step 4. Verify that the routes are no longer in the routing table.

R3# **show ip route**

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is not set

```
          172.16.0.0/22 is subnetted, 1 subnets
S       172.16.0.0 [1/0] via 192.168.1.2
C       192.168.1.0/24 is directly connected, Serial0/0/1
C       192.168.2.0/24 is directly connected, FastEthernet0/0
```

R3 now only has one route to any host belonging to networks 172.16.0.0/24, 172.16.1.0/24, 172.16.2.0/24, and 172.16.3.0/24. Traffic destined for these networks will be sent to R2 at 192.168.1.2.

Step 5. Use **ping** to check connectivity between the host PC3 and PC1.

From the host PC3, is it possible to ping the host PC1? **yes**

This ping should be successful this time because there is a route to the 172.16.3.0 network on the R3 router, and the R1 router can return the packet using the default route.

Task 12: Summary, Reflection, and Documentation

With the completion of this lab, you have

- Configured your first network with a combination of static and default routing to provide full connectivity to all networks
- Observed how a route is installed in the routing table when you correctly configure and activate an interface
- Learned how to statically configure routes to destinations that are not directly connected
- Learned how to configure a default route that is used to forward packets to unknown destinations
- Learned how to summarize a group of networks into one static route to reduce the size of a routing table

Finally, you should document your network implementation. On each router, capture the following command output to a text (.txt) file and save for future reference.

```
show running-config
show ip route
show ip interface brief
```

If you need to review the procedures for capturing command output, see “Lab 1-1: Cabling a Network and Basic Router Configuration (1.5.1).”

Task 13: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Task 14: Challenge

In the following exercise, fill in the blanks to document the process as the ping travels from source to destination.

1. The ICMP process on PC3 formulates a ping request to PC2 and sends the reply to the IP process.
2. The IP process on PC3 encapsulates the ping packet with a source IP address of 192.168.2.10 and destination IP address of 172.16.1.10.
3. PC3 then frames the packet with the source MAC address of (indicate device name) PC3 and the destination MAC address of (indicate device name) R3.
4. Next, PC3 sends the frame out on the media as an encoded bit stream.
5. R3 receives the bit stream on its Fa0/0 interface. Because the destination MAC address matches the receiving interface’s MAC address, R3 strips off the Ethernet header.
6. R3 looks up the destination network address 172.16.1.0/24 in its routing table. This destination has a next-hop IP address of 192.168.1.2. The next-hop IP address is reachable out interface S0/0/1.
7. R3 encapsulates the packet in an HDLC frame and forwards the frame out the correct interface. (Because this is a point-to-point link, no address is needed. However, the address field in the HDLC packet contains the value 0x8F.)
8. R2 receives the frame on the S0/0/1 interface. Because the frame is HDLC, R2 strips off the header and looks up the network address 172.16.1.0/24 in its routing table. This destination address is directly connected to the Fa0/0 interface.
9. R2 encapsulates the ping request in a frame with the source MAC address of (indicated device name) R2 and the destination MAC address of (indicate device name) PC2.
10. R2 then sends the frame out on the media as an encoded bit stream.
11. PC2 receives the bit stream on its Ethernet (NIC) interface. Because the destination MAC address matches the MAC address of PC2, PC2 strips off the Ethernet header.
12. The IP process on PC2 examines the 172.16.1.10 IP address to make sure that it matches its own IP address. Then PC2 passes the data to the ICMP process.

13. The ICMP process on PC2 formulates a ping reply to PC3 and sends the reply to the IP process.
14. The IP process on PC2 encapsulates the ping packet with a source IP address of [172.16.1.10](#) and destination IP address of [192.168.2.10](#).
15. PC2 then frames the packet with the source MAC address of (indicate device name) [PC2](#) and the destination MAC address of (indicate device name) [R2](#).
16. PC2 then sends the frame out on the media as an encoded bit stream.
17. R2 receives the bit stream on its [Fa0/0](#) interface. Because the destination MAC address matches the receiving interface's MAC address, R2 strips off the Ethernet header.
18. R2 looks up the destination network address [192.168.2.0/24](#) in its routing table. This destination has a next-hop IP address of [192.168.1.1](#). The next-hop IP address is reachable out interface [S0/0/1](#).
19. R2 encapsulates the packet in an HDLC frame and forwards the frame out the correct interface. (Because this is a point-to-point link, no address is needed. However, the address field in the HDLC packet contains the value 0x8F.)
20. R3 receives the frame on the [S0/0/1](#) interface. Because the frame is HDLC, R3 strips off the header and looks up the destination network address [192.168.2.0/24](#) in its routing table. This destination address is directly connected to the [Fa0/0](#) interface.
21. R3 encapsulates the ping request in a frame with the source MAC address of (indicated device name) [R3](#) and the destination MAC address of (indicate device name) [PC3](#).
22. R3 then sends the frame out on the media as an encoded bit stream.
23. PC3 receives the bit stream on its [Ethernet \(NIC\)](#) interface. Because the destination MAC address matches the MAC address of PC3, PC3 strips off the Ethernet header.
24. The IP process on PC3 examines the [192.168.2.10](#) IP address to make sure that it matches its own IP address. Then PC3 passes the data to the ICMP process.
25. ICMP sends a "success" message to the requesting application.



Packet Tracer Companion: Basic Static Route Configuration (2.8.1)

You can now open the file LSG02-Lab281.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.



Lab 2-2: Challenge Static Route Configuration (2.8.2)

Upon completion of this lab, you will be able to

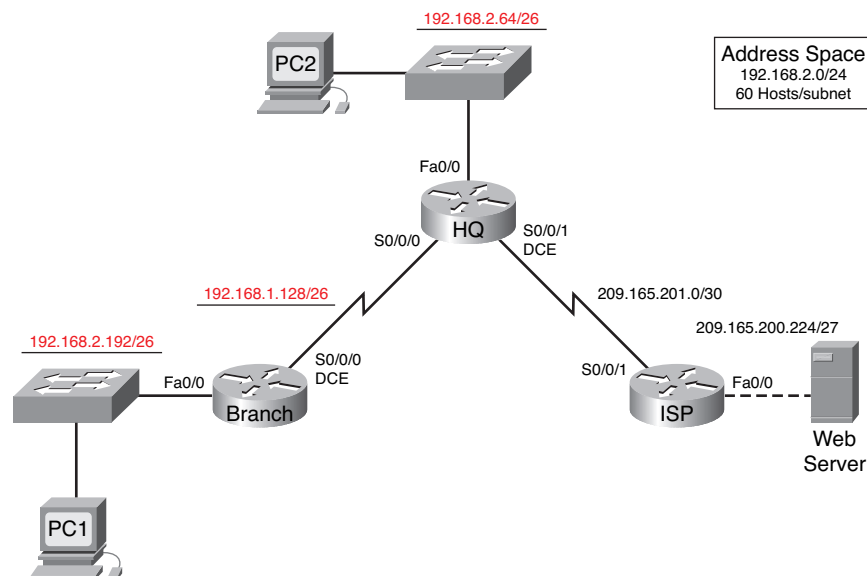
- Subnet an address space given requirements
- Assign appropriate addresses to interfaces and document
- Cable a network according to the topology diagram

- Erase the startup configuration and reload a router to the default state
- Perform basic configuration tasks on a router
- Configure and activate serial and Ethernet interfaces
- Determine appropriate static, summary, and default routes
- Test and verify configurations
- Reflect on and document the network implementation

Scenario

In this lab activity, you will be given a network address that must be subnetted to complete the addressing of the network shown in the topology diagram in Figure 2-11. The addressing for the LAN connected to the ISP router and the link between the HQ and ISP routers has already been completed. Static routes will also need to be configured so that hosts on networks that are not directly connected will be able to communicate with each other.

Figure 2-11 Topology Diagram for Lab 2-2 (Answer)



Task 1: Subnet the Address Space

Step 1. Examine the network requirements.

The addressing for the LAN connected to the ISP router and the link between the HQ and ISP routers has already been completed. You have been given the 192.168.2.0/24 address space to complete the network design. Subnet this network to provide enough IP addresses to support 60 hosts.

Step 2. Consider the following questions when creating your network design:

How many subnets need to be created from the 192.168.2.0/24 network? **3**

What are the network addresses of the subnets?

Subnet 0: **192.168.2.0/26**

Subnet 1: **192.168.2.64/26**

Subnet 2: [192.168.2.128/26](#)

Subnet 3: [192.168.2.192/26](#)

What is the subnet mask for these networks in dotted decimal format? [255.255.255.192](#)

What is the subnet mask for the network in slash format? [/26](#)

How many usable hosts are there per subnet? [62](#)

Step 3. Assign subnetwork addresses to the topology diagram in Figure 2-11.

1. Assign subnet 1 to the LAN attached to HQ.
2. Assign subnet 2 to the WAN link between HQ and BRANCH.
3. Assign subnet 3 to the LAN attached to BRANCH.
4. Subnet 0 will be available for future expansion.

Task 2: Determine Interface Addresses

Step 1. Assign appropriate addresses to the device interfaces.

1. Assign the first valid host address in subnet 1 to the LAN interface on HQ.
2. Assign the last valid host address in subnet 1 to PC2.
3. Assign the first valid host address in subnet 2 to the WAN interface on BRANCH.
4. Assign the second valid host address in subnet 2 to the WAN interface on HQ.
5. Assign the first valid host address in subnet 3 to the LAN interface of BRANCH.
6. Assign the last valid host address in subnet 3 to PC1.

Step 2. Document the addresses to be used in the Table 2-4.

Table 2-4 Addressing Table for Lab 2-2

Device	Interface	IP Address	Subnet Mask	Default Gateway
BRANCH	Fa0/0	192.168.2.193	255.255.255.192	—
	S0/0/0	192.168.2.129	255.255.255.192	—
HQ	Fa0/0	192.168.2.65	255.255.255.192	—
	S0/0/0	192.168.2.130	255.255.255.192	—
	S0/0/1	209.165.201.2	255.255.255.252	—
ISP	Fa0/0	209.165.200.225	255.255.255.224	—
	S0/0/1	209.165.201.1	255.255.255.252	—
PC1	NIC	192.168.2.254	255.255.255.192	192.168.2.193
PC2	NIC	192.168.2.126	255.255.255.192	192.168.2.65
Web Server	NIC	209.165.200.254	255.255.255.224	209.165.200.225

Task 3: Prepare the Network

Step 1. Cable a network that is similar to the one in the topology diagram in Figure 2-11.

You can use any current router in your lab as long as it has the required interfaces as shown in the topology.

Step 2. Clear any existing configurations on the routers.

Task 4: Perform Basic Router Configurations

Perform basic configuration of the BRANCH, HQ, and ISP routers according to the following guidelines:

1. Configure the router host name.
2. Disable DNS lookup.
3. Configure an EXEC mode password.
4. Configure a message-of-the-day banner.
5. Configure a password for console connections.
6. Configure a password for VTY connections.
7. Synchronize unsolicited messages and debug output with solicited output and prompts for the console and virtual terminal lines.
8. Configure an EXEC timeout of 15 minutes.

Task 5: Configure and Activate Serial and Ethernet Addresses

Step 1. Configure the interfaces on the BRANCH, HQ, and ISP routers.

Configure the interfaces on the BRANCH, HQ, and ISP routers with the IP addresses from the table provided under the topology diagram. When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 2. Configure the Ethernet interfaces.

Configure the Ethernet interfaces on PC1, PC2, and the web server with the IP addresses from the table provided under the topology diagram.

Task 6: Verify Connectivity to Next-Hop Device

You should *not* have connectivity between end devices yet. However, you can test connectivity between two routers and between an end device and its default gateway.

Step 1. Verify BRANCH and HQ connectivity.

Verify that BRANCH can ping across the WAN link to HQ and that HQ can ping across the WAN link that it shares with ISP.

Step 2. Verify PC1, PC2, and web server connectivity.

Verify that PC1, PC2, and the web server can ping their respective default gateways.

Task 7: Configure Static Routing on BRANCH

Step 1. Consider the type of static routing that is needed on BRANCH.

What networks are present in the BRANCH routing table? List the networks with slash notation.

192.168.2.128/26

192.168.2.192/26

What networks are missing from the BRANCH routing table? List the networks with slash notation.

192.168.2.64/26

209.165.201.0/30

209.165.200.224/27

Can one summary route that includes all the missing networks be created? no

How many WAN routes are available to traffic leaving the LAN connected to BRANCH? 1

Step 2. Configure BRANCH with a default static route pointing to HQ.

Because BRANCH is a stub router, you should configure BRANCH with a default static route pointing to HQ. Record the command to configure a default static route using the appropriate exit interface.

```
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 serial0/0/0
```

Step 3. View the routing table of BRANCH to verify the new static route entry.

You should see a gateway of last resort set on BRANCH.

Without testing it first, do you think that PC1 can now successfully ping PC2? no

Why or why not?

PC1 cannot successfully ping PC2. Although PC2 will receive the ping packet from PC1 and send a ping reply to HQ, HQ does not yet know how to route packets back to PC1's subnet.

Task 8: Configure Static Routing on HQ

Step 1. Consider the type of static routing that is needed on HQ.

What networks are present in the HQ routing table? List the networks with slash notation.

192.168.2.128/26

192.168.2.64/26

209.165.201.0/30

What networks are missing from the HQ routing table? List the networks with slash notation.

192.168.2.192/26

209.165.200.224/27

Can one summary route that includes all the missing networks be created? no

HQ is in a unique position as the hub router in this hub-and-spoke topology. Traffic from the BRANCH LAN destined for the Internet must pass through HQ. HQ must be able to send any traffic for which it does not have a route to ISP. What kind of route would you need to configure on HQ to solve this problem?

A default static route pointing to ISP

HQ is also the intermediary for any traffic from the Internet destined for the BRANCH LAN. Therefore, HQ must be able to route to that LAN. What kind of route would you need to configure on HQ to solve this problem?

A static route pointing to the BRANCH LAN

Step 2. Configure HQ with a static route.

Configure HQ with a static route to the BRANCH LAN using the Serial 0/0/0 interface of HQ as the exit interface. Record the command that you used.

HQ(config)# ip route 192.168.2.192 255.255.255.192 serial 0/0/0

Step 3. Configure HQ with a default static route.

Configure the HQ router with a default static route pointing to ISP using the next-hop IP address. Record the command you used.

HQ(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.1

Step 4. View the routing table of HQ to verify the new static route entries.

Without testing it first, do you think that PC1 can now successfully ping PC2? yes

Why or why not?

PC1 can now successfully ping PC2. HQ now has a route back to the BRANCH LAN.

Without testing it first, do you think that PC1 or PC2 can now successfully ping the web server? no

Why or why not?

PC1 and PC2 cannot successfully ping the web server. Although the web server will receive the ping packets from PC1 and PC2 (HQ is sending default traffic to ISP), ISP does not yet know how to route packets back to HQ or BRANCH networks.

Task 9: Configure Static Routing on ISP

In a real-world implementation of this topology, you would not be configuring the ISP router. However, your service provider is an active partner in solving your connectivity needs. Service provider administrators are human, too, and make mistakes. Therefore, it is important that you understand the types of errors an ISP could make that would cause your networks to lose connectivity.

Step 1. Consider the type of static routing that is needed on ISP.

What networks are present in the ISP routing table? List the networks with slash notation.

[209.165.201.0/30](#)

[209.165.200.224/27](#)

What networks are missing from the ISP routing table? List the networks with slash notation.

[192.168.2.64/26](#)

[192.168.2.128/26](#)

[192.168.2.192/26](#)

Can one summary route that includes all the missing networks be created? [yes](#)

Step 2. Configure ISP with a summary static route.

Using the next-hop IP address, configure ISP with a summary static route that includes all the subnets that are missing from the routing table. Record the command that you used.

[ISP\(config\)# ip route 192.168.2.0 255.255.255.0 209.165.201.2](#)

Step 3. View the routing table of R3 to verify the new static route entry.

Task 10: Verify the Configurations

Answer the following questions to verify that the network is operating as expected.

From PC2, is it possible to ping PC1? [yes](#)

From PC2, is it possible to ping the web server? [yes](#)

From PC1, is it possible to ping the web server? [yes](#)

The answer to these questions should be **yes**. If any of the above pings failed, check your physical connections and configurations. For a review of basic troubleshooting techniques, see “Lab 1-1: Cabling a Network and Basic Router Configuration (1.5.1).”

What routes are present in the routing table of BRANCH?

[192.168.2.128/26](#)

[192.168.2.192/26](#)

[0.0.0.0/0](#)

What routes are present in the routing table of HQ?

[192.168.2.64/26](#)

[192.168.2.128/26](#)

[192.168.2.192/26](#)

[209.165.201.0/30](#)

[0.0.0.0/0](#)

What routes are present in the routing table of ISP?

[192.168.2.0/24](#)

[209.165.200.0/27](#)

[209.165.201.0/30](#)

Task 11: Reflection

If a default static route was not configured on BRANCH, how many individual static routes would be needed for hosts on the BRANCH LAN to communicate with all the networks in the topology diagram in Figure 2-11? [3](#)

If a summary static route was not configured on ISP, how many individual static routes would be needed for hosts on the ISP LAN to communicate with all the networks in the topology diagram? [3](#)

Task 12: Document the Router Configurations

On each router, capture the following command output to a text (.txt) file and save for future reference:

- Running configuration
- Routing table
- Interface summarization

Task 13: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.



Packet Tracer Companion: Challenge Static Route Configuration (2.8.2)

You can now open the file LSG02-Lab282.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.



Lab 2-3: Troubleshooting Static Routes (2.8.3)

Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Load the routers with supplied scripts

- Discover points where the network is not converged
- Gather information about errors in the network
- Propose solutions to network errors
- Implement solutions to network errors
- Document the corrected network

Scenario

In this lab, you will begin by loading configuration scripts on each of the routers. These scripts contain errors that will prevent end-to-end communication across the network. You will need to troubleshoot each router to determine the configuration errors, and then use the appropriate commands to correct the configurations. When you have corrected all the configuration errors, all the hosts on the network should be able to communicate with each other.

Figure 2-12 shows the topology for this lab, and Table 2-5 shows the IP addressing, subnet, and default gateway information for the devices in the topology.

Figure 2-12 Topology Diagram for Lab 2-3

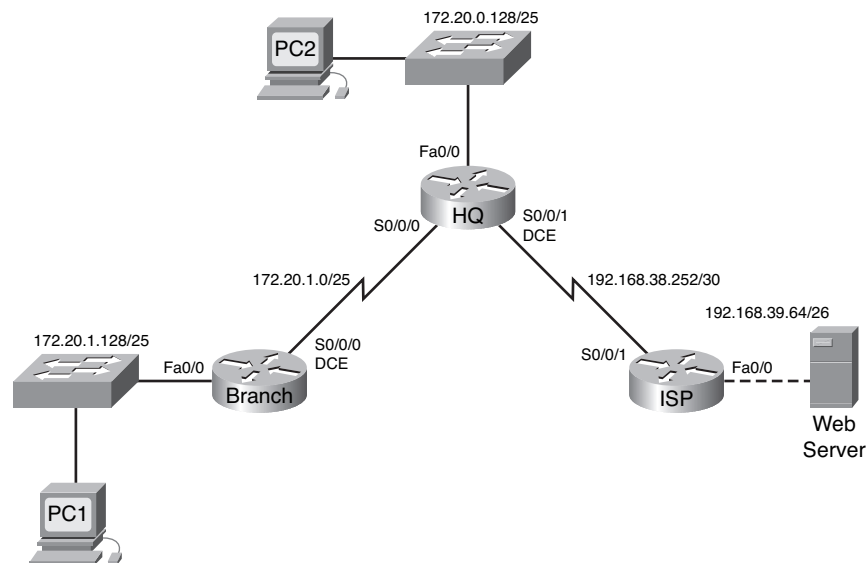


Table 2-5 Addressing Table for Lab 2-3

Device	Interface	IP Address	Subnet Mask	Default Gateway
BRANCH	Fa0/0	172.20.1.129	255.255.255.128	—
	S0/0/0	172.20.1.1	255.255.255.128	—
HQ	Fa0/0	172.20.0.129	255.255.255.128	—
	S0/0/0	172.20.1.2	255.255.255.128	—
	S0/0/1	192.168.38.254	255.255.255.252	—
ISP	FA0/0	192.168.39.65	255.255.255.192	—
	S0/0/1	192.168.38.253	255.255.255.252	—

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC1	NIC	172.20.1.135	255.255.255.128	172.20.1.129
PC2	NIC	172.20.0.135	255.255.255.128	172.20.0.129
Web Server	NIC	192.168.39.70	255.255.255.192	192.168.39.65

Task 1: Cable, Erase, and Reload the Routers

Step 1. Cable a network that is similar to the one in the topology diagram shown in Figure 2-12.

Step 2. Clear the configuration on each router.

Clear the configuration on each of routers using the **erase startup-config** command and then reload the routers. Answer **no** if asked to save changes.

Task 2: Load Routers with the Supplied Scripts

Step 1. Load the following script onto the BRANCH router:

```
hostname BRANCH
!
!
no ip domain-lookup
!
interface FastEthernet0/0
 ip address 172.20.1.129 255.255.255.128
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 ip address 172.20.1.1 255.255.255.128
 clock rate 64000
 no shutdown
!
ip route 0.0.0.0 0.0.0.0 172.20.0.129
```

!The destination in the **ip route** command should be 172.20.1.2.

```
!
!
!
!
line con 0
line vty 0 4
 password cisco
 login
!
end
```

Corrected Script:

```
hostname BRANCH
```

```
!
```

```
!  
no ip domain-lookup  
!  
interface FastEthernet0/0  
  ip address 172.20.1.129 255.255.255.128  
  duplex auto  
  speed auto  
  no shutdown  
!  
interface Serial0/0/0  
  ip address 172.20.1.1 255.255.255.128  
  clock rate 64000  
  no shutdown  
!  
ip route 0.0.0.0 0.0.0.0 172.20.1.2  
!  
!  
!  
!  
line con 0  
line vty 0 4  
password cisco  
  login  
!  
end
```

The error in the student script is that the destination address in the default route is incorrect. The correct command is **ip route 0.0.0.0 0.0.0.0 172.20.1.2**.

Step 2. Load the following script onto the HQ router:

```
hostname HQ  
!  
!  
no ip domain-lookup  
!  
interface FastEthernet0/0  
  ip address 172.20.0.129 255.255.255.128  
  duplex auto  
  speed auto  
  no shutdown  
!  
interface Serial0/0/0  
  ip address 172.20.1.2 255.255.255.128  
  no shutdown  
!  
interface Serial0/0/1  
  ip address 192.168.38.254 255.255.255.252
```

!The **clock rate 64000** command is missing.

```
no shutdown
!  
ip route 192.168.39.64 255.255.255.192 192.168.38.253
```

!The **ip route** statement for the BRANCH LAN is missing.

```
!  
!  
!  
line con 0  
line vty 0 4  
password cisco  
login  
!  
end
```

Corrected Script:

```
hostname HQ  
!  
!  
no ip domain-lookup  
!  
interface FastEthernet0/0  
ip address 172.20.0.129 255.255.255.128  
duplex auto  
speed auto  
no shutdown  
!  
interface Serial0/0/0  
ip address 172.20.1.2 255.255.255.128  
no shutdown  
!  
interface Serial0/0/1  
ip address 192.168.38.254 255.255.255.252  
clock rate 64000  
no shutdown  
!  
ip route 192.168.39.64 255.255.255.192 192.168.38.253  
ip route 172.20.1.128 255.255.255.128 17.20.1.1  
!  
!  
!  
!  
line con 0  
line vty 0 4  
password cisco
```

```
login
!  
end
```

The errors in the student scripts are as follows:

- The clock rate is not configured on the Serial 0/0/1 interface.
- The **ip route** statement for the BRANCH LAN is missing. The command should be **ip route 172.20.1.128 255.255.255.128 Serial0/0/0** or **ip route 172.20.1.128 255.255.255.128 172.20.1.1**.

Step 3. Load the following script onto the ISP router:

```
hostname ISP
!  
!  
no ip domain-lookup
!  
interface FastEthernet0/0
  ip address 192.168.39.65 255.255.255.192
!  
!  
!no shutdown
!  
interface Serial0/0/1
  ip address 192.168.38.253 255.255.255.252
  no shutdown
!  
ip route 172.20.0.0 255.255.255.0 192.168.38.254
```

!The subnet mask for this route should be 255.255.254.0.

```
!  
!  
!  
line con 0
line vty 0 4
password cisco
login
!  
end
```

Corrected Script:

```
hostname ISP
!  
!  
no ip domain-lookup
!  
interface FastEthernet0/0
  ip address 192.168.39.65 255.255.255.192
  no shutdown
!  
interface Serial0/0/1
```



```

ip address 192.168.38.253 255.255.255.252
no shutdown
!
ip route 172.20.0.0 255.255.254.0 192.168.38.254
!
!
!
!
!
line con 0
line vty 0 4
password cisco
login
!
end

```

The errors in the student scripts are as follows:

- The **no shutdown** command is missing from the FastEthernet0/0 interface.
- The incorrect subnet mask is used in the **ip route** statement.

Task 3: Troubleshoot the BRANCH Router

Step 1. Begin troubleshooting at the host connected to the BRANCH router.

From the host PC1, is it possible to ping PC2? no

From the host PC1, is it possible to ping the web server on the ISP LAN? no

From the host PC1, is it possible to ping the default gateway? yes

Step 2. Examine the BRANCH router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the status of the interfaces? no

If there are any problems with the status of the interfaces, record any commands that will be necessary to correct the configuration errors.

Step 3. If you have recorded any commands, apply them to the router configuration now.

Step 4. View a summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors? **no**

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

Step 5. Troubleshoot the static routing configuration on the BRANCH router.

Begin by viewing the routing table.

What routes are shown in the routing table?

172.20.1.0 is directly connected, Serial0/0/0

172.20.1.128 is directly connected, FastEthernet0/0

Are there any problems with the routing table?

The static default route to the HQ router is missing from the routing table because the destination address in the **ip route** statement is incorrect.

If there are any problems with the routing table, record any commands that will be necessary to correct the configuration errors.

```
BRANCH(config)# no ip route 0.0.0.0 0.0.0.0 172.20.0.129
```

```
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 172.20.1.2
```

Step 6. If you have recorded any commands, apply them to the router configuration now.

Step 7. View the routing information.

If any changes were made to the configuration in the previous step, view routing table again.

Does the information in the routing table indicate any configuration errors? **no**

If the answer is **yes**, troubleshoot the routing table again.

Step 8. Attempt to ping between the hosts again.

From the host PC1, is it possible to ping PC2? **no**

From the host PC1, is it possible to ping the web server on the ISP LAN? **no**

From the host PC1, is it possible to ping the Serial 0/0/0 interface of HQ? **yes**

Task 4: Troubleshoot the HQ Router

Step 1. Begin troubleshooting at the host connected to the HQ router.

From the host PC2, is it possible to ping PC1? no

From the host PC2, is it possible to ping the web server on the ISP LAN? no

From the host PC2, is it possible to ping the default gateway? yes

Step 2. Examine the HQ router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the status of the interfaces?

Yes, the interface status and the protocol on Serial 0/0/1 are both down.

If there are any problems with the status of the interfaces, record any commands that will be necessary to correct the configuration errors.

HQ(config)# interface Serial0/0/1

HQ(config-if)# clock rate 64000

Step 3. If you have recorded any commands above, apply them to the router configuration now.

Step 4. View a summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors? no

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

Step 5. Troubleshoot the static routing configuration on the HQ router.

Begin by viewing the routing table.

What routes are shown in the routing table?

172.20.1.0 is directly connected, Serial0/0/0

192.168.38.252 is directly connected, Serial0/0/1

Are there any problems with the routing table?

The route for the BRANCH LAN, 172.20.1.128/25, is missing from the routing table.

If there are any problems with the routing table, record any commands that will be necessary to correct the configuration errors.

HQ(config)# ip route 172.20.1.128 255.255.255.128 172.20.1.1

Step 6. If you have recorded any commands above, apply them to the router configuration now.

Step 7. View the routing information.

If any changes were made to the configuration in the previous step, view the routing table again.

Does the information in the routing table indicate any configuration errors? no

If the answer is **yes**, troubleshoot the routing table again.

Step 8. Attempt to ping between the hosts again.

From the host PC2, is it possible to ping PC1? yes

From the host PC2, is it possible to ping the Serial 0/0/1 interface of the ISP router? yes

From the host PC1, is it possible to ping the web server on the ISP LAN? no

Task 5: Troubleshoot the ISP Router

Step 1. Begin troubleshooting at the host connected to the ISP router.

From the web server on the ISP LAN, is it possible to ping PC1? no

From the web server on the ISP LAN, is it possible to ping PC2? no

From the web server on the ISP LAN, is it possible to ping the default gateway? yes

Step 2. Examine the ISP router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the status of the interfaces?

The FastEthernet 0/0 interface is administratively down.

If there are any problems with the status of the interfaces, record any commands that will be necessary to correct the configuration errors.

ISP(config)# interface FastEthernet0/0

ISP(config-if)# no shutdown

Step 3. If you have recorded any commands, apply them to the router configuration now.

Step 4. View a summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors? no

If the answer is yes, troubleshoot the interface status of the interfaces again.

Step 5. Troubleshoot the static routing configuration on the ISP router.

Begin by viewing the routing table.

What routes are shown in the routing table?

172.20.0.0 [1/0] via 192.168.38.254

192.168.38.252 is directly connected, Serial0/0/1

192.168.39.64 is directly connected, FastEthernet0/0

Are there any problems with the routing table?

The wrong subnet mask is used in the ip route statement for the 172.0.0.0 network.

If there are any problems with the routing table, record any commands that will be necessary to correct the configuration errors.

ISP(config)# no ip route 172.20.0.0 255.255.255.0 192.168.38.254

ISP(config)# ip route 172.20.0.0 255.255.254.0 192.168.38.254

- Step 6.** If you have recorded any commands, apply them to the router configuration now.
- Step 7.** View the routing information.
- If any changes were made to the configuration in the previous step, view routing table again.
- Does the information in the routing table indicate any configuration errors? **no**
- If the answer is **yes**, troubleshoot the routing table again.
- Step 8.** Attempt to ping between the hosts again.
- From the web server on the ISP LAN, is it possible to ping PC1? **yes**
- From the web server on the ISP LAN, is it possible to ping PC2? **yes**
- From the Web Server on the ISP LAN, is it possible to ping the WAN interface of the BRANCH router? **yes**

Task 6: Reflection

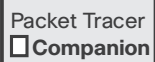
There were a number of configuration errors in the scripts that were provided for this lab. Use the space below to write a brief description of the errors that you found.

Task 7: Documentation

On each router, capture the output from the following commands to a text (.txt) file and save for future reference.

```
show running-config
show ip route
show ip interface brief
```

If you need to review the procedures for capturing command output, see “Lab 1-1: Cabling a Network and Basic Router Configuration (1.5.1).”



Packet Tracer Companion: Troubleshooting Static Routes (2.8.3)

You can now open the file LSG02-Lab283.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.

Packet Tracer Skills Integration Challenge

Introduction

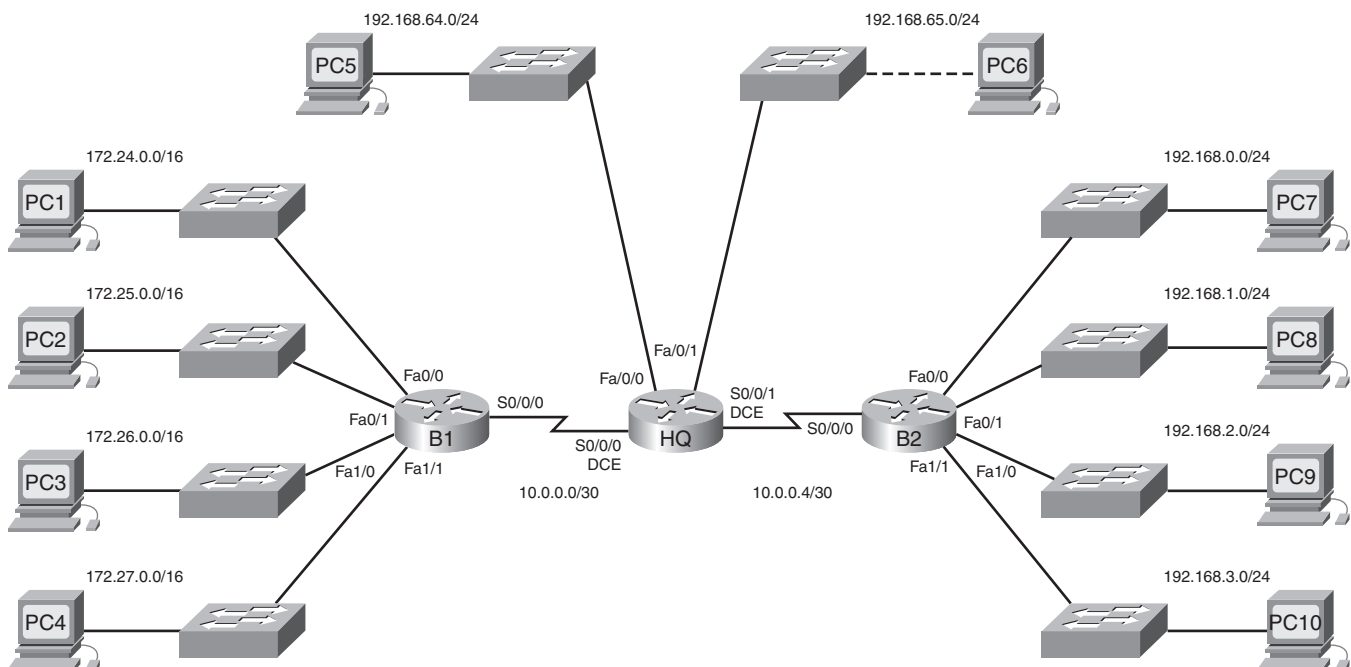
This activity focuses on basic device configurations and static routing. The addressing scheme has already been determined. After you configure all devices, test for end-to-end connectivity and examine your configuration. Open the file LSG02-PTskills2.pka on the CD-ROM that accompanies this book.

Upon completion of this lab, you will be able to

- Cable the devices
- Apply a basic configuration to the devices
- Configure static and default routing
- Test connectivity and examine the configuration

Figure 2-13 shows the topology for this lab.

Figure 2-13 Packet Tracer Skills Integration Challenge Topology



Task 1: Cable the Devices

Cable the WAN. HQ s0/0/0 connects to B1 S0/0/0 and HQ s0/0/01 connects to B2 s0/0/0. HQ is the DCE side of both WAN links. HQ is the DCE side of both WAN links.

Task 2: Apply a Basic Configuration

Configure the routers with basic configurations including addressing.

- For the WAN links, assign the first address to HQ and the second address to the other router.
- For the LANs, assign the first address to the router interface. Make sure to also configure hostnames.
- Assign the .10 address to the PCs. Make sure to include the default gateway.
- Use **cisco** as the line passwords and **class** as the secret password.
- Use **64000** as the clock rate.

Task 3: Configure Static and Default Routing

- Configure HQ with exactly two static routes using the local interface.
- Configure B1 and B2 with exactly one default route using the local interface.

Task 4: Test Connectivity and Examine the Configuration

Step 1. Test connectivity.

- You should now have end-to-end connectivity. Use **ping** to test connectivity across the network.
- Troubleshoot until pings are successful.

Step 2. Examine the configuration.

Use verification commands to make sure that your configurations are complete.

End Notes

¹Zinin, A. *Cisco IP Routing: Packet Forwarding and Intra-domain Routing Protocols*. Boston, MA: Addison-Wesley; 2002.

Introduction to Dynamic Routing Protocols

The Study Guide portion of this chapter uses a combination of matching, fill-in-the-blank, multiple-choice, and open-ended question exercises to test your knowledge of dynamic routing protocol concepts.

The Labs and Activities portion of this chapter includes all the online curriculum labs to ensure that you have mastered the hands-on skills needed to design an addressing scheme.

As you work through this chapter, use Chapter 3 in *Routing Protocols and Concepts, CCNA Exploration Companion Guide* or use the corresponding Chapter 3 in the Exploration Routing Protocols and Concepts online curriculum for assistance.

Study Guide

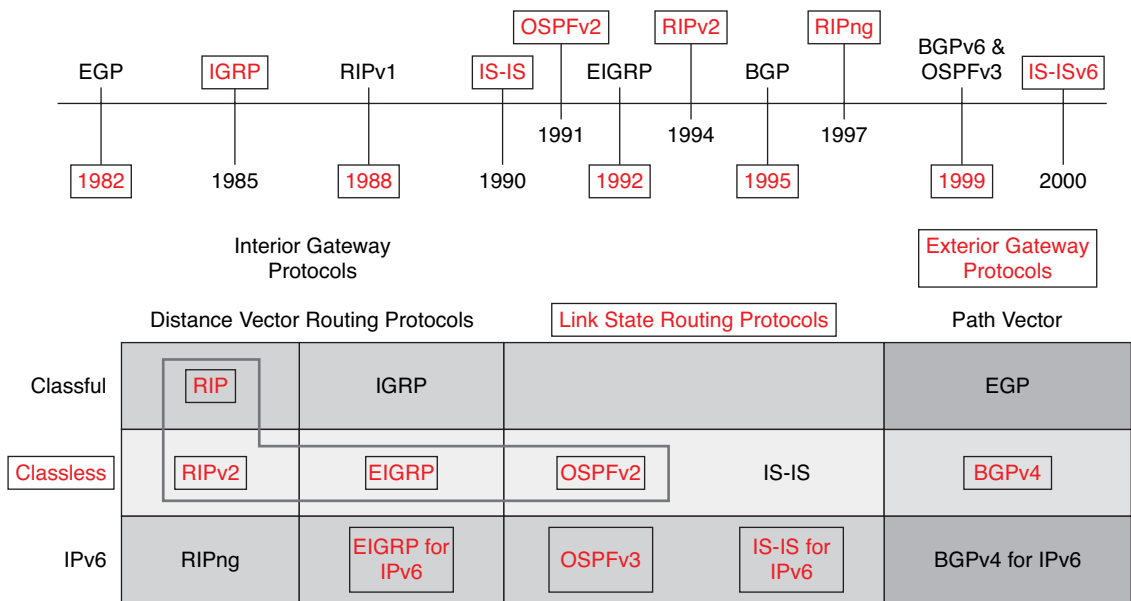
Introduction and Advantages

Dynamic routing protocols play an important role in today’s networks. The following sections include exercises to reinforce your basic knowledge of dynamic routing protocols.

Routing Protocols Evolution and Classification Exercise

Figure 3-1 shows a timeline of IP routing protocols and a chart classifying the various IP routing protocols. Both the timeline and the chart are incomplete. Fill in the missing information.

Figure 3-1 Routing Protocols Evolution and Classification (Answer)



Vocabulary Exercise: Matching (Key Words)

Match the definition on the left with a term on the right. This exercise is not necessarily a one-to-one matching. Some definitions might be used more than once, and some terms might have multiple definitions.

Definitions

- a. A protocol that *does not* include subnet mask information in its messages
- b. Routing protocols that operate *between* autonomous systems
- c. A topology that consists of a major network separating the subnets of another major network
- d. The ability to specify a different subnet mask for the same network number on different subnets
- e. Rating of trustworthiness of a routing information source
- f. A collection of routers under a common administration
- g. Speed and ability of a group of routers to agree on the topology of the network after a change in that topology
- h. Classification of a routing protocol that uses the shortest path first or Dijkstra algorithm
- i. Classification of a routing protocol that uses the Bellman-Ford algorithm to determine the best path
- j. A finite list of steps used by routing protocols for best-path determination
- k. Routing protocols that operate *within* autonomous systems
- l. A protocol that *does* include subnet mask information in its message
- m. A state when routers all have the same consistent network topology in their routing table

Terms

- e administrative distance
- j algorithm
- f autonomous system
- a classful routing protocols
- l classless routing protocols
- m converged
- g convergence
- c discontinuous network
- i distance vector
- b exterior gateway protocols
- k interior gateway protocols
- h link-state
- d VLSM

Dynamic Routing Protocol Concepts Exercise

Perspective and Background

As networks have evolved and become more complex, new routing protocols have emerged. One of the earliest routing protocols, [Routing Information Protocol \(RIP\)](#), has evolved into a newer version, [RIPv2](#). To address the needs of larger networks, two advanced routing protocols were developed: [Open Shortest Path First \(OSPF\)](#) and [Intermediate System-to-Intermediate System \(IS-IS\)](#). Cisco developed [Interior Gateway Routing Protocol \(IGRP\)](#) and [Enhanced IGRP \(EIGRP\)](#), which also scales well in larger network implementations.

Additionally, there was the need to interconnect different internetworks and provide routing among them. [Border Gateway Protocol \(BGP\)](#) is now used between Internet service providers (ISP) as well as between ISPs and their larger private clients to exchange routing information.

With the advent of numerous consumer devices using IP, the [IPv4](#) addressing space is nearly exhausted. Thus, [IPv6](#) has emerged, which has required newer versions of the IP routing protocols to be developed.

Role of Dynamic Routing Protocols

Routing protocols determine the best [path](#) to each network, which is then added to the [routing table](#). One of the primary benefits of using a dynamic routing protocol is that routers exchange routing information whenever there is a [topology change](#).

Compared to static routing, dynamic routing protocols require less [administrative](#) overhead. However, the expense of using dynamic routing protocols is dedicating part of a router's [resources](#) for protocol operation, including [CPU](#) time and network link [bandwidth](#).

Purpose of Dynamic Routing Protocols

A routing protocol is a set of processes, [algorithms](#), and messages that are used to exchange routing information and populate the [routing table](#) with the routing protocol's choice of best [paths](#).

List the four purposes of a routing protocol.

- [Discovery of remote networks](#)
- [Maintaining up-to-date routing information](#)
- [Choosing the best path to destination networks](#)
- [Ability to find a new best path if the current path is no longer available](#)

List and briefly describe the main components of a routing protocol.

- **Data structures:** [Some routing protocols use tables and/or databases for their operations. This information is kept in RAM.](#)
- **Algorithm:** [An algorithm is a finite list of steps used in accomplishing a task. Routing protocols use algorithms for facilitating routing information and for best-path determination.](#)
- **Routing protocol messages:** [Routing protocols use various types of messages to discover neighboring routers and exchange routing information, and do other tasks to learn and maintain accurate information about the network.](#)

Dynamic Routing Protocol Operation

The method that a routing protocol uses to accomplish its purpose depends on the [algorithm](#) it uses and the operational characteristics of that protocol.

Describe the basic operations of a dynamic routing protocol.

- The router sends and receives routing messages on its interfaces.
- The router shares routing messages and routing information with other routers that are using the same routing protocol.
- Routers exchange routing information to learn about remote networks.
- When a router detects a topology change, the routing protocol can advertise this change to other routers.

Dynamic Versus Static Routing Exercise

Dynamic routing certainly has several advantages over static routing. However, static routing is still used in networks today. In fact, networks typically use a combination of both static and dynamic routing.

Consider each of the features in Table 3-1, and briefly list the advantages and disadvantage of dynamic routing and static routing.

Table 3-1 Dynamic Versus Static Routing

Feature	Dynamic Routing	Static Routing
Configuration complexity	Generally independent of the network size	Increases with network size
Requires administrator knowledge	Advanced knowledge required	No extra knowledge required
Topology changes	Automatically adapts to topology changes	Administrator intervention required
Scaling	Suitable for simple and complex topologies	Suitable for simple topologies
Security	Less secure	More secure
Resource usage	Uses CPU, memory, link bandwidth	No extra resources needed
Predictability	Route depends on the current topology	Route to destination is always the same

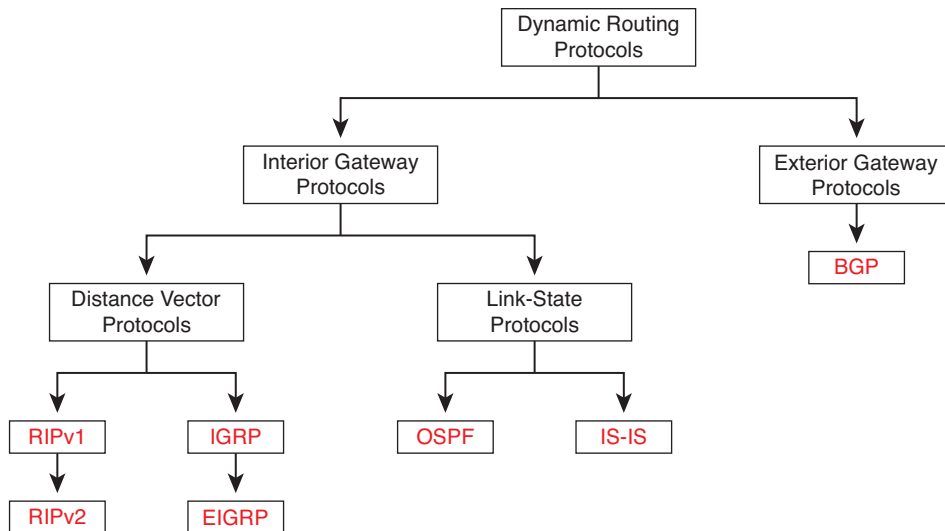
Classifying Dynamic Routing Protocols

The following sections give an overview of the most common IP routing protocols. Most of these routing protocols will be examined in detail later in this course. For now, work through these exercises to reinforce your knowledge of dynamic routing protocol classifications.

Dynamic Routing Protocols Classification Chart

The chart in Figure 3-2 is a succinct way to represent the major classifications of dynamic routing protocols. For each of the empty boxes, write in the missing protocol.

Figure 3-2 Classifying Dynamic Routing Protocols (Answer)



Dynamic Routing Protocols Classification Exercise

Routing protocols can be classified into different groups according to their characteristics.

IGP and EGP

An [autonomous system](#) (AS)—otherwise known as a [routing domain](#)—is a collection of routers under a common [administration](#). Because the Internet is based on the [autonomous system](#) concept, two types of routing protocols are required:

- [Interior gateway protocols](#) (IGP)
- [Exterior gateway protocols](#) (EGP)

Characteristics of IGPs and EGPs

An IGP is used to route [within](#) an [autonomous system](#). IGPs for IP include [RIP](#), [IGRP](#), [EIGRP](#), [OSPF](#), and [IS-IS](#). EGPs, on the other hand, are designed for use [between](#) different [autonomous systems](#) that are under the control of different [administrations](#). [BGP](#) is the only currently viable EGP and is the routing protocol used by the [Internet](#). [BGP](#) is a [path vector](#) protocol that can use many different [attributes](#) to measure routes.

Distance Vector and Link-State

IGPs can be classified as two types:

- [Distance vector](#) routing protocols
- [Link-state](#) routing protocols

Distance Vector Routing Protocol Operation

Distance vector means that routes are advertised as **vectors** of distance and **direction**. Distance is defined in terms of a **metric**, such as hop count, and **direction** is simply the **next-hop** router or **exit interface**. Distance vector protocols typically use the **Bellman-Ford** algorithm for the best-path route determination.

Some distance vector protocols **periodically** send complete routing tables to all connected neighbors. In large networks, these routing updates can become enormous, causing significant traffic on the links.

Distance vector protocols use routers as sign posts along the path to the final destination. The only information a router knows about a remote network is the distance or **metric** to reach that network and which path or **interface** to use to get there. Distance vector routing protocols do not have an actual map of the network **topology**.

List four situations in which distance vector routing protocols are a good choice.

- The network is simple and flat and does not require a special hierarchical design.
- The administrators do not have enough knowledge to configure and troubleshoot link-state protocols.
- Specific types of networks, such as hub-and-spoke networks, are being implemented.
- Worst-case convergence times in a network are not a concern.

Link-State Protocol Operation

In contrast to distance vector routing protocol operation, a router configured with a link-state routing protocol can create a “complete view,” or **topology**, of the network. A link-state router uses **link-state** information to create a **topology** map and to select the best path to all destination networks in the **topology**.

Link-state routing protocols do not use **periodic** updates. After the network has **converged**, a link-state update is only sent when there is a change in the topology.

List three situations in which link-state routing protocols are a good choice.

- The network design is hierarchical, usually occurring in large networks.
- The administrators have a good knowledge of the implemented link-state routing protocol.
- Fast convergence of the network is crucial.

Classful and Classless Protocols

All routing protocols can also be classified as either

- Classful routing protocols
- Classless routing protocols

Classful Routing Protocols

What feature makes a routing protocol a *classful* routing protocol?

Classful routing protocols do not send subnet mask information in routing updates.

There are other limitations to classful routing protocols, including their inability to support **discontiguous** networks—a topology that consists of a major network separating the subnets of another major network.

Classful routing protocols include **RIPv1** and **IGRP**.

Classless Routing Protocols

What feature makes a routing protocol a *classless* routing protocol?

Classless routing protocols include the subnet mask with the network address in routing updates.

Classless routing protocols are required in most networks today because of their support for VLSM and discontiguous networks, among other features.

Classless routing protocols are RIPv2, EIGRP, OSPF, IS-IS, and BGP.

Convergence

Briefly describe convergence and explain why is it important?

Convergence is when all routers' routing tables are at a state of consistency. The network has converged when all routers have complete and accurate information about the network. Convergence time is the time it takes routers to share information, calculate best paths, and update their routing tables. A network is not completely operable until the network has converged; therefore, most networks require short convergence times.

Convergence properties include the speed of propagation of routing information and the calculation of optimal paths. Routing protocols can be rated based on the speed to convergence; the faster the convergence, the better the routing protocol. Generally, RIP and IGRP are slow to converge, whereas EIGRP and OSPF are faster to converge.

Metrics

There are cases when a routing protocol learns of more than one route to the same destination. To select the best path, the routing protocol must be able to evaluate and differentiate among the available paths. For this purpose, a metric is used. The exercise in the following section reinforces your knowledge of metrics.

Metric Parameters Exercise

Two different routing protocols might choose different paths to the same destination because of using different metrics.

In the following list, fill in the missing metric.

- **Hop count:** A simple metric that counts the number of routers a packet must traverse
- **Bandwidth:** Influences path selection by preferring the path with the highest bandwidth
- **Load:** Considers the traffic utilization of a certain link
- **Delay:** Considers the time a packet takes to traverse a path
- **Reliability:** Assesses the probability of a link failure, calculated from the interface error count or previous link failures
- **Cost:** A value determined either by the IOS or by the network administrator to indicate a preference for a route

In the following list, fill in the missing metric or metrics for the routing protocol.

- **RIP: Hop count**—Best path is chosen by the route with the lowest hop count.
- **IGRP and EIGRP: Bandwidth, delay, reliability, and load**—Best path is chosen by the route with the smallest composite metric value calculated from these multiple parameters. By default, only **bandwidth** and **delay** are used.
- **IS-IS and OSPF: Cost**—Best path is chosen by the route with the lowest **cost**. The Cisco implementation of OSPF uses **bandwidth**.

Administrative Distances

Before the routing process can determine which route to use when forwarding a packet, it must first determine which routes to include in the routing table. In some cases, a router can learn a route to a remote network from more than one routing source. The exercises in the following sections reinforce your knowledge of the concept of administrative distance.

Concept of Administrative Distance Exercise

A router might learn of a route to the same network from more than one **source**. For example, a **static** route might have been configured for the same network/subnet mask that was learned dynamically by a dynamic routing protocol. Although less common, more than one dynamic routing protocol can be deployed in the same network. Administrative distance (AD) defines the **preference** of a routing source.

Administrative distance is an integer value from **0** to **255**. The **lower** the value the more preferred the route source. An administrative distance of **0** is the most preferred, which is the AD value for a **directly connected** network.

An administrative distance of **255** means that the router will not believe the source of that route and it will not be installed in the routing table.

One way to see the AD value for a route source is to look at the routing table. In Example 3-1, circle the AD values for the route sources that show an AD value.

Example 3-1 Routing Table with AD Value

```
R2# show ip route
<output omitted>

Gateway of last resort is not set

D    192.168.1.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
D    192.168.6.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
R    192.168.7.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
R    192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:08, Serial0/0/1
```

Answer: The value 90 should be circled for the 192.168.1.0/24 and 192.168.6.0/24 networks. The value 120 should be circled for the 192.168.5.0/24, 192.168.7.0/24, and 192.168.8.0/24 networks.

What other command can be used to verify the administrative distance used by a routing protocol?

show ip protocols

Notice that the directly connected networks in Example 3-1 do not show an administrative distance. What command would show the administrative distance (list as simply “distance”) for the 192.168.2.0 route in R2’s routing table?

show ip route 192.168.2.0

R2 might have knowledge of more networks than is shown in the routing table. What command will display all the RIP routes learned by R2, whether or not the RIP route is installed in the routing table?

show ip rip database

Routing Sources and Administrative Distance Exercise

Table 3-2 shows an incomplete chart of the different administrative distance values for various routing protocols. Fill in the missing information.

Table 3-2 Default Administrative Distances

Route Source	AD
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200
Unknown	255

Identifying Elements of the Routing Table Exercise

The purpose of this exercise is to practice how to correctly identify the route source, administrative distance, and metric for a given route based on output from the **show ip route** command.

The output is not common for most routing tables. Running more than one routing protocol on the same router is rare. Running three, as shown here, is more of an academic exercise and has value in that it will help you learn to interpret the routing table output.

From the **show ip route** information in Example 3-2, fill in missing spaces in Table 3-3.

Example 3-2 Multiple Routing Sources in the Routing Table

```
R2# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    10.0.0.0/16 is subnetted, 1 subnets
S       10.4.0.0 is directly connected, Serial0/0
    172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0
D       172.16.3.0 [90/2172416] via 172.16.2.1, 00:00:18, Serial0/0
C       192.168.1.0/24 is directly connected, Serial0/1
O       192.168.100.0/24 [110/65] via 172.16.2.1, 00:00:03, Serial0/0
O       192.168.110.0/24 [110/65] via 172.16.2.1, 00:00:03, Serial0/0
R       192.168.120.0/24 [120/1] via 172.16.2.1, 00:00:18, Serial0/0
```

Table 3-3 Route Sources, AD Values, and Metrics

Route	Route Source	AD	Metric
10.4.0.0/16	Static	1	0
172.16.1.0/24	Connected	0	0
172.16.2.0/24	Connected	0	0
172.16.3.0/24	EIGRP	90	2172416
192.168.1.0/24	Connected	0	0
192.168.100.0/24	OSPF	110	65
192.168.110.0/24	OSPF	110	65
192.168.120.0/24	RIP	120	1

Labs and Activities

Command Reference

In Table 3-4, record the command, *including the correct router prompt*, that fits the description.

Table 3-4 Commands for Chapter 3, Introduction to Dynamic Routing Protocols

Command	Description
Router# show ip rip database	Displays all the routes known by RIP—even routes that are not currently in the routing table
Router# show ip protocols	Displays detailed information about dynamic routing processes currently running on the router
Router# show ip route 172.16.3.0	Displays detailed information about the route 172.16.3.0



Lab 3-1: Subnetting Scenario 1 (3.5.2)

Upon completion of this lab, you will be able to

- Determine the number of subnets needed
- Determine the number of hosts needed
- Design an appropriate addressing scheme
- Assign addresses and subnet mask pairs to device interfaces and hosts
- Examine the use of the available network address space
- Determine how static routing could be applied to the network

Scenario

In this lab, you have been given the network address 192.168.9.0/24 to subnet and provide the IP addressing for the network shown in Figure 3-3. The network has the following addressing requirements:

- The BRANCH1 LAN 1 will require 10 host IP addresses.
- The BRANCH1 LAN 2 will require 10 host IP addresses.
- The BRANCH2 LAN 1 will require 10 host IP addresses.
- The BRANCH2 LAN 2 will require 10 host IP addresses.
- The HQ LAN will require 20 host IP addresses.
- The link from HQ to BRANCH1 will require an IP address for each end of the link.
- The link from HQ to BRANCH2 will require an IP address for each end of the link.

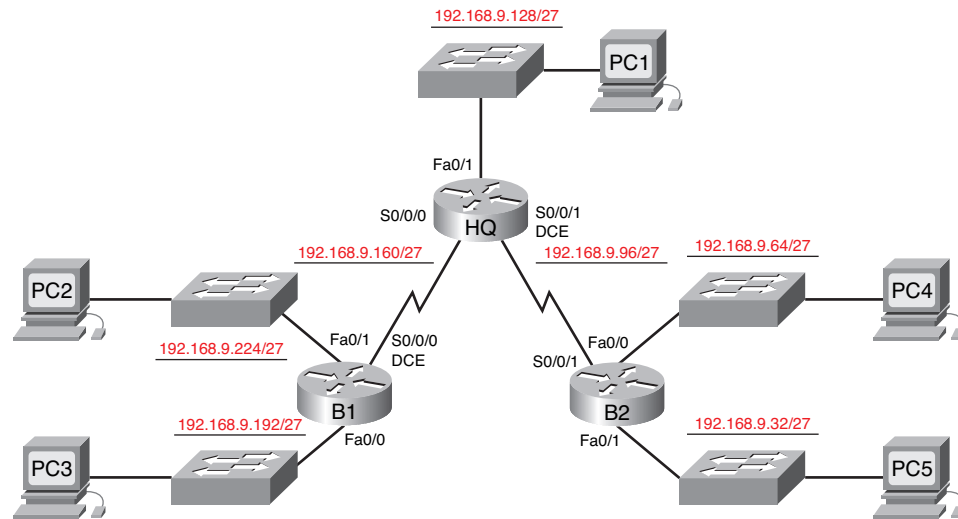
Figure 3-3 Topology Diagram for Subnetting Scenario 1 (Answer)

Table 3-5 provides a rough outline for the IP addresses, subnet masks, and default gateways (where applicable) for the devices shown in the network topology of Figure 3-3.

Table 3-5 Addressing Table for Lab 3-1

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	Fa0/0	192.168.9.129	255.255.255.224	—
	S0/0/0	192.168.9.161	255.255.255.224	—
	S0/0/1	192.168.9.97	255.255.255.224	—
BRANCH1	Fa0/0	192.168.9.193	255.255.255.224	—
	Fa0/1	192.168.9.225	255.255.255.224	—
	S0/0/0	192.168.9.190	255.255.255.224	—
BRANCH2	Fa0/0	192.168.9.65	255.255.255.224	—
	Fa0/1	192.168.9.33	255.255.255.224	—
	S0/0/1	192.168.9.126	255.255.255.224	—
PC1	NIC	192.168.9.158	255.255.255.224	192.168.9.129
PC2	NIC	192.168.9.222	255.255.255.224	192.168.9.193
PC3	NIC	192.168.9.254	255.255.255.224	192.168.9.225
PC4	NIC	192.168.9.94	255.255.255.224	192.168.9.65
PC5	NIC	192.168.9.62	255.255.255.224	192.168.9.33

Task 1: Examine the Network Requirements

Examine the network requirements and answer the questions below. Keep in mind that IP addresses will be needed for each of the LAN interfaces.

How many subnets are needed? 7

What is the maximum number of IP addresses that are needed for a single subnet? 21

How many IP addresses are needed for each of the branch LANs? 11

What is the total number of IP addresses that are needed? 69

Task 2: Design an IP Addressing Scheme

Step 1. Subnet the 192.168.9.0 network into the appropriate number of subnets.

What will the subnet mask be for the subnetworks? 255.255.255.224 or /27

How many usable host IP addresses are there per subnet? 30

Fill in Table 3-6 with the subnet information.

Table 3-6 Subnetting Chart for Lab 3-1

Subnet Number	Subnet Address	First Usable Host Address	Last Usable Host Address	Broadcast Address
0	192.168.9.0	192.168.9.1	192.168.9.30	192.168.9.31
1	192.168.9.32	192.168.9.33	192.168.9.62	192.168.9.63
2	192.168.9.64	192.168.9.65	192.168.9.94	192.168.9.95
3	192.168.9.96	192.168.9.97	192.168.9.126	192.168.9.127
4	192.168.9.128	192.168.9.129	192.168.9.158	192.168.9.159
5	192.168.9.160	192.168.9.161	192.168.9.190	192.168.9.191
6	192.168.9.192	192.168.9.193	192.168.9.222	192.168.9.223
7	192.168.9.224	192.168.9.225	192.168.9.254	192.168.9.255

Step 2. Assign the subnets to the network shown in the topology diagram in Figure 3-3.

When assigning the subnets, keep in mind that routing will need to occur to allow information to be sent throughout the network. The subnets will be assigned to the networks to allow route summarization on each of the routers.

1. Assign subnet 1 to the BRANCH2 LAN 2: 192.168.9.32 /27
2. Assign subnet 2 to BRANCH2 LAN 1 subnet address: 192.168.9.64 /27
3. Assign subnet 3 to link from HQ to BRANCH2 subnet address: 192.168.9.96 /27
4. Assign subnet 4 to HQ LAN subnet address: 192.168.9.128 /27
5. Assign subnet 5 to link from HQ to BRANCH1 subnet address: 192.168.9.160 /27
6. Assign subnet 6 to BRANCH1 LAN 2 subnet address: 192.168.9.192 /27
7. Assign subnet 7 to BRANCH1 LAN 1 subnet address: 192.168.9.224 /27

Task 3: Assign IP Addresses to the Network Devices

Assign the appropriate addresses to the device interfaces. Document the addresses to be used in Table 3-5 shown earlier.

Step 1. Assign addresses to the HQ router.

1. Assign the first valid host address in the HQ LAN subnet to the LAN interface.
2. Assign the first valid host address in the link from HQ to BRANCH1 subnet to the S0/0/0 interface.
3. Assign the first valid host address in the link from HQ to BRANCH2 subnet to the S0/0/1 interface.

Step 2. Assign addresses to the BRANCH1 router.

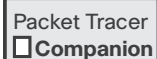
1. Assign the first valid host address in the BRANCH1 LAN 1 subnet to the Fa0/0 LAN interface.
2. Assign the first valid host address in the BRANCH1 LAN 2 subnet to the Fa0/1 LAN interface.
3. Assign the last valid host address in the link from HQ to BRANCH1 subnet to the WAN interface.

Step 3. Assign addresses to the BRANCH2 router.

1. Assign the first valid host address in the BRANCH2 LAN 1 subnet to the Fa0/0 LAN interface.
2. Assign the first valid host address in the BRANCH2 LAN 2 subnet to the Fa0/1 LAN interface.
3. Assign the last valid host address in the link from HQ to BRANCH2 subnet to the WAN interface.

Step 4. Assign addresses to the host PCs.

1. Assign the last valid host address in the HQ LAN subnet to PC1.
2. Assign the last valid host address in the BRANCH1 LAN 1 subnet to PC2.
3. Assign the last valid host address in the BRANCH1 LAN 2 subnet to PC3.
4. Assign the last valid host address in the BRANCH2 LAN 1 subnet to PC4.
5. Assign the last valid host address in the BRANCH2 LAN 2 subnet to PC5.



Task 4: Test the Network Design

You can now open the file LSG02-Lab352.pka on the CD-ROM that accompanies this book to apply and verify your addressing scheme. Check to see that all devices on directly connected networks can ping each other.

Task 5: Reflection

How many IP address in the 192.168.9.0 network are wasted in this design? [185](#)

What would the command be to add a default static route on the WAN interface of the BRANCH1 router?

[ip route 0.0.0.0 0.0.0.0 serial 0/0/0](#)

Can both of the BRANCH1 LANs be summarized into one route on the HQ router? [yes](#)

What would be the command used to add this summary route to the routing table?

[ip route 192.168.9.192 255.255.255.192 serial 0/0/0](#)

Can both of the BRANCH2 LANs be summarized into one route on the HQ router? [yes](#)

What would be the command used to add this summary route to the routing table?

[ip route 192.168.9.0 255.255.255.128 serial 0/0/1](#)

Can the HQ LAN and both of the BRANCH1 LANs be summarized into one route on the BRANCH2 router? This summarized route should also include the link between the HQ and BRANCH1 routers.

[yes](#)

What would be the command used to add this summary route to the routing table?

[ip route 192.168.9.128 255.255.255.128 serial 0/0/0](#)



Lab 3-2: Subnetting Scenario 2 (3.5.3)

Upon completion of this lab, you will be able to

- Determine the number of subnets needed
- Determine the number of hosts needed
- Design an appropriate addressing scheme
- Assign addresses and subnet mask pairs to device interfaces and hosts
- Examine the use of the available network address space
- Determine how static routing could be applied to the network

Scenario

In this lab, you have been given the network address 172.16.0.0/16 to subnet and provide the IP addressing for the network shown in Figure 3-4. The network has the following addressing requirements:

- The Branch 1 LAN will require 100 host IP addresses.
- The Branch 2 LAN will require 100 host IP addresses.
- The Branch 3 LAN will require 100 host IP addresses.
- The Branch 4 LAN will require 100 host IP addresses.
- The West LAN will require 400 hosts.
- The East LAN will require 400 hosts.

- The HQ LAN will require 500 host IP addresses.
- The links between each of the routers will require an IP address for each end of the link.

The IP addresses for the link from the HQ router to the ISP have already been assigned. The Serial 0/1/0 address of the HQ router is 209.165.200.226/27. The IP address of the Serial 0/0/0 interface of the ISP router is 209.165.200.225/27.

Figure 3-4 Topology Diagram for Subnetting Scenario 2 (Answer)

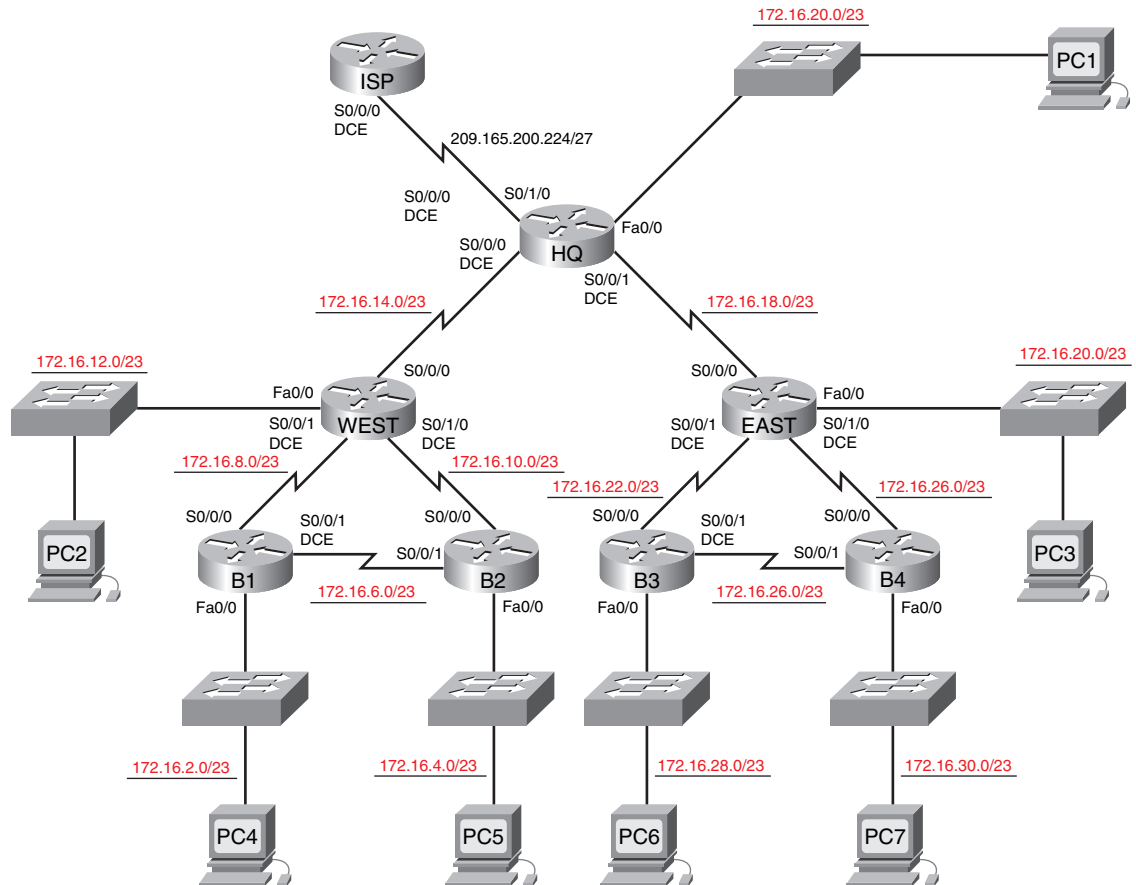


Table 3-7 provides a rough outline for the IP addresses, subnet masks, and default gateways (where applicable) for the devices shown in the network topology shown in Figure 3-4.

Table 3-7 Addressing Table for Lab 3-2

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	Fa0/0	172.16.16.1	255.255.254.0	—
	S0/0/0	172.16.14.1	255.255.254.0	—
	S0/0/1	172.16.18.1	255.255.254.0	—
	S0/1/0	209.165.200.226	255.255.255.224	—

continues

Table 3-7 Addressing Table for Lab 3-2 *continued*

Device	Interface	IP Address	Subnet Mask	Default Gateway
West	Fa0/0	172.16.12.1	255.255.254.0	—
	S0/0/0	172.16.15.254	255.255.254.0	—
	S0/0/1	172.16.8.1	255.255.254.0	—
	S0/1/0	172.16.10.1	255.255.254.0	—
East	Fa0/0	172.16.20.1	255.255.254.0	—
	S0/0/0	172.16.19.254	255.255.254.0	—
	S0/0/1	172.16.22.1	255.255.254.0	—
	S0/1/0	172.16.24.1	255.255.254.0	—
Branch 1	Fa0/0	172.16.2.1	255.255.254.0	—
	S0/0/0	172.16.9.254	255.255.254.0	—
	S0/0/1	172.16.6.1	255.255.254.0	—
Branch 2	Fa0/0	172.16.4.1	255.255.254.0	—
	S0/0/0	172.16.11.254	255.255.254.0	—
	S0/0/1	172.16.7.254	255.255.254.0	—
Branch 3	Fa0/0	172.16.28.1	255.255.254.0	—
	S0/0/0	172.16.23.254	255.255.254.0	—
	S0/0/1	172.16.26.1	255.255.254.0	—
Branch 4	Fa0/0	172.16.30.1	255.255.254.0	—
	S0/0/0	172.16.25.254	255.255.254.0	—
	S0/0/1	172.16.27.254	255.255.254.0	—
PC1	NIC	172.16.17.254	255.255.254.0	172.16.16.1
PC2	NIC	172.16.13.254	255.255.254.0	172.16.12.1
PC3	NIC	172.16.21.254	255.255.254.0	172.16.20.1
PC4	NIC	172.16.3.254	255.255.254.0	172.16.2.1
PC5	NIC	172.16.5.254	255.255.254.0	172.16.4.1
PC6	NIC	172.16.29.254	255.255.254.0	172.16.28.1
PC7	NIC	172.16.31.254	255.255.254.0	172.16.30.1

Task 1: Examine the Network Requirements

Examine the network requirements and answer the questions that follow. Keep in mind that IP addresses will be needed for each of the LAN interfaces.

How many subnets are needed? [15](#)

What is the maximum number of IP addresses that are needed for a single subnet? [501](#)

How many IP addresses are needed for each of the branch LANs? [101](#)

How many IP addresses are needed for all the connections between routers? [16](#)

What is the total number of IP addresses that are needed? [1723](#)

Task 2: Design an IP Addressing Scheme

Step 1. Subnet the 172.16.0.0 network into the appropriate number of subnets.

What will the subnet mask be for the subnetworks? [255.255.254.0 or /23](#)

How many usable host IP addresses are there per subnet? [510](#)

Fill in Table 3-8 with the subnet information.

Table 3-8 Subnetting Chart for Lab 3-2

Subnet Number	Subnet IP	First Usable Host IP	Last Usable Host IP	Broadcast Address
0	172.16.0.0	172.16.0.1	172.16.1.254	172.16.1.255
1	172.16.2.0	172.16.2.1	172.16.3.254	172.16.3.255
2	172.16.4.0	172.16.4.1	172.16.5.254	172.16.5.255
3	172.16.6.0	172.16.6.1	172.16.7.254	172.16.7.255
4	172.16.8.0	172.16.8.1	172.16.9.254	172.16.9.255
5	172.16.10.0	172.16.10.1	172.16.11.254	172.16.11.255
6	172.16.12.0	172.16.12.1	172.16.13.254	172.16.13.255
7	172.16.14.0	172.16.14.1	172.16.15.254	172.16.15.255
8	172.16.16.0	172.16.16.1	172.16.17.254	172.16.17.255
9	172.16.18.0	172.16.18.1	172.16.19.254	172.16.19.255
10	172.16.20.0	172.16.20.1	172.16.21.254	172.16.21.255
11	172.16.22.0	172.16.22.1	172.16.23.254	172.16.23.255
12	172.16.24.0	172.16.24.1	172.16.25.254	172.16.25.255
13	172.16.26.0	172.16.26.1	172.16.27.254	172.16.27.255
14	172.16.28.0	172.16.28.1	172.16.29.254	172.16.29.255
15	172.16.30.0	172.16.30.1	172.16.31.254	172.16.31.255

Step 2. Assign the subnets to the network shown in the topology diagram in Figure 3-4.

When assigning the subnets, keep in mind that routing will need to occur to allow information to be sent throughout the network. The subnets will be assigned to the networks to allow route summarization on each of the routers.

1. Assign subnet 1 to the Branch 1 LAN subnet: [172.16.2.0 /23](#)
2. Assign subnet 2 to the Branch 2 LAN subnet: [172.16.4.0 /23](#)
3. Assign subnet 3 to the link between the Branch 1 and Branch 2 routers: [172.16.6.0 /23](#)
4. Assign subnet 4 to the link between the Branch 1 and West routers: [172.16.8.0 /23](#)
5. Assign subnet 5 to the link between the Branch 2 and West routers: [172.16.10.0 /23](#)
6. Assign subnet 6 to the West LAN subnet: [172.16.12.0 /23](#)
7. Assign subnet 7 to the link between the West and HQ routers: [172.16.14.0 /23](#)
8. Assign subnet 8 to the HQ LAN subnet: [172.16.16.0 /23](#)
9. Assign subnet 9 to the link between the HQ and East routers: [172.16.18.0 /23](#)
10. Assign subnet 10 to the East LAN subnet: [172.16.20.0 /23](#)
11. Assign subnet 11 to the link between the Branch 3 and East routers: [172.16.22.0 /23](#)
12. Assign subnet 12 to the link between the Branch 4 and East routers: [172.16.24.0 /23](#)
13. Assign subnet 13 to the link between the Branch 3 and Branch 4 routers: [172.16.26.0 /23](#)
14. Assign subnet 14 to the Branch 3 LAN subnet: [172.16.28.0 /23](#)
15. Assign subnet 15 to the Branch 4 LAN subnet: [172.16.30.0 /23](#)

Task 3: Assign IP Addresses to the Network Devices

Assign the appropriate addresses to the device interfaces. Document the addresses to be used in Table 3-7 shown earlier.

Step 1. Assign addresses to the HQ router.

1. Assign the first valid host address in the HQ LAN subnet to the LAN interface.
2. Assign the first valid host address in the link from HQ to West subnet to the S0/0/0 interface.
3. Assign the first valid host address in the link from HQ to East subnet to the S0/0/1 interface.

Step 2. Assign addresses to the West router.

1. Assign the first valid host address in the West LAN subnet to the LAN interface.
2. Assign the last valid host address in the link from HQ to West subnet to the S0/0/0 interface.

3. Assign the first valid host address in the link from West to Branch 1 subnet to the S0/0/1 interface.
4. Assign the first valid host address in the link from West to Branch 2 subnet to the S0/1/0 interface.

Step 3. Assign addresses to the East router.

1. Assign the first valid host address in the East LAN subnet to the LAN interface.
2. Assign the last valid host address in the link from HQ to East subnet to the S0/0/0 interface.
3. Assign the first valid host address in the link from East to Branch 3 subnet to the S0/0/1 interface.
4. Assign the first valid host address in the link from East to Branch 4 subnet to the S0/1/0 interface.

Step 4. Assign addresses to the Branch 1 router.

1. Assign the first valid host address in the Branch 1 LAN subnet to the LAN interface.
2. Assign the last valid host address in the link from West to Branch 1 subnet to the S0/0/0 interface.
3. Assign the first valid host address in the link from Branch 1 to Branch 2 subnet to the S0/0/1 interface.

Step 5. Assign addresses to the Branch 2 router.

1. Assign the first valid host address in the Branch 2 LAN subnet to the LAN interface.
2. Assign the last valid host address in the link from West to Branch 2 subnet to the S0/0/0 interface.
3. Assign the last valid host address in the link from Branch 1 to Branch 2 subnet to the S0/0/1 interface.

Step 6. Assign addresses to the Branch 3 router.

1. Assign the first valid host address in the Branch 3 LAN subnet to the LAN interface.
2. Assign the last valid host address in the link from East to Branch 3 subnet to the S0/0/0 interface.
3. Assign the first valid host address in the link from Branch 3 to Branch 4 subnet to the S0/0/1 interface.

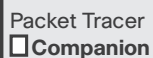
Step 7. Assign addresses to the Branch 4 router.

1. Assign the first valid host address in the Branch 4 LAN subnet to the LAN interface.
2. Assign the last valid host address in the link from East to Branch 4 subnet to the S0/0/0 interface.
3. Assign the last valid host address in the link from Branch 3 to Branch 4 subnet to the S0/0/1 interface.

Step 8. Assign addresses to the host PCs.

1. Assign the last valid host address in the HQ LAN subnet to PC1.
2. Assign the last valid host address in the West LAN subnet to PC2.

3. Assign the last valid host address in the East 1 LAN subnet to PC3.
4. Assign the last valid host address in the Branch 1 LAN subnet to PC4.
5. Assign the last valid host address in the Branch 2 LAN subnet to PC5.
6. Assign the last valid host address in the Branch 3 LAN subnet to PC6.
7. Assign the last valid host address in the Branch 4 LAN subnet to PC7.



Task 4: Test the Network Design

You can now open the file LSG02-Lab353.pka on the CD-ROM that accompanies this book to apply and verify your addressing scheme. Check to see that all devices on directly connected networks can ping each other.

Task 5: Reflection

How many IP addresses in the 172.16.0.0 network are wasted in this design? [63811](#)

What would be the command to add a default static route for your entire network design from the HQ router to the ISP router?

[ip route 0.0.0.0 0.0.0.0 209.165.200.227](#)

Can the West, Branch 1, and Branch 2 networks be summarized into one route on the HQ router? This summarized route should also include the serial links that connect the West, Branch 1, and Branch 2 routers. [yes](#)

What would be the command used to add this summary route to the routing table?

[ip route 172.16.0.0 255.255.240.0 serial 0/0/0](#)

Can the East, Branch 3, and Branch 4 networks be summarized into one route on the HQ router? This summarized route should also include the serial links that connect the East, Branch 3, and Branch 4 routers. [yes](#)

What would be the command used to add this summary route to the routing table?

[ip route 172.16.16.0 255.255.240.0 serial 0/0/1](#)

What would be the command to add a default static route on the West router to send traffic for all unknown destinations to the HQ router?

[ip route 0.0.0.0 0.0.0.0 serial 0/0/0](#)

What would be the command to add a default static route on the East router to send traffic for all unknown destinations to the HQ router?

[ip route 0.0.0.0 0.0.0.0 serial 0/0/0](#)

Can the Branch 1 and Branch 2 networks be summarized into one route on the West router? This summarized route should also include the serial link that connects the Branch 1 and Branch 2 routers. [yes](#)

What would be the command to add this summary route to the routing table? Use the S0/0/1 interface of the West router as the exit interface.

[ip route 172.16.0.0 255.255.248.0 serial 0/0/1](#)

Can the Branch 3 and Branch 4 networks be summarized into one route on the East router? This summarized route should also include the serial link that connects the Branch 3 and Branch 4 routers. [yes](#)

What would be the command to add this summary route to the routing table? Use the S0/0/1 interface of the East router as the exit interface.

[ip route 172.16.24.0 255.255.248.0 serial 0/0/1](#)

The Branch 1 router requires a static route for traffic destined for Branch 2. All other traffic should be sent to the West router using a default static route. What commands would be used to accomplish this?

[ip route 172.16.4.0 255.255.254.0 serial 0/0/1](#)

[ip route 0.0.0.0 0.0.0.0 serial 0/0/0](#)

The Branch 2 router requires a static route for traffic destined for Branch 1. All other traffic should be sent to the West router using a default static route. What commands would be used to accomplish this?

[ip route 172.16.2.0 255.255.254.0 serial 0/0/1](#)

[ip route 0.0.0.0 0.0.0.0 serial 0/0/0](#)

The Branch 3 router requires a static route for traffic destined for Branch 4. All other traffic should be sent to the East router using a default static route. What commands would be used to accomplish this?

[ip route 172.16.30.0 255.255.254.0 serial 0/0/1](#)

[ip route 0.0.0.0 0.0.0.0 serial 0/0/0](#)

The Branch 4 router requires a static route for traffic destined for Branch 3. All other traffic should be sent to the East router using a default static route. What commands would be used to accomplish this?

[ip route 172.16.28.0 255.255.254.0 serial 0/0/1](#)

[ip route 0.0.0.0 0.0.0.0 serial 0/0/0](#)



Lab 3-3: Subnetting Scenario 3 (3.5.4)

Instructor note: This lab is impossible to complete with fixed-length subnet masking. Use this lab as a scaffolding exercise to link the student to the concept of VLSM, which is discussed in Chapter 6, “VLSM and CIDR.” Avoid offering the student any help in solving the problem of not having enough address space.

Upon completion of this lab, you will be able to

- Determine the number of subnets needed
- Determine the number of hosts needed
- Design an appropriate addressing scheme
- Conduct research to find a possible solution

Scenario

In this lab, you have been given the network address 192.168.1.0/24 to subnet and provide the IP addressing for the network shown in Figure 3-5. The network has the following addressing requirements:

- The BRANCH1 LAN 1 will require 15 host IP addresses.
- The BRANCH1 LAN 2 will require 15 host IP addresses.
- The BRANCH2 LAN 1 will require 15 host IP addresses.
- The BRANCH2 LAN 2 will require 15 host IP addresses.
- The HQ LAN will require 30 host IP addresses.
- The link from HQ to BRANCH1 will require an IP address for each end of the link.
- The link from HQ to BRANCH2 will require an IP address for each end of the link.
- The link from HQ to Branch 3 will require an IP address for each end of the link.

Figure 3-5 Topology Diagram for Subnetting Scenario 3

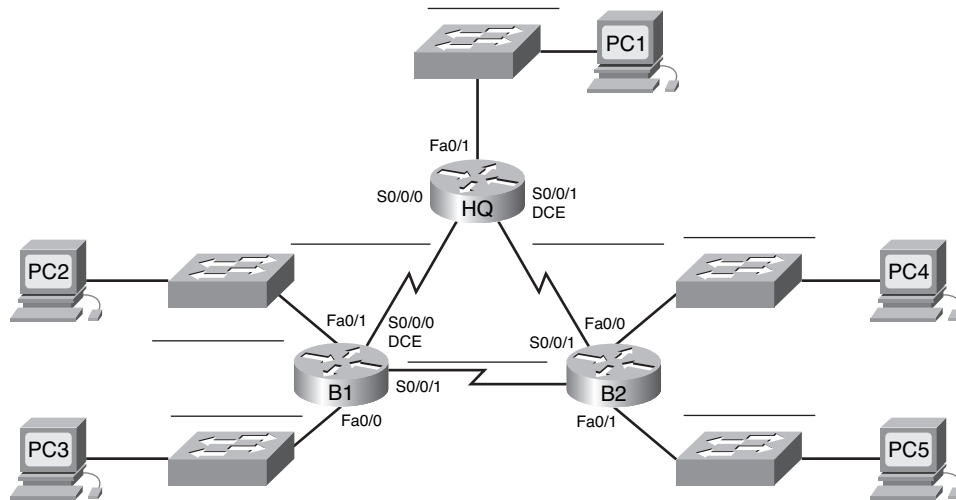


Table 3-9 provides a rough outline for you to assign the IP addresses, subnet masks, and default gateways (where applicable) for the devices shown in the network topology of Figure 3-5.

Table 3-9 Addressing Table for Lab 3-3

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	Fa0/1			—
	S0/0/0			—
	S0/0/1			—
BRANCH1	Fa0/0			—
	Fa0/1			—
	S0/0/0			—
	S0/0/1			—
BRANCH2	Fa0/0			—
	Fa0/1			—
	S0/0/0			—
	S0/0/1			—

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC1	NIC			
PC2	NIC			
PC3	NIC			
PC4	NIC			
PC5	NIC			

Task 1: Examine the Network Requirements

Examine the network requirements and answer the questions that follow. Keep in mind that IP addresses will be needed for each of the LAN interfaces.

How many subnets are needed? [8](#)

What is the maximum number of IP addresses that are needed for a single subnet? [31](#)

How many IP addresses are needed for each of the branch LANs? [16](#)

What is the total number of IP addresses that are needed? [101](#)

Task 2: Design an IP Addressing Scheme

Subnet the 192.168.1.0/24 network into the appropriate number of subnets.

Can the 192.168.1.0/24 network be subnetted to fit the network requirements? [no](#)

If the “number of subnets” requirement is met, what is the maximum number of hosts per subnet? [30](#)

If the “maximum number of hosts” requirement is met, what is the number of subnets that will be available to use? [2](#)

Task 3: Reflection

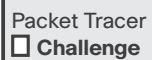
You do not have enough address space to implement an addressing scheme. Research this problem and propose a possible solution. Increasing the size of your original address space is not an acceptable solution. (Hint: We will discuss solutions to this problem in Chapter 6, “VLSM and CIDR.”)



Attempt to implement your solution using Packet Tracer. You can now open the file LSG02-Lab354.pka on the CD-ROM that accompanies this book to apply and verify your addressing scheme. Check to see that all devices on directly connected networks can ping each other.

Successful implementation of a solution requires that

- Only the 192.168.1.0/24 address space is used.
- PCs and routers can ping all IP addresses.



Packet Tracer Skills Integration Challenge

Introduction

This activity focuses on subnetting skills, basic device configurations, and static routing. After you configure all devices, test for end-to-end connectivity and examine your configuration. Open the file LSG02-PTskills3.pka on the CD-ROM that accompanies this book. Use the topology in Figure 3-6 and the addressing table in Table 3-10 to document your design.

Upon completion of this lab, you will be able to

- Design and document an addressing scheme based on requirements
- Select appropriate equipment and cable the devices
- Apply a basic configuration to the devices
- Configure static and default routing
- Verify full connectivity between all devices in the topology

Figure 3-6 Packet Tracer Skills Integration Challenge Topology

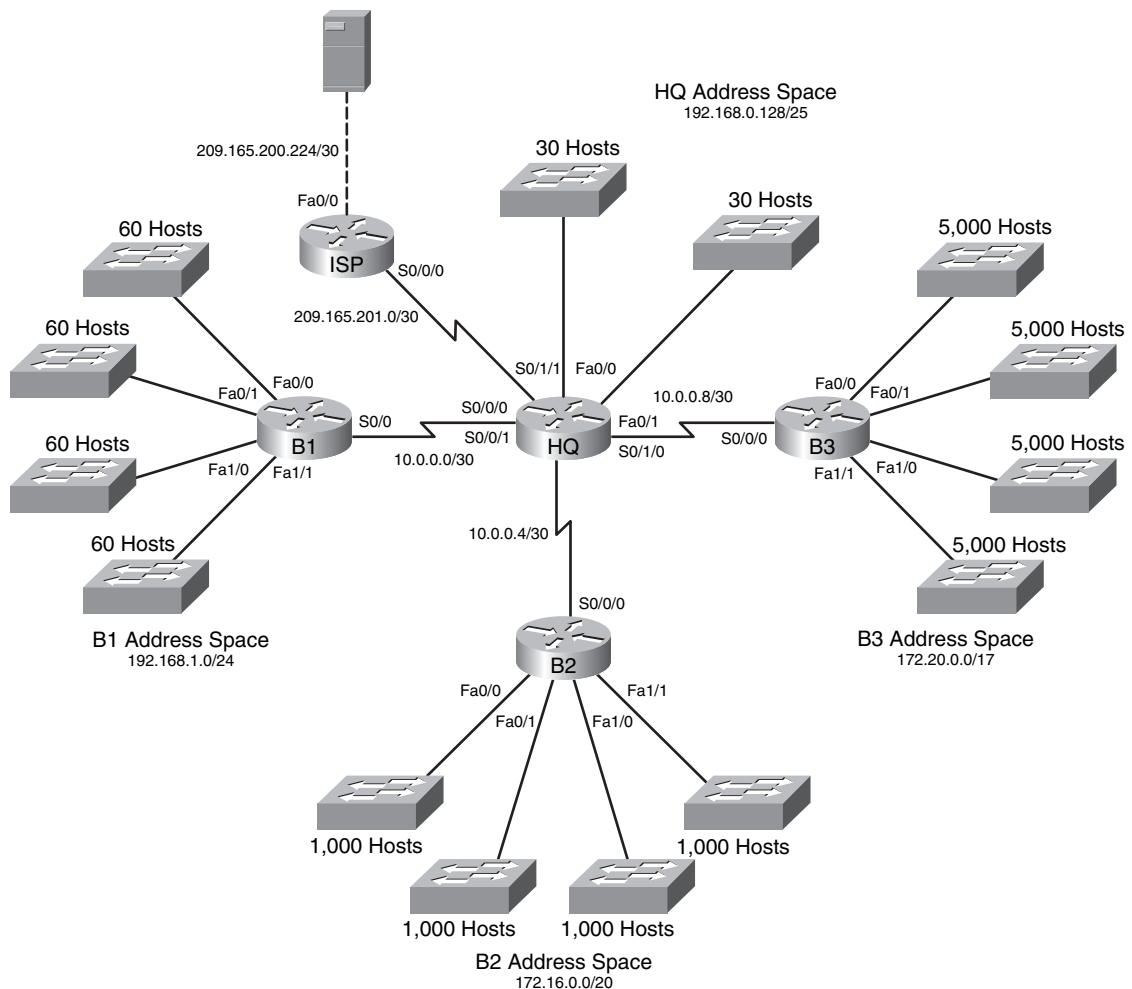


Table 3-10 provides a rough outline for you to assign the IP addresses and subnet masks for the devices shown in the network topology of Figure 3-6.

Table 3-10 Addressing Table for Packet Tracer Skills Integration Challenge

Device	Interface	IP Address	Subnet Mask
HQ	Fa0/0	192.168.0.129	255.255.255.224
	Fa0/1	192.168.0.161	255.255.255.224
	S0/0/0	10.0.0.1	255.255.255.252
	S0/0/1	10.0.0.5	255.255.255.252
	S0/1/0	10.0.0.9	255.255.255.252
	S0/1/1	209.165.201.2	255.255.255.252
B1	Fa0/0	192.168.1.1	255.255.255.192
	Fa0/1	192.168.1.65	255.255.255.192
	Fa1/0	192.168.1.129	255.255.255.192
	Fa1/1	192.168.1.193	255.255.255.192
	S0/0/0	10.0.0.2	255.255.255.252
B2	Fa0/0	172.16.0.1	255.255.252.0
	Fa0/1	172.16.4.1	255.255.252.0
	Fa1/0	172.16.8.1	255.255.252.0
	Fa1/1	172.16.12.1	255.255.252.0
	S0/0/0	10.0.0.6	255.255.255.252
B3	Fa0/0	172.20.0.1	255.255.224.0
	Fa0/1	172.20.32.1	255.255.224.0
	Fa1/0	172.20.64.1	255.255.224.0
	Fa1/1	172.20.96.1	255.255.224.0
	S0/0/0	10.0.0.10	255.255.255.252
ISP	S0/0/0	209.165.201.1	255.255.255.252
	Fa0/0	209.165.200.225	255.255.255.252
Web Server	NIC	209.165.200.226	255.255.255.252

Task 1: Design and Document an Addressing Scheme

Step 1. Design an addressing scheme.

Based on the network requirements shown in Figure 3-6, design an appropriate addressing scheme.

- The HQ, B1, B2, and B3 routers each have an address space. Subnet the address space based on the host requirements.
- For each address space, assign subnet 0 to the Fa0/0 LAN, subnet 1 to the Fa0/1, and so on.

Step 2. Document the addressing scheme.

- Use Table 3-10 to document the IP addresses and subnet masks. Assign the first IP address to the router interface.
- For the WAN links, assign the first IP address to HQ.

Task 2: Apply a Basic Configuration

Using your documentation, configure the routers with basic configurations including addressing and host names. Use **cisco** as the line passwords and **class** as the secret password. Use **64000** as the clock rate. ISP is the DCE in its WAN link to HQ, and HQ is the DCE for all other WAN links.

Task 3: Configure Static and Default Routing

Configure static and default routing using the exit interface argument, according to the following criteria:

- HQ should have three static routes and one default route.
- B1, B2, and B3 should have one default route.
- ISP should have seven static routes. This will include the three WAN links between HQ and the branch routers B1, B2, and B3.

Task 4: Test Connectivity and Examine the Configuration

Step 1. Test connectivity.

You should now have end-to-end connectivity. Use ping to test connectivity across the network. Each router should be able to ping all other router interfaces and the web server.

Use extended ping to test LAN connectivity to the web server. For example, to test the Fa0/0 interface on B1, you would do the following:

```
B1# ping
Protocol [ip]:
Target IP address: 209.165.200.226
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: yes
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:  
Packet sent with a source address of 192.168.1.1  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 67/118/138 ms
```

Troubleshoot until pings are successful.

Step 2. Examine the configuration.

Use verification commands to make sure that your configurations are complete.

Distance Vector Routing Protocols

The Study Guide portion of this chapter uses a combination of matching, fill-in-the-blank, multiple-choice, and open-ended question exercises to test your knowledge of distance vector routing protocols.

The Labs and Activities portion of this chapter includes the online curriculum lab to ensure that you have mastered routing table interpretation skills.

As you work through this chapter, use Chapter 4 in *Routing Protocols and Concepts, CCNA Exploration Companion Guide* or use the corresponding Chapter 4 in the Exploration Routing Protocols and Concepts online curriculum for assistance.

Study Guide

Introduction to Distance Vector Routing Protocols

One way to characterize routing protocols is by the type of routing algorithm they use to build and maintain their routing table. By doing this, routing protocols can be differentiated as a distance vector, link-state, or path vector routing protocol. In the following sections, you will review the basic concepts of distance vector routing protocols.

Distance Vector Protocols Concepts Exercise

Distance vector routing protocols include RIP, IGRP, and EIGRP. The following are some key characteristics of these protocols. Fill in the blanks to provide the missing words or phrases.

RIP

Routing Information Protocol (RIP) was originally specified in RFC 1058. It has the following key characteristics:

- Hop count is used as the metric for path selection.
- If the metric for a network is greater than 15, RIP cannot supply a route to that network.
- Routing updates are broadcast or multicast every 30 seconds, by default.

IGRP

Interior Gateway Routing Protocol (IGRP) is a proprietary protocol developed by Cisco. IGRP has the following key design characteristics:

- Bandwidth, delay, load, and reliability are used to create a composite metric.
- Routing updates are broadcast every 90 seconds, by default.
- IGRP is the predecessor of EIGRP and is now obsolete.

EIGRP

Enhanced IGRP (EIGRP) is a Cisco-proprietary distance vector routing protocol. EIGRP has these key characteristics:

- It can perform unequal-cost load balancing.
- It uses Diffusing Update Algorithm (DUAL) to calculate the shortest path.
- There are no periodic updates as with RIP and IGRP. Routing updates are sent only when there is a change in the topology.

Meaning of Distance Vector

Briefly explain what is meant by the term *distance vector*.

Routes are advertised as vectors of distance and direction. Distance is defined in terms of a metric, and direction is simply the next-hop router or exit interface.

A distance vector router only knows

- The direction or interface in which packets should be forwarded
- The distance to the destination network

Operation of Distance Vector Routing Protocols

Some distance vector routing protocols call for the router to periodically **broadcast** the entire **routing table** to each of its neighbors. This method is inefficient because the updates not only consume network **bandwidth** but also consume router **CPU** resources to process the updates.

In reference to routing protocols, what is a neighbor?

Neighbors are routers that share a link and are configured to use the same routing protocol.

Broadcast updates are sent to 255.255.255.255 (IP address). Neighboring routers that are configured with the same **routing protocol** will process the updates. All other devices will also process the update up to Layer **3** before discarding it.

At the core of the distance vector routing protocol is the **algorithm** used to calculate the best paths and then send that information to the neighbors.

Routing Protocols Characteristics Exercise

Briefly explain each of the following routing protocol characteristics.

Time to convergence

Time to convergence defines how quickly the routers in the network topology share routing information and reach a state of consistent knowledge. The faster the convergence, the more preferable the protocol. Routing loops can occur when inconsistent routing tables are not updated because of slow convergence in a changing network.

Scalability

Scalability defines how large a network can become based on the routing protocol that is deployed. The larger the network is, the more scalable the routing protocol needs to be.

Classless (use of VLSM) or classful

Classless routing protocols include the subnet mask in the updates. This feature supports the use of variable-length subnet masking (VLSM) and better route summarization. Classful routing protocols do not include the subnet mask and cannot support VLSM.

Resource usage

Resource usage includes the requirements of a routing protocol, such as memory space, CPU utilization, and link bandwidth utilization. Higher resource requirements necessitate more powerful hardware to support the routing protocol operation in addition to the packet-forwarding processes.

Implementation and maintenance

Implementation and maintenance describe the level of knowledge that is required for a network administrator to implement and maintain the network based on the routing protocol deployed.

Comparing Routing Protocol Characteristics Exercise

In Table 4-1, all the routing protocols discussed in the course are compared based on the characteristics you briefly described in the previous exercise. For each characteristic, circle the description that applies to each routing protocol. For example, RIP is slow to converge. So you would circle “slow” in the “Speed of Convergence” row under both RIPv1 and RIPv2.

Table 4-1 Comparing Routing Protocol Features

	Distance Vector				Link-State	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Speed of Convergence	Slow	Slow	Slow	Slow	Slow	Slow
	Fast	Fast	Fast	Fast	Fast	Fast
Scalability—Size of Network	Small	Small	Small	Small	Small	Small
	Large	Large	Large	Large	Large	Large
Use of VLSM	Yes	Yes	Yes	Yes	Yes	Yes
	No	No	No	No	No	No
Resource Usage	Low	Low	Low	Low	Low	Low
	Medium	Medium	Medium	Medium	Medium	Medium
	High	High	High	High	High	High
Implementation and Maintenance	Simple	Simple	Simple	Simple	Simple	Simple
	Complex	Complex	Complex	Complex	Complex	Complex

Network Discovery

Network discovery is part of the process of the routing protocol algorithm that enables routers to first learn about remote networks. In the following exercises, you will demonstrate your knowledge of the network discovery process.

Network Discovery Exercise

Cold Start

What does a router know when it first boots?

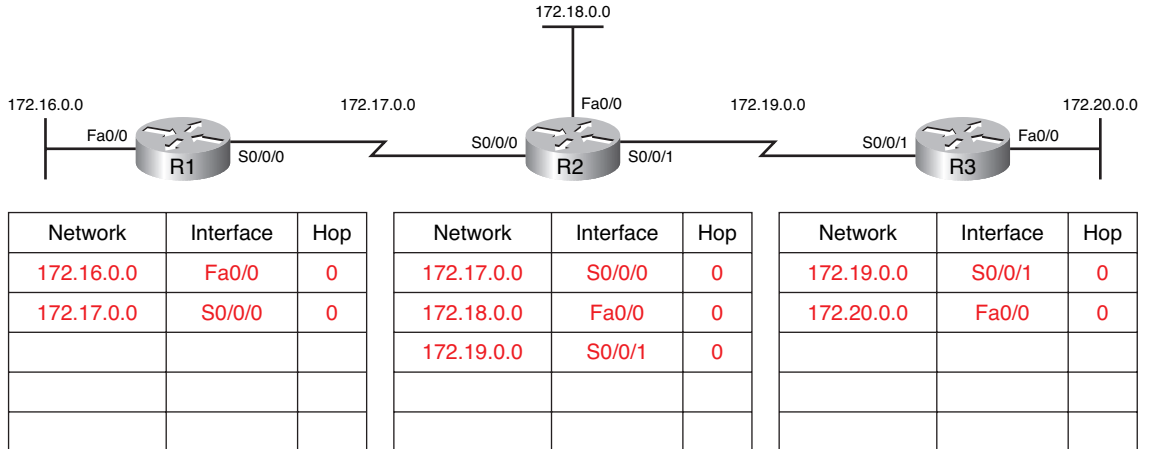
The only information that a router has is from its own saved configuration file stored in NVRAM.

After it boots, what does the router know about the network topology?

The router will initially discover its own directly connected networks.

In Figure 4-1, the routers have booted. However, they have not yet discovered any neighbors. In the tables below each router, fill in the networks, interfaces, and hop counts that each router has installed in its routing table.

Figure 4-1 Network Discovery: Cold Start (Answer)



Initial Exchange of Routing Information

What is required before the routers will start sending each other updates?

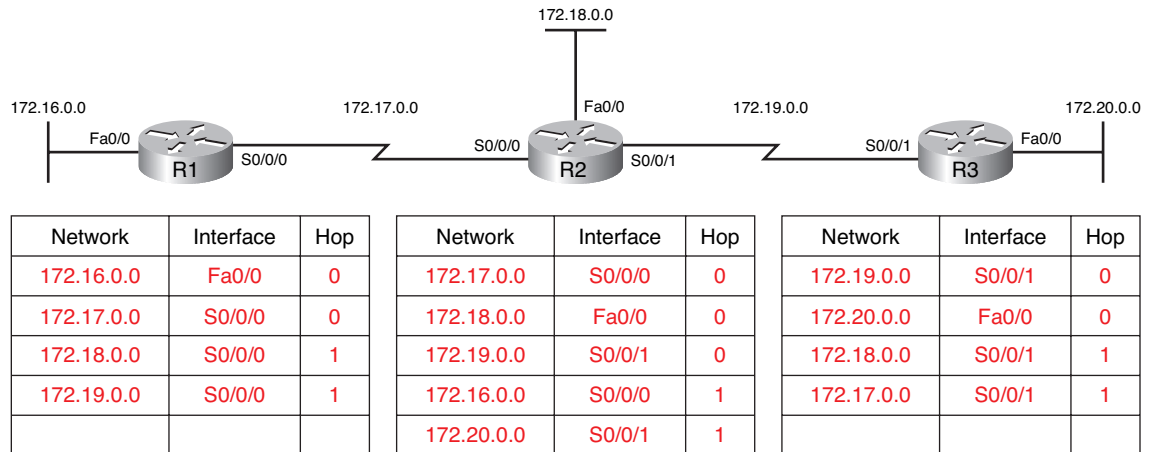
A routing protocol must be configured on each router.

For the first round of updates after a cold start, what information will the updates include?

The first round of updates only includes information about each router's directly connected networks.

In Figure 4-2, the routers have completed their initial exchange of routing updates. In the tables below each router, fill in the networks, interfaces, and hop counts that each router now has installed in its routing table.

Figure 4-2 Network Discovery: Initial Exchange (Answer)



At this point in the network discovery process, the routing tables are incomplete. In other words, the network has not yet converged.

Which routing tables and which networks still need to be discovered?

R1 does not yet know about 172.20.0.0.

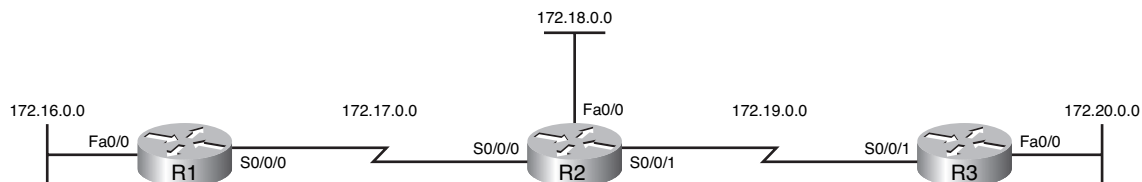
R3 does not yet know about 172.16.0.0.

Next Update

Continuing the journey toward convergence, the routers exchange the next round of periodic updates.

In Figure 4-3, the routers have completed their next round of updates. In the tables below each router, fill in the networks, interfaces, and hop counts that each router now has installed in its routing table.

Figure 4-3 Network Discovery: Next Update (Answer)



Network	Interface	Hop
172.16.0.0	Fa0/0	0
172.17.0.0	S0/0/0	0
172.18.0.0	S0/0/0	1
172.19.0.0	S0/0/0	1
172.20.0.0	S0/0/0	2

Network	Interface	Hop
172.17.0.0	S0/0/0	0
172.18.0.0	Fa0/0	0
172.19.0.0	S0/0/1	0
172.16.0.0	S0/0/0	1
172.20.0.0	S0/0/1	1

Network	Interface	Hop
172.19.0.0	S0/0/1	0
172.20.0.0	Fa0/0	0
172.18.0.0	S0/0/1	1
172.17.0.0	S0/0/1	1
172.16.0.0	S0/0/1	2

Routing Table Maintenance

After the routers have initially learned about remote networks, routing protocols must maintain the routing tables so that they have the most current routing information. How the routing protocol maintains the routing table depends on the type of routing protocol (distance vector, link-state, or path vector) as well as the routing protocol itself (RIP, EIGRP, and so on). The exercise in the following section will reinforce your knowledge of routing table maintenance.

Distance Vector Table Maintenance Techniques Exercise

Periodic Updates

Explain the term *periodic update*.

The term periodic update refers to the fact that a router sends the complete routing table to its neighbors at a predefined interval, regardless of whether there has been a topology change.

The age of routing information in a routing table is refreshed each time an update is received. This way, information in the routing table can be maintained when there is a topology change.

List four ways that changes in the topology might occur.

- Failure of a link
- Introduction of a new link
- Failure of a router
- Change of link parameters

RIP Timers

In addition to the update timer, the IOS implements three additional timers for RIP. Briefly explain what these timers are and how they are used.

Invalid timer: If an update has not been received to refresh an existing route after 180 seconds (the default), the route is marked as invalid by setting the metric to 16. The route is retained in the routing table until the flush timer expires.

Flush timer: By default, the flush timer is set for 240 seconds, which is 60 seconds longer than the invalid timer. When the flush timer expires, the route is removed from the routing table.

Hold-down timer: This timer stabilizes routing information and helps prevent routing loops during periods when the topology is converging on new information. When a route is marked as unreachable, it must stay in hold-down mode long enough for all routers in the topology to learn about the unreachable network. By default, the hold-down timer is set for 180 seconds. The hold-down timer is discussed in more detail later in this chapter.

What two commands will show timer values?

show ip route

show ip protocols

Which command shows the most information about timer values?

show ip protocols

EIGRP Updates

Unlike other distance vector routing protocols, EIGRP does not send periodic updates. Describe the type of updates EIGRP uses.

EIGRP uses the following types of updates:

- **Nonperiodic:** They are not sent out on a regular basis.
- **Partial:** These updates are sent only when there is a change in topology that influences routing information.
- **Bounded:** The propagation of partial updates is automatically bounded so that only those routers that need the information are updated.

Triggered Updates

To speed the convergence when there is a topology change, RIP uses triggered updates.

What is a triggered update?

A triggered update is a routing table update that is sent immediately in response to a routing change. Triggered updates do not wait for update timers to expire.

When are triggered updates sent?

Triggered updates are sent when

- An interface changes state (up or down)
- A route has entered (or exited) the “unreachable” state
- A route is installed in the routing table

Random Jitter

Describe random jitter and explain the problem it solves concerning routing updates.

Over time, the update interval across the routers in the topology can become synchronized, which can cause problems. As more routers’ timers become synchronized, more collisions of updates and more delays occur in the network.

To prevent the synchronization of updates between routers, the Cisco IOS uses a random variable, called RIP_JITTER, that varies the update interval randomly in a range from 25 to 30 seconds for the default 30-second interval.

Routing Loops

Routing loops can cause a severe impact on network performance. The following exercise will reinforce your knowledge of the causes and solutions of routing loops with distance vector routing protocols.

Routing Loop Concepts Exercise

Routing Loops

Briefly explain what a routing loop is.

A routing loop is a condition in which a packet is continuously transmitted within a series of routers without ever reaching its intended destination network.

How do routing loops occur?

A routing loop can occur when two or more routers have routing information that incorrectly indicates that a valid path to an unreachable destination exists.

List four ways that a routing loop can happen.

- Incorrectly configured static routes
- Incorrectly configured route redistribution (redistribution is a process of handing the routing information from one routing protocol to another routing protocol and is discussed in CCNP-level courses)
- Inconsistent routing tables not being updated because of slow convergence in a changing network
- Incorrectly configured or installed discard routes

Implications of Routing Loops

A routing loop can have a devastating effect on a network, resulting in degraded network performance or even network downtime.

List five effects that routing loops can have on a network.

- Link bandwidth will be used for traffic looping back and forth between the routers in a loop.
- A router's CPU will be strained because of looping packets.
- A router's CPU will be burdened with useless packet forwarding that will negatively impact the convergence of the network.
- Routing updates might get lost or might not be processed in a timely manner. These conditions would introduce additional routing loops, making the situation even worse.
- Packets can get lost in "black holes."

Routing Loop Prevention Mechanisms

There are five mechanisms available to eliminate routing loops:

- Defining a maximum metric to prevent a count to infinity
- Hold-down timers
- Split horizon
- Route poisoning or poison reverse
- Triggered updates

Triggered updates have already been covered. The remaining mechanisms are reviewed in the following discussion.

Count to Infinity

Explain the concept of count to infinity.

Count to infinity is a condition that exists when inaccurate routing updates increase the metric value to “infinity” for a network that is no longer reachable. Each protocol defines infinity at a different value.

To eventually stop the incrementing of the metric, “infinity” is defined by setting a maximum metric value. What is the maximum or infinity value for RIP? 16 hops

Hold-Down Timers

Briefly explain how hold-down timers prevent routing loops.

Hold-down timers are used to prevent regular update messages from inappropriately reinstating a route that might have gone bad. Hold-down timers instruct routers to hold any changes that might affect routes for a specified period of time. If a route is identified as down or possibly down, any other information for that route containing the same status, or worse, is ignored for a predetermined amount of time (the hold-down period). This means that routers will leave a route marked as unreachable in that state for a period of time that is long enough for updates to propagate the routing tables with the most current information.

Split Horizon Rule

What is the split horizon rule?

The split horizon rule says that a router should not advertise a network through the interface from which the update came.

Route Poisoning

What is route poisoning, and what is its purpose?

Route poisoning is marking a route as unreachable in a routing update that is sent to other routers. Unreachable is interpreted as a metric that is set to the maximum.

Route poisoning speeds the convergence process because the information about a downed network spreads more quickly than waiting for the hop count to reach “infinity.”

Split Horizon with Poison Reverse

What is split horizon with poison reverse, and why is it a routing loop prevention mechanism?

The rule for split horizon with poison reverse states that when sending updates out a specific interface, designate any networks that were learned on that interface as unreachable. In other words, when receiving a route poisoning from a neighbor, the router immediately sends back a poison reverse. This prevents the originating router from being susceptible to incorrect updates about the downed network.

Distance Vector Routing Protocols Today

Although link-state routing protocols have several advantages over distance vector routing protocols, distance vector routing protocols are still in use today.

Comparing Distance Vector Routing Protocols

In Table 4-2, only the distance vector routing protocols are listed. For each characteristic, write a description for that routing protocol. If you need help, refer to Table 4-1.

Table 4-2 Comparing Distance Vector Routing Protocol Features

	RIPv1	RIPv2	IGRP	EIGRP
Speed of Convergence	Slow	Slow	Slow	Fast
Scalability—Size of Network	Small	Small	Small	Large
Use of VLSM	No	Yes	No	Yes
Resource Usage	Low	Low	Low	Medium
Implementation and Maintenance	Simple	Simple	Simple	Complex

Labs and Activities



Lab 4-1: Routing Table Interpretation (4.6.1)

Upon completion of this lab, you will be able to

- Interpret router output
- Identify the IP addresses for each router
- Draw a diagram of the network topology
- Cable and configure a network based on the topology diagram
- Test and verify full connectivity
- Reflect on and document the network implementation

Scenario

In this lab activity, you must re-create a network based only on the outputs from the **show ip route** command. Match the addresses to the corresponding interfaces and enter the information in Table 4-3. Configure the routers and verify connectivity. When complete, the outputs from the **show ip route** command must be exactly the same as the supplied outputs. The **show ip route** command displays the current state of the routing table.

Task 1: Examine the Router Output

Step 1. Examine the output from the HQ router.

```
HQ# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```

      10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.252 is directly connected, Serial0/0/0
      172.16.0.0/30 is subnetted, 1 subnets
C       172.16.100.0 is directly connected, Serial0/0/1
R      192.168.1.0/24 [120/1] via 10.10.10.254, 00:00:03, Serial0/0/0
R      192.168.2.0/24 [120/1] via 10.10.10.254, 00:00:03, Serial0/0/0
R      192.168.3.0/24 [120/1] via 10.10.10.254, 00:00:03, Serial0/0/0
C      192.168.4.0/24 is directly connected, Loopback0
C      192.168.5.0/24 is directly connected, Loopback1
C      192.168.6.0/24 is directly connected, Loopback2
R      192.168.7.0/24 [120/1] via 172.16.100.2, 00:00:04, Serial0/0/1
```

```
R 192.168.8.0/24 [120/1] via 172.16.100.2, 00:00:04, Serial0/0/1
R 192.168.9.0/24 [120/1] via 172.16.100.2, 00:00:04, Serial0/0/1
```

Step 2. Examine the output from the BRANCH1 router.

```
BRANCH1# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
10.0.0.0/30 is subnetted, 1 subnets
C    10.10.10.252 is directly connected, Serial0/0/0
R    172.16.0.0/16 [120/1] via 10.10.10.253, 00:00:04, Serial0/0/0
C    192.168.1.0/24 is directly connected, Loopback0
C    192.168.2.0/24 is directly connected, Loopback1
C    192.168.3.0/24 is directly connected, Loopback2
R    192.168.4.0/24 [120/1] via 10.10.10.253, 00:00:04, Serial0/0/0
R    192.168.5.0/24 [120/1] via 10.10.10.253, 00:00:04, Serial0/0/0
R    192.168.6.0/24 [120/1] via 10.10.10.253, 00:00:04, Serial0/0/0
R    192.168.7.0/24 [120/2] via 10.10.10.253, 00:00:04, Serial0/0/0
R    192.168.8.0/24 [120/2] via 10.10.10.253, 00:00:04, Serial0/0/0
R    192.168.9.0/24 [120/2] via 10.10.10.253, 00:00:04, Serial0/0/0
```

Step 3. Examine the output from the BRANCH2 router.

```
BRANCH2# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
R 10.0.0.0/8 [120/1] via 172.16.100.1, 00:00:19, Serial0/0/1
172.16.0.0/30 is subnetted, 1 subnets
C    172.16.100.0 is directly connected, Serial0/0/1
R 192.168.1.0/24 [120/2] via 172.16.100.1, 00:00:19, Serial0/0/1
R 192.168.2.0/24 [120/2] via 172.16.100.1, 00:00:19, Serial0/0/1
R 192.168.3.0/24 [120/2] via 172.16.100.1, 00:00:19, Serial0/0/1
R 192.168.4.0/24 [120/1] via 172.16.100.1, 00:00:19, Serial0/0/1
```

```

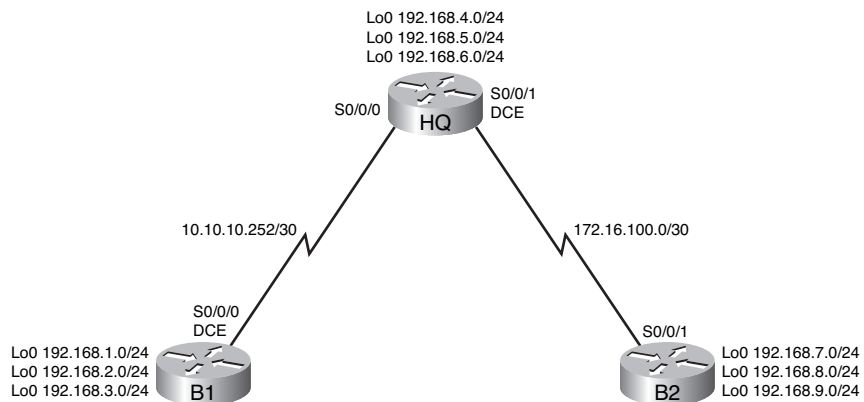
R    192.168.5.0/24 [120/1] via 172.16.100.1, 00:00:19, Serial0/0/1
R    192.168.6.0/24 [120/1] via 172.16.100.1, 00:00:19, Serial0/0/1
C    192.168.7.0/24 is directly connected, Loopback0
C    192.168.8.0/24 is directly connected, Loopback1
C    192.168.9.0/24 is directly connected, Loopback2

```

Task 2: Create a Diagram of the Network Based on the Router Output

Step 1. Draw a diagram of the network based on your interpretation of the router outputs in the following space provided.

Figure 4-4 Topology Diagram for Lab 4-1 (Answer)



Step 2. Document the interface addresses in Table 4-3.

Table 4-3 Addressing Table for Lab 4-1

Device	Interface	IP Address	Subnet Mask
HQ	S0/0/0	10.10.10.253	255.255.255.252
	S0/0/1	172.16.100.1	255.255.255.252
	Loopback0	192.168.4.1	255.255.255.0
	Loopback1	192.168.5.1	255.255.255.0
	Loopback2	192.168.6.1	255.255.255.0
BRANCH1	S0/0/0	10.10.10.254	255.255.255.252
	Loopback0	192.168.1.1	255.255.255.0
	Loopback1	192.168.2.1	255.255.255.0
	Loopback2	192.168.3.1	255.255.255.0
BRANCH2	S0/0/1	172.16.100.2	255.255.255.252
	Loopback0	192.168.7.1	255.255.255.0
	Loopback1	192.168.8.1	255.255.255.0
	Loopback2	192.168.9.1	255.255.255.0

Task 3: Create the Network

Step 1. Cable a network that is similar to the one in the topology diagram you just created in Figure 4-4.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Note: If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions will appear different.

Step 2. Clear any existing configurations on the routers.

Step 3. Configure the HQ, BRANCH1, and BRANCH2 routers.

Configure the interfaces on the HQ, BRANCH1, and BRANCH2 routers with the IP addresses from the addressing table. The clock rate, DTE assignment, and DCE assignment of the serial interfaces are at your discretion.

Task 4: Configure the Routing Protocol for Each Router

Step 1. Enable the RIP routing protocol on the BRANCH1 router.

The RIP routing protocol will be used to advertise directly connected networks to the other routers in the topology. RIP configuration will be covered in greater detail in a later lab activity. The basic configuration steps necessary for this lab activity are provided here.

To enable RIP, enter global configuration mode and use the **router rip** command.

```
BRANCH1(config)# router rip
BRANCH1(config-router)#
```

Step 2. Enter the classful network addresses for each directly connected network.

After you are in router configuration mode, enter the classful network address for each directly connected network, using the **network** command. An example of the **network** command is as follows:

```
BRANCH1(config-router)# network 192.168.1.0
BRANCH1(config-router)#
```

Be sure to configure a **network** statement for each network that is attached to a serial or loopback interface of the router.

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM:

```
BRANCH1(config-router)# end
%SYS-5-CONFIG_I: Configured from console by console
BRANCH1# copy run start
```

Step 3. Configure RIP on the HQ and BRANCH2 routers.

Use the **router rip** and **network** commands to configure the HQ and BRANCH2 routers to advertise directly connected networks to the other routers in the topology.

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

Step 4. Test and verify connectivity.

Use the **ping** command to verify that the router interfaces can communicate with each other. If you discover that two interfaces cannot ping each other, troubleshoot your IP addressing and router configuration.

Task 5: Document the Router Configurations

On each router, capture the following command output to a text file and save for future reference:

- Running configuration.
- Routing table. The output of the **show ip route** command for each of the routers should be the same as the provided outputs.
- Interface summarization.

Task 6: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.



Packet Tracer Companion: Routing Table Interpretation (4.6.1)

This lab does not have a starter file for you to open in Packet Tracer. However, create your own network from scratch using the topology in Figure 4-4 and the addressing in Table 4-3. Use the commands in Task 4 to configure routing. Then you should be able to verify that your routing tables in the Packet Tracer network you created look similar to the routing tables shown in Task 1. When finished, save your Packet Tracer file as LSG02-Lab441-end.pka.



Packet Tracer Skills Integration Challenge

Introduction

This activity focuses on subnetting skills, basic device configurations, and static routing. After you have configured all devices, test for end-to-end connectivity and examine your configuration. Open the file LSG02-PTSkills4.pka on the CD-ROM that accompanies this book. Use the topology in Figure 4-5 and the addressing table in Table 4-4 to document your design.

Upon completion of this skills integration challenge, you will be able to

- Design and document an addressing scheme based on requirements
- Apply a basic configuration to the devices
- Configure static and default routing
- Verify full connectivity between all devices in the topology

Task 1: Design and Document an Addressing Scheme

Step 1. Design an addressing scheme.

Using the topology in Figure 4-5 and the following requirements, design an addressing scheme:

- The WAN link between R1 and ISP is already configured.
- For the WAN links between R1 and the branch routers (B1, B2, B3, and B4), subnet the address space 10.0.1.0/28 to provide the necessary WAN subnets. Assign the subnets using the following guidelines:
 - Subnet 0: R1 <—> B1 [10.0.1.0/30](#)
 - Subnet 1: R1 <—> B2 [10.0.1.4/30](#)
 - Subnet 2: R1 <—> B3 [10.0.1.8/30](#)
 - Subnet 3: R1 <—> B4 [10.0.1.12/30](#)
- For the LANs attached to the branch routers, divide the address space 10.1.0.0/16 into four equal subnets. Assign the subnets using the following guidelines:
 - Subnet 0: B1 LANs [10.1.0.0/18](#)
 - Subnet 1: B2 LANs [10.1.64.0/18](#)
 - Subnet 2: B3 LANs [10.1.128.0/18](#)
 - Subnet 3: B4 LANs [10.1.192.0/18](#)
- For each branch router, divide that router's LAN subnet into four equal subnets. Assign the subnets using the following guidelines:

B1 LANs:

- Subnet 0: B1 Fa0/0 [10.1.0.0/20](#)
- Subnet 1: B1 Fa0/1 [10.1.16.0/20](#)
- Subnet 2: B1 Fa1/0 [10.1.32.0/20](#)
- Subnet 3: B1 Fa1/1 [10.1.48.0/20](#)

B2 LANs:

- Subnet 0: B2 Fa0/0 [10.1.64.0/20](#)
- Subnet 1: B2 Fa0/1 [10.1.80.0/20](#)
- Subnet 2: B2 Fa1/0 [10.1.96.0/20](#)
- Subnet 3: B2 Fa1/1 [10.1.112.0/20](#)

B3 LANs:

- Subnet 0: B3 Fa0/0 [10.1.128.0/20](#)
- Subnet 1: B3 Fa0/1 [10.1.144.0/20](#)
- Subnet 2: B3 Fa1/0 [10.1.160.0/20](#)
- Subnet 3: B3 Fa1/1 [10.1.176.0/20](#)

B4 LANs:

- Subnet 0: B4 Fa0/0 [10.1.192.0/20](#)
- Subnet 1: B4 Fa0/1 [10.1.208.0/20](#)
- Subnet 2: B4 Fa1/0 [10.1.224.0/20](#)
- Subnet 3: B4 Fa1/1 [10.1.240.0/20](#)

Step 2. Document the addressing scheme.

- On the topology in Figure 4-5, label each subnet in the blanks provided.
- In Table 4-4, document the IP addresses and subnet masks. Assign the first IP address to the router interface.
- For the WAN links, assign the first IP address to R1.

Figure 4-5 Packet Tracer Skills Integration Challenge Topology (Answer)

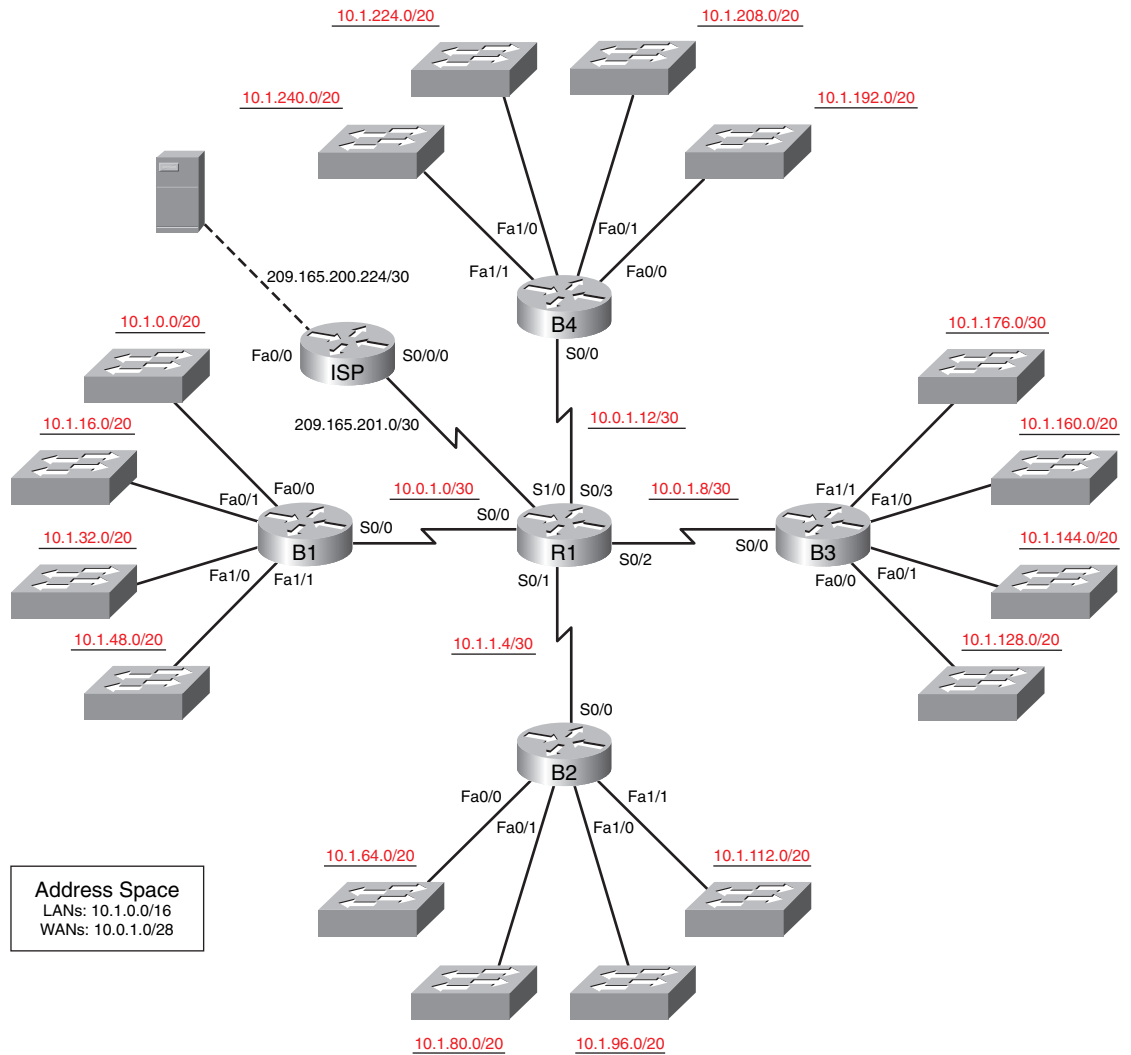


Table 4-4 Addressing Table for Packet Tracer Challenge

Device	Interface	IP Address	Subnet Mask
R1	S0/0	10.0.1.1	255.255.255.252
	S0/1	10.0.1.5	255.255.255.252
	S0/2	10.0.1.9	255.255.255.252
	S0/3	10.0.1.13	255.255.255.252
	S1/0	209.165.201.2	255.255.255.252
B1	Fa0/0	10.1.0.1	255.255.240.0
	Fa0/1	10.1.16.1	255.255.240.0
	Fa1/0	10.1.32.1	255.255.240.0
	Fa1/1	10.1.48.1	255.255.240.0
	S0/0	10.0.0.2	255.255.255.252
B2	Fa0/0	10.1.64.1	255.255.240.0
	Fa0/1	10.1.80.1	255.255.240.0
	Fa1/0	10.1.96.1	255.255.240.0
	Fa1/1	10.1.112.1	255.255.240.0
	S0/0	10.0.1.6	255.255.255.252
B3	Fa0/0	10.1.128.1	255.255.240.0
	Fa0/1	10.1.144.1	255.255.240.0
	Fa1/0	10.1.160.1	255.255.240.0
	Fa1/1	10.1.176.1	255.255.240.0
	S0/0	10.0.1.10	255.255.255.252
B4	Fa0/0	10.1.192.1	255.255.240.0
	Fa0/1	10.1.208.1	255.255.240.0
	Fa1/0	10.1.224.1	255.255.240.0
	Fa1/1	10.1.240.1	255.255.240.0
	S0/0	10.0.1.14	255.255.255.252
ISP	S0/0	209.165.201.1	255.255.255.252
	Fa0/0	209.165.200.225	255.255.255.252
Web Server	NIC	209.165.200.226	255.255.255.252

Task 2: Apply a Basic Configuration

Using your documentation, configure the routers with basic configurations including addressing. Use **cisco** as the line passwords and **class** as the secret password. Use **64000** as the clock rate.

Task 3: Configure Static and Default Routing

Configure static and default routing using the exit interface argument:

- R1 should have four static routes and one default route.
- B1, B2, B3, and B4 should have one default route each.
- ISP should have two static routes: one for the WAN address space and one for the LAN address space.

Task 4: Test Connectivity and Examine the Configuration

Step 1. Test connectivity.

- You should now have end-to-end connectivity. Use ping to test connectivity across the network. Each router should be able to ping all other router interfaces and the web server.
- Use extended ping to test LAN connectivity to the web server. For example, the test the Fa0/0 interface on B1, you would do the following:

```
B1# ping
Protocol [ip]:
Target IP address: 209.165.200.226
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: yes
Source address or interface: 10.1.0.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2
seconds:
Packet sent with a source address of 10.1.0.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 67/118/138
ms
```

- Troubleshoot until pings are successful.

Step 2. Examine the configuration.

Use verification commands to make sure that your configurations are complete.

RIP Version 1

The Study Guide portion of this chapter uses a combination of matching, fill-in-the-blank, multiple-choice, and open-ended question exercises to test your knowledge and skills of RIPv1 concepts and configuration.

The Labs and Activities portion of this chapter includes all the online curriculum labs to ensure that you have mastered the practical, hands-on skills needed to understand RIPv1 routing.

As you work through this chapter, use Chapter 5 in *Routing Protocols and Concepts, CCNA Exploration Companion Guide* or use the corresponding Chapter 5 in the Exploration Routing Protocols and Concepts online curriculum for assistance.

Study Guide

RIPv1: Distance Vector, Classful Routing Protocol

RIPv1 is a distance vector routing protocol for IPv4. RIPv1 is also a classful routing protocol. In the following sections, you will focus on the basic RIP concepts.

RIP Concepts Exercise

Background and Perspective

RIP is the oldest of the [distance vector](#) routing protocols. However, RIP is not a protocol “on the way out.” In fact, an IPv6 form of RIP called [RIPng](#) (next generation) is now available.

RIP Historical Impact

RIP evolved from an earlier protocol developed at Xerox, called [Gateway Information Protocol \(GWINFO\)](#). It later gained popularity because it was implemented in the [Berkeley Software Distribution \(BSD\)](#) as a daemon named [routed](#). Various other vendors made their own, slightly different implementations of RIP. Recognizing the need for standardization of the protocol, Charles Hedrick wrote RFC [1058](#) in 1988, in which he documented the existing protocol and specified some improvements. Since then, RIP has been improved with [RIPv2](#) in 1994 and with [RIPng](#) in 1997.

RIP Characteristics

As discussed in Chapter 4, “Distance Vector Routing Protocols,” RIP has the following key characteristics:

- It is a [distance vector](#) routing protocol.
- It uses [hop count](#) as its only metric for path selection.
- Advertised routes with [hop counts](#) greater than [15](#) are unreachable.
- Messages are broadcast every [30](#) seconds.

Figure 5-1 shows an encapsulated RIPv1. Fill in the missing field content.

Figure 5-1 Encapsulated RIPv1 Message (Answer)

Data Link Frame Header	IP Packet Header	UDP Segment Header	RIP Message (512 Bytes; Up to 25 Routes)
Data Link Frame:			
MAC Source Address = Address of Sending Interface			
MAC Destination Address = <u>Broadcast: FF-FF-FF-FF-FF-FF</u>			
IP Packet:			
IP Source Address = Address of Sending Interface			
IP Destination Address = <u>Broadcast: 255.255.255.255</u>			
Protocol Field = <u>17 for UDP</u>			
UDP Segment:			
Source Port = <u>520</u>			
Destination Port = <u>520</u>			
RIP Message:			
Command: <u>Request</u> (1); <u>Response</u> (2)			
Version = 1			
Address Family ID = 2 for IP			
Routes: Network IP Address			
Metric: <u>Hop Count</u>			

RIP Message Format: RIP Header

Figure 5-2 shows the detail of a RIPv1 message. Fill in the missing field content.

Figure 5-2 RIPv1 Message Format (Answer)

	0	7	8	15	16	23	24	31
Route Entry	<u>Command = 1 or 2</u>		<u>Version = 1</u>		Must be Zero			
	<u>Address Family Identifier (2 = IP)</u>				Must be Zero			
	<u>IP Address (Network Address)</u>							
	Must be Zero							
	Must be Zero							
	<u>Metric (Hops)</u>							
	Multiple Route Entries, upto a maximum of 25.							

RIP Message Format: Route Entry

The route entry portion of the message includes three fields with content: Address family identifier, IP address, and Metric. This route entry portion represents one destination route with its associated metric. One RIP update can contain up to 25 route entries. The maximum datagram size is 512 bytes, not including the IP or UDP headers.

RIP Operation

RIP uses two message types specified in the Command field: Request message and Response message. Each RIP-configured interface sends out a Request message on startup, requesting that all RIP neighbors send their complete routing tables. A Response message is sent back by RIP-enabled neighbors. When the requesting router receives the responses, it evaluates each route entry. If a route entry is new, the receiving router installs the route in the routing table. If the route is already in the table,

the existing entry is replaced if the new entry has a better [hop count](#). The startup router then sends a [triggered](#) update out all RIP-enabled interfaces containing its own [routing table](#) so that RIP neighbors can be informed of any new routes.

You might recall from previous studies that IP addresses assigned to hosts were initially divided into three classes: Class A, Class B, and Class C. Knowing the default subnet mask for each class is important to understanding how RIP operates. In Figure 5-3, label whether an octet is Network or Host and indicate the default subnet mask for each class.

Figure 5-3 Default Subnet Masks for Address Classes (Answer)

	8 Bits	8 Bits	8 Bits	8 Bits
Class A:	<u>Network</u> 255	<u>Host</u> 0	<u>Host</u> 0	<u>Host</u> 0
Class B:	<u>Network</u> 255	<u>Network</u> 255	<u>Host</u> 0	<u>Host</u> 0
Class C:	<u>Network</u> 255	<u>Network</u> 255	<u>Network</u> 255	<u>Host</u> 0

RIP is a classful routing protocol. As you might have realized from the previous message format discussion, RIPv1 does not send [subnet mask](#) information in the update. Therefore, a router either uses the [subnet mask](#) configured on a local [interface](#) or applies the default [subnet mask](#) based on the [address class](#). Because of this limitation, RIPv1 networks cannot be [discontiguous](#), nor can they implement [VLSM](#).

[Administrative distance](#) (AD) is the trustworthiness (or preference) of the route source. RIP has a default AD of [120](#).

What two command outputs display the AD value?

[show ip route](#)

[show ip protocols](#)

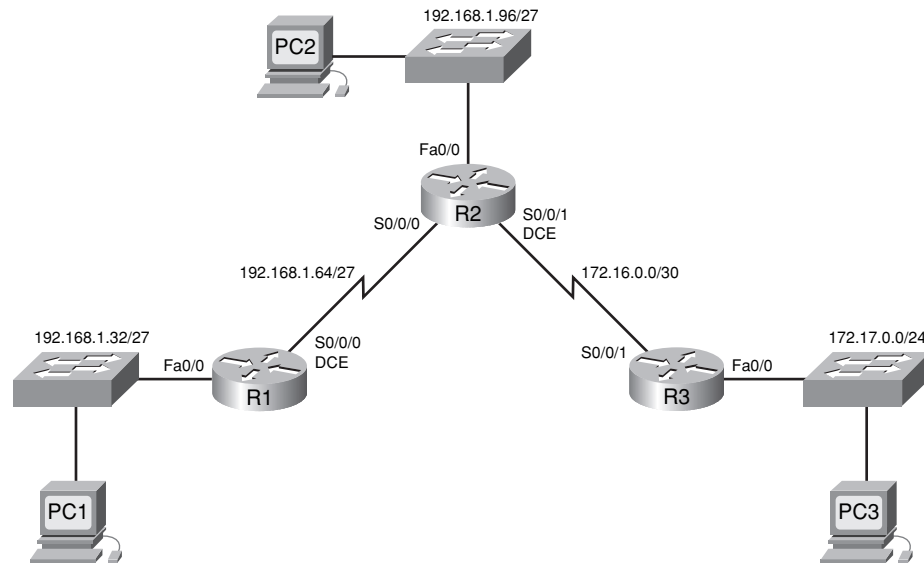
Basic RIPv1 Configuration

In the following sections, you will design an addressing scheme and then use Packet Tracer to implement it. Then you will configure RIP routing and passive interfaces.

Document the Addressing Scheme

Refer to the topology shown in Figure 5-4. Use Table 5-1 to document the IP addresses for all the interfaces and PCs. Use the following guidelines to ensure that your addresses will work with Packet Tracer Exercise 5-1.

1. Assign the first IP address for all LANs to the router interface.
2. Assign R2 the first IP address for all WAN links to the other routers.
3. Assign R1 and R3 the second IP address for the WAN link to R2.
4. Assign the last IP address in each LAN to the PC.

Figure 5-4 RIPv1 Study Guide Topology**Table 5-1** Addressing Table for RIPv1 Study Guide Topology

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.33	255.255.255.224	—
	S0/0/0	192.168.1.66	255.255.255.224	—
R2	Fa0/0	192.168.1.97	255.255.255.224	—
	S0/0/0	192.168.1.65	255.255.255.224	—
	S0/0/1	172.16.0.1	255.255.255.252	—
R3	Fa0/0	172.17.0.1	255.255.255.0	—
	S0/0/1	172.16.0.2	255.255.255.252	—
PC1	NIC	192.168.1.62	255.255.255.224	192.168.1.33
PC2	NIC	192.168.1.126	255.255.255.224	192.168.1.97
PC3	NIC	172.17.0.254	255.255.255.0	172.17.0.1

Packet Tracer
 Activity

Packet Tracer Exercise 5-1

Now you are ready to use Packet Tracer to apply your documented addressing scheme. Open file LSG02-0501.pka on the CD-ROM that accompanies this book to perform this exercise using Packet Tracer.

Task 1: Basic Router Configuration

Step 1. Use the following guidelines to configure the host name, banner, enable secret password, and lines for R1, R2, and R3. Packet Tracer will only grade the host name configurations.

- To avoid incorrect grading, make sure that the router names are configured in ALL CAPS.
- Use the following text for the banner: **Authorized Access Only**.
- For the secret password, use **class**.
- For the console and Telnet lines, configure login access with the password **cisco**.

Step 2. Configure the router interfaces according to the following guidelines.

- Use the IP address and subnet mask according to the addressing table in the section “Document the Addressing Scheme,” earlier in this chapter.
- Configure the description for each interface (Packet Tracer will not grade this configuration).
- Configure clocking signals at 64000 bps where necessary.
- Activate the interfaces.

Your completion percentage should be 60%. If not, review the previous steps to see what part of the task you left incomplete.

Step 3. Save your configurations for R1, R2, and R3.

Task 2: Configure PCs

Configure the PCs according to the addressing table in Table 5-1, with IP address, subnet mask, and connectivity to the default gateway.

Your completion percentage should be 81%. If not, review the previous step to see what part of the task you left incomplete.

After completing this task, save your Packet Tracer file to use again in the next section. Save the file as LSG02-0501-task2.pkt.

Configuring RIP as the Routing Protocol

To enter router configuration mode for RIP, enter **router rip** at the [global configuration](#) prompt.

What is the router prompt at this point?

```
R1(config-router)#
```

What command would you enter to remove the RIP routing process from a device?

```
R1(config)# no router rip
```

[This command stops the RIP process and erases all existing RIP configurations.](#)

To enable RIP routing for a network, use the **network** command in router configuration mode and enter the classful [network](#) address for each [directly connected](#) network.

What two functions does this command achieve?

- Enables RIP on all interfaces that belong to a specific network. Associated interfaces will now both send and receive RIP updates.
- Advertises the specified network in RIP routing updates sent to other routers every 30 seconds.

List the commands you will use for R1, R2 and R3.

R1 RIP configurations:

```
R1(config-router)# network 192.168.1.0
```

R2 RIP configurations:

```
R2(config-router)# network 192.168.1.0
```

```
R2(config-router)# network 172.16.0.0
```

R3 RIP configurations:

```
R3(config-router)# network 172.16.0.0
```

```
R3(config-router)# network 172.17.0.0
```



Packet Tracer Exercise 5-1 (Continued)

Open your LSG02-0501-task2.pka saved version of this Packet Tracer Exercise and complete the task that follows.

Task 3: Configure RIP Routing

Step 1. Configure RIP routing on R1, R2, and R3.

Step 2. Verify that each router has a full routing table.

Your completion percentage should be 93%. If not, review the previous steps to see what part of the task you left incomplete.

After completing this task, save your Packet Tracer file to use again in the next section. Save the file as LSG02-0501-task3.pkt.

Verification and Troubleshooting

It is important to be able to verify and troubleshoot your routing configuration. Verifying routing operations immediately after configuration will help solve any potential troubleshooting issues that might arise later. The exercises in the following sections reinforce your understanding of three important troubleshooting commands: **show ip route**, **show ip protocols**, and **debug ip rip**.

show ip route Command

Examining the routing table is an easy way to see whether the routing protocol and commands have been properly configured. In Figure 5-5, the routing table for R2 is shown. Fill in the missing parts of the command output. If necessary, refer to your saved version of LSG02-0501-task3.pka. However, you should be able to determine all the missing information using the topology shown in Figure 5-4 and the addressing information you completed in Table 5-1.

Figure 5-5 show ip route Command (Answer)

```

R2#show ip route
<code output omitted>

Gateway of last resort is not set

R      172.17.0.0/16 [120/1] via 172.16.0.2, 00:00:02, Serial0/0/1
      172.16.0.0/30 is subnetted, 1 subnets
C      172.16.0.0 is directly connected, Serial0/0/1
      192.168.1.0/27 is subnetted, 3 subnets
C      192.168.1.96 is directly connected, FastEthernet0/0
C      192.168.1.64 is directly connected, Serial0/0/0
R      192.168.1.32 [120/1] via 192.168.1.66, 00:00:12, Serial0/0/0

```

Interpreting show ip route Output

Now focus on one RIP route learned by R3 and interpret the output shown in the routing table:

```
R      192.168.1.0/24 [120/1] via 172.16.0.1, 00:00:04, Serial0/0/1
```

Table 5-2 lists the individual parts of the route in the left column. In the right column, provide a brief a description for each part of the route.

Table 5-2 Interpreting a Route

Output	Description
R	Identifies the source of the route as RIP.
192.168.1.0	Indicates the address of the remote network.
/24	Shows the subnet mask used for this network.
[120/1]	Indicates the administrative distance (120) and the metric (1 hop).
via 172.16.0.1,	Specifies the address of the next-hop router (R2) to send traffic to for the remote network.
00:00:04,	Specifies the amount of time since the route was updated (here, 4 seconds). Another update is due in 26 seconds.
Serial0/0/1	Specifies the local interface through which the remote network can be reached.

show ip protocols Command

Another useful command for verifying RIP or other routing protocols is the **show ip protocols** command. If a network is missing from the routing table, check the routing configuration using **show ip protocols**.

In Figure 5-6, the **show ip protocols** output for R2 is shown. Fill in the missing parts of the command output. If necessary, refer to your saved version of LSG02-0501-task3.pka. However, you should be able to determine all the missing information using the topology shown in Figure 5-4 and the addressing information you completed in Table 5-1.

Figure 5-6 show ip protocols Command (Answer)

```

R2#show ip protocols
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 22 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 1, receive any version
  Interface          send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0    1     1 2
  Serial0/0/0        1     1 2
  Serial0/0/1        1     1 2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
  172.16.0.0
  192.168.1.0
  Routing Information Sources:
  Gateway            Distance    Last Update
  192.168.1.66       120        00:00:10
  172.16.0.2         120        00:00:03
  Distance: (default is 120)

```

The **show ip protocols** command displays the routing protocol that is currently configured on the router. This output can be used to verify most RIP parameters to confirm that

- **RIP routing** is configured.
- The correct **interfaces** send and receive RIP **updates**.
- The router advertises the correct **networks**.
- RIP **neighbors** are sending **updates**.

debug ip rip Command

Most RIP configuration errors involve an incorrect **network** statement configuration, a missing **network** statement configuration, or the configuration of discontinuous subnets in a classful environment. The **debug** command is a useful tool to help diagnose and resolve these networking problems.

In Figure 5-7, the **debug ip rip** output for R2 is shown. Fill in the missing parts of the command output. If necessary, refer to your saved version of LSG02-0501-task3.pka. However, you should be able to determine all the missing information using the topology shown in Figure 5-4 and the addressing information you filled out in Table 5-1.

Figure 5-7 debug ip rip Command (Answer)

```

R2#debug ip rip
RIP protocol debugging is on
① { RIP: received v1 update from 192.168.1.66 on Serial0/0/0
    192.168.1.32 in 1 hops
② { RIP: received v1 update from 172.16.0.2 on Serial0/0/1
    172.17.0.0 in 1 hops
③ { RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0 (192.168.1.97)
    RIP: build update entries
        network 172.16.0.0 metric 1
        network 172.17.0.0 metric 2
        subnet 192.168.1.32 metric 2
        subnet 192.168.1.64 metric 1
④ { RIP: sending v1 update to 255.255.255.255 via Serial0/0/1 (172.16.0.1)
    RIP: build update entries
        network 192.168.1.0 metric 1
⑤ { RIP: sending v1 update to 255.255.255.255 via Serial0/0/0 (192.168.1.65)
    RIP: build update entries
        network 172.16.0.0 metric 1
        network 172.17.0.0 metric 2
        subnet 192.168.1.96 metric 1
R2#undebug all
All possible debugging has been turned off

```

Passive Interfaces

R1, R2, and R3 are currently sending out RIP updates on all interfaces—including LAN interfaces out which there is no RIP neighbor.

Describe three ways these unnecessary updates negatively impact the LAN environment.

- Bandwidth is wasted transporting unnecessary updates. Because RIP updates are broadcast, switches will forward the updates out all ports.
- All devices on the LAN must process the update up to the transport layers, where the receiving device will discard the update.
- Advertising updates on a broadcast network is a security risk. RIP updates can be intercepted with packet-sniffing software. Routing updates can be modified and sent back to the router, corrupting the routing table with false metrics that misdirect traffic.

What command, including the router prompt, do you use to stop unnecessary updates out an interface?

Router(config-router)# passive-interface interface



Packet Tracer Exercise 5-1 (Continued)

Open your LSG02-0501-task3.pka saved version of this Packet Tracer Exercise and complete the following tasks.

Task 4: Disable RIP Updates on Appropriate Interfaces

Step 1. Use the **debug ip rip** command on any of the routers. Notice that the routers are currently sending RIP updates out all active interfaces.

Step 2. On R1, R2, and R3, disable RIP updates on appropriate interfaces.

Your completion percentage should be 100%. If not, review the previous steps to see what part of the task you left incomplete.

Task 5: Verify Connectivity

All PCs and routers should have end-to-end connectivity. Pinging from any source to any destination should be successful. You can also click **Check Results** and then click the **Connectivity Tests** tab to see whether all the connectivity tests are successful.

Task 6: Save the Packet Tracer File

Save your Packet Tracer file as LSG02-0501-end.pka.

Automatic Summarization

Fewer number of routes in a routing table means that the routing table process can more quickly locate the route needed to forward the packet. Summarizing several routes into a single route is known as route summarization or route aggregation. Some routing protocols, such as RIP, automatically summarize routes on certain routers. The following sections reinforce your knowledge of automatic summarization and describe how RIP performs this automatic summarization.

Automatic Summarization Concepts

Boundary Routers and Automatic Summarization

RIP is a classful routing protocol that automatically summarizes classful networks across major network boundaries. In the topology shown earlier in Figure 5-4, which router or routers are boundary routers? Why?

R2 is a boundary router because it has interfaces in two different major classful networks: 192.168.1.0 and 172.16.0.0.

Boundary routers summarize RIP subnets from one major network to the other but advertise subnet addresses within the boundary.

What networks/subnets does R2 send to R3?

192.168.1.0

What networks/subnets does R2 send to R1?

192.168.1.96, 172.16.0.0, 172.17.0.0

If you are not sure, use **debug ip rip** on your LSG02-0501-end.pka file.

Rules for Processing RIPv1 Updates

In regard to RIP's classful operation, what two rules govern RIPv1 updates:

- If a routing update and the interface on which it is received belong to the same major network, the subnet mask of the interface is applied to the network in the routing update.
- If a routing update and the interface on which it is received belong to different major networks, the classful subnet mask of the network is applied to the network in the routing update.

Advantages and Disadvantages of Automatic Summarization

Automatic summarization has both advantages and disadvantages.

List two advantages to automatic summarization.

- Smaller routing updates are sent and received, which uses less bandwidth for routing updates between R2 and R3.
- A single route representing multiple networks results in a faster lookup process in the routing table.

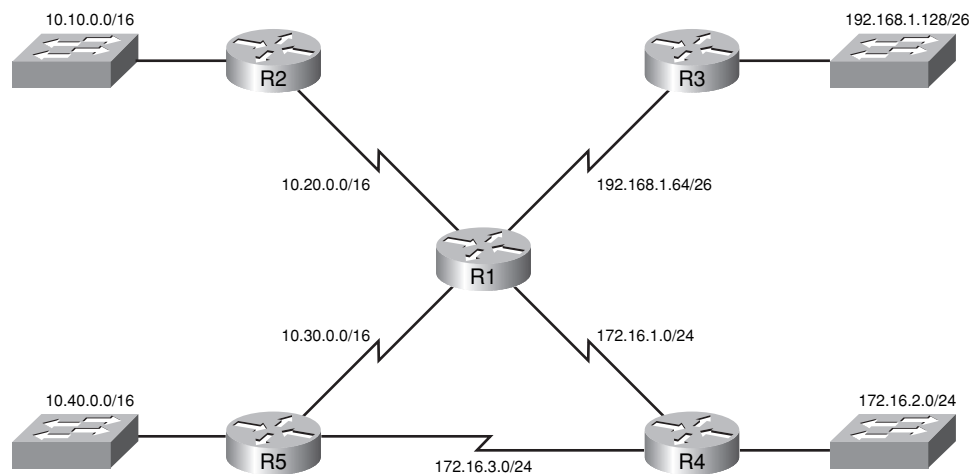
What is the main disadvantage of automatic summarization?

You cannot have discontinuous network configurations because these configurations do not converge.

Automatic Summarization Example

Figure 5-8 shows a topology with multiple classful networks. Answer the questions that follow the topology.

Figure 5-8 Automatic Summarization Example



What are the classful networks used in this topology? Also, indicate the default subnet mask for each.

10.0.0.0/8, 172.16.0.0/16, 192.168.1.0/24

Is the address assignment contiguous or discontinuous?

Contiguous

What router or routers are boundary routers, and what classful addresses are each the boundary of?

R1 is a boundary router for 10.0.0.0/8, 172.16.0.0/16, and 192.168.1.0/24.

R5 is a boundary router for 10.0.0.0/8 and 172.16.0.0/16.

Will the network be fully converged with RIPv1 routing?

Yes, because it is contiguous, RIPv1 will converge.

List the network/subnet mask entries that will be the routing table for each router. Remember that not all routers will have full knowledge of the individual subnets.

R1 routing table:

Network/subnet masks in R1's routing table:

10.10.0.0/16, 10.20.0.0/16, 10.30.0.0/16, 10.40.0.0/16, 172.16.1.0/24, 172.16.2.0/24, 172.16.3.0/24, 192.168.1.64/26, and 192.168.1.128/26

Network/subnet masks in R2's routing table:

10.10.0.0/16, 10.20.0.0/16, 10.30.0.0/16, 10.40.0.0/16, 172.16.0.0/16, and 192.168.1.0/24

Network/subnet masks in R3's routing table:

10.0.0.0/8, 172.16.0.0/16, 192.168.1.64/26 and 192.168.128/26

Network/subnet masks in R4's routing table:

10.0.0.0/8, 172.16.1.0/24, 172.16.2.0/24, 172.16.3.0/24, and 192.168.1.0/24

Network/subnet masks in R5's routing table:

10.10.0.0/16, 10.20.0.0/16, 10.30.0.0/16, 10.40.0.0/16, 172.16.1.0/24, 172.16.2.0/24, 172.16.3.0/24, and 192.168.1.0/24

Are there any other problems with this configuration?

Yes. R4 will have a suboptimal entry because it will load-balance between R1 and R5 when routing to the 10.0.0.0/8 classful network. This is suboptimal for the LAN attached to R5, which is best reached by always sending traffic directly to R5. In addition, when sending packets to the R2 LAN, R4 will load-balance between R1 and R5. This is also suboptimal because the best route is through R1.

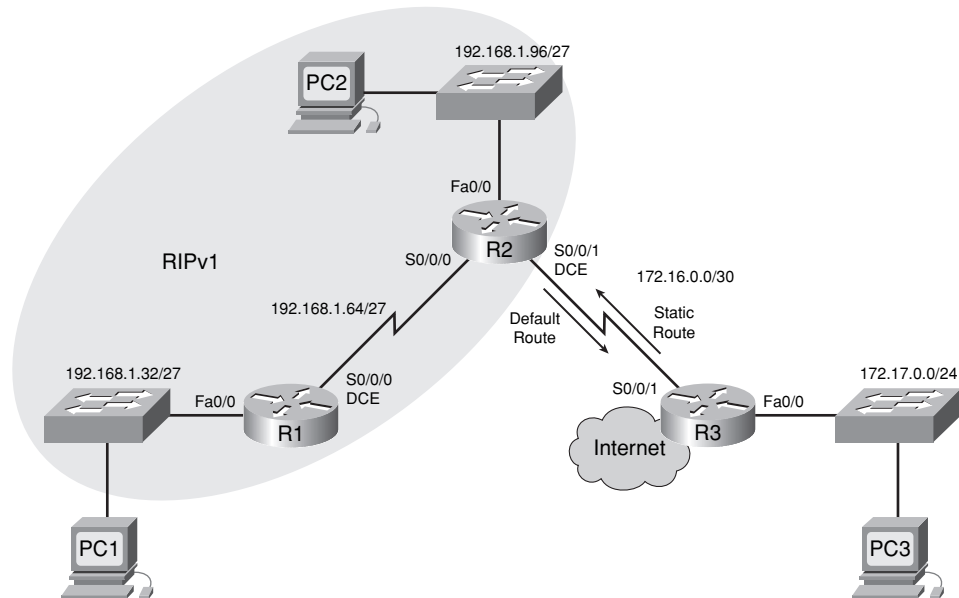
Although there is no Packet Tracer Activity file for you to use, you can test your answers to the preceding questions by building and configuring the topology shown in Figure 5-8 from scratch.

Default Routes and RIPv1

Default routes are used by routers to represent all routes that are not specifically in the routing table. In the following sections, you will configure the topology to use default routing.

Default Routing Exercise

Figure 5-9 shows the modified topology to include static and default routing. R3 is the service provider with access to the Internet, as signified by the cloud. R3 and R2 do not exchange RIP updates. Instead, R2 uses a default route to reach the R3 LAN and all other destinations that are not listed in its routing table. R3 uses a summary static route to reach the subnets of 192.168.1.0/24.

Figure 5-9 Topology with Default Routing

What commands do you need to enter on R2 and R3 to modify the topology for this configuration?

On R2:

Remove network 172.16.0.0 from RIP and set the S0/0/1 interface to passive.

R2(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1

R2(config)# router rip

R2(config-router)# no network 172.16.0.0

R2(config-router)# passive-interface s0/0/1

On R3:

R3(config)# ip route 192.168.1.0 255.255.255.0 s0/0/1

R3(config)# no router rip

To provide Internet connectivity to all other networks in the RIP routing domain, the default static route needs to be advertised to all other routers that use the dynamic routing protocol.

What command will configure R2 to propagate the default route to R1?

R2(config-router)# default-information originate



Packet Tracer Exercise 5-2

Now you are ready to use Packet Tracer to configure default and static routing on the modified topology in Figure 5-9. Open file LSG02-0502.pka on the CD-ROM that accompanies this book to perform this exercise using Packet Tracer.

Task 1: Remove RIP Routing

Step 1. Using the commands you specified in the section “Default Routing Exercise,” earlier in this chapter, disable RIP routing on R3.

Step 2. Using the commands you specified in the section “Default Routing Exercise,” complete the following configurations of R2:

- Disable RIP for the appropriate network.
- Disable RIP updates on the appropriate interface.

Your completion percentage should be 25%. If not, review the previous steps to see what part of the task you left incomplete.

Task 2: Configure Default and Static Routing

Step 1. Configure R3 with the necessary static route. Use the exit interface argument.

Step 2. Configure R2 with a default route. Use the exit interface argument.

Step 3. Configure R2 to propagate the default route to other routers (R1, in this topology).

Your completion percentage should be 100%. If not, review the previous steps to see what part of the task you left incomplete.

Task 3: Verify Connectivity

All PCs and routers should have end-to-end connectivity. Pinging from any source to any destination should be successful. You can also click **Check Results** and then click the **Connectivity Tests** tab to see whether all the connectivity tests are successful.

Task 4: Save the Packet Tracer File

Save your Packet Tracer file as LSG02-0502-end.pka.

Labs and Activities

Command Reference

In Table 5-3, record the command, *including the correct router prompt*, that fits the description. Fill in any blanks with the appropriate missing information.

Table 5-3 Commands for Chapter 5, RIPv1

Command	Description
Router(config)# router rip	Starts the RIP routing process
Router(config-router)# network 10.0.0.0	Enables RIP updates on interfaces belonging to 10.0.0.0
Router(config-router)# passive-interface fa0/0	Stops RIP updates on the FastEthernet 0/0 interface
Router(config-router)# default-information originate	Configures this router to propagate a default route in RIP updates
Router# show ip protocols	Displays detailed information about all dynamic routing processes currently running on this router
Router# debug ip rip	Enables the monitoring of RIP updates as they are sent and received



Lab 5-1: Basic RIP Configuration (5.6.1)

Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Perform basic configuration tasks on a router
- Configure and activate interfaces
- Configure RIP routing on all routers
- Verify RIP routing using **show** and **debug** commands
- Reconfigure the network to make it contiguous
- Observe automatic summarization at a boundary router
- Gather information about RIP processing using the **debug ip rip** command
- Configure a static default route
- Propagate default routes to RIP neighbors
- Document the RIP configuration

Scenarios

- Scenario A: Running RIPv1 on Classful Networks
- Scenario B: Running RIPv1 with Subnets and Between Classful Networks
- Scenario C: Running RIPv1 on a Stub Network

Scenario A: Running RIPv1 on Classful Networks

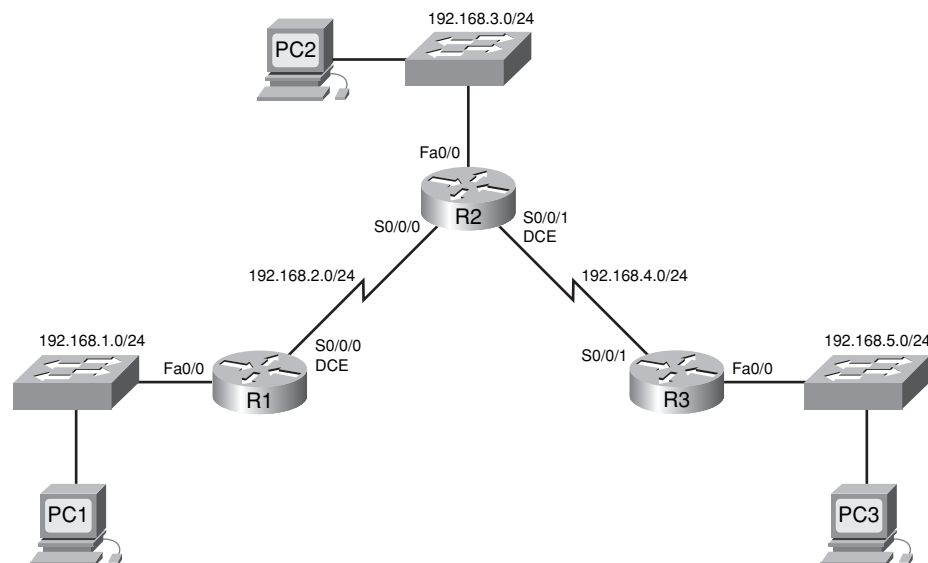
Task 1: Prepare the Network

Step 1. Cable a network that is similar to the one in the topology diagram shown in Figure 5-10.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Note: If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions will appear different.

Figure 5-10 Topology Diagram for Scenario A



Step 2. Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configurations

Perform basic configuration of the R1, R2, and R3 routers according to the following guidelines:

- Configure the router host name.
- Disable Domain Name System (DNS) lookup.
- Configure an EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for console connections.
- Configure a password for VTY connections.

Task 3: Configure and Activate Serial and Ethernet Addresses

Step 1. Configure interfaces on R1, R2, and R3.

Configure the interfaces on the R1, R2, and R3 routers with the IP addresses in Table 5-4.

Step 2. Verify IP addressing and interfaces.

Use the **show ip interface brief** command to verify that the IP addressing is correct and that the interfaces are active.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 3. Configure Ethernet interfaces of PC1, PC2, and PC3.

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses and default gateways from Table 5-4.

Step 4. Test the PC configuration by pinging the default gateway from the PC.

Table 5-4 Addressing Table for Scenario A

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	—
	S0/0/0	192.168.2.1	255.255.255.0	—
R2	Fa0/0	192.168.3.1	255.255.255.0	—
	S0/0/0	192.168.2.2	255.255.255.0	—
	S0/0/1	192.168.4.2	255.255.255.0	—
R3	Fa0/0	192.168.5.1	255.255.255.0	—
	S0/0/1	192.168.4.1	255.255.255.0	—
PC1	NIC	192.168.1.10	255.255.255.0	192.168.1.1
PC2	NIC	192.168.3.10	255.255.255.0	192.168.3.1
PC3	NIC	192.168.5.10	255.255.255.0	192.168.5.1

Task 4: Configure RIP

Step 1. Enable dynamic routing.

To enable a dynamic routing protocol, enter global configuration mode and use the **router** command.

Enter **router ?** at the global configuration prompt to see a list of available routing protocols on your router.

To enable RIP, enter the **router rip** command in global configuration mode.

```
R1(config)# router rip
R1(config-router)#
```

Step 2. Enter classful network addresses.

When you are in routing configuration mode, enter the classful network address for each directly connected network, using the **network** command:

```
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.2.0
R1(config-router)#
```

The **network** command does the following:

- Enables RIP on all interfaces that belong to this network. These interfaces will now both send and receive RIP updates.
- Advertises this network in RIP routing updates sent to other routers every 30 seconds.

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM:

```
R1(config-router)# end
%SYS-5-CONFIG_I: Configured from console by console
R1# copy run start
```

Step 3. Configure RIP on the R2 router using the **router rip** and **network** commands:

```
R2(config)# router rip
R2(config-router)# network 192.168.2.0
R2(config-router)# network 192.168.3.0
R2(config-router)# network 192.168.4.0
R2(config-router)# end
%SYS-5-CONFIG_I: Configured from console by console
R2# copy run start
```

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

Step 4. Configure RIP on the R3 router using the **router rip** and **network** commands:

```
R3(config)# router rip
R3(config-router)# network 192.168.4.0
R3(config-router)# network 192.168.5.0
R3(config-router)# end
%SYS-5-CONFIG_I: Configured from console by console
R3# copy run start
```

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

Task 5: Verify RIP Routing

Step 1. Use the **show ip route** command to verify that each router has all the networks in the topology entered in the routing table.

Routes learned through RIP are coded with an **R** in the routing table. If the tables are not converged as shown here, troubleshoot your configuration. Did you verify that the configured interfaces are active? Did you configure RIP correctly? Return to Task 3 and Task 4 to review the steps necessary to achieve convergence.

```
R1# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
<output omitted>
```

```
Gateway of last resort is not set
```

```
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:04, Serial0/0/0
R    192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:04, Serial0/0/0
R    192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:04, Serial0/0/0
```

```
R2# show ip route
```

```
<Output omitted>
```

```
R    192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:22, Serial0/0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:23, Serial0/0/1
```

```
R3# show ip route
```

```
<Output omitted>
```

```
R    192.168.1.0/24 [120/2] via 192.168.4.2, 00:00:18, Serial0/0/1
R    192.168.2.0/24 [120/1] via 192.168.4.2, 00:00:18, Serial0/0/1
R    192.168.3.0/24 [120/1] via 192.168.4.2, 00:00:18, Serial0/0/1
C    192.168.4.0/24 is directly connected, Serial0/0/1
C    192.168.5.0/24 is directly connected, FastEthernet0/0
```

Step 2. Use the **show ip protocols** command to view information about the routing processes.

The **show ip protocols** command can be used to view information about the routing processes that are occurring on the router. This output can be used to verify most RIP parameters to confirm the following:

- RIP routing is configured.
- The correct interfaces send and receive RIP updates.
- The router advertises the correct networks.
- RIP neighbors are sending updates.

```
R1# show ip protocols
```

```
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 16 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface          Send Recv Triggered RIP Key-chain
FastEthernet0/0      1    2  1
Serial0/0/0          1    2  1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  192.168.1.0
  192.168.2.0
Passive Interface(s):
Routing Information Sources:
  Gateway           Distance      Last Update
  192.168.2.2       120
Distance: (default is 120)
```

R1 is indeed configured with RIP. R1 is sending and receiving RIP updates on FastEthernet 0/0 and Serial 0/0/0. R1 is advertising networks 192.168.1.0 and 192.168.2.0. R1 has one routing information source. R2 is sending R1 updates.

Step 3. Use the **debug ip rip** command to view the RIP messages being sent and received.

Note: RIP updates are sent every 30 seconds, so you might have to wait for debug information to be displayed.

```
R1# debug ip rip
RIP: received v1 update from 192.168.2.2 on Serial0/0/0
      192.168.3.0 in 1 hops
      192.168.4.0 in 1 hops
      192.168.5.0 in 2 hops
RIP: sending v1 update to 255.255.255.255 via FastEthernet0/0
      (192.168.1.1)
RIP: build update entries
      network 192.168.2.0 metric 1
      network 192.168.3.0 metric 2
      network 192.168.4.0 metric 2
      network 192.168.5.0 metric 3
RIP: sending v1 update to 255.255.255.255 via Serial0/0/0 (192.168.2.1)
RIP: build update entries
      network 192.168.1.0 metric 1
```

The debug output shows that R1 receives an update from R2. Notice how this update includes all the networks that R1 does not already have in its routing table. Because the FastEthernet 0/0 interface belongs to the 192.168.1.0 network configured under RIP, R1

builds an update to send out that interface. The update includes all networks known to R1 except the network of the interface. Finally, R1 builds an update to send to R2. Because of split horizon, R1 only includes the 192.168.1.0 network in the update.

Step 4. Discontinue the debug output with the **undebug all** command.

```
R1# undebug all
All possible debugging has been turned off
```



Packet Tracer Companion: Basic RIP Configuration (5.6.1a)

You can now open the file LSG02-Lab561a.pka on the CD-ROM that accompanies this book to repeat this portion of the hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.

Scenario B: Running RIPv1 with Subnets and Between Classful Networks

Task 1: Make Changes Between Scenario A and Scenario B

Step 1. Change the IP addressing on the interfaces as shown in Figure 5-11 and Table 5-5.

Figure 5-11 Topology Diagram for Scenario B

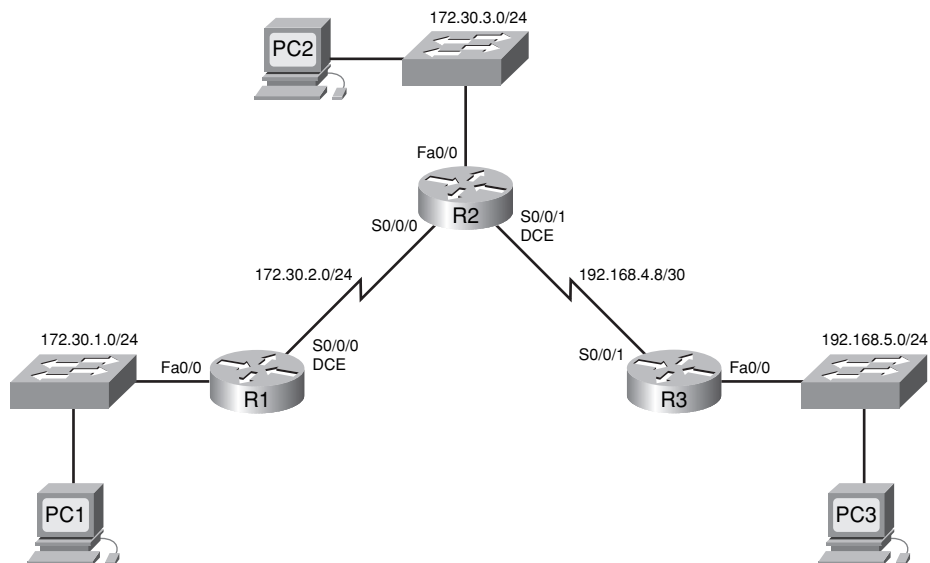


Table 5-5 Addressing Table for Scenario B

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.30.1.1	255.255.255.0	—
	S0/0/0	172.30.2.1	255.255.255.0	—
R2	Fa0/0	172.30.3.1	255.255.255.0	—
	S0/0/0	172.30.2.2	255.255.255.0	—
	S0/0/1	192.168.4.9	255.255.255.252	—
R3	Fa0/0	192.168.5.1	255.255.255.0	—
	S0/0/1	192.168.4.10	255.255.255.252	—
PC1	NIC	172.30.1.10	255.255.255.0	172.30.1.1
PC2	NIC	172.30.3.10	255.255.255.0	172.30.3.1
PC3	NIC	192.168.5.10	255.255.255.0	192.168.5.1

Sometimes when changing the IP address on a serial interface, you might need to reset that interface by using the **shutdown** command, waiting for the **LINK-5-CHANGED** message, and then using the **no shutdown** command. This process will force the IOS to starting using the new IP address:

```
R1(config)# int s0/0/0
R1(config-if)# ip add 172.30.2.1 255.255.255.0
R1(config-if)# shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to administratively
down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to down
R1(config-if)# no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
```

Step 2. Verify that routers are active.

After reconfiguring all the interfaces on all three routers, verify that all necessary interfaces are active with the **show ip interface brief** command.

Step 3. Remove the RIP configurations from each router.

Although you can remove the old **network** commands with the **no** version of the command, it is more efficient to simply remove RIP and start over. Remove the RIP configurations from each router with the **no router rip** global configuration command. This will remove all the RIP configuration commands including the **network** commands:

```
R1(config)# no router rip
R2(config)# no router rip
R3(config)# no router rip
```

Task 2: Configure RIP

Step 1. Configure RIP routing on R1 as shown here.

```
R1(config)# router rip  
R1(config-router)# network 172.30.0.0
```

Notice that only a single **network** statement is needed for R1. This statement includes both interfaces on different subnets of the 172.30.0.0 major network.

Step 2. Configure R1 to stop sending updates out the FastEthernet 0/0 interface.

Sending updates out this interface wastes the bandwidth and processing resources of all devices on the LAN. In addition, advertising updates on a broadcast network is a security risk. RIP updates can be intercepted with packet-sniffing software. Routing updates can be modified and sent back to the router, corrupting the router table with false metrics that misdirect traffic.

The **passive-interface fastethernet 0/0** command is used to disable sending RIPv1 updates out that interface. When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM:

```
R1(config-router)# passive-interface fastethernet 0/0  
R1(config-router)# end  
%SYS-5-CONFIG_I: Configured from console by console  
R1# copy run start
```

Step 2. Configure RIP routing on R2 as shown here.

```
R2(config)# router rip  
R2(config-router)# network 172.30.0.0  
R2(config-router)# network 192.168.4.0  
R2(config-router)# passive-interface fastethernet 0/0  
R2(config-router)# end  
%SYS-5-CONFIG_I: Configured from console by console  
R2# copy run start
```

Again notice that only a single **network** statement is needed for the two subnets of 172.30.0.0. This statement includes both interfaces, on different subnets, of the 172.30.0.0 major network. The network for the WAN link between R2 and R3 is also configured.

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

Step 3. Configure RIP routing on R3 as shown here.

```
R3(config)# router rip  
R3(config-router)# network 192.168.4.0  
R3(config-router)# network 192.168.5.0  
R3(config-router)# passive-interface fastethernet 0/0  
R3(config-router)# end  
%SYS-5-CONFIG_I: Configured from console by console  
R3# copy run start
```

When you are finished with the RIP configuration, return to privileged EXEC mode and save the current configuration to NVRAM.

Task 3: Verify RIP Routing

Step 1. Use the **show ip route** command to verify that each router has all the networks in the topology in its routing table.

```
R1# show ip route
```

```
<Output omitted>
```

```

      172.30.0.0/24 is subnetted, 3 subnets
C       172.30.1.0 is directly connected, FastEthernet0/0
C       172.30.2.0 is directly connected, Serial0/0/0
R       172.30.3.0 [120/1] via 172.30.2.2, 00:00:22, Serial0/0/0
R      192.168.4.0/24 [120/1] via 172.30.2.2, 00:00:22, Serial0/0/0
R      192.168.5.0/24 [120/2] via 172.30.2.2, 00:00:22, Serial0/0/0

```

Note: RIPv1 is a classful routing protocol. Classful routing protocols do not send the subnet mask with network in routing updates. For example, 172.30.1.0 is sent by R1 to R2 without any subnet mask information.

```
R2# show ip route
```

```
<Output omitted>
```

```

      172.30.0.0/24 is subnetted, 3 subnets
R       172.30.1.0 [120/1] via 172.30.2.1, 00:00:04, Serial0/0/0
C       172.30.2.0 is directly connected, Serial0/0/0
C       172.30.3.0 is directly connected, FastEthernet0/0
      192.168.4.0/30 is subnetted, 1 subnets
C       192.168.4.8 is directly connected, Serial0/0/1
R      192.168.5.0/24 [120/1] via 192.168.4.10, 00:00:19, Serial0/0/1

```

```
R3# show ip route
```

```
<Output omitted>
```

```

R      172.30.0.0/16 [120/1] via 192.168.4.9, 00:00:22, Serial0/0/1
      192.168.4.0/30 is subnetted, 1 subnets
C       192.168.4.8 is directly connected, Serial0/0/1
C      192.168.5.0/24 is directly connected, FastEthernet0/0

```

Step 2. Verify that all necessary interfaces are active.

If one or more routing tables do not have a converged routing table, first make sure that all necessary interfaces are active with **show ip interface brief**.

Then use **show ip protocols** to verify the RIP configuration. Notice in the output from this command that the FastEthernet 0/0 interface is no longer listed under **Interface** but is now listed under a new section of the output: **Passive Interface(s)**.

```

R1# show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 10 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface          Send Recv Triggered RIP Key-chain
  Serial0/0/0        1     2  1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  172.30.0.0
Passive Interface(s):
  FastEthernet0/0
Routing Information Sources:
  Gateway           Distance      Last Update
  172.30.2.2        120          00:00:13
Distance: (default is 120)

```

Step 3. View the RIP messages being sent and received.

To view the RIP messages being sent and received, use the **debug ip rip** command. Notice that RIP updates are not sent out of the Fa0/0 interface because of the **passive-interface fastethernet 0/0** command:

```

R1# debug ip rip
RIP: sending v1 update to 255.255.255.255 via Serial0/0/0 (172.30.2.1)
RIP: build update entries
      network 172.30.1.0 metric 1
RIP: received v1 update from 172.30.2.2 on Serial0/0/0
      172.30.3.0 in 1 hops

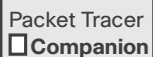
```

Step 4. Discontinue the debug output with the **undebug all** command.

```

R1# undebug all
All possible debugging has been turned off

```



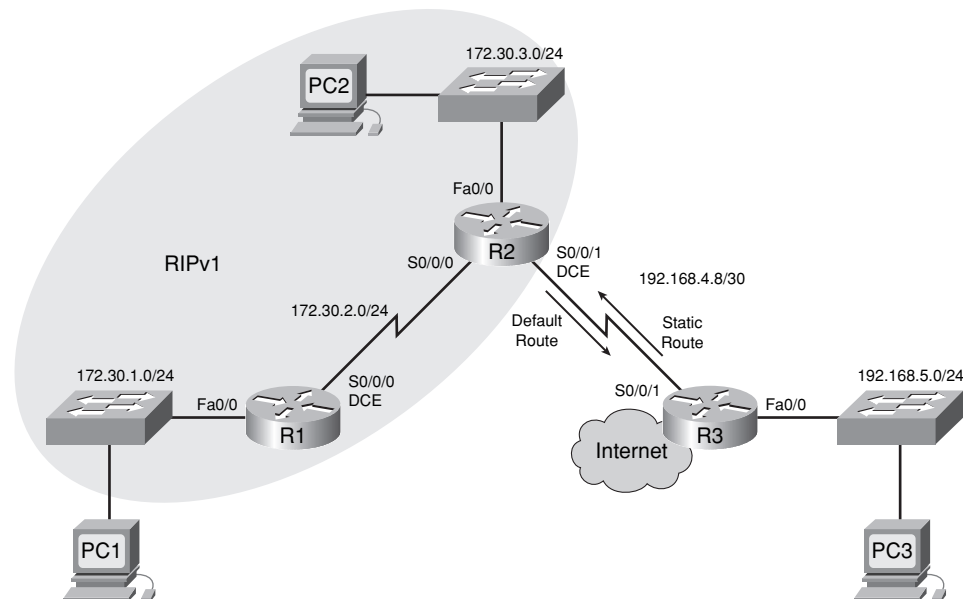
Packet Tracer Companion: Basic RIP Configuration (5.6.1b)

You can now open the file LSG02-Lab561b.pka on the CD-ROM that accompanies this book to repeat this portion of the hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.

Scenario C: Running RIPv1 on a Stub Network

In this scenario, you will modify Scenario B to only run RIP between R1 and R2. Scenario C is a typical configuration for most companies connecting a stub network to a central headquarters router or an ISP. Typically, a company runs a dynamic routing protocol (RIPv1 in our case) within the local network but finds it unnecessary to run a dynamic routing protocol between the company's gateway router and the ISP. For example, colleges with multiple campuses often run a dynamic routing protocol between campuses but use default routing to the ISP for access to the Internet. In some cases, remote campuses can even use default routing to the main campus, choosing to use dynamic routing only locally. Refer to Figure 5-12 for the discussion of Scenario C.

Figure 5-12 Topology Diagram for Scenario C



To keep our example simple, for Scenario C, we left the addressing intact from Scenario B. Assume that R3 is the ISP for Company XYZ, which consists of the R1 and R2 routers using the 172.30.0.0/16 major network, subnetted with a /24 mask. Company XYZ is a stub network, meaning that there is only one way in and one way out of the 172.30.0.0/16 network: in through R2 (the gateway router) and out through R3 (the ISP). It doesn't make sense for R2 to send R3 RIP updates for the 172.30.0.0 network every 30 seconds, because R3 has no other way to get to 172.30.0.0 except through R2. It makes more sense for R3 to have a static route configured for the 172.30.0.0/16 network pointing to R2.

How about traffic from Company XYZ toward the Internet? It makes no sense for R3 to send over 120,000 summarized Internet routes to R2. All R2 needs to know is that if a packet is not destined for a host on the 172.30.0.0 network, it should send the packet to the ISP, R3. This is the same for all other Company XYZ routers (only R1 in our case). They should send all traffic not destined for the 172.30.0.0 network to R2. R2 would then forward the traffic to R3.

Task 1: Make Changes Between Scenario B and Scenario C

Step 1. Remove network 192.168.4.0 from the RIP configuration for R2.

Remove network 192.168.4.0 because no updates will be sent between R2 and R3, and you don't want to advertise the 192.168.4.0 network to R1:

```
R2(config)# router rip
R2(config-router)# no network 192.168.4.0
```

Step 2. Remove RIP routing from R3.

```
R3(config)# no router rip
```

Task 2: Configure the Static Route on R3 for the 172.30.0.0/16 Network

Because R3 and R2 are not exchanging RIP updates, you need to configure a static route on R3 for the 172.30.0.0/16 network:

```
R3(config)# ip route 172.30.0.0 255.255.0.0 serial0/0/1
```

This will send all 172.30.0.0/16 traffic to R2.

Task 3: Configure a Default Static Route on R2

Step 1. Configure R2 to send default traffic to R3.

Configure a default static route on R2 that will send all default traffic—packets with destination IP addresses that do not match a specific route in the routing table—to R3:

```
R2(config)# ip route 0.0.0.0 0.0.0.0 serial 0/0/1
```

Step 2. Configure R2 to send default static route information to R1.

The **default-information originate** command is used to configure R2 to include the default static route with its RIP updates. Configure this command on R2 so that the default static route information is sent to R1:

```
R2(config)# router rip
R2(config-router)# default-information originate
R2(config-router)#
```

Note: Sometimes it is necessary to clear the RIP routing process before the default-information originate command will work. First, try the clear ip route * command on both R1 and R2. This command will cause the routers to immediately flush routes in the routing table and request updates from each other. Sometimes this does not work with RIP. If the default route information is still not sent to R1, save the configuration on R1 and R2 and then reload both routers. Doing this will reset the hardware, and both routers will restart the RIP routing process.

Task 4: Verify RIP Routing

Step 1. Use the **show ip route** command to view the routing table on R2 and R1.

```
R2# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

```

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
```

```

172.30.0.0/24 is subnetted, 3 subnets
C    172.30.2.0 is directly connected, Serial0/0/0
C    172.30.3.0 is directly connected, FastEthernet0/0
R    172.30.1.0 [120/1] via 172.30.2.1, 00:00:16, Serial0/0/0
192.168.4.0/30 is subnetted, 1 subnets
C    192.168.4.8 is directly connected, Serial0/0/1
S*  0.0.0.0/0 is directly connected, Serial0/0/1

```

Note: Notice that R2 now has a static route tagged as a **candidate default**.

```

R1# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

```

```
Gateway of last resort is 172.30.2.2 to network 0.0.0.0
```

```

172.30.0.0/24 is subnetted, 3 subnets
C    172.30.2.0 is directly connected, Serial0/0/0
R    172.30.3.0 [120/1] via 172.30.2.2, 00:00:05, Serial0/0/0
C    172.30.1.0 is directly connected, FastEthernet0/0
R*  0.0.0.0/0 [120/1] via 172.30.2.2, 00:00:19, Serial0/0/0

```

Notice that R1 now has a RIP route tagged as a **candidate default** route. The route is the “quad-zero” default route sent by R2. R1 will now send default traffic to the **Gateway of last resort** at 172.30.2.2, which is the IP address of R2.

Step 2. View the RIP updates that are sent and received on R1 with the **debug ip rip** command.

```

R1# debug ip rip
RIP protocol debugging is on
RIP: sending v1 update to 255.255.255.255 via Serial0/0/0 (172.30.2.1)
RIP: build update entries
      network 172.30.1.0 metric 1
RIP: received v1 update from 172.30.2.2 on Serial0/0/0
      0.0.0.0 in 1 hops
      172.30.3.0 in 1 hops

```

Notice that R1 is receiving the default route from R2.

Step 3. Discontinue the debug output with the **undebug all** command.

```
R1# undebug all
```

All possible debugging has been turned off

Step 4. Use the **show ip route** command to view the routing table on R3.

```
R3# show ip route
```

```
<Output omitted>
```

```
S 172.30.0.0/16 is directly connected, Serial0/0/1
  192.168.4.0/30 is subnetted, 1 subnets
C   192.168.4.8 is directly connected, Serial0/0/1
C   192.168.5.0/24 is directly connected, FastEthernet0/0
```

Notice that RIP is not being used on R3. The only route that is not directly connected is the static route.

Task 5: Document the Router Configurations

On each router, capture the following command output to a text file and save for future reference:

- Running configuration
- Routing table
- Interface summarization
- Output from **show ip protocols**

Task 6: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.



Packet Tracer Companion: Basic RIP Configuration (5.6.1c)

You can now open the file LSG02-Lab561c.pka on the CD-ROM that accompanies this book to repeat this portion of the hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.



Lab 5-2: Challenge RIP Configuration (5.6.2)

Upon completion of this lab, you will be able to

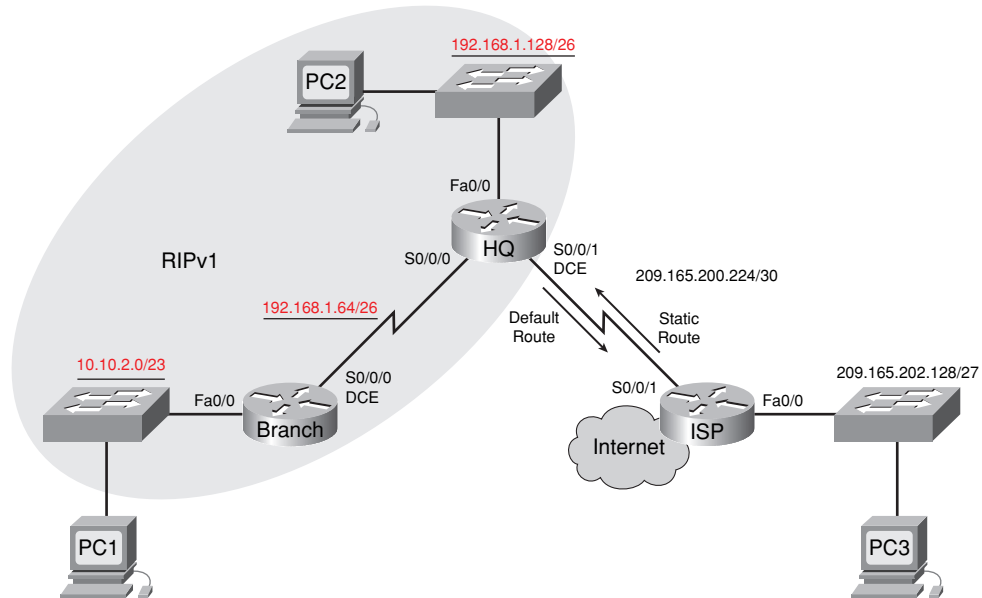
- Subnet an address space given requirements
- Assign appropriate addresses to interfaces and document them in the addressing table
- Cable a network according to the topology diagram in Figure 5-13
- Erase the startup configuration and reload a router to the default state
- Configure RIPv1 routing on all routers
- Configure and propagate a static default route
- Verify RIPv1 operation
- Test and verify full connectivity
- Reflect on and document the network implementation

Table 5-6 Addressing Table for Lab 5-2

Device	Interface	IP Address	Subnet Mask	Default Gateway
BRANCH	Fa0/0	10.10.2.1	255.255.254.0	—
	S0/0/0	192.168.1.126	255.255.255.192	—
HQ	Fa0/0	192.168.1.129	255.255.255.192	—
	S0/0/0	192.168.1.65	255.255.255.192	—
	S0/0/1	209.165.200.226	255.255.255.252	—
ISP	Fa0/0	209.165.202.129	255.255.255.224	—
	S0/0/1	209.165.200.225	255.255.255.252	—
PC1	NIC	10.10.3.254	255.255.254.0	10.10.2.1
PC2	NIC	192.168.1.190	255.255.255.192	192.168.1.129
PC3	NIC	209.165.202.158	255.255.255.224	209.165.202.129

Scenario

In this lab activity, you will be given a network address that must be subnetted to complete the addressing of the network shown in Figure 5-13. A combination of RIPv1 and static routing will be required so that hosts on networks that are not directly connected will be able to communicate with each other. Use the information in Table 5-6 for reference. Step 2 of Task 2 asks you to complete the information in Table 5-6 for documentation purposes.

Figure 5-13 Topology Diagram for Lab 5-2 (Answer)

Task 1: Subnet the Address Space

Step 1. Examine the network requirements.

The addressing for the network has the following requirements:

- The ISP LAN will use the 209.165.202.128/27 network.
- The link between the ISP router and the HQ router will use the 209.165.200.224/30 network.
- The 192.168.1.0/24 network must be subnetted for use in the HQ LAN and the link between the HQ and BRANCH routers. The HQ LAN will require 50 host IP addresses.
- The BRANCH LAN will use the 10.10.2.0/23 network.

Step 2. Consider the following questions when creating your network design:

How many subnets need to be created from the 192.168.1.0/24 network? 2

What is the subnet mask for this network in dotted decimal format? 255.255.255.192

What is the subnet mask for the network in slash format? /26

What are the network addresses of the subnets?

Subnet 0: 192.168.1.0/26

Subnet 1: 192.168.1.64/26

Subnet 2: 192.168.1.128/26

How many usable host IP addresses are there per subnet? 62

How many usable hosts IP addresses are available in the BRANCH LAN? 510

Step 3. Assign subnetwork addresses to the topology diagram in Figure 5-13.

- Assign subnet 1 in the 192.168.1.0 network to the WAN link between the HQ and BRANCH routers.
- Assign subnet 2 in the 192.168.1.0 network to the LAN attached to the HQ router.

Task 2: Determine Interface Addresses

Step 1. Assign appropriate addresses to the device interfaces.

- Assign the first valid host address in the 209.165.202.128/27 network to the LAN interface on the ISP router.
- Assign the last valid host address in the 209.165.202.128/27 network to PC3.
- Assign the first valid host address in the 209.165.200.224/30 network to the WAN interface of the ISP router.
- Assign the last valid host address in the 209.165.200.224/30 network to the Serial 0/0/1 interface of the HQ router.
- Assign the first valid host address in the HQ LAN network to the LAN interface of the HQ router.
- Assign the last valid host address in the HQ LAN network to PC 2.
- Assign the first valid host address in the HQ/BRANCH WAN link to the Serial 0/0/0 interface of the HQ router.
- Assign the last valid host address in the HQ/BRANCH WAN link to the Serial 0/0/0 interface of the BRANCH router.
- Assign the first valid host address in the 10.10.2.0/23 network to the LAN interface on the BRANCH router.
- Assign the last valid host address in the 10.10.2.0/23 network to PC1.

Step 2. Document the addresses to be used in Table 5-6.

Task 3: Prepare the Network

Step 1. Cable a network that is similar to the one shown in Figure 5-13.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

Note: If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions will appear different.

Step 2. Clear any existing configurations on the routers.

Task 4: Perform Basic Router Configurations

Perform basic configuration on the BRANCH, HQ, and ISP routers according to the following guidelines:

- Configure the router host name.
- Disable DNS lookup.

- Configure an EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for console connections.
- Configure a password for VTY connections.
- Synchronize unsolicited messages and debug output with solicited output and prompts for the console and virtual terminal lines.
- Configure an EXEC timeout of 15 minutes.

Task 5: Configure and Activate Serial and Ethernet Addresses

Step 1. Configure the BRANCH, HQ, and ISP routers.

Configure the interfaces on the BRANCH, HQ, and ISP routers with the IP addresses from the addressing table provided under the topology diagram.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 2. Configure the Ethernet interfaces of PC1, PC2, and PC3.

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses from Table 5-6.

Task 6: Verify Connectivity to Next-Hop Device

You should *not* have connectivity between end devices yet. However, you can test connectivity between two routers and between an end device and its default gateway.

Step 1. Verify BRANCH connectivity.

Verify that BRANCH can ping across the WAN link to HQ and that HQ can ping across the WAN link it shares with ISP.

Step 2. Verify Ethernet interface connectivity.

Verify that PC1, PC2, and PC3 can ping their respective default gateways.

Task 7: Configure RIP Routing on the BRANCH Router

Consider the networks that need to be included in the RIP updates that are sent out by the BRANCH router.

What networks are currently present in the BRANCH routing table before RIP is configured? List the networks with slash notation.

10.0.0.0/23

192.168.1.0/26

What commands are required to enable RIP version 1 and include these networks in the routing updates?

router rip

network 10.0.0.0

network 192.168.1.0

Are there any router interfaces that do not need to have RIP updates sent out? [yes](#)

What command is used to disable RIP updates on this interface?

BRANCH(config-router)# passive-interface FastEthernet0/0

Task 8: Configure RIP and Static Routing on the HQ Router

Consider the type of static routing that is needed on HQ.

What networks are present in the HQ routing table? List the networks with slash notation.

[192.168.1.0/26](#)

[209.165.200.224/30](#)

A static default route will need to be configured to send all packets with destination addresses that are not in the routing table to the ISP router. What command is needed to accomplish this? Use the appropriate exit interface on the HQ router in the command.

HQ(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/1

What commands are required to enable RIPv1 and include the LAN network in the routing updates?

router rip

network 192.168.1.0

Are there any router interfaces that do not need to have RIP updates sent out? [yes](#)

What command is used to disable RIP updates on this interface?

HQ(config-router)# passive-interface FastEthernet0/0

The HQ router needs to send the default route information to the BRANCH router in the RIP updates. What command is used to configure this?

HQ(config-router)# default-information originate

Task 9: Configure Static Routing on the ISP Router

Static routes will need to be configured on the ISP router for all traffic that is destined for the RFC 1918 addresses that are used on the BRANCH LAN, HQ LAN, and the link between the BRANCH and HQ routers.

What are the commands that will need to be configured on the ISP router to accomplish this?

ISP(config)# ip route 10.10.2.0 255.255.254.0 Serial0/0/1

ISP(config)# ip route 192.168.1.0 255.255.255.0 Serial0/0/1

Task 10: Verify the Configurations

Answer the following questions to verify that the network is operating as expected.

From PC2, is it possible to ping PC1? [yes](#)

From PC2, is it possible to ping PC3? [yes](#)

From PC1, is it possible to ping PC3? [yes](#)

The answer to the preceding questions should be **yes**. If any of the pings failed, check your physical connections and configurations. Refer to the basic troubleshooting techniques used in the labs in Chapter 1, “Introduction to Routing and Packet Forwarding.”

What routes are present in the routing table of the BRANCH router?

[10.0.0.0/23](#)

[192.168.1.0/26](#)

[0.0.0.0/0](#)

What is the gateway of last resort in the routing table of the BRANCH router?

[192.168.1.65 to network 0.0.0.0](#)

What routes are present in the routing table of the HQ router?

[10.0.0.0/8](#)

[192.168.1.0/26](#)

[209.165.200.224/30](#)

[0.0.0.0/0](#)

What networks are present in the routing table of the ISP router?

[10.0.0.0/23](#)

[192.168.1.0/24](#)

[209.165.200.224/30](#)

[209.165.202.0/27](#)

What networks, including the metric, are present in the RIP updates sent from the HQ router?

[network 0.0.0.0 metric 1](#)

[network 192.168.1.128 metric 1](#)

What networks, including the metric, are present in the RIP updates sent from the BRANCH router?

[network 10.0.0.0 metric 1](#)

Task 11: Reflection

If static routing were used instead of RIP on the BRANCH router, how many individual static routes would be needed for hosts on the BRANCH LAN to communicate with all the networks in the topology diagram shown in Figure 5-13? [Three](#)

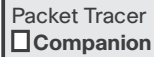
Task 12: Document the Router Configurations

On each router, capture the following command output to a text file and save for future reference:

- Running configuration
- Routing table
- Interface summarization

Task 13: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.



Packet Tracer Companion: Challenge RIP Configuration (5.6.2)

You can now open the file LSG02-Lab562.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.

Lab 5-3: RIP Troubleshooting (5.6.3)

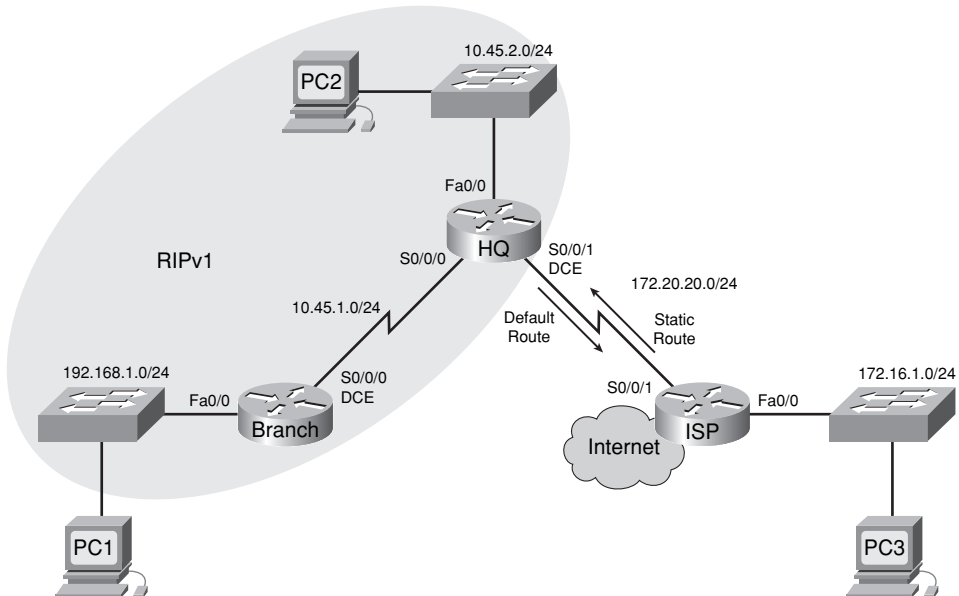
Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram in Figure 5-14
- Erase the startup configuration and reload a router to the default state
- Load the routers with supplied scripts
- Discover where convergence is not complete
- Gather information about the nonconverged portion of the network along with any other errors
- Analyze information to determine why convergence is not complete
- Propose solutions to network errors
- Implement solutions to network errors
- Document the corrected network

Scenario

In this lab, you will begin by loading configuration scripts on each of the routers. These scripts contain errors that will prevent end-to-end communication across the network. You will need to troubleshoot each router to determine the configuration errors and then use the appropriate commands to correct the configurations. When you have corrected all the configuration errors, all the hosts on the network should be able to communicate with each other.

Figure 5-14 shows the topology diagram for this lab, and Table 5-7 shows interface, IP address, subnet mask, and default gateway (where applicable) information for all devices in the network.

Figure 5-14 Topology Diagram for Lab 5-3**Table 5-7 Addressing Table for Lab 5-3**

Device	Interface	IP Address	Subnet Mask	Default Gateway
BRANCH	Fa0/0	192.168.1.1	255.255.255.0	—
	S0/0/0	10.45.1.254	255.255.255.0	—
HQ	Fa0/0	10.45.2.1	255.255.255.0	—
	S0/0/0	10.45.1.1	255.255.255.0	—
	S0/0/1	172.20.20.254	255.255.255.0	—
ISP	FA0/0	172.16.1.1	255.255.255.0	—
	S0/0/1	172.20.20.1	255.255.255.0	—
PC1	NIC	192.168.1.254	255.255.255.0	192.168.1.1
PC2	NIC	10.45.2.254	255.255.255.0	10.45.2.1
PC3	NIC	172.16.1.254	255.255.255.0	172.16.1.1

The network should meet the following requirements:

- RIPv1 routing is configured on the BRANCH router.
- RIPv1 routing is configured on the HQ router.
- RIP updates must be disabled on the BRANCH and HQ LAN interfaces.
- A static default route is configured on the HQ router and shared with the BRANCH router through RIP updates.
- Static routes for all HQ and BRANCH networks are to be configured on the ISP router. The routes must be summarized wherever possible.

Task 1: Cable, Erase, and Reload the Routers

Step 1. Cable a network.

Cable a network that is similar to the one shown in the Figure 5-14.

Step 2. Clear the configuration on each router.

Clear the configuration on each of routers using the **erase startup-config** command and then reload the routers. Answer **no** if asked to save changes.

Task 2: Load Routers with the Supplied Scripts

Step 1. Load the following script onto the BRANCH router.

```
hostname BRANCH
!
!
no ip domain-lookup
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
 !The no shutdown command is missing
!
interface Serial0/0/0
 ip address 10.45.1.254 255.255.255.0
 clock rate 64000
 no shutdown
!
router rip
 passive-interface FastEthernet0/0
 network 10.0.0.0
 !The network statement is missing for the 192.168.1.0 network
!
!
!
!
line con 0
line vty 0 4
 password cisco
 login
!
end
```

Corrected script:

```
hostname Branch
!
!
no ip domain-lookup
!
interface FastEthernet0/0
```

```
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!The no shutdown command is missing
!
interface Serial0/0/0
ip address 10.45.1.254 255.255.255.0
clock rate 64000
no shutdown
!
router rip
passive-interface FastEthernet0/0
network 10.0.0.0
network 192.168.1.0
!
!
!
!
line con 0
line vty 0 4
password cisco
login
!
end
```

The errors in the student scripts are as follows:

- The **no shutdown** command is missing from the FastEthernet 0/0 interface.
- The **network** statement for the 192.168.1.0 network is missing from the RIP configuration.

Step 2. Load the following script onto the HQ router.

```
hostname HQ
!
!
no ip domain-lookup
!
interface FastEthernet0/0
ip address 10.45.2.1 255.255.255.0
duplex auto
speed auto
no shutdown
!
interface Serial0/0/0
ip address 10.45.1.1 255.255.255.0
no shutdown
!
interface Serial0/0/1
ip address 172.20.20.254 255.255.255.0
clock rate 64000
no shutdown
```

```
!  
router rip  
  passive-interface Serial0/0/0  
  ! Fa0/0 should be configured as passive, not S0/0/0  
  network 10.0.0.0  
  !The default-information originate command is missing  
!  
ip route 0.0.0.0 0.0.0.0 Serial0/0/1  
!  
!  
!  
line con 0  
line vty 0 4  
  password cisco  
  login  
!  
end
```

Corrected script:

```
hostname HQ  
!  
!  
no ip domain-lookup  
!  
interface FastEthernet0/0  
  ip address 10.45.2.1 255.255.255.0  
  duplex auto  
  speed auto  
  no shutdown  
!  
interface Serial0/0/0  
  ip address 10.45.1.1 255.255.255.0  
  no shutdown  
!  
interface Serial0/0/1  
  ip address 172.20.20.254 255.255.255.0  
  clock rate 64000  
  no shutdown  
!  
router rip  
  passive-interface FastEthernet0/0/0  
  network 10.0.0.0  
  default-information originate  
!  
ip route 0.0.0.0 0.0.0.0 Serial0/0/1  
!  
!  
!  
!
```

```
line con 0
line vty 0 4
  password cisco
  login
!
end
```

The errors in the student scripts are as follows:

- The FastEthernet 0/0 interface should be configured as passive, not the Serial 0/0/0 interface.
- The **default-information originate** command is missing from the RIP configuration.

Step 3. Load the following script onto the ISP router.

```
hostname ISP
!
!
no ip domain-lookup
!
interface FastEthernet0/0
  ip address 172.16.1.1 255.255.255.0
  duplex auto
  speed auto
  no shutdown
!
interface Serial0/0/1
  ip address 172.20.20.1 255.255.255.0
  no shutdown
!
ip route 10.45.0.0 255.255.254.0 Serial0/0/1
! The subnet mask is incorrect
ip route 192.168.1.0 255.255.255.0 Serial0/0/1
!
!
!
!
line con 0
line vty 0 4
  password cisco
  login
!
end
```

Corrected script:

```
hostname ISP
!
!
no ip domain-lookup
!
interface FastEthernet0/0
  ip address 172.16.1.1 255.255.255.0
```

```

duplex auto
speed auto
no shutdown
!
interface Serial0/0/1
 ip address 172.20.20.1 255.255.255.0
 no shutdown
!
ip route 10.45.0.0 255.255.252.0 Serial 0/0/1
ip route 192.168.1.0 255.255.255.0 Serial0/0/1
!
!
!
!
line con 0
line vty 0 4
 password cisco
 login
!
end

```

The error in the student script was caused by an incorrect IP address and subnet mask in the route to the 10.45.1.0/22 network.

Task 3: Troubleshoot the BRANCH Router

Step 1. Begin troubleshooting at the host connected to the BRANCH router.

From the host PC1, is it possible to ping PC2? no

From the host PC1, is it possible to ping PC3? no

From the host PC1, is it possible to ping the default gateway? no

Step 2. Examine the BRANCH router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the status of the interfaces?

Interface Fa0/0 is administratively down.

If there are any problems with the status of the interfaces, record any commands that will be necessary to correct the configuration errors.

configure terminal

interface Fa0/0

no shutdown

Step 3. If you have recorded any commands, apply them to the router configuration now.

Step 4. View a summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors? no

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

Step 5. Troubleshoot the routing configuration on the BRANCH router.

What networks are shown in the routing table?

10.0.0.0/24

192.168.1.0/24

Are there any problems with the routing table?

There is no way to reach remote networks.

If there are any problems with the routing table, record any commands that will be necessary to correct the configuration errors.

What networks are included in the RIP updates?

No RIP updates are being sent.

Are there any problems with the RIP updates that are being sent out from the router?

The 192.168.1.0/24 should be advertised in RIP updates.

If there are any problems with the RIP configuration, record any commands that will be necessary to correct the configuration errors.

configure terminal

router rip

network 192.168.1.0

Step 6. If you have recorded any commands, apply them to the router configuration now.

Step 7. View the routing information.

If any changes were made to the configuration in the previous steps, view the routing information again.

Does the information in the routing table indicate any configuration errors? no

Does the information included in the RIP updates that are sent out indicate any configuration errors? no

If the answer to either of these questions is **yes**, troubleshoot the routing configuration again.

What networks are included in the RIP updates?

192.168.1.0

Step 8. Attempt to ping between the hosts again.

From the host PC1, is it possible to ping PC2? no

From the host PC1, is it possible to ping PC3? no

From the host PC1, is it possible to ping the Serial 0/0 interface of the HQ router? yes

Task 4: Troubleshoot the HQ Router

Step 1. Begin troubleshooting at the host connected to the R2 router.

From the host PC2, is it possible to ping PC1? **no**

From the host PC2, is it possible to ping PC3? **no**

From the host PC2, is it possible to ping the default gateway? **yes**

Step 2. Examine the HQ router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the status of the interfaces? **no**

If there are any problems with the status of the interfaces, record any commands that will be necessary to correct the configuration errors.

Step 3. If you have recorded any commands, apply them to the router configuration now.

Step 4. View the summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors? **no**

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

Step 5. Troubleshoot the routing configuration on the HQ router.

What networks are shown in the routing table?

0.0.0.0/0

10.0.0.0/24

192.168.1.0/24

172.20.20.0/24

Are there any problems with the routing table? **no**

If there are any problems with the routing table, record any commands that will be necessary to correct the configuration errors.

What networks are included in the RIP updates?

0.0.0.0

10.45.1.0

192.168.1.0

Are there any problems with the RIP updates that are being sent out from the router?

Routing updates are not being sent out of the Serial 0/0/0 interface because of the **passive-interface Serial 0/0** command. This command should be replaced by the **passive-interface FastEthernet0/0** command.

If there are any problems with the RIP configuration, record any commands that will be necessary to correct the configuration errors.

configure terminal

router rip

no passive-interface Serial 0/0/0

passive-interface FastEthernet 0/0

Step 6. If you have recorded any commands, apply them to the router configuration now.

Step 7. View the routing information.

If any changes were made to the configuration in the previous steps, view the routing information again.

Does the information in routing table indicate any configuration errors? **no**

Does the information included in the RIP updates that are sent out indicate any configuration errors? **no**

If the answer to either of these questions is **yes**, troubleshoot the routing configuration again.

What networks are included in the RIP updates?

0.0.0.0

10.45.2.0

Step 8. Verify that the HQ router is sending a default route to the BRANCH router.

Is there a default route in the BRANCH routing table? **no**

If not, what commands are needed to configure this on the HQ router?

configure terminal

router rip

default-information originate

Step 9. If you have recorded any commands, apply them to the HQ router configuration now.

Step 10. View the BRANCH routing table.

If any changes were made to the configuration in the previous step, view the BRANCH routing table again.

Is there a default route in the BRANCH routing table? **yes**

If the answer is **no**, troubleshoot the RIP configuration again.

Step 11. Attempt to ping between the hosts again.

From the host PC2, is it possible to ping PC1? **yes**

From the host PC2, is it possible to ping the Serial 0/1 interface of the ISP router? **no**

From the host PC1, is it possible to ping PC3? **yes**

Task 5: Troubleshoot the ISP Router

Step 1. Begin troubleshooting at the host connected to the ISP router.

From the host PC3, is it possible to ping PC1? yes

From the host PC3, is it possible to ping PC2? no

From the host PC3, is it possible to ping the default gateway? yes

Step 2. Examine the ISP router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the status of the interfaces? no

If there are any problems with the status of the interfaces, record any commands that will be necessary to correct the configuration errors.

Step 3. If you have recorded any commands, apply them to the router configuration now.

Step 4. View the summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors? no

If the answer is yes, troubleshoot the interface status of the interfaces again.

Step 5. Troubleshoot the static routing configuration on the ISP router.

Begin by viewing the routing table.

What networks are shown in the routing table?

10.0.0.0/23

172.16.0.0/24

172.20.0.0/24

192.168.1.0/24

Are there any problems with the routing configuration?

In the routing table, the subnet mask on the 10.0.0.0 network should be /22. The route summarization for the 10.45.1.0/24 and 10.45.2.0/24 networks has been done incorrectly.

If there are any problems with the routing configuration, record any commands that will be necessary to correct the configuration errors.

configure terminal

no ip route 10.45.0.0 255.255.254.0 Serial0/1

ip route 10.45.0.0 255.255.252.0 Serial0/1

Step 6. If you have recorded any commands, apply them to the router configuration now.

Step 7. View the routing table.

If any changes were made to the configuration in the previous step, view the routing table again.

Does the information in the routing table indicate any configuration errors? no

If the answer is **yes**, troubleshoot the routing configuration again.

Step 8. Attempt to ping between the hosts again.

From the host PC3, is it possible to ping PC1? yes

From the host PC3, is it possible to ping PC2? yes

From the host PC3, is it possible to ping the WAN interface of the BRANCH router? yes

Task 6: Reflection

There were a number of configuration errors in the scripts that were provided for this lab. Use the space below to write a brief description of the errors that you found.

Task 7: Documentation

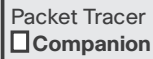
On each router, capture output from the following commands to a text (.txt) file and save for future reference:

```
show running-config
show ip route
show ip interface brief
show ip protocols
```

If you need to review the procedures for capturing command output, refer to “Lab 1-1: Cabling a Network and Basic Router Configuration (1.5.1).”

Task 8: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.



Packet Tracer Companion: RIP Troubleshooting (5.6.3)

You can now open the file LSG02-Lab563.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.

Packet Tracer Skills Integration Challenge

Introduction

This activity focuses on subnetting skills, basic device configurations, static routing, and RIP routing. After you configure all devices, test for end-to-end connectivity and examine your configuration. Open the file LSG02-PTSkills5.pka on the CD-ROM that accompanies this book. Use the topology in Figure 5-15 and the addressing tables in Tables 5-9 and 5-10 to document your design.

Upon completion of this challenge, you will be able to

- Design and document an addressing scheme based on requirements
- Apply a basic configuration to the devices
- Configure static routing between ISP routers
- Configure RIPv1 routing in Region 1 and Region 2
- Disable RIP updates on appropriate interfaces
- Configure default routes and redistribute through RIP
- Verify full connectivity between all devices in the topology

Open the file LSG02-PTSkills5.pka on the CD-ROM that accompanies this book. You will use the topology in Figure 5-15 and the addressing tables in Tables 5-8 and 5-9 to document your design.

Figure 5-15 Packet Tracer Skills Integration Challenge Topology

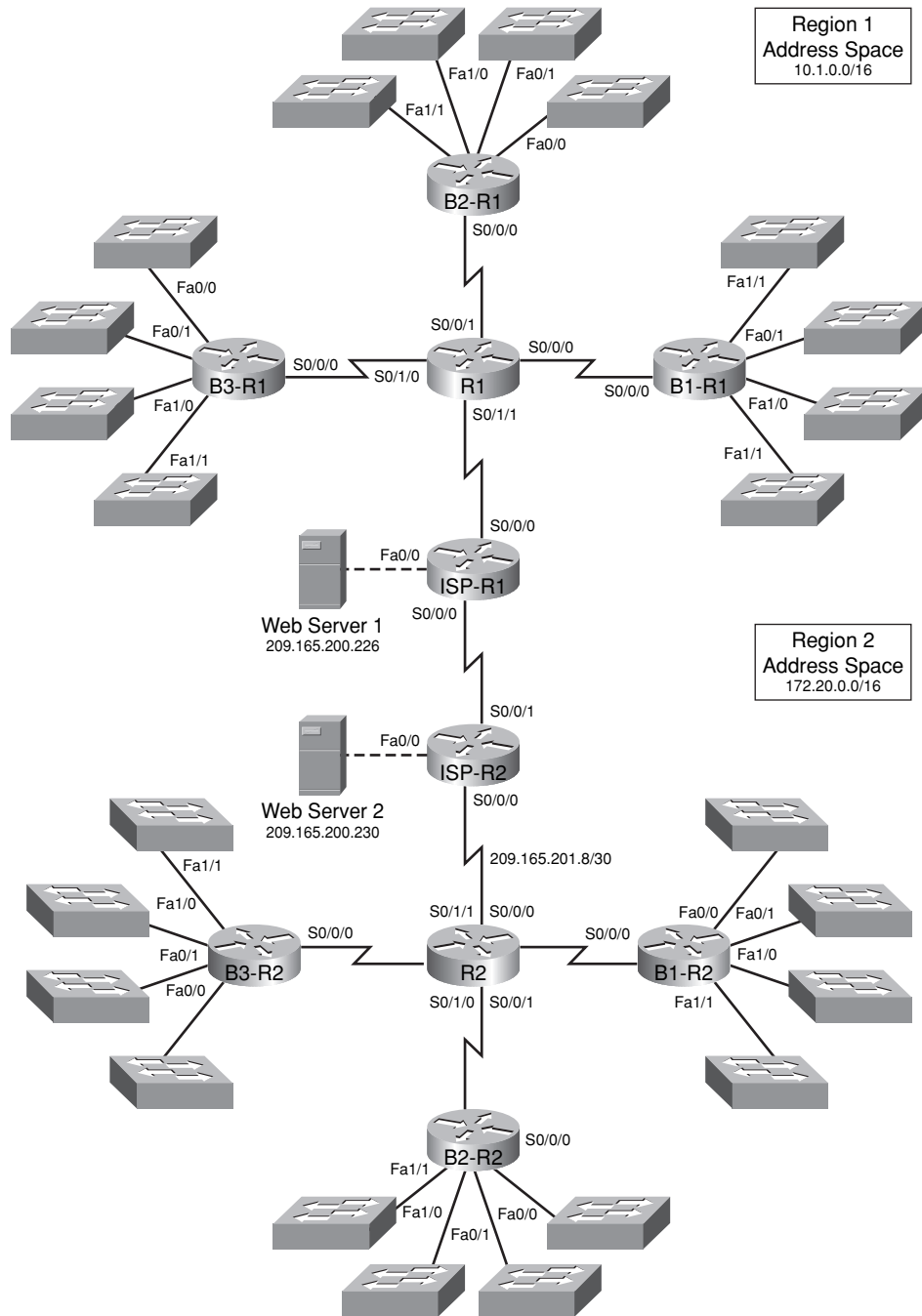


Table 5-8 Addressing Table for R1

Device	Interface	IP Address	Subnet Mask
R1	S0/0/0	10.1.244.1	255.255.252.0
	S0/0/1	10.1.248.1	255.255.252.0
	S0/1/0	10.1.252.1	255.255.252.0
	S0/1/1	209.165.201.2	255.255.255.252
B1-R1	Fa0/0	10.1.0.1	255.255.252.0
	Fa0/1	10.1.4.1	255.255.252.0
	Fa1/0	10.1.8.1	255.255.252.0
	Fa1/1	10.1.12.1	255.255.252.0
	S0/0/0	10.1.244.2	255.255.252.0
B2-R1	Fa0/0	10.1.16.1	255.255.252.0
	Fa0/1	10.1.20.1	255.255.252.0
	Fa1/0	10.1.24.1	255.255.252.0
	Fa1/1	10.1.28.1	255.255.252.0
	S0/0/0	10.1.248.2	255.255.252.0
B3-R1	Fa0/0	10.1.32.1	255.255.252.0
	Fa0/1	10.1.36.1	255.255.252.0
	Fa1/0	10.1.40.1	255.255.252.0
	Fa1/1	10.1.44.1	255.255.252.0
	S0/0/0	10.1.252.2	255.255.252.0
ISP-R1	S0/0/0	209.165.201.1	255.255.255.252
	S0/0/1	209.165.201.5	255.255.255.252
	Fa0/0	209.165.200.225	255.255.255.252
Web Server 1	NIC	209.165.200.226	255.255.255.252

Table 5-9 Addressing Table for R2

Device	Interface	IP Address	Subnet Mask
R2	S0/0/0	172.20.250.1	255.255.254.0
	S0/0/1	172.20.252.1	255.255.254.0
	S0/1/0	172.20.254.1	255.255.254.0
	S0/1/1	209.165.201.10	255.255.255.252

continues

Table 5-9 Addressing Table for R2 *continued*

Device	Interface	IP Address	Subnet Mask
B1-R2	Fa0/0	172.20.0.1	255.255.254.0
	Fa0/1	172.20.2.1	255.255.254.0
	Fa1/0	172.20.4.1	255.255.254.0
	Fa1/1	172.20.6.1	255.255.254.0
	S0/0/0	172.20.250.2	255.255.254.0
B2-R2	Fa0/0	172.20.8.1	255.255.254.0
	Fa0/1	172.20.10.1	255.255.254.0
	Fa1/0	172.20.12.1	255.255.254.0
	Fa1/1	172.20.14.1	255.255.254.0
	S0/0/0	172.20.252.2	255.255.254.0
B3-R2	Fa0/0	172.20.16.1	255.255.254.0
	Fa0/1	172.20.18.1	255.255.254.0
	Fa1/0	172.20.20.1	255.255.254.0
	Fa1/1	172.20.22.1	255.255.254.0
	S0/0/0	172.20.254.2	255.255.254.0
ISP-R2	S0/0/0	209.165.201.6	255.255.255.252
	S0/0/1	209.165.201.9	255.255.255.252
	Fa0/0	209.165.200.229	255.255.255.252
Web Server 2	NIC	209.165.200.230	255.255.255.252

Task 1: Design and Document an Addressing Scheme

Step 1. Design an addressing scheme.

Use the topology shown in Figure 5-15, along with the following requirements, to design an addressing scheme:

- The WAN links between R1 and R2 and their respective ISP routers are already configured. Also, the links between the ISPs and the Web Servers are already configured.
- Because RIPv1 is a classful routing protocol, you cannot implement variable-length subnet masking (VLSM). Subnet each region's address space using the following guidelines:
 - The largest subnet in Region 1's address space is 1000 hosts. What is the subnet mask you should use for the 10.1.0.0/16 address space? [255.255.252.0](#)
 - The largest subnet in Region 2's address space is 500 hosts. What is the subnet mask you should use for the 172.20.0.0/16 address space? [255.255.254.0](#)

- For the LANs in Region 1, assign subnet 0 to the LAN attached to FastEthernet 0/0 on B1-R1. Continue to assign LANs in sequence. Subnet 1 is assigned to the LAN attached to FastEthernet 0/1 on B1-R1, Subnet 2 to FastEthernet 1/0, Subnet 3 to FastEthernet 1/1, and so on.
- For the WANs in Region 1, assign the last subnet to the link between R1 and B3-R1, the second-to-last subnet to the link between R1 and B2-R1, and the third-to-last subnet to the link between R1 and B1-R1.
- Record the Region 1 subnet assignments in Table 5-10.

Table 5-10 Subnets for Region 1

Router	Subnet Number	Subnet Address
B1-R1 Fa0/0	0	10.1.0.0
B1-R1 Fa0/1	1	10.1.4.0
B1-R1 Fa1/0	2	10.1.8.0
B1-R1 Fa1/1	3	10.1.12.0
B2-R1 Fa0/0	4	10.1.16.0
B2-R1 Fa0/1	5	10.1.20.0
B2-R1 Fa1/0	6	10.1.24.0
B2-R1 Fa1/1	7	10.1.28.0
B3-R1 Fa0/0	8	10.1.32.0
B3-R1 Fa0/1	9	10.1.36.0
B3-R1 Fa1/0	10	10.1.40.0
B3-R1 Fa1/1	11	10.1.44.0
B1-R1 <—> R1	3rd-to-last	10.1.244.0
B2-R1 <—> R1	2nd-to-last	10.1.248.0
B3-R1 <—> R1	Last	10.1.252.0

- For the LANs in Region 2, follow the same format for assigning subnets that you used for Region 1: Subnet 0 to the Fa0/0 interface on B1-R2, Subnet 1 to Fa0/1, and so on.
- For the WANs in Region 2, assign the last subnet to the link between R2 and B3-R2, the second-to-last subnet to the link between R2 and B2-R2, and the third-to-last subnet to the link between R2 and B1-R2.
- Record the Region 2 subnet assignments in Table 5-11.

Table 5-11 Subnets for Region 2

Router	Subnet Number	Subnet Address
B1-R2 Fa0/0	0	172.20.0.0
B1-R2 Fa0/1	1	172.20.2.0

continues

Table 5-11 Subnets for Region 2 *continued*

Router	Subnet Number	Subnet Address
B1-R2 Fa1/0	2	172.20.4.0
B1-R2 Fa1/1	3	172.20.6.0
B2-R2 Fa0/0	4	172.20.8.0
B2-R2 Fa0/1	5	172.20.10.0
B2-R2 Fa1/0	6	172.20.12.0
B2-R2 Fa1/1	7	172.20.14.0
B3-R2 Fa0/0	8	172.20.16.0
B3-R2 Fa0/1	9	172.20.18.0
B3-R2 Fa1/0	10	172.20.20.0
B3-R2 Fa1/1	11	172.20.22.0
B1-R2 <—> R2	3rd-to-last	172.20.250.0
B2-R2 <—> R2	2nd-to-last	172.20.252.0
B3-R2 <—> R2	Last	172.20.254.0

Step 2. Document the addressing scheme.

- Optional: On the topology, label each subnet. To save space, use only the last two octets because only these octets change.
- Use Tables 5-8 and 5-9 to document the IP addresses and subnet masks. Assign the first IP address to the router interface.
- For the WAN links, assign the first IP address to R1 and R2 for links to each router's respective B1, B2, and B3 routers.

Task 3: Apply a Basic Configuration

Using your documentation, configure the routers with basic configurations including addressing. Use **cisco** as the line passwords and **class** as the secret password. Use **64000** as the clock rate.

Task 4: Configure Static Routing Between ISP Routers

Each ISP router already has two static routes to the other ISP router's directly connected WANs. Implement static routing on each ISP router to ensure connectivity between the two regions.

Task 5: Configure RIPv1 Routing in Region 1 and Region 2

Configure RIP routing on all regional routers. Remember, the ISP routers are only using static routing.

Task 6: Disable RIP Updates on Appropriate Interfaces

RIP updates do not need to be sent out all the router interfaces. Disable RIP updates on appropriate interfaces.

Task 7: Configure Default Routes and Redistribute Through RIP

Determine which routers need a default route. Then configure that router to redistribute the default route to other routers in the region.

Task 8: Verify Full Connectivity Between All Devices in the Topology

Step 1. Test connectivity.

You should now have end-to-end connectivity. Use **ping** to test connectivity across the network. Each router should be able to ping all other router interfaces and both Web Servers.

Troubleshoot until pings are successful.

Step 2. Examine the configuration.

Use verification commands to make sure that your configurations are complete.

VLSM and CIDR

The Study Guide portion of this chapter uses a combination of matching, fill-in-the-blank, multiple-choice, and open-ended question exercises to test your knowledge and skills of basic VLSM addressing and CIDR.

The Labs and Activities portion of this chapter includes all the online curriculum activities to ensure that you have mastered the practical, hands-on skills needed to understand VLSM addressing and summarizing addresses with CIDR.

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

Study Guide

Classful and Classless Addressing

One of the ways to characterize routing protocols is either as classful or classless. This is a result of the evolution from classful to classless IPv4 addressing. As networks began to use classless addressing, classless routing protocols had to be modified or developed to include the subnet mask in the routing update. The exercises in the following section review classful and classless addressing.

Move from Classful to Classless Addressing Exercise

As of January 2007, there were over 433 million hosts on the Internet. Without the introduction of [VLSM](#) and [CIDR](#) notation in 1993 (RFC [1519](#)), [Network Address Translation](#) (NAT) in 1994 (RFC [1631](#)), and private addressing in 1996 (RFC [1918](#)), the IPv4 32-bit address space would now be exhausted.

High-Order Bits

Class A, B, and C addresses were defined with a specific format for the high-order bits, which are the leftmost bits in a 32-bit address. Table 6-1 lists the first octet in binary of sample IP addresses. For each octet, identify the type of address by designating whether it would belong to a Class A, Class B, Class C, multicast, or experimental address.

Table 6-1 High-Order Bits

First Octet of the Address in Binary	Type of Address
10100010	Class B
11100000	Multicast
01110100	Class A
11110000	Experimental
11001100	Class C

IPv4 Classful Addressing Structure

List the default subnet mask for each class.

[Class A: 255.0.0.0](#)

[Class B: 255.255.0.0](#)

[Class C: 255.255.255.0](#)

In Table 6-2, complete the table by filling in the missing information.

Table 6-2 Number of Networks and Hosts per Network for Each Class

Address Class	First Octet Range	Number of Possible Networks	Number of Hosts per Network
Class A	0 to 127	128 (2 are reserved)	16,777,214
Class B	128 to 191	16,384	65,534
Class C	192 to 223	2,097,152	254

Class A networks used the **first** octet for network assignment, which translated to a **255.0.0.0** classful subnet mask. Because only 7 bits were left in the first octet (remember, the first bit is always 0), this made 2^7 , or **128**, networks.

With **24** bits in the host portion, each Class A address had the potential for over 16 million individual host addresses.

Class B networks used the **first two** octets for network assignment, which translated to a **255.255.0.0** classful subnet mask. With the first 2 bits already established as 1 and 0, **14** bits remained for assigning networks, which resulted in **16,384** Class B network addresses. Because each Class B network address contained **16** bits in the host portion, it controlled **65,534** addresses.

Class C networks used the **first three** octets for network assignment, which translated to a **255.255.255.0** classful subnet mask. With the first 3 bits already established as 1, 1, and 0, **21** bits remained for assigning networks, for over 2 million Class C networks. But, each Class C network only had 8 bits in the host portion, or **254** possible host addresses.

Classful Routing Protocol

Remember, a classful routing protocol does not include the **subnet mask** in the routing update. It could be determined by the value of the first octet, or more accurately, the first 3 bits of the address.

Classless IP Addressing

In 1993, the Internet Engineering Task Force (IETF) introduced **classless interdomain routing**, or CIDR (RFC **1517**).

What two major provisions did CIDR allow?

- **More efficient use of IPv4 address space**
- **Prefix aggregation, which reduced the size of routing tables**

To CIDR-compliant routers, address class is meaningless. The network portion of the address is determined by the network subnet mask, also known as the network **prefix**, or **prefix** length (/8, /19, and so on). The network address is no longer determined by the class of the address.

CIDR and Route Summarization

CIDR uses **variable-length subnet masks** (VLSM) to allocate IP addresses to subnets according to individual need rather than by class. CIDR allowed prefix aggregation, which you already know as **route summarization**. Recall from Chapter 2, “Static Routing,” that you can create one static route for multiple networks. Internet routing tables were now able to benefit from the same type of aggregation of routes by combining multiple class addresses into one **supernet**, which summarizes multiple network addresses with a mask less than the classful mask.

Classless Routing Protocol

Classless routing protocols include [RIPv2](#), [EIGRP](#), [OSPF](#), [IS-IS](#), and [BGP](#). These routing protocols include the [subnet mask](#) with the network address in their routing updates.

VLSM

In a previous course, you learned how variable-length subnet masking (VLSM) allows the use of different masks for each subnet. After a network address is subnetted, those subnets can be further subnetted. As you most likely recall, VLSM is simply subnetting a subnet. VLSM can be thought of as sub-subnetting.

In the following sections, you will work through four VLSM exercises and six VLSM scenarios.

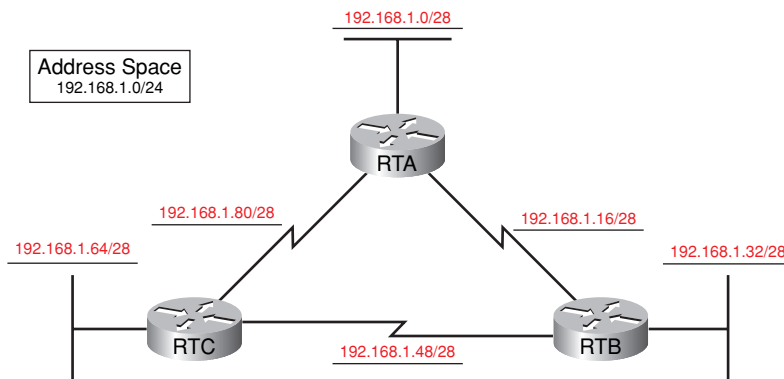
VLSM Addressing Design Exercises

In the following VLSM addressing design exercises, you will apply your VLSM addressing skills to a three-router topology. Each exercise is progressively more difficult than the previous one. There might be more than one correct answer in some situations. However, you should always practice good addressing design by assigning your subnets contiguously. This will allow the summary of a group of subnets into one aggregate route, thus decreasing the size of routing tables.

Exercise 1

Assume that 4 bits were borrowed from the host portion of 192.168.1.0/24. You are *not* using VLSM. Starting with subnet 0, label Figure 6-1 contiguously with subnets. Start with the LAN on RTA and proceed clockwise.

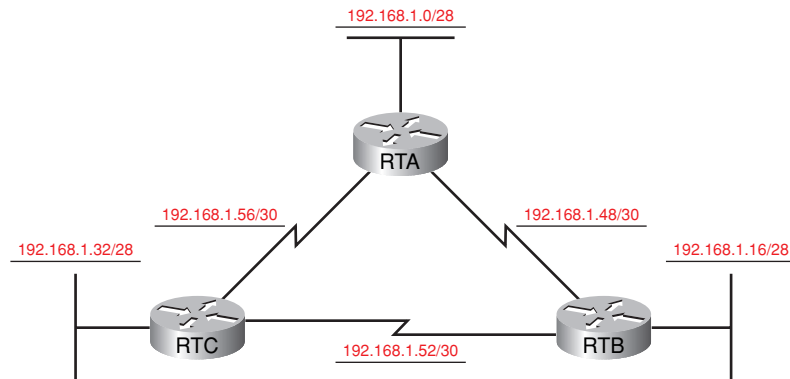
Figure 6-1 Addressing Design Exercise 1 Topology: Subnets (Answer)



How many TOTAL valid host addresses will be wasted on the WAN links?

We assigned three WAN subnets with 14 hosts each. Two hosts are used; therefore, 12 hosts x 3 WAN subnets = 36 wasted host addresses.

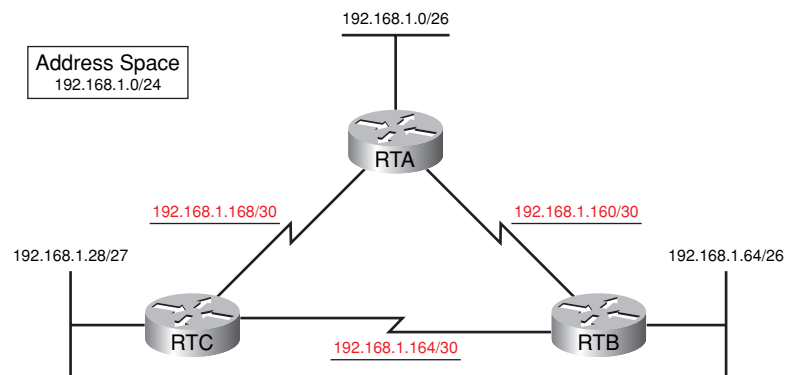
Now come up with a better addressing scheme using VLSM. Start with the same 4 bits borrowed from the host portion of 192.168.1.0/24. Label each of the LANs with a subnet. Then subnet the next available subnet to provide WAN subnets without wasting any host addresses. Label Figure 6-2 with the subnets.

Figure 6-2 Addressing Design Exercise 1 Topology: VLSM Subnets (Answer)

List the address space that is still available for future expansion.

For the solution shown in Figure 6-2, address space still available is .60/30, .64/26, and .128/25.

The topology shown in Figure 6-3 has LAN subnets already assigned out of the 192.168.1.0/24 address space. Using VLSM, create and label the WANs with subnets from the remaining address space.

Figure 6-3 Addressing Design Exercise 1 Topology: WAN Subnets (Answer)

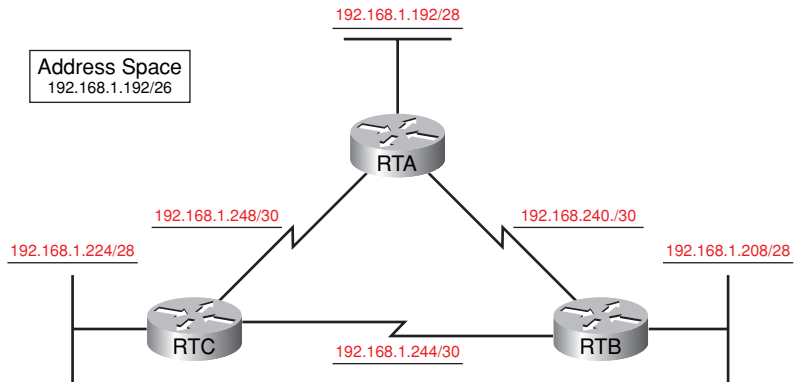
List the address space that is still available for future expansion.

Answers can vary. In the answer shown in Figure 6-3, the available address space is .172/30, .176/28, and .192/26.

Exercise 2

Your address space is 192.168.1.192/26. Each LAN needs to support ten hosts. Use VLSM to create a contiguous IP addressing scheme. Label Figure 6-4 with your addressing scheme. Don't forget the WAN links.

Figure 6-4 Addressing Design Exercise 2 Topology (Answer)



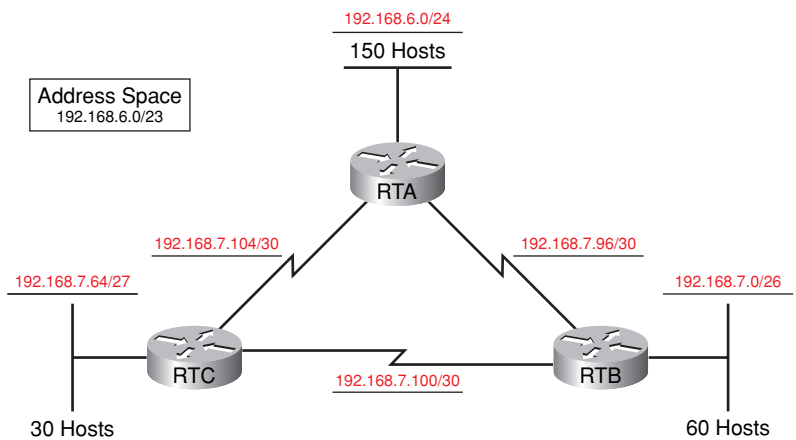
List the address space that is still available for future expansion.

There is only on subnet left: .252/30.

Exercise 3

Your address space is 192.168.6.0/23. The number of hosts needed for each LAN is shown in Figure 6-5. Use VLSM to create a contiguous IP addressing scheme. Label Figure 6-5 with your addressing scheme. Don't forget the WAN links.

Figure 6-5 Addressing Design Exercise 3 Topology (Answer)

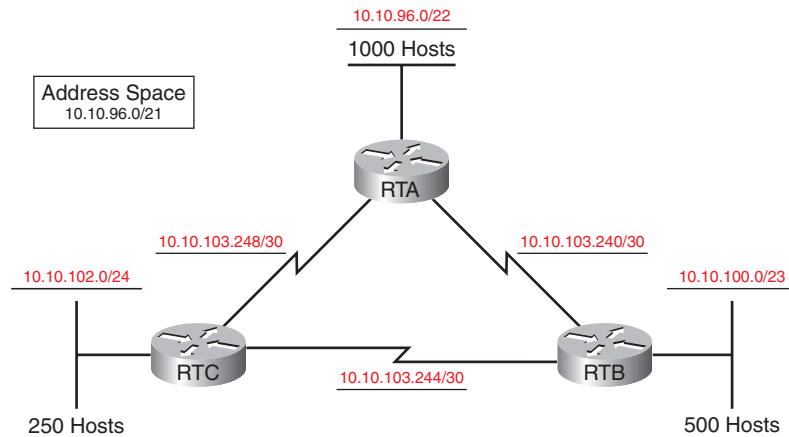


List the address space that is still available for future expansion.

For the solution shown in Figure 6-5, the address space still available is .7.108/30, .7.112/28, and .7.128/25.

Exercise 4

Your address space is 10.10.96.0/21. The number of hosts needed for each LAN is shown in Figure 6-6. Use VLSM to create a contiguous IP addressing scheme. Label Figure 6-6 with your addressing scheme. Don't forget the WAN links.

Figure 6-6 Addressing Design Exercise 4 Topology (Answer)

List the address space that is still available for future expansion.

For the solution shown in Figure 6-6, the address space still available is .103.252/30, .103.224/28, .103.192/27, .103.128/26, and .103.0/25.

VLSM Addressing Design Scenarios

The following VLSM addressing design scenarios will build upon your addressing design skills. In these scenarios, you will fully document your network design, including IP addresses for interfaces and hosts.

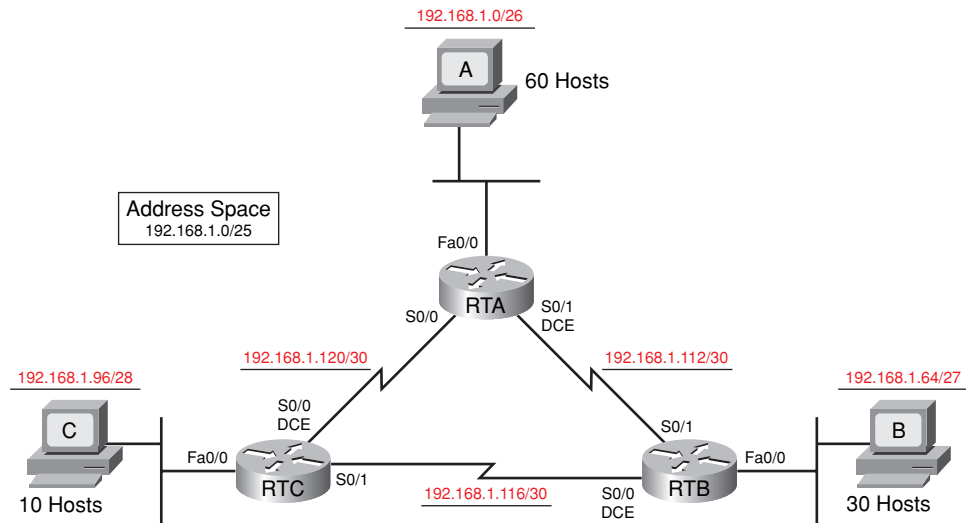
Instructor note: After students have successfully completed a scenario, you could have them test it on real equipment or in Packet Tracer.

Scenario 1

Complete Addressing Design Scenario 1 using the following list of requirements:

- Address space: 192.168.1.0/25
 - RTA LAN, 60 hosts; RTB LAN, 30 hosts; RTC LAN, 10 hosts
1. Using good VLSM design practices, contiguously assign subnets to the topology shown in Figure 6-7.

Figure 6-7 Addressing Design Scenario 1 Topology (Answer)



- Fill in Table 6-3 with all necessary IP address configuration information for all devices. Use dotted decimal format for the subnet mask.

Table 6-3 Addressing Table for VLSM Design Scenario 1

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	Fa0/0	192.168.1.1	255.255.255.192	—
	S0/1	192.168.1.113	255.255.255.252	—
	S0/0	192.168.1.121	255.255.255.252	—
RTB	Fa0/0	192.168.1.65	255.255.255.224	—
	S0/1	192.168.1.114	255.255.255.252	—
	S0/0	192.168.1.117	255.255.255.252	—
RTC	Fa0/0	192.168.1.97	255.255.255.240	—
	S0/1	192.168.1.118	255.255.255.252	—
	S0/0	192.168.1.122	255.255.255.252	—
HostA	NIC	192.168.1.2	255.255.255.192	192.168.1.1
HostB	NIC	192.168.1.66	255.255.255.224	192.168.1.65
HostC	NIC	192.168.1.98	255.255.255.240	192.168.1.97

- List the address space that is still available for future expansion.

For the solution shown in Figure 6-7, the address space still available is .124/30.

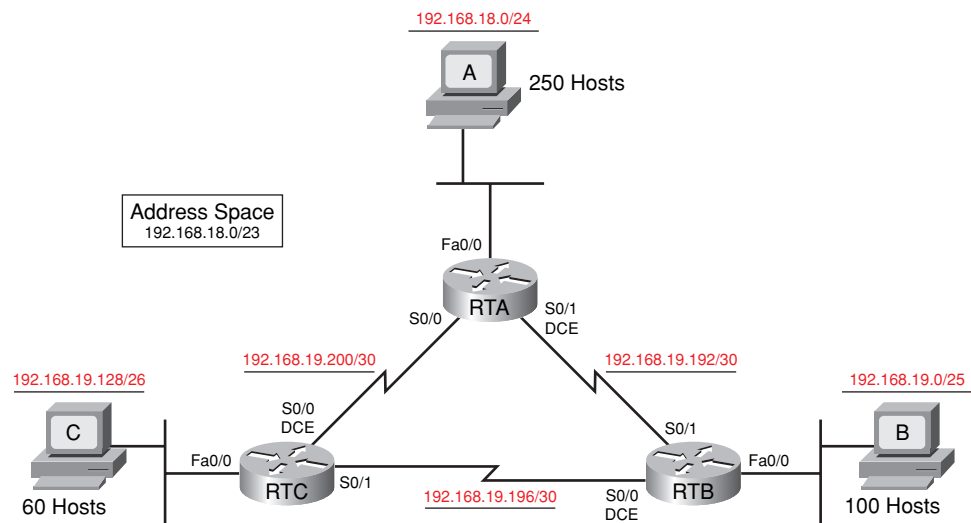
Because the given address space is /25, there is no more available space except for the one leftover WAN subnet.

Scenario 2

Complete Addressing Design Scenario 2 using the following list of requirements:

- Address space: 192.168.18.0/23
 - RTA LAN, 250 hosts; RTB LAN, 100 hosts; RTC LAN, 60 hosts
1. Using good VLSM design practices, contiguously assign subnets to the topology shown in Figure 6-8.

Figure 6-8 Addressing Design Scenario 2 Topology (Answer)



2. Fill in Table 6-4 with all necessary IP address configuration information for all devices. Use dotted decimal format for the subnet mask.

Table 6-4 Addressing Table for VLSM Scenario 2

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	Fa0/0	192.168.18.1	255.255.255.0	—
	S0/1	192.168.19.193	255.255.255.252	—
	S0/0	192.168.19.201	255.255.255.252	—
RTB	Fa0/0	192.168.19.1	255.255.255.128	—
	S0/1	192.168.19.194	255.255.255.252	—
	S0/0	192.168.19.197	255.255.255.252	—
RTC	Fa0/0	192.168.19.129	255.255.255.192	—
	S0/1	192.168.19.198	255.255.255.252	—
	S0/0	192.168.19.202	255.255.255.252	—
HostA	NIC	192.168.18.2	255.255.255.0	192.168.18.1
HostB	NIC	192.168.19.2	255.255.255.128	192.168.19.1
HostC	NIC	192.168.19.130	255.255.255.192	192.168.19.129

- List the address space that is still available for future expansion.

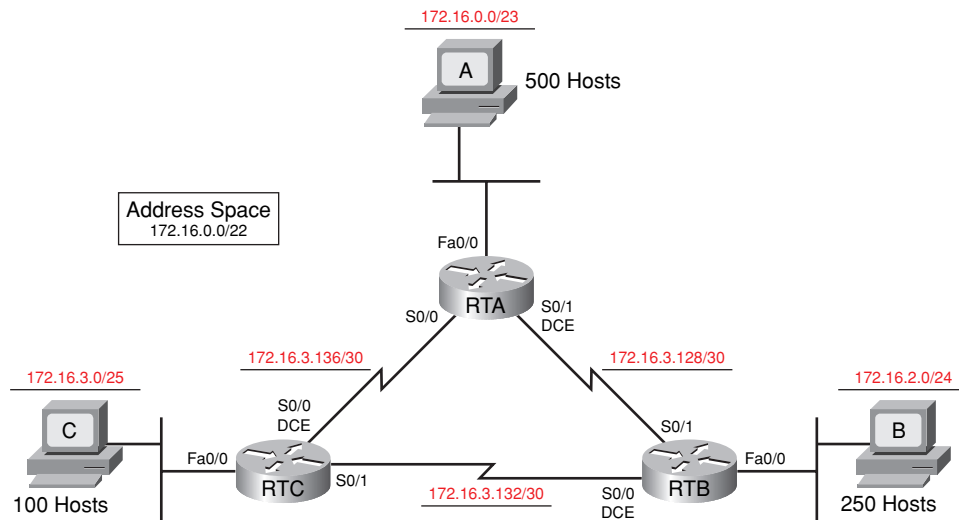
For the solution shown in Figure 6-8, the address space still available is .19.204/30, .19.208/28, and .19.224/27.

Scenario 3

Complete Addressing Design Scenario 3 using the following list of requirements:

- Address space: 172.16.0.0/22
 - RTA LAN, 500 hosts; RTB LAN, 250 hosts; RTC LAN, 100 hosts
- Using good VLSM design practices, contiguously assign subnets to the topology shown in Figure 6-9.

Figure 6-9 Addressing Design Scenario 3 Topology (Answer)



- Fill in Table 6-5 with all necessary IP address configuration information for all devices. Use dotted decimal format for the subnet mask.

Table 6-5 Addressing Table for VLSM Scenario 3

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	Fa0/0	172.16.0.1	255.255.254.0	—
	S0/1	172.16.3.129	255.255.255.252	—
	S0/0	172.16.3.137	255.255.255.252	—
RTB	Fa0/0	172.16.2.1	255.255.255.0	—
	S0/1	172.16.3.130	255.255.255.252	—
	S0/0	172.16.3.133	255.255.255.252	—
RTC	Fa0/0	172.16.3.1	255.255.255.128	—
	S0/1	172.16.3.134	255.255.255.252	—
	S0/0	172.16.3.138	255.255.255.252	—

Device	Interface	IP Address	Subnet Mask	Default Gateway
HostA	NIC	172.16.0.2	255.255.254.0	172.16.0.1
HostB	NIC	172.16.2.2	255.255.255.0	172.16.2.1
HostC	NIC	172.16.3.2	255.255.255.128	172.16.3.1

- List the address space that is still available for future expansion.

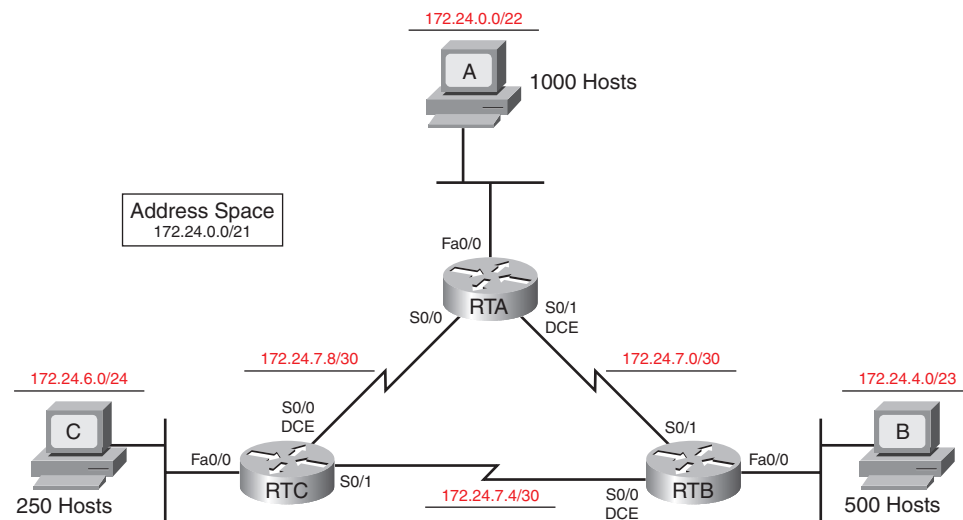
For the solution shown in Figure 6-9, the address space still available is .3.140/30, .3.144/28, .3.160/27, and .3.192/27.

Scenario 4

Complete Addressing Design Scenario 4 using the following list of requirements:

- Address space: 172.24.0.0/21
 - RTA LAN, 1000 hosts; RTB LAN, 500 hosts; RTC LAN, 250 hosts
- Using good VLSM design practices, contiguously assign subnets to the topology shown in Figure 6-10.

Figure 6-10 Addressing Design Scenario 4 Topology (Answer)



- Fill in Table 6-6 with all necessary IP address configuration information for all devices. Use dotted decimal format for the subnet mask.

Table 6-6 Addressing Table for VLSM Scenario 4

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	Fa0/0	172.24.0.1	255.255.252.0	—
	S0/1	172.24.7.1	255.255.255.252	—
	S0/0	172.24.7.9	255.255.255.252	—

continues

Table 6-6 Addressing Table for VLSM Scenario 4 *continued*

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTB	Fa0/0	172.24.4.1	255.255.254.0	—
	S0/1	172.24.7.2	255.255.255.252	—
	S0/0	172.24.7.5	255.255.255.252	—
RTC	Fa0/0	172.24.6.1	255.255.255.0	—
	S0/1	172.24.7.6	255.255.255.252	—
	S0/0	172.24.7.10	255.255.255.252	—
HostA	NIC	172.24.0.2	255.255.252.0	172.24.0.1
HostB	NIC	172.24.4.2	255.255.254.0	172.24.4.1
HostC	NIC	172.24.6.2	255.255.255.0	172.24.6.1

- List the address space that is still available for future expansion.

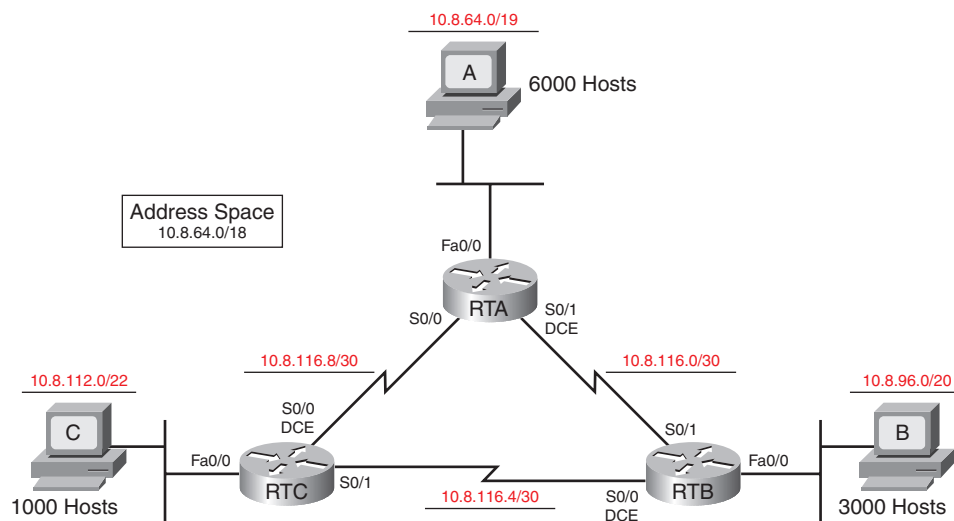
For the solution shown in Figure 6-10, the address space still available is .7.12/30, .7.16/28, .7.32/27, .7.64/26, and .7.128/25.

Scenario 5

Complete Addressing Design Scenario 5 using the following list of requirements:

- Address space: 10.8.64.0/18
 - RTA LAN, 6000 hosts; RTB LAN, 3000 hosts; RTC LAN, 1000 hosts
- Using good VLSM design practices, contiguously assign subnets to the topology shown in Figure 6-11.

Figure 6-11 Addressing Design Scenario 5 Topology (Answer)



2. Fill in Table 6-7 with all necessary IP address configuration information for all devices. Use dotted decimal format for the subnet mask.

Table 6-7 Addressing Table for VLSM Scenario 5

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	Fa0/0	10.8.64.1	255.255.224.0	—
	S0/1	10.8.116.1	255.255.255.252	—
	S0/0	10.8.116.9	255.255.255.252	—
RTB	Fa0/0	10.8.96.1	255.255.240.0	—
	S0/1	10.8.116.2	255.255.255.252	—
	S0/0	10.8.116.5	255.255.255.252	—
RTC	Fa0/0	10.8.112.1	255.255.252.0	—
	S0/1	10.8.116.6	255.255.255.252	—
	S0/0	10.8.116.10	255.255.255.252	—
HostA	NIC	10.8.64.2	255.255.224.0	10.8.64.1
HostB	NIC	10.8.96.2	255.255.240.0	10.8.96.1
HostC	NIC	10.8.112.2	255.255.252.0	10.8.112.1

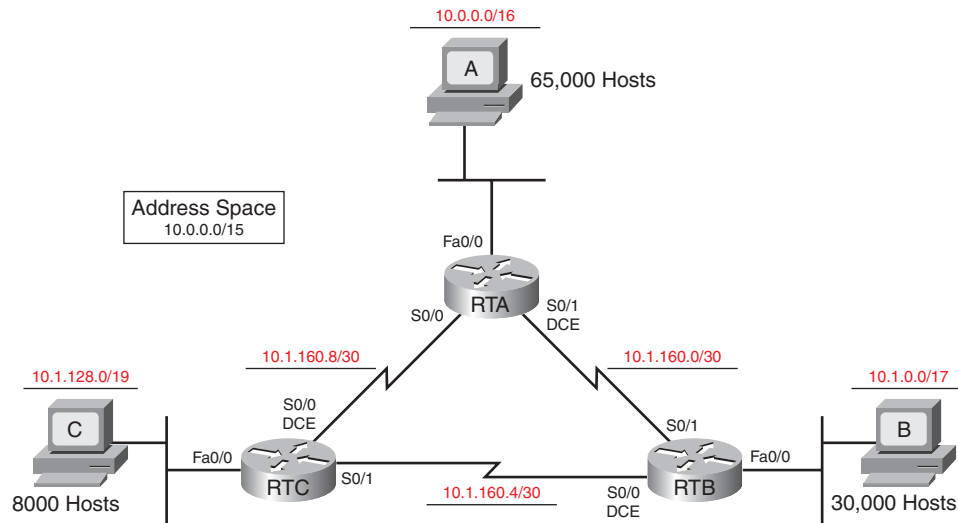
3. List the address space that is still available for future expansion.

For the solution shown in Figure 6-11, the address space still available is 116.12/30, .116.16/28, .116.32/27, .116.64/26, .116.128/25, .117.0/24, .118.0/23, and .120.0/21.

Scenario 6

Complete Addressing Design Scenario 6 using the following list of requirements:

- Address space: 10.0.0.0/15
 - RTA LAN, 65,000 hosts; RTB LAN, 30,000 hosts; RTC LAN, 8000 hosts
1. Using good VLSM design practices, contiguously assign subnets to the topology shown in Figure 6-12.

Figure 6-12 Addressing Design Scenario 6 Topology (Answer)

- Fill in Table 6-8 with all necessary IP address configuration information for all devices. Use dotted decimal format for the subnet mask.

Table 6-8 Addressing Table for VLSM Scenario 6

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	Fa0/0	10.0.0.1	255.255.0.0	—
	S0/1	10.1.160.1	255.255.255.252	—
	S0/0	10.1.160.9	255.255.255.252	—
RTB	Fa0/0	10.1.0.1	255.255.128.0	—
	S0/1	10.1.160.2	255.255.255.252	—
	S0/0	10.1.160.5	255.255.255.252	—
RTC	Fa0/0	10.1.128.1	255.255.224.0	—
	S0/1	10.1.160.6	255.255.255.252	—
	S0/0	10.1.160.10	255.255.255.252	—
HostA	NIC	10.0.0.2	255.255.0.0	10.0.0.1
HostB	NIC	10.1.0.2	255.255.128.0	10.1.0.1
HostC	NIC	10.1.128.2	255.255.224.0	10.1.128.1

- List the address space that is still available for future expansion.

For the solution shown in Figure 6-12, the address space still available is [10.1.160.12/30](#), [10.1.160.16/28](#), [10.1.160.32/27](#), [10.1.160.64/26](#), [10.1.160.128/25](#), [10.1.161.0/24](#), [10.1.162.0/23](#), [10.1.164.0/22](#), [10.1.168.0/21](#), [10.1.176.0/20](#), and [10.1.192.0/18](#).

CIDR

CIDR (classless interdomain routing) is a prefix-based standard for the interpretation of IP addresses. CIDR allows routing protocols to summarize multiple networks, a block of addresses, as a single route. With CIDR, IP addresses and their subnet masks are written as four octets, separated by periods, followed by a forward slash and a number that represents the subnet mask (slash notation). For example, 172.16.1.0/24.

As you previously learned, route summarization, also known as route aggregation, is the process of advertising a contiguous set of addresses as a single address with a less-specific, shorter subnet mask. Remember that CIDR is a form of route summarization and is synonymous with the term *supernetting*.

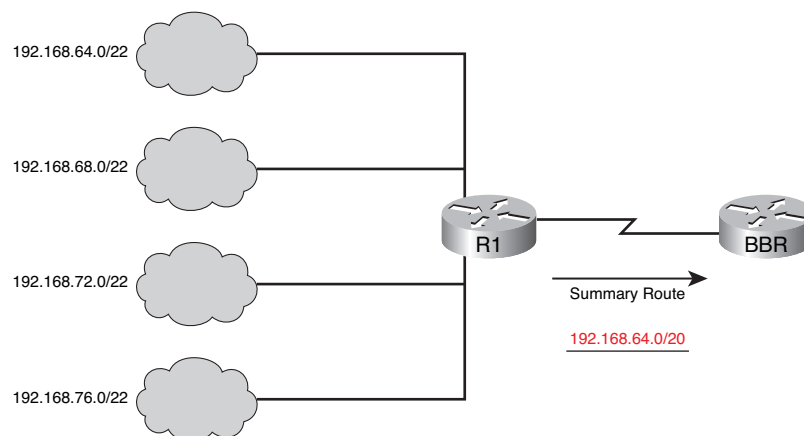
Calculating a Summary Route Exercises

To review your route summarization skills, complete the following activities. These are simply modifications of the same exercises from Chapter 2. You can also repeat those exercises for extra practice.

Exercise 1

Referring to Figure 6-13, what summary route would R1 send to BBR for the four networks? Write your answer in the space provided.

Figure 6-13 Summary Route Exercise 1 (Answer)



```

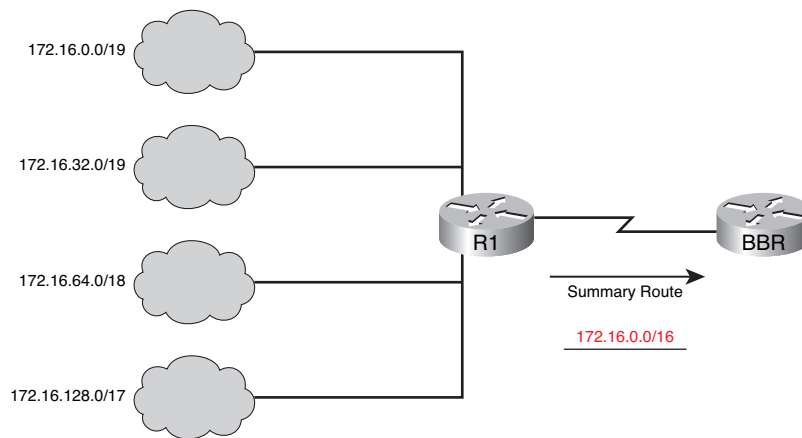
11000000.10101000.01000000.00000000
11000000.10101000.01000100.00000000
11000000.10101000.01001000.00000000
11000000.10101000.01001100.00000000
    
```

Summary route: 192.168.64.0/20

Exercise 2

Referring to Figure 6-14, what summary route would R1 send to BBR for the four networks? Write your answer in the space provided.

Figure 6-14 Summary Route Exercise 2 (Answer)



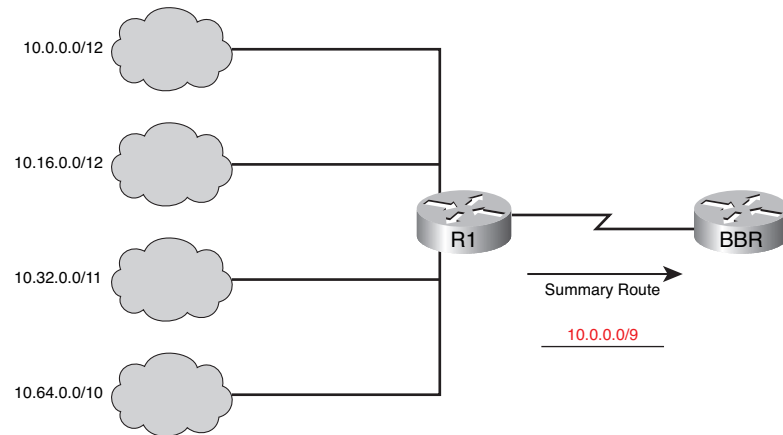
```

10101100.00010000.00000000.00000000
10101100.00010000.00100000.00000000
10101100.00010000.01000000.00000000
10101100.00010000.10000000.00000000
    
```

Summary route: 172.16.0.0/16

Exercise 3

Referring to Figure 6-15, what summary route would R1 send to BBR for the four networks? Write your answer in the space provided.

Figure 6-15 Summary Route Exercise 3 (Answer)

```

00001010.00000000.00000000.00000000
00001010.00010000.00000000.00000000
00001010.00100000.00000000.00000000
00001010.01000000.00000000.00000000

```

Summary route: 10.0.0/9

Labs and Activities

Activity 6-1: Basic VLSM Calculation and Addressing Design (6.4.1)

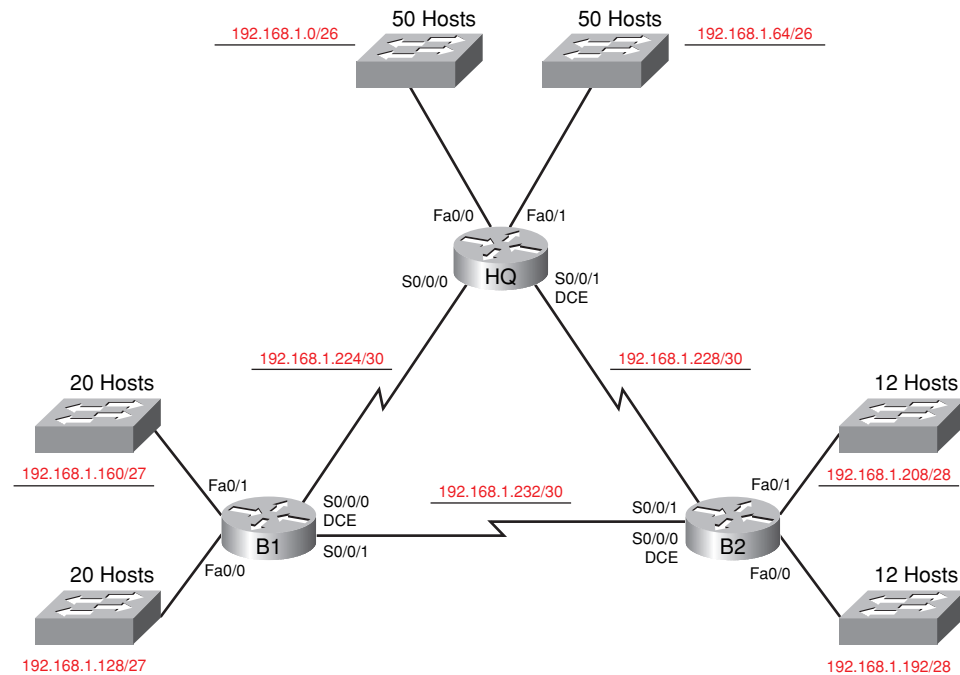
Upon completion of this activity, you will be able to

- Determine the number of subnets needed
- Determine the number of hosts needed for each subnet
- Design an appropriate addressing scheme using VLSM
- Assign addresses and subnet mask pairs to device interfaces
- Examine the use of the available network address space

Scenario

In this activity, you have been given the network address 192.168.1.0/24 to subnet and provide the IP addressing for the network shown in Figure 6-16. VLSM will be used so that the addressing requirements can be met using the 192.168.1.0/24 network. The network has the following addressing requirements:

- The HQ LAN1 will require 50 host IP addresses.
- The HQ LAN2 will require 50 host IP addresses.
- The Branch1 LAN1 will require 20 host IP addresses.
- The Branch1 LAN2 will require 20 host IP addresses
- The Branch2 LAN1 will require 12 host IP addresses.
- The Branch2 LAN2 will require 12 host IP addresses.
- The link from HQ to Branch1 will require an IP address for each end of the link.
- The link from HQ to Branch2 will require an IP address for each end of the link.
- The link from Branch1 to Branch2 will require an IP address for each end of the link.

Figure 6-16 Topology Diagram for Activity 6-1 (Answer)

Task 1: Examine the Network Requirements

Examine the network requirements and answer the questions that follow. Keep in mind that IP addresses will be needed for each of the LAN interfaces.

1. How many subnets are needed? 9
2. What is the maximum number of IP addresses that are needed for a single subnet? 51
3. How many IP addresses are needed for each of the Branch1 LANs? 21
4. How many IP addresses are needed for each of the Branch2 LANs? 13
5. How many IP addresses are needed for each of the WAN links between routers? 2
6. What is the total number of IP addresses that are needed? 176
7. What is the total number of IP addresses that are available in the 192.168.1.0/24 network? 254
8. Can the network addressing requirements be met using the 192.168.1.0/24 network? yes

Task 2: Design an IP Addressing Scheme

Step 1. Determine the subnet information for the largest network segment or segments.

In this case, the two HQ LANs are the largest subnets.

1. How many IP addresses are needed for each LAN? 51
2. What is the smallest-size subnet that can be used to meet this requirement? /26
3. What is the maximum number of IP addresses that can be assigned in this size subnet? 62

Step 2. Assign subnets to HQ LANs.

Start at the beginning of the 192.168.1.0/24 network.

1. Assign the first available subnet to the HQ LAN1.
2. Fill in the following table with the appropriate information.

HQ LAN1 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
192.168.1.0	255.255.255.192	/26	192.168.1.1	192.168.1.62	192.168.1.63

3. Assign the next available subnet to the HQ LAN2.
4. Fill in the following table with the appropriate information.

HQ LAN2 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
192.168.1.64	255.255.255.192	/26	192.168.1.65	192.168.1.126	192.168.1.127

Step 3. Determine the subnet information for the next largest network segment or segments.

In this case, the two Branch1 LANs are the next largest subnets.

1. How many IP addresses are needed for each LAN? [21](#)
2. What is the smallest-size subnet that can be used to meet this requirement? [/27](#)
3. What is the maximum number of IP addresses that can be assigned in this size subnet? [30](#)

Step 4. Assign subnets to BRANCH1 LANs.

Start with the IP address following the HQ LAN subnets.

1. Assign the next subnet to the Branch1 LAN1.
2. Fill in the following table with the appropriate information.

Branch1 LAN1 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
192.168.1.128	255.255.255.224	/27	192.168.1.129	192.168.1.158	192.168.1.159

3. Assign the next available subnet to the Branch1 LAN2.
4. Fill in the following table with the appropriate information.

Branch1 LAN2 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
192.168.1.160	255.255.255.224	/27	192.168.1.161	192.168.1.190	192.168.1.191

Step 5. Determine the subnet information for the next largest network segment or segments.

In this case, the two Branch2 LANs are the next largest subnets.

1. How many IP addresses are needed for each LAN? 13
2. What is the smallest-size subnet that can be used to meet this requirement? /28
3. What is the maximum number of IP addresses that can be assigned in this size subnet? 14

Step 6. Assign subnets to BRANCH2 LANs.

Start with the IP address following the Branch1 LAN subnets.

1. Assign the next subnet to the Branch2 LAN1. Fill in the following table with the appropriate information.

Branch2 LAN1 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
192.168.1.192	255.255.255.240	/28	192.168.1.193	192.168.1.206	192.168.1.207

2. Assign the next available subnet to the Branch2 LAN2.
3. Fill in the following table with the appropriate information.

Branch2 LAN2 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
192.168.1.208	255.255.255.240	/28	192.168.1.209	192.168.1.222	192.168.1.223

Step 7. Determine the subnet information for the links between the routers.

1. How many IP addresses are needed for each link? 2
2. What is the smallest-size subnet that can be used to meet this requirement? /30
3. What is the maximum number of IP addresses that can be assigned in this size subnet? 2

Step 8. Assign subnets to links.

Start with the IP address following the Branch2 LAN subnets.

1. Assign the next available subnet to the link between the HQ and Branch1 routers.
2. Fill in the following table with the appropriate information.

Link Between HQ and Branch1 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
192.168.1.224	255.255.255.252	/30	192.168.1.225	192.168.1.226	192.168.1.227

3. Assign the next available subnet to the link between the HQ and Branch2 routers.
4. Fill in the following table with the appropriate information.

Link Between HQ and Branch2 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
192.168.1.228	255.255.255.252	/30	192.168.1.229	192.168.1.230	192.168.1.231

5. Assign the next available subnet to the link between the Branch1 and Branch2 routers.
6. Fill in the following table with the appropriate information.

Link Between Branch1 and Branch2 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
192.168.1.232	255.255.255.252	/30	192.168.1.233	192.168.1.234	192.168.1.235

Task 3: Assign IP Addresses to the Network Devices

Assign the appropriate addresses to the device interfaces. Document the addresses to be used in Table 6-9.

Step 1. Assign addresses to the HQ router.

1. Assign the first valid host address in the HQ LAN 1 subnet to the Fa0/0 LAN interface.
2. Assign the first valid host address in the HQ LAN 2 subnet to the Fa0/1 LAN interface.
3. Assign the first valid host address in the link between HQ and the Branch1 subnet to the S0/0/0 interface.
4. Assign the first valid host address in the link between HQ and the Branch2 subnet to the S0/0/1 interface.

Step 2. Assign addresses to the Branch1 router.

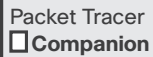
1. Assign the first valid host address in the Branch1 LAN1 subnet to the Fa0/0 LAN interface.
2. Assign the first valid host address in the Branch1 LAN2 subnet to the Fa0/1 LAN interface.
3. Assign the last valid host address in the link between Branch1 and the HQ subnet to the S0/0/0 interface.
4. Assign the first valid host address in the link between Branch1 and the Branch2 subnet to the S0/0/1 interface.

Step 3. Assign addresses to the Branch2 router.

1. Assign the first valid host address in the Branch2 LAN1 subnet to the Fa0/0 LAN interface.
2. Assign the first valid host address in the Branch2 LAN2 subnet to the Fa0/1 LAN interface.
3. Assign the last valid host address on the link between HQ and the Branch2 subnet to the S0/0/1 interface.
4. Assign the last valid host address on the link between Branch1 and the Branch2 subnet to the S0/0/0 interface.

Table 6-9 Addressing Table for Activity 6-1

Device	Interface	IP Address	Subnet Mask
HQ	Fa0/0	192.168.1.1	255.255.255.192
	Fa0/1	192.168.1.65	255.255.255.192
	S0/0/0	192.168.1.225	255.255.255.252
	S0/0/1	192.168.1.229	255.255.255.252
Branch1	Fa0/0	192.168.1.129	255.255.255.224
	Fa0/1	192.168.1.161	255.255.255.224
	S0/0/0	192.168.1.226	255.255.255.252
	S0/0/1	192.168.1.233	255.255.255.252
Branch2	Fa0/0	192.168.1.193	255.255.255.240
	Fa0/1	192.168.1.209	255.255.255.240
	S0/0/0	192.168.1.234	255.255.255.252
	S0/0/1	192.168.1.230	255.255.255.252



Packet Tracer Companion: Basic VLSM Calculation and Addressing Design (6.4.1)

You can now open the file LSG02-Lab641.pka on the CD-ROM that accompanies this book to repeat this activity using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.

Activity 6-2: Challenge VLSM Calculation and Addressing Design (6.4.2)

Upon completion of this activity, you will be able to

- Determine the number of subnets needed
- Determine the number of hosts needed for each subnet
- Design an appropriate addressing scheme using VLSM

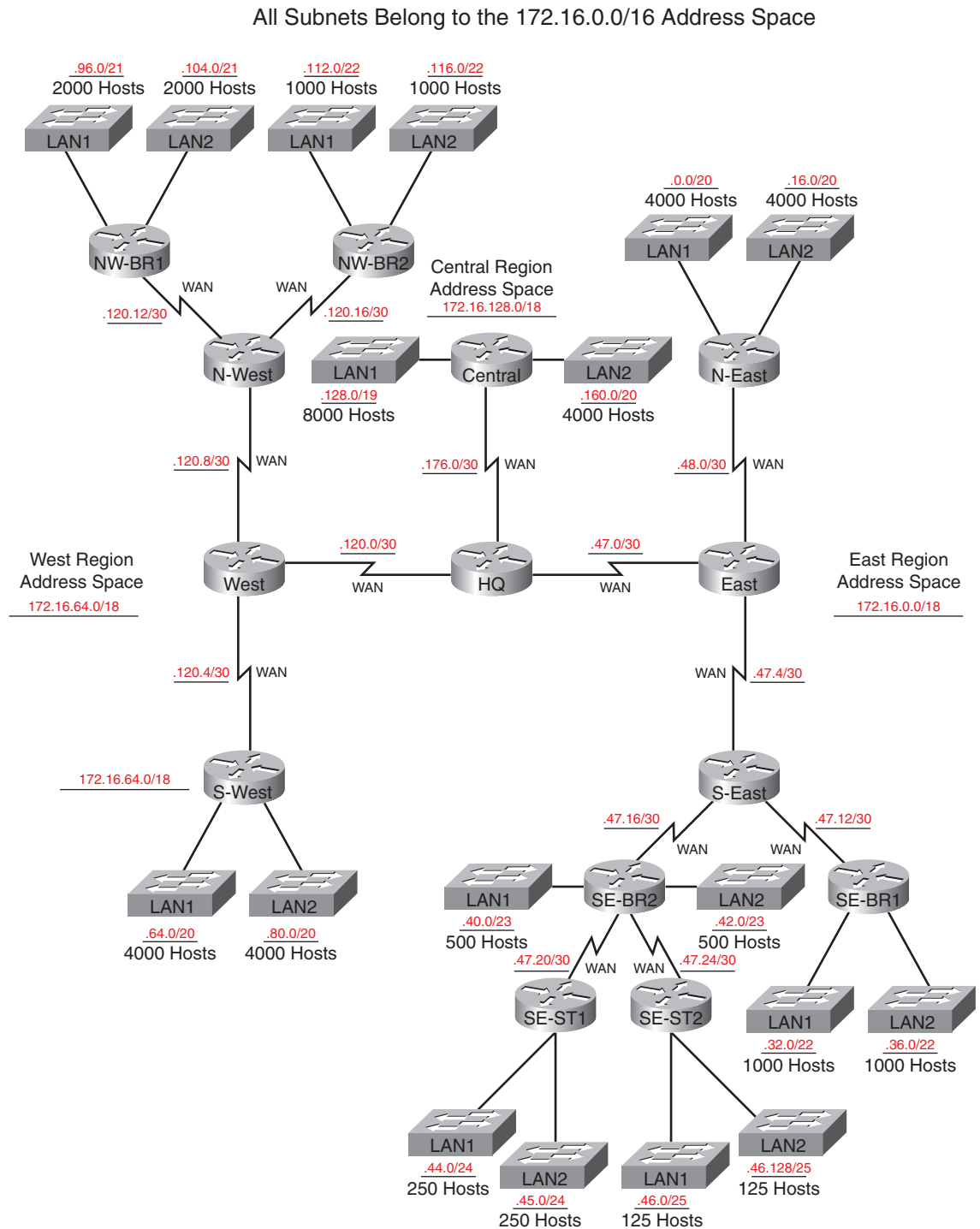
Scenario

In this activity, you have been given the network address 172.16.0.0/16 to subnet and provide the IP addressing for the network shown in Figure 6-17. VLSM will be used so that the addressing requirements can be met using the 172.16.0.0/16 network.

The network has the following addressing requirements:

- **East network section:**
 - The N-EAST (Northeast) LAN1 will require 4000 host IP addresses.
 - The N-EAST (Northeast) LAN2 will require 4000 host IP addresses.
 - The SE-BR1 (Southeast Branch1) LAN1 will require 1000 host IP addresses.
 - The SE-BR1 (Southeast Branch1) LAN2 will require 1000 host IP addresses.
 - The SE-BR2 (Southeast Branch2) LAN1 will require 500 host IP addresses.
 - The SE-BR2 (Southeast Branch2) LAN2 will require 500 host IP addresses.
 - The SE-ST1 (Southeast Satellite1) LAN1 will require 250 host IP addresses.
 - The SE-ST1 (Southeast Satellite1) LAN2 will require 250 host IP addresses.
 - The SE-ST2 (Southeast Satellite2) LAN1 will require 125 host IP addresses.
 - The SE-ST2 (Southeast Satellite2) LAN2 will require 125 host IP addresses.
- **West network section:**
 - The S-WEST (Southwest) LAN1 will require 4000 host IP addresses.
 - The S-WEST (Southwest) LAN2 will require 4000 host IP addresses.
 - The NW-BR1 (Northwest Branch1) LAN2 will require 2000 host IP addresses.
 - The NW-BR1 (Northwest Branch1) LAN1 will require 2000 host IP addresses.
 - The NW-BR2 (Northwest Branch2) LAN1 will require 1000 host IP addresses.
 - The NW-BR2 (Northwest Branch2) LAN2 will require 1000 host IP addresses.

Figure 6-17 Topology Diagram for Activity 6-2 (Answer)



- **Central network section:**

- The Central LAN1 will require 8000 host IP addresses.
- The Central LAN2 will require 4000 host IP addresses.

- The WAN links between each of the routers will require an IP address for each end of the link.

Task 1: Examine the Network Requirements

Examine the network requirements and answer the questions that follow. Keep in mind that IP addresses will be needed for each of the LAN interfaces.

1. How many LAN subnets are needed? [18](#)
2. How many subnets are needed for the WAN links between routers? [13](#)
3. How many total subnets are needed? [31](#)
4. What is the maximum number of host IP addresses that are needed for a single subnet? [8000](#)
5. What is the least number of host IP addresses that are needed for a single subnet? [125](#)
6. How many IP addresses are needed for the East portion of the network? Be sure to include the WAN links between the routers as well as an IP address for each LAN interface. [11,774](#)
7. How many IP addresses are needed for the West portion of the network? Be sure to include the WAN links between the routers as well as an IP address for each LAN interface. [14,016](#)
8. How many IP addresses are needed for the Central portion of the network? Be sure to include the WAN links between the routers as well as an IP address for each LAN interface. [12,004](#)
9. What is the total number of IP addresses that are needed? [37,794](#)
10. What is the total number of IP addresses that are available in the 172.16.0.0/16 network? [65,534](#)
11. Can the network addressing requirements be met using the 172.16.0.0/16 network? [yes](#)

Task 2: Divide the Network into Three Subnetworks

Step 1. Determine the subnet information for each network section.

To keep the subnets of each of the major network sections contiguous, begin by creating a main subnet for each of the East, West, and Central network sections.

1. What is the smallest-size subnet that can be used to meet the addressing requirement for the East network? [/18](#)
2. What is the maximum number of IP addresses that can be assigned in this size subnet? [16,382](#)
3. What is the smallest-size subnet that can be used to meet the addressing requirement for the West network? [/18](#)
4. What is the maximum number of IP addresses that can be assigned in this size subnet? [16,384](#)
5. What is the smallest-size subnet that can be used to meet the addressing requirement for the Central network? [/18](#)
6. What is the maximum number of IP addresses that can be assigned in this size subnet? [16,384](#)

Step 2. Assign subnets.

1. Start at the beginning of the 172.16.0.0/16 network. Assign the first available subnet to the East section of the network.

- Fill in the following table with the appropriate information.

East Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.0.0	255.255.192.0	/18	172.16.0.1	172.16.63.254	172.16.63.255

- Assign the next available subnet to the West section of the network.
- Fill in the following table with the appropriate information.

West Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.64.0	255.255.192.0	/18	172.16.64.1	172.16.127.254	172.16.127.255

- Assign the next available subnet to the Central section of the network.
- Fill in the following table with the appropriate information.

Central Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.128.0	255.255.192.0	/18	172.16.128.1	172.16.191.254	172.16.191.255

Task 3: Design an IP Addressing Scheme for the Central Network

Step 1. Determine the subnet information for the Central LAN1.

Use the address space that was designated for the Central network in Task 1.

- What is the smallest-size subnet that can be used to meet this requirement? [/19](#)
- What is the maximum number of IP addresses that can be assigned in this size subnet? [8190](#)

Step 2. Assign a subnet to Central LAN1.

Start at the beginning of the address space designated for the Central network.

- Assign the first subnet to the Central LAN1.
- Fill in the following table with the appropriate information.

Central LAN1 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.128.0	255.255.224.0	/19	172.16.128.1	172.16.159.254	172.16.159.255

Step 3. Determine the subnet information for the Central LAN2.

1. What is the smallest-size subnet that can be used to meet this requirement? [/20](#)
2. What is the maximum number of IP addresses that can be assigned in this size subnet? [4094](#)

Step 4. Assign a subnet to Central LAN2.

1. Assign the next available subnet to the Central LAN2.
2. Fill in the following table with the appropriate information.

Central LAN2 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.160.0	255.255.240.0	/20	172.16.160.1	172.16.175.254	172.16.175.255

Step 5. Determine the subnet information for the WAN link between the Central router and the HQ router.

1. What is the smallest-size subnet that can be used to meet this requirement? [/30](#)
2. What is the maximum number of IP addresses that can be assigned in this size subnet? [2](#)

Step 6. Assign a subnet to the WAN link.

1. Assign the next available subnet to the WAN link between the Central router and the HQ router.
2. Fill in the following table with the appropriate information.

WAN Link Between the Central and HQ Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.176.0	255.255.255.252	/30	172.16.176.1	172.16.176.2	172.16.176.3

Task 4: Design an IP Addressing Scheme for the West Network

Step 1. Determine the subnet information for the S-WEST LAN1.

Use the address space that was designated for the West network in Task 1.

1. What is the smallest-size subnet that can be used to meet this requirement? [/20](#)

2. What is the maximum number of IP addresses that can be assigned in this size subnet? [4094](#)

Step 2. Assign a subnet to S-WEST LAN1.

Start at the beginning of the address space designated for the West network.

1. Assign the first subnet to the S-WEST LAN1.
2. Fill in the following table with the appropriate information.

S-WEST LAN1 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.64.0	255.255.240.0	/20	172.16.64.1	172.16.79.254	172.16.79.255

Step 3. Determine the subnet information for the S-WEST LAN2.

1. What is the smallest-size subnet that can be used to meet this requirement? [/20](#)
2. What is the maximum number of IP addresses that can be assigned in this size subnet? [4094](#)

Step 4. Assign a subnet to S-WEST LAN2.

1. Assign the next available subnet to the S-WEST LAN2.
2. Fill in the following table with the appropriate information.

S-WEST LAN2 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.80.0	255.255.240.0	/20	172.16.80.1	172.16.95.254	172.16.95.255

Step 5. Determine the subnet information for the NW-BR1 LAN1.

1. What is the smallest-size subnet that can be used to meet this requirement? [/21](#)
2. What is the maximum number of IP addresses that can be assigned in this size subnet? [2046](#)

Step 6. Assign a subnet to NW-BR1 LAN1.

1. Assign the next available subnet to the NW-BR1 LAN1.
2. Fill in the following table with the appropriate information.

NW-BR1 LAN1 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.96.0	255.255.248.0	/21	172.16.96.1	172.16.103.254	172.16.103.255

Step 7. Determine the subnet information for the NW-BR1 LAN2.

1. What is the smallest-size subnet that can be used to meet this requirement? [/21](#)
2. What is the maximum number of IP addresses that can be assigned in this size subnet? [2046](#)

Step 8. Assign a subnet to NW-BR1 LAN2.

1. Assign the next available subnet to the NW-BR1 LAN2.
2. Fill in the following table with the appropriate information.

NW-BR1 LAN2 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.104.0	255.255.248.0	/21	172.16.104.1	172.16.111.254	172.16.111.255

Step 9. Determine the subnet information for the NW-BR2 LAN1.

1. What is the smallest-size subnet that can be used to meet this requirement? [/22](#)
2. What is the maximum number of IP addresses that can be assigned in this size subnet? [1022](#)

Step 10. Assign a subnet to NW-BR2 LAN1.

1. Assign the next available subnet to the NW-BR2 LAN1.
2. Fill in the following table with the appropriate information.

NW-BR2 LAN1 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.112.0	255.255.252.0	/22	172.16.112.1	172.16.115.254	172.16.115.255

Step 11. Determine the subnet information for the NW-BR2 LAN2.

1. What is the smallest-size subnet that can be used to meet this requirement? [/22](#)
2. What is the maximum number of IP addresses that can be assigned in this size subnet? [1022](#)

Step 12. Assign a subnet to NW-BR2 LAN2.

1. Assign the next available subnet to the NW-BR2 LAN2.
2. Fill in the following table with the appropriate information.

NW-BR2 LAN2 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.116.0	255.255.252.0	/22	172.16.116.1	172.16.119.254	172.16.119.255

Step 13. Determine the subnet information for the WAN links between the routers in the West network.

1. How many router-to-router WAN links are present in the West network? 5
2. How many IP addresses are needed for each of these WAN links? 2
3. What is the smallest-size subnet that can be used to meet this requirement? /30
4. What is the maximum number of IP addresses that can be assigned in this size subnet? 2

Step 14. Assign subnets to WAN links.

1. Assign the next available subnets to the WAN links between the routers.
2. Fill in the following table with the appropriate information.

WAN Links Between the Routers in the West Network

WAN Link	Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
HQ to WEST	172.16.120.0	255.255.255.252	/30	172.16.120.1	172.16.120.2	172.16.120.3
WEST to						
S-WEST	172.16.120.4	255.255.255.252	/30	172.16.120.5	172.16.120.6	172.16.120.7
WEST to N-WEST	172.16.120.8	255.255.255.252	/30	172.16.120.9	172.16.120.10	172.16.120.11
N-WEST to NW-BR1	172.16.120.12	255.255.255.252	/30	172.16.120.13	172.16.120.14	172.16.120.15
N-WEST to NW-BR2	172.16.120.16	255.255.255.252	/30	172.16.120.17	172.16.120.18	172.16.120.19

Task 5: Design an IP Addressing Scheme for the East Network

Step 1. Determine the subnet information for the N-EAST LAN1.

Use the address space that was designated for the East network in Task 1.

1. What is the smallest-size subnet that can be used to meet this requirement? /20
2. What is the maximum number of IP addresses that can be assigned in this size subnet? 4094

Step 2. Assign a subnet to N-EAST LAN1.

Start at the beginning of the address space designated for the East network.

1. Assign the first subnet to the N-EAST LAN1.
2. Fill in the following table with the appropriate information.

N-EAST LAN1 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.0.0	255.255.240.0	/20	172.16.0.1	172.16.15.254	172.16.15.255

Step 3. Determine the subnet information for the N-EAST LAN2.

1. What is the smallest-size subnet that can be used to meet this requirement? /20
2. What is the maximum number of IP addresses that can be assigned in this size subnet? 4094

Step 4. Assign a subnet to N-EAST LAN2.

1. Assign the next available subnet to the N-EAST LAN2.
2. Fill in the following table with the appropriate information.

N-EAST LAN2 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.16.0	255.255.240.0	/20	172.16.16.1	172.16.31.254	172.16.31.255

Step 5. Determine the subnet information for the SE-BR1 LAN1.

1. What is the smallest-size subnet that can be used to meet this requirement? /22
2. What is the maximum number of IP addresses that can be assigned in this size subnet? 1022

Step 6. Assign a subnet to SE-BR1 LAN1.

1. Assign the next available subnet to the SE-BR1 LAN1.
2. Fill in the following table with the appropriate information.

SE-BR1 LAN1 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.32.0	255.255.252.0	/22	172.16.32.1	172.16.35.254	172.16.35.255

Step 7. Determine the subnet information for the SE-BR1 LAN2.

1. What is the smallest-size subnet that can be used to meet this requirement? /22

2. What is the maximum number of IP addresses that can be assigned in this size subnet? [1022](#)

Step 8. Assign a subnet to SE-BR1 LAN2.

1. Assign the next available subnet to the SE-BR1 LAN2.
2. Fill in the following table with the appropriate information.

SE-BR1 LAN2 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.36.0	255.255.252.0	/22	172.16.36.1	172.16.39.254	172.16.39.255

Step 9. Determine the subnet information for the SE-BR2 LAN1.

1. What is the smallest-size subnet that can be used to meet this requirement? [/23](#)
2. What is the maximum number of IP addresses that can be assigned in this size subnet? [510](#)

Step 10. Assign a subnet to SE-BR2 LAN1.

1. Assign the next available subnet to the SE-BR2 LAN1.
2. Fill in the following table with the appropriate information.

SE-BR2 LAN1 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.40.0	255.255.254.0	/23	172.16.40.1	172.16.41.254	172.16.41.255

Step 11. Determine the subnet information for the SE-BR2 LAN2.

1. What is the smallest-size subnet that can be used to meet this requirement? [/23](#)
2. What is the maximum number of IP addresses that can be assigned in this size subnet? [510](#)

Step 12. Assign a subnet to SE-BR2 LAN2.

1. Assign the next available subnet to the SE-BR2 LAN2.
2. Fill in the following table with the appropriate information.

SE-BR2 LAN2 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.42.0	255.255.254.0	/23	172.16.42.1	172.16.43.254	172.16.43.255

Step 13. Determine the subnet information for the SE-ST1 LAN1.

1. What is the smallest size subnet that can be used to meet this requirement? [/24](#)
2. What is the maximum number of IP addresses that can be assigned in this size subnet? [254](#)

Step 14. Assign a subnet to SE-ST1 LAN1.

1. Assign the next available subnet to the SE-ST1 LAN1.
2. Fill in the following table with the appropriate information.

SE-ST1 LAN1 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.44.0	255.255.255.0	/24	172.16.44.1	172.16.44.254	172.16.44.255

Step 15. Determine the subnet information for the SE-ST1 LAN2.

1. What is the smallest-size subnet that can be used to meet this requirement? [/24](#)
2. What is the maximum number of IP addresses that can be assigned in this size subnet? [254](#)

Step 16. Assign a subnet to SE-ST1 LAN2.

1. Assign the next available subnet to the SE-ST1 LAN2.
2. Fill in the following table with the appropriate information.

SE-ST1 LAN2 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.45.0	255.255.255.0	/24	172.16.45.1	172.16.45.254	172.16.45.255

Step 17. Determine the subnet information for the SE-ST2 LAN1.

1. What is the smallest-size subnet that can be used to meet this requirement? [/25](#)
2. What is the maximum number of IP addresses that can be assigned in this size subnet? [126](#)

Step 18. Assign a subnet to SE-ST2 LAN1.

1. Assign the next available subnet to the SE-ST2 LAN1.
2. Fill in the following table with the appropriate information.

SE-ST2 LAN1 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.46.0	255.255.255.128	/25	172.16.46.1	172.16.46.126	172.16.46.127

Step 19. Determine the subnet information for the SE-ST2 LAN2.

1. What is the smallest-size subnet that can be used to meet this requirement? [/25](#)
2. What is the maximum number of IP addresses that can be assigned in this size subnet? [126](#)

Step 20. Assign a subnet to SE-ST2 LAN2.

1. Assign the next available subnet to the SE-ST2 LAN2.
2. Fill in the following table with the appropriate information.

SE-ST2 LAN2 Subnet

Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
172.16.46.128	255.255.255.128	/25	172.16.46.129	172.16.46.254	172.16.46.255

Step 21. Determine the subnet information for the WAN links between the routers in the East network.

1. How many router-to-router WAN links are present in the East network? [7](#)
2. How many IP addresses are needed for each of these WAN links? [2](#)
3. What is the smallest-size subnet that can be used to meet this requirement? [/30](#)
4. What is the maximum number of IP addresses that can be assigned in this size subnet? [2](#)

Step 22. Assign subnets to WAN links.

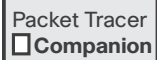
1. Assign the next available subnets to the WAN links between the routers.
2. Fill in the following table with the appropriate information.

WAN Links Between the Routers in the East Network

WAN Link	Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
HQ to EAST	172.16.47.0	255.255.255.252	/30	172.16.47.1	172.16.47.2	172.16.47.3
EAST to S-EAST	172.16.47.4	255.255.255.252	/30	172.16.47.5	172.16.47.6	172.16.47.7
EAST to N-EAST	172.16.47.8	255.255.255.252	/30	172.16.47.9	172.16.47.10	172.16.47.11
S-EAST to SE-BR1	172.16.47.12	255.255.255.252	/30	172.16.47.13	172.16.47.14	172.16.47.15
S-EAST to SE-BR2	172.16.47.16	255.255.255.252	/30	172.16.47.17	172.16.47.18	172.16.47.19

continues

WAN Link	Network Address	Decimal Subnet Mask	CIDR Subnet Mask	First Usable IP Address	Last Usable IP Address	Broadcast Address
SE-BR2 to SE-ST1	172.16.47.20	255.255.255.252	/30	172.16.47.21	172.16.47.22	172.16.47.23
SE-BR2 to SE-ST2	172.16.47.24	255.255.255.252	/30	172.16.47.25	172.16.47.26	172.16.47.27



Packet Tracer Companion: Challenge VLSM Calculation and Addressing Design (6.4.2)

You can now open the file LSG02-Lab642.pka on the CD-ROM that accompanies this book to repeat this activity using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.

Activity 6-3: Troubleshooting a VLSM Addressing Design (6.4.3)

Upon completion of this activity, you will be able to

- Discover errors in a VLSM design
- Propose solutions for VLSM design errors
- Document the corrected VLSM assignments

Scenario

In this activity, the network address 172.16.128.0/17 has been used to provide the IP addressing for the network shown in Figure 6-18. VLSM has been used to subnet the address space incorrectly. You will need to troubleshoot the addressing that has been assigned for each subnet (see Table 6-10) to determine where errors are present and then determine the correct addressing assignments, where needed.

Figure 6-18 Topology Diagram for Activity 6-3

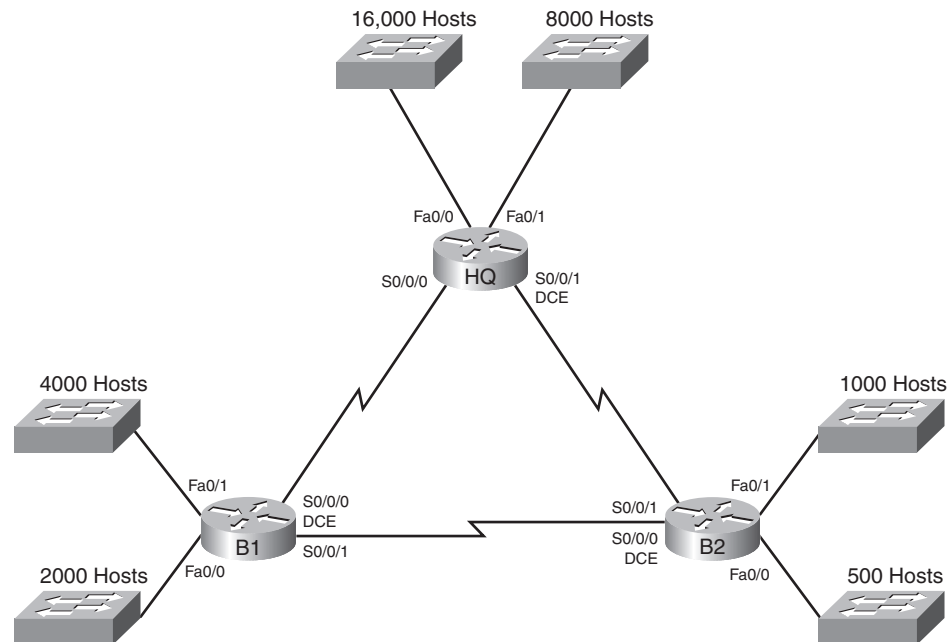


Table 6-10 Network Address Space Assignments for Activity 6-3

Subnet	Number of IP Addresses Needed	Network Address
HQ LAN1	16,000	172.16.128.0/19
HQ LAN2	8000	172.16.192.0/18
Branch1 LAN1	4000	172.16.224.0/20
Branch1 LAN2	2000	172.16.240.0/21
Branch2 LAN1	1000	172.16.248.0/24
Branch2 LAN2	500	172.16.252.0/23
Link from HQ to Branch1	2	172.16.254.0/28
Link from HQ to Branch2	2	172.16.154.6/30
Link from Branch1 to Branch2	2	172.16.254.8/30

Task 1: Examine the Addressing for the HQ LANs

Step 1. Examine the addressing assignment for the HQ LAN1 subnet and answer the questions that follow.

- How many IP addresses are needed for the HQ LAN1 subnet? **16,000**
- How many IP addresses are available in the currently assigned subnet? **8190**
- Will the currently assigned subnet fulfill the size requirement for the HQ LAN1 subnet? **no**

If the answer to the previous question is **no**, propose a new subnet mask that will allow the correct number of IP addresses. [/18 or 255.255.192.0](#)

4. Does the subnet overlap with any of the other currently assigned networks? **no**

If the answer to the previous question is **yes**, propose a new subnet mask that will allow the correct number of IP addresses without overlapping into any other subnets.

Step 2. Examine the addressing assignment for the HQ LAN2 subnet and answer the questions that follow.

1. How many IP addresses are needed for the HQ LAN2 subnet? [8000](#)
2. How many IP addresses are available in the currently assigned subnet? [16,382](#)
3. Will the currently assigned subnet fulfill the size requirement for the HQ LAN2 subnet? **yes**

If the answer to the previous question is **no**, propose a new subnet mask that will allow the correct number of IP addresses.

4. Does the subnet overlap with any of the other currently assigned networks? **yes**

If the answer to the previous question is **yes**, propose a new subnet mask that will allow the correct number of IP addresses without overlapping into any other subnets. [/19 or 255.255.224.0](#)

Task 2: Examine the Addressing for the Branch1 LANs

Step 1. Examine the addressing assignment for the Branch1 LAN1 subnet and answer the questions that follow.

1. How many IP addresses are needed for the Branch1 LAN1 subnet? [4000](#)
2. How many IP addresses are available in the currently assigned subnet? [4094](#)
3. Will the currently assigned subnet fulfill the size requirement for the Branch1 LAN1 subnet? **yes**

If the answer to the previous question is **no**, propose a new subnet mask that will allow the correct number of IP addresses.

4. Does the subnet overlap with any of the other currently assigned networks? **no**

If the answer to the previous question is **yes**, propose a new subnet mask that will allow the correct number of IP addresses without overlapping into any other subnets.

Step 2. Examine the addressing assignment for the Branch1 LAN2 and answer the questions that follow.

1. How many IP addresses are needed for the Branch1 LAN2 subnet? [2000](#)
2. How many IP addresses are available in the currently assigned subnet? [2046](#)
3. Will the currently assigned subnet fulfill the size requirement for the Branch1 LAN2 subnet? **yes**

If the answer to the previous question is **no**, propose a new subnet mask that will allow the correct number of IP addresses.

4. Does the subnet overlap with any of the other currently assigned networks? **no**

If the answer to the previous question is **yes**, propose a new network address that will allow the correct number of IP addresses without overlapping into any other subnets.

Task 3: Examine the Addressing for the Branch2 LANs

Step 1. Examine the addressing assignment for the Branch2 LAN1 subnet and answer the questions that follow.

1. How many IP addresses are needed for the Branch2 LAN1 subnet? 1000
2. How many IP addresses are available in the currently assigned subnet? 254
3. Will the currently assigned subnet fulfill the size requirement for the Branch2 LAN1 subnet? no

If the answer to the previous question is **no**, propose a new subnet mask that will allow the correct number of IP addresses. /22 or 255.255.252.0

4. Does the subnet overlap with any of the other currently assigned networks? no

If the answer to the previous question is **yes**, propose a new subnet mask that will allow the correct number of IP addresses without overlapping into any other subnets.

Step 2. Examine the addressing assignment for the Branch2 LAN2 and answer the questions that follow.

1. How many IP addresses are needed for the Branch2 LAN2 subnet? 500
2. How many IP addresses are available in the currently assigned subnet? 510
3. Will the currently assigned subnet fulfill the size requirement for the Branch2 LAN2 subnet? yes

If the answer to the previous question is **no**, propose a new subnet mask that will allow the correct number of IP addresses.

4. Does the subnet overlap with any of the other currently assigned networks? no

If the answer to the previous question is **yes**, propose a new network address that will allow the correct number of IP addresses without overlapping into any other subnets.

Task 4: Examine the Addressing for the Links Between Routers

Step 1. Examine the addressing assignment for the link between the HQ and Branch1 routers and answer the questions that follow.

1. How many IP addresses are needed for the link between the HQ and Branch1 routers? 2
2. How many IP addresses are available in the currently assigned subnet? 14
3. Will the currently assigned subnet fulfill the size requirement for the link between the HQ and Branch1 routers? yes

If the answer to the previous question is **no**, propose a new subnet mask that will allow the correct number of IP addresses.

4. Does the subnet overlap with any of the other currently assigned networks? **yes**

If the answer to the previous question is **yes**, propose a new subnet mask that will allow the correct number of IP addresses without overlapping into any other subnets.
/30 or 255.255.255.252

Step 2. Examine the addressing assignment for the link between the HQ and Branch2 routers and answer the questions that follow.

1. How many IP addresses are needed for the link between the HQ and Branch2 routers? 2
2. How many IP addresses are available in the currently assigned subnet? 2
3. Will the currently assigned subnet fulfill the size requirement for the link between the HQ and Branch2 routers? **yes**

If the answer to the previous question is **no**, propose a new subnet mask that will allow the correct number of IP addresses.

4. Does the subnet overlap with any of the other currently assigned networks? **yes**

If the answer to the previous question is **yes**, propose a new network address that will allow the correct number of IP addresses without overlapping into any other subnets.
172.16.154.4

Step 3. Examine the addressing assignment for the link between the Branch1 and Branch2 routers and answer the questions that follow.

1. How many IP addresses are needed for the link between the Branch1 and Branch2 routers? 2
2. How many IP addresses are available in the currently assigned subnet? 2
3. Will the currently assigned subnet fulfill the size requirement for the link between the Branch1 and Branch2 routers? **yes**

If the answer to the previous question is **no**, propose a new subnet mask that will allow the correct number of IP addresses.

4. Does the subnet overlap with any of the other currently assigned networks? **no**

If the answer to the previous question is **yes**, propose a new subnet mask that will allow the correct number of IP addresses without overlapping into any other subnets.

Task 5: Document the Corrected Addressing Information

Record the corrected addressing information in Table 6-11.

Table 6-11 Correct Network Address Space Assignments for Lab 6-3

Subnet	Number of IP Addresses Needed	Network Address
HQ LAN1	16,000	172.16.128.0/18
HQ LAN2	8000	172.16.192.0/19
Branch1 LAN1	4000	172.16.224.0/20
Branch1 LAN2	2000	172.16.240.0/21

Subnet	Number of IP Addresses Needed	Network Address
Branch2 LAN1	1000	172.16.248.0/22
Branch2 LAN2	500	172.16.252.0/23
Link from HQ to Branch1	2	172.16.254.0/30
Link from HQ to Branch2	2	172.16.254.4/30
Link from Branch1 to Branch2	2	172.16.254.8/30

Packet Tracer
Companion

Packet Tracer Companion: Troubleshooting a VLSM Addressing Design (6.4.3)

You can now open the file LSG02-Lab643.pka on the CD-ROM that accompanies this book to repeat this activity using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.

Activity 6-4: Basic Route Summarization (6.4.4)

Upon completion of this activity, you will be able to determine summarized routes that can be used to reduce the size of routing tables.

Scenario

In this activity, you have been given the network shown in Figure 6-19. The subnetting and address assignments have already been completed for the network segments, as shown in Table 6-12. Determine summarized routes that can be used to reduce the number of entries in the routing tables.

Figure 6-19 Topology Diagram for Activity 6-4

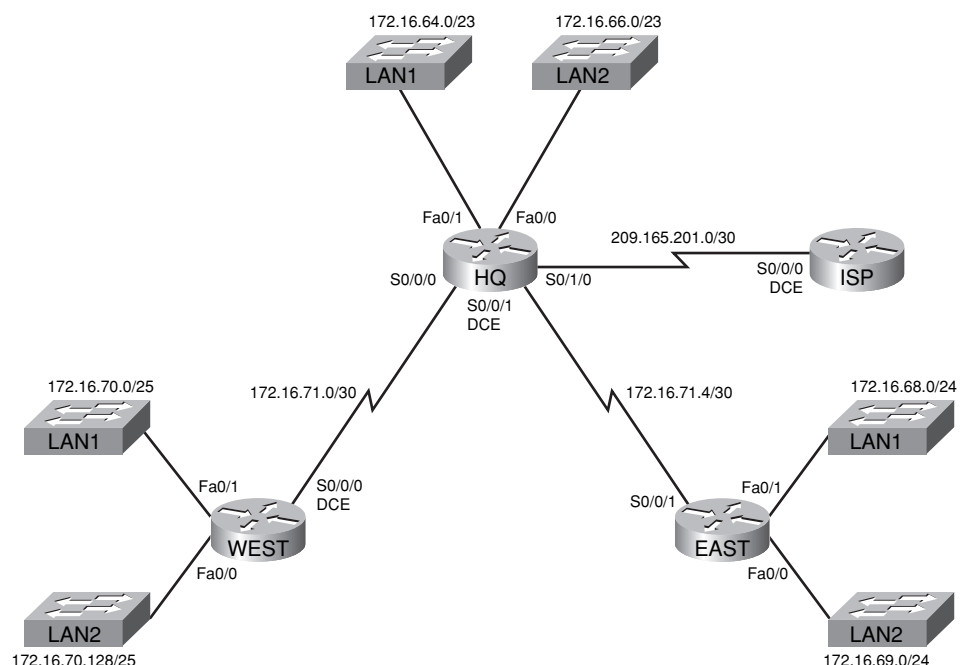


Table 6-12 Network Address Space Assignment for Lab 6-4

Subnet	Network Address
HQ LAN1	172.16.64.0/23
HQ LAN2	172.16.66.0/23
EAST LAN1	172.16.68.0/24
EAST LAN2	172.16.69.0/24
WEST LAN1	172.16.70.0/25
WEST LAN2	172.16.70.128/25
Link from HQ to EAST	172.16.71.4/30
Link from HQ to WEST	172.16.71.0/30
Link from HQ to ISP	209.165.201.0/30

Task 1: Determine the Summary Route for the HQ LANs

Step 1. List the HQ LAN1 and LAN2 in binary format.

LAN1: 10101100.00010000.01000000.00000000

LAN2: 10101100.00010000.01000010.00000000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the two networks? 22
2. What is the subnet mask for the summary route in decimal format? 255.255.252.0

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What are the matching bits for the two networks? 10101100.00010000.010000
2. Add 0s to make up the remainder of the network address in binary form.
10101100.00010000.01000000.00000000
3. What is the network address for the summary route in decimal format? 172.16.64.0

Task 2: Determine the Summary Route for the EAST LANs

Step 1. List the EAST LAN1 and LAN2 in binary format.

LAN1: 10101100.00010000.01000100.00000000

LAN2: 10101100.00010000.01000101.00000000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the two networks? 23
2. What is the subnet mask for the summary route in decimal format? 255.255.254.0

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What are the matching bits for the two networks? 10101100.00010000.0100010

2. Add 0s to make up the remainder of the network address in binary form.
10101100.00010000.01000100.00000000
3. What is the network address for the summary route in decimal format? 172.16.68.0

Task 3: Determine the Summary Route for the WEST LANs

Step 1. List the WEST LAN1 and LAN2 in binary format.

LAN1: 10101100.00010000.01000110.00000000

LAN2: 10101100.00010000.01000110.10000000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the two networks? 24
2. What is the subnet mask for the summary route in decimal format? 255.255.255.0

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What are the matching bits for the two networks? 10101100.00010000.01000110
2. Add 0s to make up the remainder of the network address in binary form.
10101100.00010000.01000110.00000000
3. What is the network address for the summary route in decimal format? 172.16.70.0

Task 4: Determine the Summary Route for the HQ, EAST, and WEST LANs

Step 1. List summary networks for the HQ, EAST, and WEST LANs in binary format.

HQ summary route: 10101100.00010000.01000000.00000000

EAST summary route: 10101100.00010000.01000100.00000000

WEST summary route: 10101100.00010000.01000110.00000000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the three summary routes? 21
2. What is the subnet mask for the summary route in decimal format? 255.255.248.0

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What are the matching bits for the three summary routes?
10101100.00010000.01000000
2. Add 0s to make up the remainder of the network address in binary form.
10101100.00010000.01000000.00000000
3. What is the network address for the summary route in decimal format? 172.16.64.0



Packet Tracer Companion: Basic Route Summarization (6.4.4)

You can now open the file LSG02-Lab644.pka on the CD-ROM that accompanies this book to repeat this activity using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.

Activity 6-5: Challenge Route Summarization (6.4.5)

Upon completion of this activity, you will be able to determine summarized routes that can be used to reduce the size of routing tables.

Scenario

In this activity, you have been given the network shown in Figure 6-20. The subnetting and address assignments have already been completed for the network segments, as shown in Table 6-13. Determine summarized routes that can be used to reduce the number of entries in routing tables.

Figure 6-20 Topology Diagram for Activity 6-5

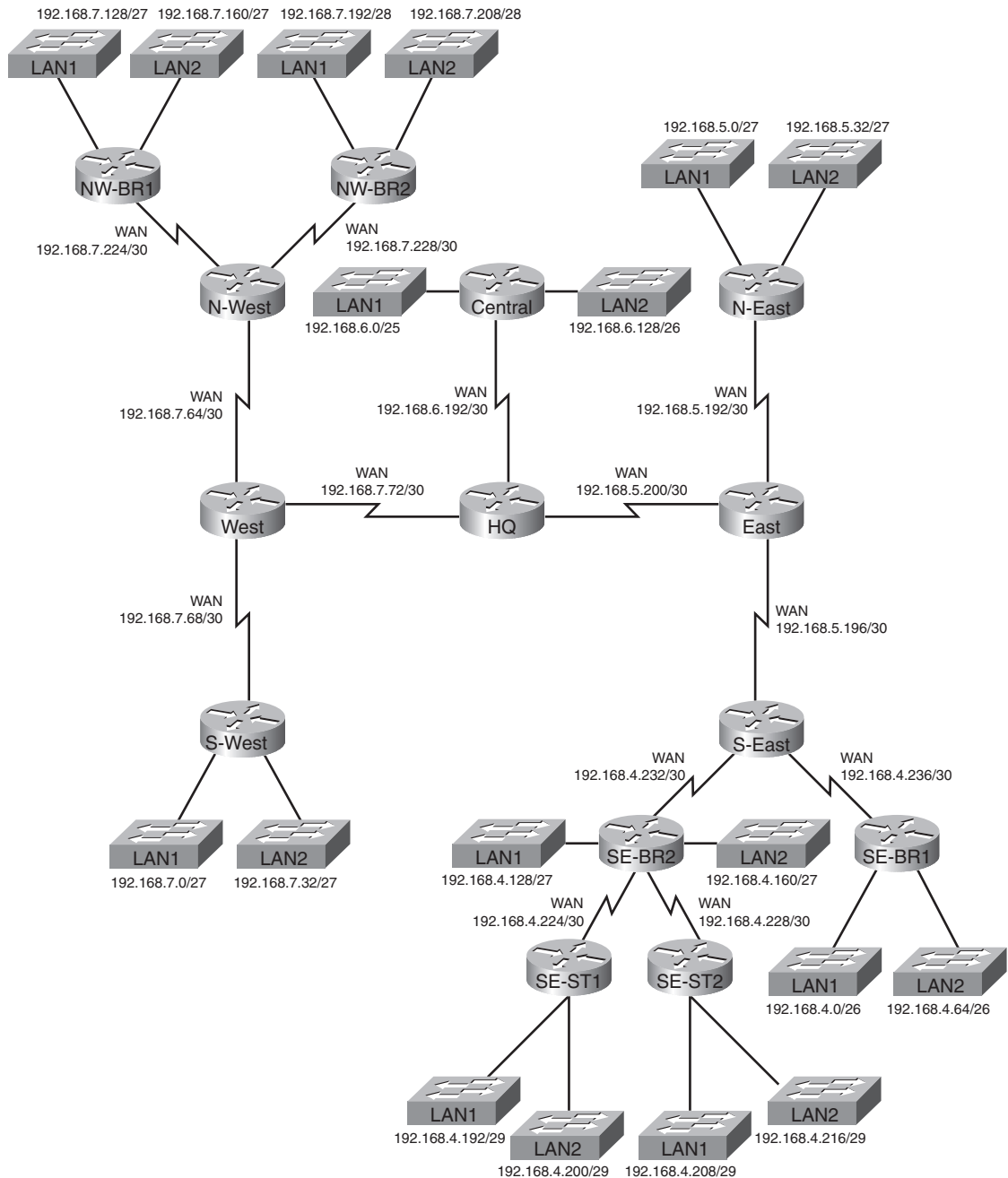


Table 6-13 Network Address Space Assignment

Subnet	Network Address
S-WEST LAN1	192.168.7.0/27
S-WEST LAN2	192.168.7.32/27
Link from WEST to N-WEST	192.168.7.64/30
Link from WEST to S-WEST	192.168.7.68/30
Link from HQ to WEST	192.168.7.72/30
NW-BR1 LAN1	192.168.7.128/27
NW-BR1 LAN2	192.168.7.160/27
NW-BR2 LAN1	192.168.7.192/28
NW-BR2 LAN2	192.168.7.208/28
Link from N-WEST to NW-BR1	192.168.7.224/30
Link from N-WEST to NW-BR2	192.168.7.228/30
CENTRAL LAN1	192.168.6.0/25
CENTRAL LAN2	192.168.6.128/26
Link from HQ to CENTRAL	192.168.6.192/30
N-EAST LAN1	192.168.5.0/27
N-EAST LAN2	192.168.5.32/27
Link from EAST to N-EAST	192.168.5.192/30
Link from EAST to S-EAST	192.168.5.196/30
Link from HQ to EAST	192.168.5.200/30
SE-BR1 LAN1	192.168.4.0/26
SE-BR1 LAN2	192.168.4.64/26
SE-BR2 LAN1	192.168.4.128/27
SE-BR2 LAN2	192.168.4.160/27
SE-ST1 LAN1	192.168.4.192/29
SE-ST1 LAN2	192.168.4.200/29
SE-ST2 LAN1	192.168.4.208/29
SE-ST2 LAN2	192.168.4.216/29
Link from SE-BR2 to SE-ST1	192.168.4.224/30
Link from SE-BR2 to SE-ST2	192.168.4.228/30
Link from S-EAST to SE-BR2	192.168.4.232/30
Link from S-EAST to SE-BR1	192.168.4.236/30

Task 1: Determine the Summary Route for the S-WEST LANs

Step 1. List the S-WEST LAN1 and LAN2 in binary format.

LAN1: 11000000.10101000.00000111.00000000

LAN2: 11000000.10101000.00000111.00100000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the two networks? 26
2. What is the subnet mask for the summary route in decimal format? 255.255.255.192

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What is the summary route in binary form? 11000000.10101000.00000111.00000000
2. What is the network address for the summary route in decimal format? 192.168.7.0

Task 2: Determine the Summary Route for the NW-BR1 LANs

Step 1. List the NW-BR1 LAN1 and LAN2 in binary format.

LAN1: 11000000.10101000.00000111.10000000

LAN2: 11000000.10101000.00000111.10100000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the networks? 26
2. What is the subnet mask for the summary route in decimal format? 255.255.255.192

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What is the summary route in binary form? 11000000.10101000.00000111.10000000
2. What is the network address for the summary route in decimal format?
192.168.7.128

Task 3: Determine the Summary Route for the NW-BR2 LANs

Step 1. List the NW-BR2 LAN1 and LAN2 in binary format.

LAN1: 11000000.10101000.00000111.11000000

LAN2: 11000000.10101000.00000111.11010000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the networks? 27
2. What is the subnet mask for the summary route in decimal format? 255.255.255.224

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What is the summary route in binary form? 11000000.10101000.00000111.11000000
2. What is the network address for the summary route in decimal format?
192.168.7.192

Task 4: Determine the Summary Route for the Northwest Portion of the Network

Use the networks listed here to determine a summary route for the Northwest portion of the network.

Step 1. List the Northwest network segments in binary format.

NW-BR1 summary: 11000000.10101000.00000111.10000000

NW-BR2 summary: 11000000.10101000.00000111.11000000

Link from N-WEST to NW-BR1: 11000000.10101000.00000111.11100000

Link from N-WEST to NW-BR2: 11000000.10101000.00000111.11100100

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the networks? 25
2. What is the subnet mask for the summary route in decimal format? 255.255.255.128

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What is the summary route in binary form? 11000000.10101000.00000111.10000000
2. What is the network address for the summary route in decimal format?
192.168.7.128

Task 5: Determine the Summary Route for the West Portion of the Network

Use the networks in the list that follows to determine a summary route for the West portion of the network.

Step 1. List the West network segments in binary format.

S-WEST summary: 11000000.10101000.00000111.00000000

N-WEST summary: 11000000.10101000.00000111.10000000

Link from WEST to N-WEST: 11000000.10101000.00000111.01000000

Link from WEST to S-WEST: 11000000.10101000.00000111.01000100

Link from HQ to WEST: 11000000.10101000.00000111.01001000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the networks? 24
2. What is the subnet mask for the summary route in decimal format? 255.255.255.0

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What is the summary route in binary form? 11000000.10101000.00000111.00000000
2. What is the network address for the summary route in decimal format? 192.168.7.0

Task 6: Determine the Summary Route for the Central Portion of the Network

Use the networks in the list that follows to determine a summary route for the Central portion of the network.

Step 1. List the Central network segments in binary format.

CENTRAL LAN1: 11000000.10101000.00000110.00000000

CENTRAL LAN2: 11000000.10101000.00000110.10000000

Link from HQ to CENTRAL: 11000000.10101000.00000110.11000000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the networks? 24
2. What is the subnet mask for the summary route in decimal format? 255.255.255.0

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What is the summary route in binary form? 11000000.10101000.00000110.00000000
2. What is the network address for the summary route in decimal format? 192.168.6.0

Task 7: Determine the Summary Route for the N-EAST LANs

Step 1. List the N-EAST LAN1 and LAN2 in binary format.

LAN1: 11000000.10101000.00000101.00000000

LAN2: 11000000.10101000.00000101.00100000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the networks? 26
2. What is the subnet mask for the summary route in decimal format? 255.255.255.192

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What is the summary route in binary form? 11000000.10101000.00000101.00000000
2. What is the network address for the summary route in decimal format? 192.168.5.0

Task 8: Determine the Summary Route for the SE-BR1 LANs

Step 1. List the SE-BR1 LAN1 and LAN2 in binary format.

LAN1: 11000000.10101000.00000100.00000000

LAN2: 11000000.10101000.00000100.01000000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the networks? 25
2. What is the subnet mask for the summary route in decimal format? 255.255.255.128

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What is the summary route in binary form? 11000000.10101000.00000100.00000000
2. What is the network address for the summary route in decimal format? 192.168.4.0

Task 9: Determine the Summary Route for the SE-BR2 LANs

Step 1. List the SE-BR2 LAN1 and LAN2 in binary format.

LAN1: 11000000.10101000.00000100.10000000

LAN2: 11000000.10101000.00000100.10100000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the networks? 26
2. What is the subnet mask for the summary route in decimal format? 255.255.255.192

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What is the summary route in binary form? 11000000.10101000.00000100.10000000
2. What is the network address for the summary route in decimal format?
192.168.4.128

Task 10: Determine the Summary Route for the SE-ST1 LANs

Step 1. List the SE-ST1 LAN1 and LAN2 in binary format.

LAN1: 11000000.10101000.00000100.11000000

LAN2: 11000000.10101000.00000100.11001000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the networks? 28
2. What is the subnet mask for the summary route in decimal format? 255.255.255.240

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What is the summary route in binary form? 11000000.10101000.00000100.11000000
2. What is the network address for the summary route in decimal format?
192.168.4.192

Task 11: Determine the Summary Route for the SE-ST2 LANs

Step 1. List the SE-ST2 LAN1 and LAN2 in binary format.

LAN1: 11000000.10101000.00000100.11010000

LAN2: 11000000.10101000.00000100.11011000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the networks? 28
2. What is the subnet mask for the summary route in decimal format? 255.255.255.240

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What is the summary route in binary form? 11000000.10101000.00000100.11010000
2. What is the network address for the summary route in decimal format?
192.168.4.208

Task 12: Determine the Summary Route for the Southeast Portion of the Network

Use the networks in the list that follows to determine a summary route for the Southeast portion of the network.

Step 1. List the Southeast network segments in binary format.

SE-BR1 summary: 11000000.10101000.00000100.00000000

SE-BR2 summary: 11000000.10101000.00000100.10000000

SE-ST1 summary: 11000000.10101000.00000100.11000000

SE-ST2 summary: 11000000.10101000.00000100.11010000

Link from SE-BR2 to SE-ST1: 11000000.10101000.00000100.11100000

Link from SE-BR2 to SE-ST2: 11000000.10101000.00000100.11100100

Link from S-EAST to SE-BR1: 11000000.10101000.00000100.11101100

Link from S-EAST to SE-BR2: 11000000.10101000.00000100.11101000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the networks? 24
2. What is the subnet mask for the summary route in decimal format? 255.255.255.0

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What is the summary route in binary form? 11000000.10101000.00000100.00000000
2. What is the network address for the summary route in decimal format? 192.168.4.0

Task 13: Determine the Summary Route for the East Portion of the Network

Use the networks in the list that follows to determine a summary route for the East portion of the network.

Step 1. List the East network segments in binary format.

S-EAST summary: 11000000.10101000.00000100.00000000

N-EAST summary: 11000000.10101000.00000101.00000000

Link from EAST to N-EAST: 11000000.10101000.00000101.11000000

Link from EAST to S-EAST: 11000000.10101000.00000101.11000100

Link from HQ to EAST: 11000000.10101000.00000101.11001000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the networks? 23
2. What is the subnet mask for the summary route in decimal format? 255.255.254.0

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What is the summary route in binary form? 11000000.10101000.00000100.00000000
2. What is the network address for the summary route in decimal format? 192.168.4.0

Task 14: Determine the Summary Route for the Entire Network

Use the networks in the list that follows to determine a summary route for the entire network.

Step 1. List the East, West, and Central summary routes in binary format.

EAST summary: 11000000.10101000.00000100.00000000

WEST summary: 11000000.10101000.00000111.00000000

CENTRAL summary: 11000000.10101000.00000110.00000000

Step 2. Count the number of leftmost matching bits to determine the mask for the summary route.

1. How many leftmost matching bits are present in the networks? 22
2. What is the subnet mask for the summary route in decimal format? 255.255.252.0

Step 3. Copy the matching bits and then add all 0s to determine the summarized network address.

1. What is the summary route in binary form? 11000000.10101000.00000100.00000000
2. What is the network address for the summary route in decimal format? 192.168.4.0

Packet Tracer
Companion

Packet Tracer Companion: Challenge Route Summarization (6.4.5)

You can now open the file LSG02-Lab645.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.

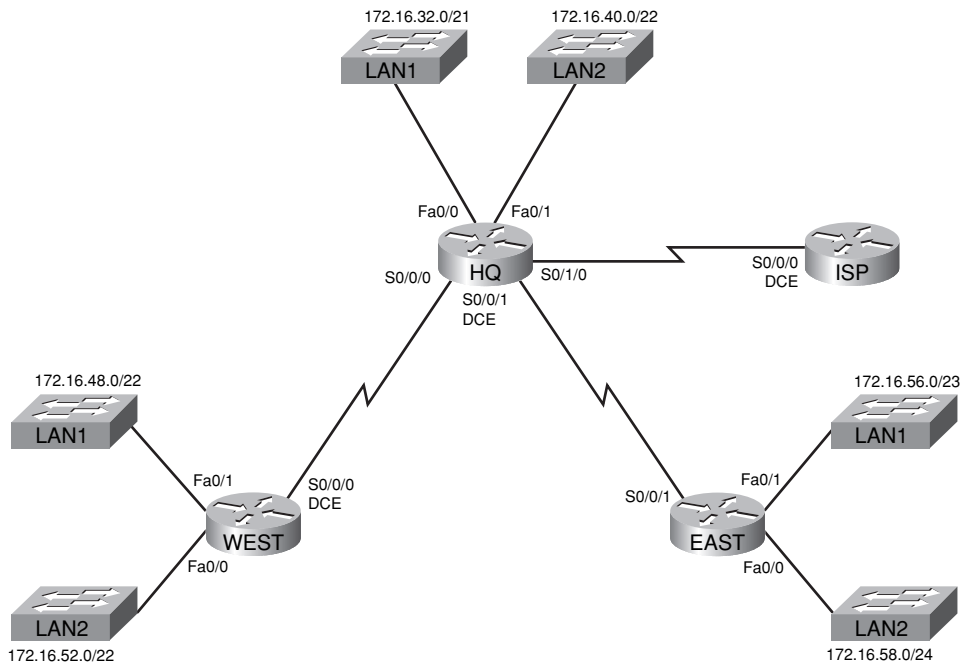
Activity 6-6: Troubleshooting Route Summarization (6.4.6)

Upon completion of this activity, you will be able to

- Discover errors in route summarization
- Propose solutions for summarized routes
- Document the corrected summarized routes

Scenario

In this activity, the LAN IP addressing has already been completed for the network shown in Figure 6-21. VLSM has been used to subnet the address space. The summary static routes shown in Table 6-14 are incorrect. You will need to troubleshoot the summary routes that have been assigned to determine where errors are present and determine the correct summary routes where needed.

Figure 6-21 Topology Diagram for Activity 6-6**Table 6-14 Network Address Space Assignment for Activity 6-6**

Router	Summary Route	Network Address
HQ	WEST LANs	172.16.52.0/21
HQ	EAST LANs	172.16.56.0/23
WEST	HQ LANs	172.16.32.0/19
WEST	EAST LANs	172.16.58.0/23
EAST	HQ LANs	172.16.30.0/20
EAST	WEST LANs	172.16.48.0/21
ISP	HQ, WEST, and EAST LANs	172.16.32.0/18

Task 1: Examine the Summary Routes on the HQ Router

Examine the summary routes on the HQ router and answer the questions that follow.

1. What is the summary route for the WEST LANs? [172.16.52.0/21](#)
2. Is this summary route correct? **no**
3. If the route is not correct, what is the correct summary route for the WEST LANs? [172.16.48.0/21](#)
4. What is the summary route for the EAST LANs? [172.16.56.0/23](#)
5. Is this summary route correct? **no**
6. If the route is not correct, what is the correct summary route for the EAST LANs? [172.16.56.0/22](#)

Task 2: Examine the Summary Routes on the WEST Router

Examine the summary routes on the WEST router and answer the questions that follow.

1. What is the summary route for the HQ LANs? [172.16.32.0/19](#)
2. Is this summary route correct? **no**
3. If the route is not correct, what is the correct summary route for the HQ LANs? [172.16.32.0/20](#)
4. What is the summary route for the EAST LANs? [172.16.58.0/23](#)
5. Is this summary route correct? **no**
6. If the route is not correct, what is the correct summary route for the EAST LANs?
[172.16.56.0/24](#)

Task 3: Examine the Summary Routes on the EAST Router

Examine the summary routes on the EAST router and answer the questions that follow.

1. What is the summary route for the WEST LANs? [172.16.48.0/19](#)
2. Is this summary route correct? **no**
3. If the route is not correct, what is the correct summary route for the WEST LANs?
[172.16.48.0/21](#)
4. What is the summary route for the HQ LANs? [172.16.30.0/20](#)
5. Is this summary route correct? **no**
6. If the route is not correct, what is the correct summary route for the HQ LANs? [172.16.32.0/20](#)

Task 4: Examine the Summary Route on the ISP Router

Examine the summary route on the ISP router and answer the questions that follow.

1. What is the summary route for the HQ, WEST, and EAST LANs? [172.16.32.0/18](#)
2. Is this summary route correct? **no**
3. If the route is not correct, what is the correct summary route for the HQ, WEST, and EAST LANs? [172.16.32.0/19](#)

Task 5: Document the Corrected Summary Routes

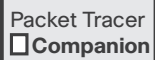
Record the corrected summary routes in Table 6-15.

Table 6-15 Correct Network Address Space Assignment for Lab 6-6

Router	Summary Route	Network Address
HQ	WEST LANs	172.16.48.0/21
HQ	EAST LANs	172.16.56.0/22
WEST	HQ LANs	172.16.32.0/20
WEST	EAST LANs	172.16.56.0/24

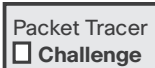
Table 6-15 Correct Network Address Space Assignment for Lab 6-6 *continued*

Router	Summary Route	Network Address
EAST	HQ LANs	172.16.32.0/20
EAST	WEST LANs	172.16.48.0/21
ISP	HQ, WEST, and EAST LANs	172.16.32.0/19



Packet Tracer Companion: Troubleshooting Route Summarization (6.4.6)

You can now open the file LSG02-Lab646.pka on the CD-ROM that accompanies this book to repeat this activity using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.



Packet Tracer Skills Integration Challenge: VLSM and CIDR

Upon completion of this challenge, you will be able to

- Design and document an addressing scheme based on requirements
- Apply a basic configuration to the devices
- Configure static routing between ISP routers
- Configure RIPv2 routing in Region 1 (commands provided) and static routing in Region 2
- Disable RIP updates on appropriate interfaces
- Configure default routes and redistribute through RIP
- Verify full connectivity between all devices in the topology

Open the file LSG02-PTSkills6.pka on the CD-ROM that accompanies this book. You will use the topology in Figure 6-22 and the addressing tables in Tables 6-16 and 6-17 to document your design.

Figure 6-22 Packet Tracer Skills Integration Challenge Topology

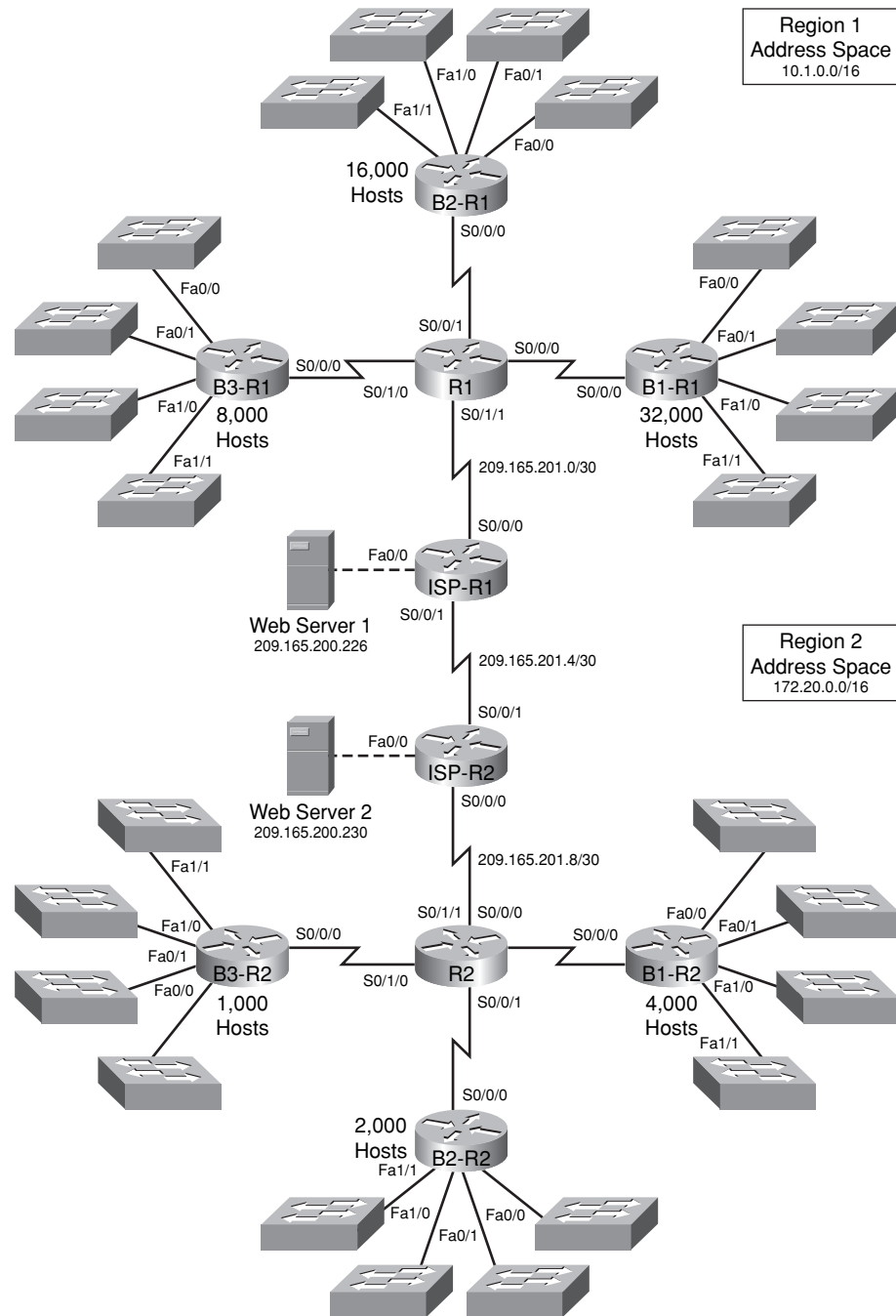


Table 6-16 Addressing Table for R1

Device	Interface	IP Address	Subnet Mask
R1	S0/0/0	10.1.255.241	255.255.255.252
	S0/0/1	10.1.255.245	255.255.255.252
	S0/1/0	10.1.255.249	255.255.255.252
	S0/1/1	209.165.201.2	255.255.255.252
B1-R1	Fa0/0	10.1.0.1	255.255.224.0
	Fa0/1	10.1.32.1	255.255.224.0
	Fa1/0	10.1.64.1	255.255.224.0
	Fa1/1	10.1.96.1	255.255.224.0
	S0/0/0	10.1.255.242	255.255.255.252
B2-R1	Fa0/0	10.1.128.1	255.255.240.0
	Fa0/1	10.1.144.1	255.255.240.0
	Fa1/0	10.1.160.1	255.255.240.0
	Fa1/1	10.1.176.1	255.255.240.0
	S0/0/0	10.1.255.246	255.255.255.252
B3-R1	Fa0/0	10.1.192.1	255.255.248.0
	Fa0/1	10.1.200.1	255.255.248.0
	Fa1/0	10.1.208.1	255.255.248.0
	Fa1/1	10.1.216.1	255.255.248.0
	S0/0/0	10.1.255.250	255.255.255.252
ISP-R1	S0/0/0	209.165.201.1	255.255.255.252
	S0/0/1	209.165.201.5	255.255.255.252
	Fa0/0	209.165.200.225	255.255.255.252
Web Server 1	NIC	209.165.200.226	255.255.255.252

Table 6-17 Addressing Table for R2

Device	Interface	IP Address	Subnet Mask
R2	S0/0/0	172.20.255.241	255.255.255.252
	S0/0/1	172.20.255.245	255.255.255.252
	S0/1/0	172.20.255.249	255.255.255.252
	S0/1/1	209.165.201.10	255.255.255.252

Device	Interface	IP Address	Subnet Mask
B1-R2	Fa0/0	172.20.0.1	255.255.252.0
	Fa0/1	172.20.4.1	255.255.252.0
	Fa1/0	172.20.8.1	255.255.252.0
	Fa1/1	172.20.12.1	255.255.252.0
	S0/0/0	172.20.255.242	255.255.255.252
B2-R2	Fa0/0	172.20.16.1	255.255.254.0
	Fa0/1	172.20.18.1	255.255.254.0
	Fa1/0	172.20.20.1	255.255.254.0
	Fa1/1	172.20.22.1	255.255.254.0
	S0/0/0	172.20.255.246	255.255.255.252
B3-R2	Fa0/0	172.20.24.1	255.255.255.0
	Fa0/1	172.20.25.1	255.255.255.0
	Fa1/0	172.20.26.1	255.255.255.0
	Fa1/1	172.20.27.1	255.255.255.0
	S0/0/0	172.20.255.250	255.255.255.252
ISP-R2	S0/0/0	209.165.201.9	255.255.255.252
	S0/0/1	209.165.201.6	255.255.255.252
	Fa0/0	209.165.200.229	255.255.255.252
Web Server 2	NIC	209.165.200.230	255.255.255.252

Task 1: Design and Document an Addressing Scheme

Step 1. Design an addressing scheme.

Using the topology in Figure 6-22 and the following requirements, design an addressing scheme:

- The WAN links between R1 and R2 and their respective ISP routers are already configured. Also, the links between the ISPs and the web servers are already configured.
- The address space for Region 1 is 10.1.0.0/16. Each branch router (B1-R1, B2-R1, and B3-R1) should be allotted address space based on the following requirements. Starting with the largest requirement, assign address space to each router:
 - B1-R1 needs space for 32,000 hosts: [10.1.0.0/17](#)
 - B2-R1 needs space for 16,000 hosts: [10.1.128.0/18](#)
 - B3-R1 needs space for 8000 hosts: [10.1.192.0/19](#)
- Divide the address space for each branch router into four equal subnets. Record the subnets in the following tables.

Router B1-R1 Interface	Subnet Number	Subnet Address
Fa0/0	0	10.1.0.0/19
Fa0/1	1	10.1.32.0/19
Fa1/0	2	10.1.64.0/19
Fa1/1	3	10.1.96.0/19

Router B2-R1 Interface	Subnet Number	Subnet Address
Fa0/0	0	10.1.128.0/20
Fa0/1	1	10.1.144.0/20
Fa1/0	2	10.1.160/20
Fa1/1	3	10.1.176.0/20

Router B3-R1 Interface	Subnet Number	Subnet Address
Fa0/0	0	10.1.192.0/21
Fa0/1	1	10.1.200.0/21
Fa1/0	2	10.1.208.0/21
Fa1/1	3	10.1.216.0/21

- For the WANs in Region 1, subnet the address space 10.1.255.240/28. Record the subnets in the following table.

Router	Subnet Number	Subnet Address
B1-R1 <—> R1	0	10.1.255.240/30
B2-R1 <—> R1	1	10.1.255.244/30
B3-R1 <—> R1	2	10.1.255.248/30

- The address space for Region 2 is 172.20.0.0/16. Each branch router (B1-R2, B2-R2, and B3-R2) should be allotted address space based on the following requirements. Starting with the largest requirement, assign address space to each router.
 - B1-R2 needs space for 4000 hosts [172.20.0.0/20](#)
 - B2-R2 needs space for 2000 hosts [172.20.16.0/21](#)
 - B3-R2 needs space for 1000 hosts [172.20.24.0/22](#)
- Divide the address space for each branch router into four equal subnets. Record the subnets in the following tables.

Router B1-R2 Interface	Subnet Number	Subnet Address
Fa0/0	0	172.20.0.0/22
Fa0/1	1	172.20.4.0/22
Fa1/0	2	172.20.8.0/22
Fa1/1	3	172.20.12.0/22

Router B2-R2 Interface	Subnet Number	Subnet Address
Fa0/0	0	172.20.16.0/23
Fa0/1	1	172.20.18.0/23
Fa1/0	2	172.20.20.0/23
Fa1/1	3	172.20.22.0/23

Router B3-R2 Interface	Subnet Number	Subnet Address
Fa0/0	0	172.20.24.0/24
Fa0/1	1	172.20.25.0/24
Fa1/0	2	172.20.26.0/24
Fa1/1	3	172.20.27.0/24

- For the WANs in Region 2, subnet the address space 172.20.255.240/28. Record the subnets in the following table.

Router	Subnet Number	Subnet Address
B1-R2 <—> R2	0	172.20.255.240/30
B2-R2 <—> R2	1	172.20.255.244/30
B3-R2 <—> R2	2	172.20.255.248/30

Step 2. Document the addressing scheme.

- (Optional) In Figure 6-22, label each subnet. To save space, use only the last two octets because only these octets change.
- Use Table 6-16 for Region 1 and Table 6-17 for Region 2 to document the IP addresses and subnet masks. Assign the first IP address to the router interface.
- For the WAN links, assign the first IP address to R1 and R2 for links to each router's perspective B1, B2, and B3 routers.

Task 3: Apply a Basic Configuration

Using your documentation, configure the routers with basic configurations including addressing. Use **cisco** as the line passwords and **class** as the secret password. Use **64000** as the clock rate.

Task 4: Configure Static Routing Between ISP Routers

Each ISP router already has two static routes to the other ISP router's directly connected WANs. Implement static routing on each ISP router to ensure connectivity between the two regions.

Task 5: Configure RIPv2 Routing in Region 1 and Static Routing in Region 2

Step 1. Configure RIPv2 routing in Region 1.

Configure all routers in Region 1 (R1, B1-R1, B2-R1, and B3-R1) with RIP as the dynamic routing protocol. To fully appreciate the implementation of your VLSM design in a dynamic routing environment, add the following two commands to your RIP configurations:

```
Router(config-router)# version 2  
Router(config-router)# no auto-summary
```

The **version 2** command enables RIPv2, which includes the sending of subnet mask information in routing updates. By default, RIPv2 summarizes updates at classful boundaries just like RIPv1. The **no auto-summary** command disables auto-summarization. These two commands will be fully explained in the next chapter.

Step 2. Configure static routing in Region 2.

Region 2 is not using a dynamic routing protocol. Configure the routers with the necessary static and default routes to ensure full end-to-end connectivity:

- R2 should have three static routes and one default route.
- B1-R2, B2-R2, and B3-R2 should have one default route each.

Task 6: Disable RIP Updates on Appropriate Interfaces

RIP updates do not need to be sent out all the router interfaces. Disable RIP updates on appropriate interfaces.

Task 7: Configure Default Routes and Redistribute Through RIP

In Region 1, determine which router needs a default route. Then configure that router to redistribute the default route to other routers in the region.

Task 8: Verify Full Connectivity Between All Devices in the Topology

Step 1. Test connectivity.

You should now have end-to-end connectivity. Use **ping** to test connectivity across the network. Each router should be able to ping all other router interfaces and both web servers.

Troubleshoot until pings are successful.

Step 2. Examine the configuration.

Use verification commands to make sure that your configurations are complete.

The Study Guide portion of this chapter uses a combination of matching, fill-in-the-blank, multiple-choice, and open-ended question exercises to test your knowledge and skills of RIPv2 concepts and configuration.

The Labs and Activities portion of this chapter includes all the online curriculum labs to ensure that you have mastered the practical, hands-on skills needed to understand RIPv2 routing.

As you work through this chapter, use Chapter 7 in *Routing Protocols and Concepts, CCNA Exploration Companion Guide* or use the corresponding Chapter 7 in the Exploration Routing Protocols and Concepts online curriculum for assistance.

Study Guide

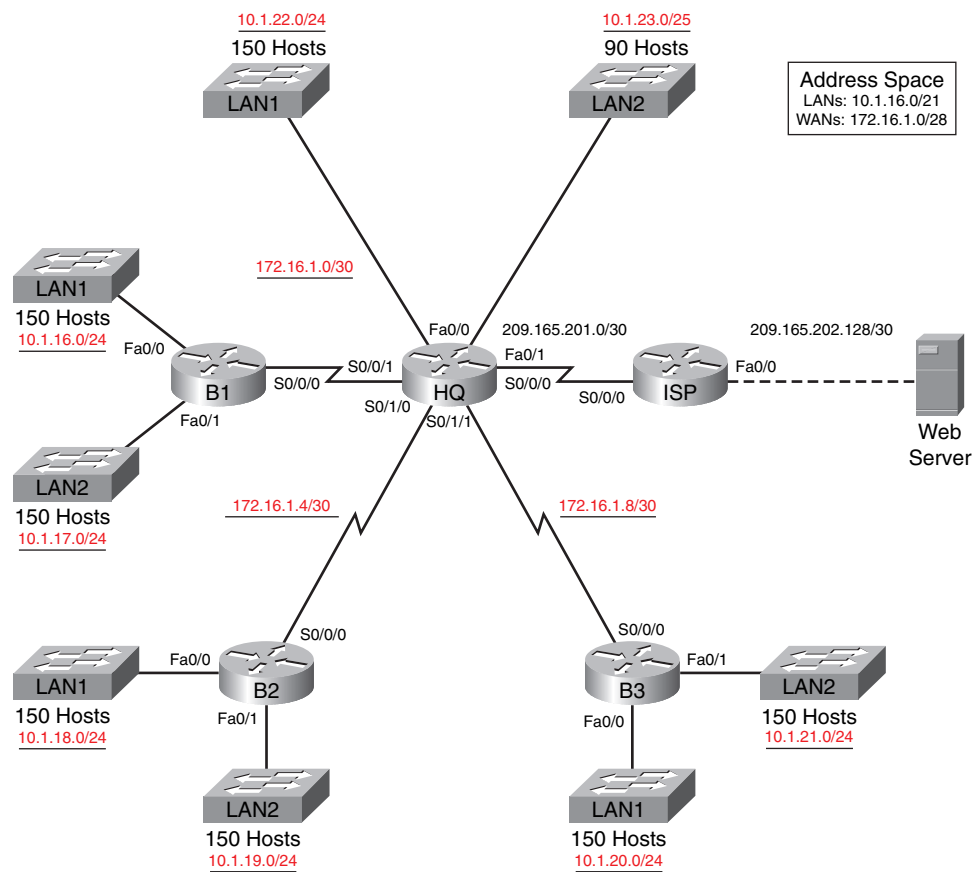
RIPv1 Limitations

The main limitation of RIPv1 is that it is a classful routing protocol. As you know, classful routing protocols do not include the subnet mask with the network address in routing updates. This can cause problems with discontinuous subnets or networks that use variable-length subnet masking (VLSM). In the following sections of the Study Guide, you will design a discontinuous addressing scheme and answer questions related to its implementation.

Documenting the Addressing Scheme

Refer to the topology shown in Figure 7-1. Using the 10.1.16.0/21 address space for LANs and the 172.16.1.0/28 address space for WANs, you will design an appropriate addressing scheme.

Figure 7-1 RIPv2 Study Guide Topology (Answer)



LAN Subnets

To begin your design, you will need to determine the subnets that you will use. To use the available address space most efficiently, start with your largest host requirements and work sequentially to the smallest host requirement. Starting with the LAN subnets, answer the following questions and fill in the subnets in Table 7-1.

10.1.16.0/21 belongs to which classful network?

[10.0.0.0/8](#)

Using the address space 10.1.16.0/21, create subnets for the LANs. All LANs except for the Fa0/1 LAN on HQ need enough address space for 150 hosts. Starting with the Fa0/0 LAN attached to B1, begin assigning subnets. Use Table 7-1 to document your subnets.

Table 7-1 LAN Subnets for 150 Hosts

Subnet No.	Assign To	Subnet Address	Subnet Mast
0	B1 LAN1	10.1.16.0	255.255.255.0
1	B1 LAN2	10.1.17.0	255.255.255.0
2	B2 LAN1	10.1.18.0	255.255.255.0
3	B2 LAN2	10.1.19.0	255.255.255.0
4	B3 LAN1	10.1.20.0	255.255.255.0
5	B3 LAN2	10.1.21.0	255.255.255.0
6	HQ LAN1	10.1.22.0	255.255.255.0

LAN2 attached to HQ only needs 100 hosts. What subnet is still available to create the remaining subnet for LAN2 attached to HQ and the WAN links between HQ and the Branch routers? [10.1.23.0/24](#)

Subnet this remaining subnet to provide enough addresses for LAN2 attached to HQ. Assign subnet 0. What is the subnet? [10.1.23.0/25](#)

Using CIDR notation, label the LANs in the topology shown earlier in Figure 7-1 with the subnet address and subnet mask.

WAN Subnets

For the WAN links, you have been assigned the 172.16.1.0/28 address space. Answer the following questions and fill in the subnets in Table 7-2.

172.16.1.0/28 belongs to which classful network? [172.16.0.0/16](#)

Using the 172.16.1.0/28 address space, create subnets for the WANs between HQ and the Branch routers. Use Table 7-2 to document your WAN subnets.

Table 7-2 WAN Subnets Between HQ and Branch Routers

Subnet No.	Assign To	Subnet Address	Subnet Mast
0	B1/HQ WAN	172.16.1.0	255.255.255.252
1	B2/HQ WAN	172.16.1.8	255.255.255.252
2	B3/HQ WAN	172.16.1.8	255.255.255.252

Using CIDR notation, label the WANs in the topology shown earlier in Figure 7-1 with the subnet address and subnet mask.

Document Interface Addresses

Use Table 7-3 to document the IP addresses for all the interfaces. Use the following guidelines to ensure that your addresses will work with Packet Tracer Exercise 7-1.

1. Assign the first IP address for all LANs to the router interface.
2. Assign HQ the first IP address for all WAN links to Branch routers.

Table 7-3 Addressing Table for RIPv2 Study Guide Topology

Device	Interface	IP Address	Subnet Mask
HQ	Fa0/0	10.1.22.1	255.255.255.0
	Fa0/1	10.1.23.1	255.255.255.128
	S0/0/0	209.165.201.2	255.255.255.252
	S0/0/1	172.16.1.1	255.255.255.252
	S0/1/0	172.16.1.5	255.255.255.252
	S0/1/1	172.16.1.9	255.255.255.252
B1	Fa0/0	10.1.16.1	255.255.255.0
	Fa0/1	10.1.17.1	255.255.255.0
	S0/0/0	172.16.1.2	255.255.255.252
B2	Fa0/0	10.1.18.1	255.255.255.0
	Fa0/1	10.1.19.1	255.255.255.0
	S0/0/0	172.16.1.6	255.255.255.252
B3	Fa0/0	10.1.20.1	255.255.255.0
	Fa0/1	10.1.21.1	255.255.255.0
	S0/0/0	172.16.1.10	255.255.255.252
ISP	Fa0/0	209.165.202.129	255.255.255.252
	S0/0/0	209.165.201.1	255.255.255.252
Web Server	NIC	209.165.202.130	255.255.255.252



Packet Tracer Exercise 7-1

Now you are ready to use Packet Tracer to apply your documented addressing scheme. Open file LSG02-0701.pka on the CD-ROM that accompanies this book to perform this exercise using Packet Tracer.

Task 1: Basic Router Configuration

- Step 1.** ISP is already configured. Use the following guidelines to configure the host name, banner, enable secret password, and lines for HQ, B1, B2, and B3. Packet Tracer will only grade the host name configurations.

- To avoid incorrect grading, make sure that the router names are configured in ALL CAPS.
- Use the following text for the banner: **Authorized Access Only**.
- For the secret password, use **class**.
- For the console and Telnet lines, configure login access with the password **cisco**.

Step 2. Configure the interfaces according to the following guidelines.

- Use the IP address and subnet mask according to the addressing table in the section “Documenting the Addressing Scheme,” earlier in this chapter.
- Configure a description for each interface (Packet Tracer will not grade this configuration).
- Configure clocking signals at 64000 bps where necessary.
- Activate the interfaces.

Your completion percentage should be 64%. If not, review the previous steps to see what part of the task you left incomplete.

Step 3. Save your configurations for H1, B1, B2, and B3.

After completing the basic configurations, be sure to test for connectivity with directly connected neighbors. Save your Packet Tracer file to use again in the next section. Save the file as LSG02-0701-task1.pkt.

Dynamic and Static Routing Configuration

Now that you have an addressing scheme and your routers have a basic configuration, it is time to configure routing. In this exercise, you will continue to use Figure 7-1 and Table 7-1 as your documentation.

RIPv1 Configuration

HQ and the Branch routers use dynamic routing. Starting at the global configuration command prompt, record the commands that each router will need to correctly configure RIPv1 routing.

```
router rip
network 10.0.0.0
network 172.16.0.0
```

Each RIP router also has interfaces that should not participate in RIP updates. Record the commands for each router to stop RIP updates where appropriate. HQ will not be sending RIP updates to ISP.

HQ configurations:

```
HQ(config-router)# passive-interface fa0/0
HQ(config-router)# passive-interface fa0/1
HQ(config-router)# passive-interface s0/0/0
```

B1, B2, and B3 configurations:

```
passive-interface fa0/0
```

```
passive-interface fa0/1
```

Static and Default Routing

HQ and ISP use static and default routing. To ensure that all routers have access to ISP, HQ will also need to propagate a default route. Record the commands necessary to configure static routing on HQ and ISP, including the command HQ needs to propagate the default route. ISP will need two summary static routes back to HQ. For all routes, use the exit interface argument.

HQ configurations:

```
HQ(config)# ip route 0.0.0.0 0.0.0.0 s0/0/0
```

```
HQ(config)# router rip
```

```
HQ(config-router)# default-information originate
```

ISP configurations:

```
ISP(config)# ip route 10.1.16.0 255.255.248.0 s0/0/0
```

```
ISP(config)# ip route 172.16.1.0 255.255.255.240 s0/0/0
```

Packet Tracer
Activity

Packet Tracer Exercise 7-1

Open your LSG02-0701-task1.pka saved version of this Packet Tracer Exercise. According to your answers to the questions in the “Dynamic and Static Routing Configuration” exercise, complete the steps in Task 2.

Task 2: Dynamic and Static Routing Configuration

- Step 1.** Configure RIP routing on HQ and the Branch routers (B1, B2, B3). Include the commands to stop unnecessary RIP updates.
- Step 2.** Configure static and default routing between HQ and ISP. HQ should propagate the default route to the Branch routers.
- Step 3.** View the routing tables for all routers. Notice that some routers have not yet converged on all the networks.

Your completion percentage should be 90%. If not, review the previous steps to see what part of the task you left incomplete.

After completing the routing configurations, save your Packet Tracer file to use again in the next section. Save the file as LSG02-0701-task2.pkt. Keep the file open to use for the next section.

Concept Questions

Based on the current configuration, RIPv1 will have limited connectivity. Answer the questions that follow based on the routing tables for B2, HQ, and ISP shown in Example 7-1.

Example 7-1 Routing Tables for B2, HQ, and ISP

```

B2# show ip route
<code output omitted>

Gateway of last resort is 172.16.1.5 to network 0.0.0.0

    172.16.0.0/30 is subnetted, 3 subnets
R       172.16.1.0 [120/1] via 172.16.1.5, 00:00:21, Serial0/0/0
C       172.16.1.4 is directly connected, Serial0/0/0
R       172.16.1.8 [120/1] via 172.16.1.5, 00:00:21, Serial0/0/0
    10.0.0.0/24 is subnetted, 2 subnets
C       10.1.18.0 is directly connected, FastEthernet0/0
C       10.1.19.0 is directly connected, FastEthernet0/1
R*    0.0.0.0/0 [120/1] via 172.16.1.5, 00:00:21, Serial0/0/0
-----
HQ# show ip route
<code output omitted>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

    172.16.0.0/30 is subnetted, 3 subnets
C       172.16.1.8 is directly connected, Serial0/1/1
C       172.16.1.4 is directly connected, Serial0/1/0
C       172.16.1.0 is directly connected, Serial0/0/1
    209.165.201.0/30 is subnetted, 1 subnets
C       209.165.201.0 is directly connected, Serial0/0/0
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.22.0/24 is directly connected, FastEthernet0/0
C       10.1.23.0/25 is directly connected, FastEthernet0/1
S*    0.0.0.0/0 is directly connected, Serial0/0/0
-----
ISP# show ip route
<code output omitted>

Gateway of last resort is not set

    172.16.0.0/29 is subnetted, 1 subnets
S       172.16.1.0 is directly connected, Serial0/0/0
    209.165.201.0/30 is subnetted, 1 subnets
C       209.165.201.0 is directly connected, Serial0/0/0
    209.165.202.0/30 is subnetted, 1 subnets

```

continues

continued

```

10.0.0.0/21 is subnetted, 1 subnets
C      209.165.202.128 is directly connected, FastEthernet0/0
S      10.1.16.0 is directly connected, Serial0/0/0

```

Note: Your version of Packet Tracer might not correctly display the routing tables. Use the routing tables shown in Example 7-1 to answer the following questions.

1. Does B2 have connectivity to the web server? Why or why not?

Yes, when B2 and HQ both have default routes to ISP. ISP can route back to B2 because the ping request to the web server is sourced from 172.16.1.6, the Serial 0/0/0 interface on B2. ISP has a static route to 172.16.0.0/29, and HQ is directly connected to 172.16.1.4/30.

2. Do the LANs attached to B2 have connectivity to the web server?

No. Although the pings will reach the web server and ISP will route replies back to HQ, HQ does not have routes to the 10.1.18.0/24 or 10.1.19.0/24 LAN.

3. Do the LANs attached to B2 have connectivity to any of the LANs on HQ, B1, or B3?

No. B2 will drop pings for all those LANs because HQ is not advertising subnets of the 10.1.16.0/21 address spaces. HQ is sending B2 a route to 10.0.0.0, which B2 is ignoring because it is connected to that classful network.

4. What is the main reason why connectivity fails for some locations?

RIPv1 is a classful routing protocol that does not support discontinuous addressing schemes.

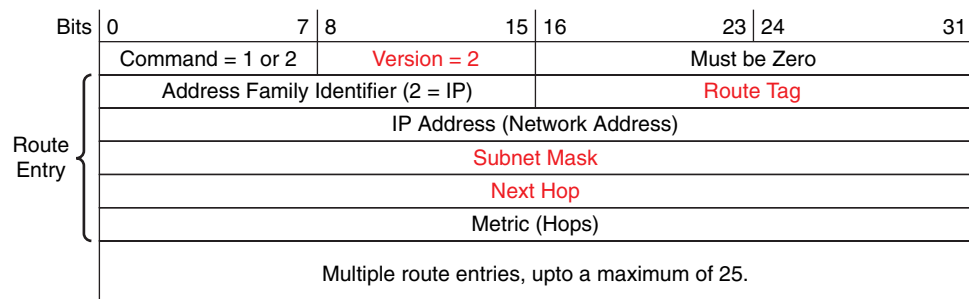
Configuring RIPv2

The configuration of RIPv2 is straightforward. Although the commands will be reviewed, the following sections of the Study Guide will focus on the differences between RIPv1 and RIPv2 rather than the details of implementing RIPv2.

RIPv2 Message Format

RIPv2 is defined in RFC [1723](#). Like version 1, RIPv2 is encapsulated in a [UDP](#) segment using port [520](#) and can carry up to 25 routes. Fill in the missing field names for the RIPv2 message format in Figure 7-2.

Figure 7-2 RIPv2 Message Format (Answer)



RIPv2 Configurations

By default, when a RIP process is configured on a Cisco router, it is running RIPv1. However, even though the router only sends RIPv1 messages, it can process both RIPv1 and RIPv2 messages. A RIPv1 router will just ignore the RIPv2 fields in the route entry. The `show ip protocols` command verifies that a router is configured with RIPv1 but receives messages for both versions.

You will configure RIPv2 on all four routers: HQ, B1, B2, and B3. Starting at the global configuration command prompt, what commands must you enter to configure RIPv2?

```
Router(config)# router rip
```

```
Router(config-router)# version 2
```

The output in Example 7-2 is for the routing table on HQ.

Example 7-2 HQ Routing Table

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

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
R       10.0.0.0/8 [120/1] via 172.16.1.6, 00:00:11, Serial0/1/0
          [120/1] via 172.16.1.2, 00:00:12, Serial0/0/1
          [120/1] via 172.16.1.10, 00:00:08, Serial0/1/1
C       10.1.22.0/24 is directly connected, FastEthernet0/0
C       10.1.23.0/25 is directly connected, FastEthernet0/1
        172.16.0.0/30 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, Serial0/0/1
C       172.16.1.4 is directly connected, Serial0/1/0
C       172.16.1.8 is directly connected, Serial0/1/1
        209.165.201.0/30 is subnetted, 1 subnets
C       209.165.201.0 is directly connected, Serial0/0/0
S*    0.0.0.0/0 is directly connected, Serial0/0/0
```

1. What can you determine from this output?

The Branch routers are automatically summarizing the 10.0.0.0 subnets to the classful network 10.0.0.0/8 and sending this as the route entry to HQ. HQ has now installed these routes in the routing table, showing the variable subnet masks it now has for 10.0.0.0.

2. By default, RIPv2 summarizes at the classful boundary just like RIPv1. Starting at the global configuration command prompt, what commands must you enter on all four routers so that HQ and the Branch routers will advertise the 10.0.0.0 subnets?

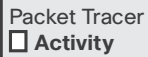
```
Router(config)# router rip
```

```
Router(config-router)# no auto-summary
```

3. How many RIP routes do HQ and the Branch routers each have in the routing table for the 10.0.0.0 network?

All four routers should now have six RIP routes to subnets of the 10.0.0.0 network.

4. Do all LANs now have full connectivity to other LANs and the Internet? Yes



Packet Tracer Exercise 7-1

Open your LSG02-0701-task2.pka saved version of this Packet Tracer Exercise and complete the steps in Task 3 and 4.

Task 3: RIPv2 Configuration

Step 1. Enter the commands on HQ, B1, B2, and B3 to convert to RIP version 2. Make sure that you disable automatic summarization.

Step 2. View the routing tables for all routers. Each router should now have a route to all other destinations or a default route. If one or more of your routes have not yet converged with RIPv2, use the **clear ip route *** command to force the router to request RIP updates from its neighbors.

Your completion percentage should be 100%. You can also check the Connectivity Tests. All tests should now show **Correct** status. If not, review the previous steps to see what part of the task you left incomplete.

Step 3. Save your configurations.

Task 4: Save the Packet Tracer File

Save your Packet Tracer file as LSG02-0701-end.pka.

VLSM and CIDR

Because RIPv2 is a classless routing protocol, subnet masks are included in the routing updates, making RIPv2 more compatible with modern routing environments. Therefore, it is essential that you be very familiar with two skills directly related to classless routing protocols: subnetting a subnet and summarizing routes. See Chapter 6, “VLSM and CIDR,” if you need to review creating VLSM addressing schemes or summarizing routes.

RIPv2 and VLSM

RIPv2 is a classless routing protocol, which means that it carries both the network address and the subnet mask in routing updates. Therefore, RIPv2 does not need to summarize networks to their classful boundaries.

RIPv2 and CIDR

CIDR stands for [classless interdomain routing](#). Defined in RFC [1519](#), CIDR uses the concept of [supernetting](#). A [supernet](#) is a block of contiguous classful networks represented as a single [network](#) address with a [smaller](#) mask than the classful mask.

For example, given the route 172.16.0.0/12, how many classful network addresses are included in the route and what are they?

[16 Class B routes from 172.16.0.0/16 through 172.31.0.0/16](#)

Verifying and Troubleshooting RIPv2

There are several ways to verify and troubleshoot RIPv2. Many of the same commands used for RIPv2 can be used to verify and troubleshoot other routing protocols.

It is always best to begin with the basics:

1. Make sure that all the links (interfaces) are up and operational.
2. Check the cabling.
3. Check to make sure that you have the correct IP address and subnet mask on each interface.
4. Remove any configuration commands that are no longer necessary or have been replaced by other commands.

Verification and Troubleshooting Commands

The [show ip route](#) command is the first command to use to check for network convergence. This command displays the routing table so that you can verify that all routes are listed.

The [show ip interface brief](#) command can be used to verify that directly connected networks are appropriately configured.

If all the interfaces are properly configured, check the routing protocol configuration with the [show ip protocols](#) command. This command verifies many critical items, including RIP version, networks configured, and RIP neighbors.

If these three commands do not provide enough information to solve a RIP routing problem, use the [debug ip rip](#) command to watch RIP updates as they are sent and received. Many times, a route is received but not added to the routing table. List at least one reason why this might happen:

[RIP is operating as a classful protocol because automatic summarization is in effect.](#)

[A static route is configured for the network. Static routes have a lower AD and will be preferred over a RIP route to the same destination.](#)

The [ping](#) command is a quick way to test round-trip connectivity between a source and a destination.

The [show running-config](#) command is the last command you should use to verify and troubleshoot your configuration. Usually, other commands are more efficient and provide more information than a simple listing of the current configuration.

Common RIPv2 Issues

When troubleshooting issues specific to RIPv2, there are several areas to examine. A good place to begin troubleshooting a network that is running RIP is to verify that the **version 2** command is configured on all routers. Another source of problems might be incorrect or missing **network** statements configured with the **network** command. This will cause routing updates to not be sent and received on an interface. If there is a need to send specific subnets of a classful network, make sure that automatic summarization has been disabled with the **no auto-summary** command. Also, make sure that RIP updates have not been inadvertently disabled with the **passive-interface** command.

Authentication

A security concern of any routing protocol is the possibility of accepting invalid routing updates. The source of these invalid routing updates could be an **attacker** maliciously attempting to disrupt the network or trying to capture packets by tricking the router into sending its updates to the wrong destination. Another source of invalid updates could be a **misconfigured** router or even a host computer that is running the routing protocol unbeknownst to its user.

Whatever the reason, it is good practice to authenticate routing information. RIPv2, Enhanced IGRP (EIGRP), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Border Gateway Protocol (BGP) can be configured to encrypt and authenticate routing information. This practice hides the content of the routing information, and routers will only accept routing information from other routers that have been configured with the same password or authentication information.

Labs and Activities

Command Reference

In the Table 7-4, record the command, *including the correct router prompt*, that fits the description.

Table 7-4 Commands for Chapter 7, RIPv2

Command	Description
Router(config)# router rip	Turns on the RIP routing process.
Router(config-router)# version 2	Turns on version 2 of the routing process.
Router(config-router)# network a.b.c.d	Configures the network number of the directly connected classful network that you want to advertise.
Router(config-router)# no auto-summary	RIPv2 automatically summarizes networks at the classful boundary. This command turns off auto-summarization.
Router# debug ip rip	Displays all RIP activity in real time.



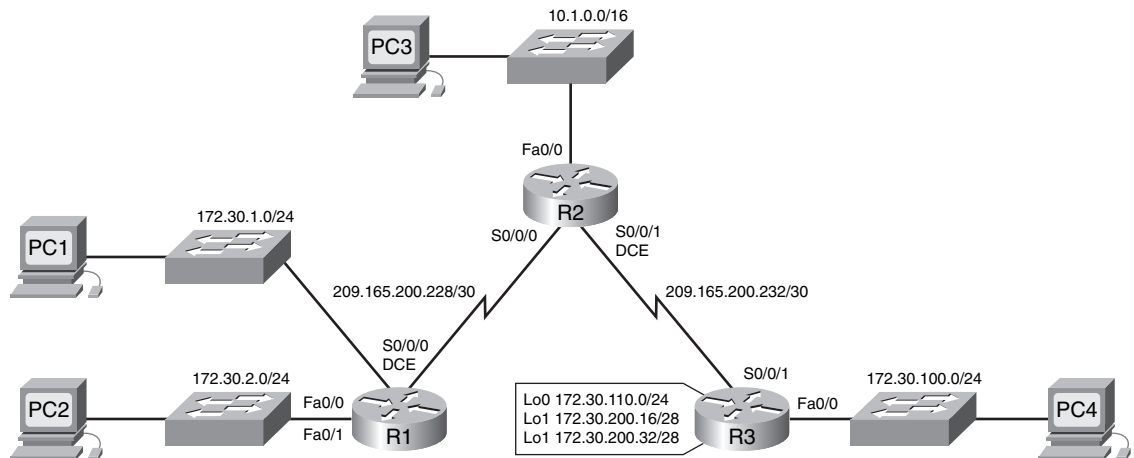
Lab 7-1: RIPv2 Basic Configuration (7.5.1)

Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram in Figure 7-3
- Load provided scripts onto the routers
- Examine the current status of the network
- Configure RIPv2 on all routers
- Examine the automatic summarization of routes
- Examine routing updates with **debug ip rip**
- Disable automatic summarization
- Examine the routing tables
- Verify network connectivity
- Document the RIPv2 configuration

Scenario

The network shown in Figure 7-3 contains a discontinuous network, 172.30.0.0. This network has been subnetted using VLSM. The 172.30.0.0 subnets are physically and logically divided by at least one other classful or major network, in this case the two serial networks 209.165.200.228/30 and 209.165.200.232/30. This can be an issue when the routing protocol used does not include enough information to distinguish the individual subnets. RIPv2 is a classless routing protocol that can be used to provide subnet mask information in the routing updates. This will allow VLSM subnet information to be propagated throughout the network. Table 7-5 documents the interface IP address, subnet masks, and default gateways (where applicable) for all the network devices in the topology diagram in Figure 7-3.

Figure 7-3 Topology Diagram for Lab 7-1**Table 7-5** Addressing Table for Lab 7-1

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.30.1.1	255.255.255.0	—
	Fa0/1	172.30.2.1	255.255.255.0	—
	S0/0/0	209.165.200.230	255.255.255.252	—
R2	Fa0/0	10.1.0.1	255.255.0.0	—
	S0/0/0	209.165.200.229	255.255.255.252	—
	S0/0/1	209.165.200.233	255.255.255.252	—
R3	Fa0/0	172.30.100.1	255.255.255.0	—
	S0/0/1	209.165.200.234	255.255.255.252	—
	Lo0	172.30.110.1	255.255.255.0	—
	Lo1	172.30.200.17	255.255.255.240	—
	Lo2	172.30.200.33	255.255.255.240	—
PC1	NIC	172.30.1.10	255.255.255.0	172.30.1.1
PC2	NIC	172.30.2.10	255.255.255.0	172.30.2.1
PC3	NIC	10.1.0.10	255.255.0.0	10.1.0.1
PC4	NIC	172.30.100.10	255.255.255.0	172.30.100.1

Task 1: Cable, Erase, and Reload the Routers

Step 1. Cable a network.

Cable a network that is similar to the one shown in Figure 7-3.

Step 2. Clear the configuration on each router.

Clear the configuration on each of routers using the **erase startup-config** command and then reload the routers. Answer **no** if asked to save changes.

Task 2: Load Routers with the Supplied Scripts

Step 1. Load the following script onto R1.

```
hostname R1
!
!
!
interface FastEthernet0/0
 ip address 172.30.1.1 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1
 ip address 172.30.2.1 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 ip address 209.165.200.230 255.255.255.252
 clock rate 64000
 no shutdown
!
router rip
 passive-interface FastEthernet0/0
 passive-interface FastEthernet0/1
 network 172.30.0.0
 network 209.165.200.0
!
line con 0
line vty 0 4
 login
!
end
```

Step 2. Load the following script onto R2.

```
hostname R2
!
!
!
interface FastEthernet0/0
 ip address 10.1.0.1 255.255.0.0
 duplex auto
 speed auto
```

```
no shutdown
!
interface Serial0/0/0
 ip address 209.165.200.229 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 209.165.200.233 255.255.255.252
 clock rate 64000
 no shutdown
!
router rip
 passive-interface FastEthernet0/0
 network 10.0.0.0
 network 209.165.200.0
!
line con 0
line vty 0 4
 login
!
end
```

Step 3. Load the following script onto R3.

```
hostname R3
!
!
!
interface FastEthernet0/0
 ip address 172.30.100.1 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/1
 ip address 209.165.200.234 255.255.255.252
 no shutdown
!
interface Loopback0
 ip address 172.30.110.1 255.255.255.0
!
interface Loopback1
 ip address 172.30.200.17 255.255.255.240
!
interface Loopback2
 ip address 172.30.200.33 255.255.255.240
!
router rip
 passive-interface FastEthernet0/0
 network 172.30.0.0
 network 209.165.200.0
```



```

!
line con 0
line vty 0 4
  login
!
end

```

Task 3: Examine the Current Status of the Network

Step 1. Verify that both serial links are up.

The two serial links can quickly be verified using the **show ip interface brief** command on R2:

```

R2# show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.1.0.1	YES	manual	up	up
FastEthernet0/1	unassigned	YES	manual	administratively down	down
Serial0/0/0	209.165.200.229	YES	manual	up	up
Serial0/0/1	209.165.200.233	YES	manual	up	up
Vlan1	unassigned	YES	manual	administratively down	down

Step 2. Check the connectivity from R2 to the hosts on the R1 and R3 LANs.

From the R2 router, how many ICMP messages are successful when pinging PC1?

Could be 40 (2/5) or 60 (3/5)%

From the R2 router, how many ICMP messages are successful when pinging PC4?

Could be 40 (2/5) or 60 (3/5)%

Step 3. Check the connectivity between the PCs.

From the PC1, is it possible to ping PC2? yes

What is the success rate? 100%

From the PC1, is it possible to ping PC3? yes

What is the success rate? 50%

From the PC1, is it possible to ping PC4? no

What is the success rate? 0%

From the PC4, is it possible to ping PC2? no

What is the success rate? 0%

From the PC4, is it possible to ping PC3? yes

What is the success rate? 50%

Step 4. View the routing table on R2.

```

R2# show ip route

```

Output omitted

```

    10.0.0.0/16 is subnetted, 1 subnets
C       10.1.0.0 is directly connected, FastEthernet0/0
R       172.30.0.0/16 [120/1] via 209.165.200.230, 00:00:24, Serial0/0/0
        [120/1] via 209.165.200.234, 00:00:15, Serial0/0/1
    209.165.200.0/30 is subnetted, 2 subnets
C       209.165.200.228 is directly connected, Serial0/0/0
C       209.165.200.232 is directly connected, Serial0/0/1

```

Both the R1 and R3 are advertising routes to the 172.30.0.0/16 network; therefore, there are two entries for this network in the R2 routing table. The R2 routing table shows only the major classful network address of 172.30.0.0. It does not show any of the subnets for this network that are used on the LANs attached to R1 and R3. Because the routing metric is the same for both entries, the router alternates the routes that are used when forwarding packets that are destined for the 172.30.0.0/16 network.

Step 5. Examine the routing table on the R1 router.

```
R1# show ip route
```

Output omitted

```

R       10.0.0.0/8 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0
    172.30.0.0/24 is subnetted, 2 subnets
C       172.30.1.0 is directly connected, FastEthernet0/0
C       172.30.2.0 is directly connected, FastEthernet0/1
    209.165.200.0/30 is subnetted, 2 subnets
C       209.165.200.228 is directly connected, Serial0/0/0
R       209.165.200.232 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0

```

Both R1 and R3 are configured with interfaces on a discontinuous network, 172.30.0.0. The 172.30.0.0 subnets are physically and logically divided by at least one other classful or major network—in this case, the two serial networks 209.165.200.228/30 and 209.165.200.232/30. Classful routing protocols like RIPv1 summarize networks at major network boundaries. Both R1 and R3 will be summarizing 172.30.0.0 subnets to 172.30.0.0. Because the route to 172.30.0.0/16 is directly connected, and because R1 does not have any specific routes for the 172.30.0.0 subnets on R3, packets destined for the R3 LANs will not be forwarded properly.

Step 6. Examine the routing table on the R3 router.

```
R3# show ip route
```

Output omitted

```

R       10.0.0.0/8 [120/1] via 209.165.200.233, 00:00:19, Serial0/0/1
    172.30.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.30.100.0/24 is directly connected, FastEthernet0/0
C       172.30.110.0/24 is directly connected, Loopback0
C       172.30.200.16/28 is directly connected, Loopback1
C       172.30.200.32/28 is directly connected, Loopback2
    209.165.200.0/30 is subnetted, 2 subnets

```

```
R      209.165.200.228 [120/1] via 209.165.200.233, 00:00:19, Serial0/0/1
C      209.165.200.232 is directly connected, Serial0/0/1
```

R3 only shows its own subnets for the 172.30.0.0 network: 172.30.100/24, 172.30.110/24, 172.30.200.16/28, and 172.30.200.32/28. R3 does not have any routes for the 172.30.0.0 subnets on R1.

Step 7. Examine the RIPv1 packets that are being received by R2.

Use the **debug ip rip** command to display RIP routing updates.

```
R2# debug ip rip
```

```
RIP protocol debugging is on
```

```
RIP: received v1 update from 209.165.200.234 on Serial0/0/1
      172.30.0.0 in 1 hops
```

```
RIP: received v1 update from 209.165.200.230 on Serial0/0/0
      172.30.0.0 in 1 hops
```

```
RIP: sending v1 update to 255.255.255.255 via Serial0/0/1
      (209.165.200.233)
```

```
RIP: build update entries
```

```
      network 10.0.0.0 metric 1
```

```
      network 209.165.200.228 metric 1
```

```
RIP: sending v1 update to 255.255.255.255 via Serial0/0/0
      (209.165.200.229)
```

```
RIP: build update entries
```

```
      network 10.0.0.0 metric 1
```

```
      network 209.165.200.232 metric 1
```

R2 is receiving the route 172.30.0.0, with 1 hop, from both R1 and R3. Because these are equal-cost metrics, both routes are added to the R2 routing table. Because RIPv1 is a classful routing protocol, no subnet mask information is sent in the update.

R2 is sending only the routes for the 10.0.0.0 LAN and the two serial connections to R1 and R3. R1 and R3 are not receiving any information about the 172.30.0.0 subnet routes.

When you are finished, turn off the debugging.

```
R2# undebug all
```

Task 4: Configure RIP Version 2

Step 1. Use the **version 2** command to enable RIP version 2 on each of the routers.

```
R2(config)# router rip
```

```
R2(config-router)# version 2
```

```
R1(config)# router rip
```

```
R1(config-router)# version 2
```

```
R3(config)# router rip
```

```
R3(config-router)# version 2
```

RIPv2 messages include the subnet mask in a field in the routing updates. This allows subnets and their masks to be included in the routing updates. However, by default, RIPv2 summarizes networks at major network boundaries, just like RIPv1, except that the subnet mask is included in the update.

Step 2. Verify that RIPv2 is running on the routers.

The **debug ip rip**, **show ip protocols**, and **show run** commands can all be used to confirm that RIPv2 is running. The output of the **show ip protocols** command for R1 is as follows:

```
R1# show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 7 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive 2
    Interface          Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0      2     2
  FastEthernet0/1      2     2
  Serial0/0/0          2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  172.30.0.0
  209.165.200.0
Passive Interface(s):
  FastEthernet0/0
  FastEthernet0/1
Routing Information Sources:
  Gateway             Distance      Last Update
  209.165.200.229     120
Distance: (default is 120)
```

Task 5: Examine the Automatic Summarization of Routes

The LANs connected to R1 and R3 are still composed of discontinuous networks. R2 still shows two equal-cost paths to the 172.30.0.0/16 network in the routing table. R2 still shows only the major classful network address of 172.30.0.0 and does not show any of the subnets for this network.

R2# **show ip route**

Output omitted

```
10.0.0.0/16 is subnetted, 1 subnets
C    10.1.0.0 is directly connected, FastEthernet0/0
R    172.30.0.0/16 [120/1] via 209.165.200.230, 00:00:07, Serial0/0/0
      [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
209.165.200.0/30 is subnetted, 2 subnets
```

```
C      209.165.200.228 is directly connected, Serial0/0/0
C      209.165.200.232 is directly connected, Serial0/0/1
```

R1 still shows only its own subnets for the 172.30.0.0 network. R1 still does not have any routes for the 172.30.0.0 subnets on R3.

```
R1# show ip route
```

Output omitted

```
R      10.0.0.0/8 [120/1] via 209.165.200.229, 00:00:09, Serial0/0/0
      172.30.0.0/24 is subnetted, 2 subnets
C      172.30.1.0 is directly connected, FastEthernet0/0
C      172.30.2.0 is directly connected, FastEthernet0/1
      209.165.200.0/30 is subnetted, 2 subnets
C      209.165.200.228 is directly connected, Serial0/0/0
R      209.165.200.232 [120/1] via 209.165.200.229, 00:00:09, Serial0/0/0
```

R3 still only shows its own subnets for the 172.30.0.0 network. R3 still does not have any routes for the 172.30.0.0 subnets on R1.

```
R3# show ip route
```

Output omitted

```
R      10.0.0.0/8 [120/1] via 209.165.200.233, 00:00:16, Serial0/0/1
      172.30.0.0/16 is variably subnetted, 4 subnets, 2 masks
C      172.30.100.0/24 is directly connected, FastEthernet0/0
C      172.30.110.0/24 is directly connected, Loopback0
C      172.30.200.16/28 is directly connected, Loopback1
C      172.30.200.32/28 is directly connected, Loopback2
      209.165.200.0/30 is subnetted, 2 subnets
R      209.165.200.228 [120/1] via 209.165.200.233, 00:00:16, Serial0/0/1
C      209.165.200.232 is directly connected, Serial0/0/1
```

Use the output of the **debug ip rip** command to answer the following questions.

What entries are included in the RIP updates sent out from R3?

[10.0.0.0/8](#)

[172.30.100.0/24](#)

[172.30.110.0/24](#)

[172.30.200.16/28](#)

[209.165.200.0/24](#)

On R2, what routes are in the RIP updates that are received from R3? [172.30.0.0/16](#)

R3 is not sending any of the 172.30.0.0 subnets—only the summarized route of 172.30.0.0/16, including the subnet mask. This is why R2 and R1 are not seeing the 172.30.0.0 subnets on R3.

Task 6: Disable Automatic Summarization

The **no auto-summary** command is used to turn off automatic summarization in RIPv2. Disable auto summarization on all routers. The routers will no longer summarize routes at major network boundaries.

```
R2(config)# router rip
R2(config-router)# no auto-summary
R1(config)# router rip
R1(config-router)# no auto-summary
R3(config)# router rip
R3(config-router)# no auto-summary
```

The **show ip route** and **ping** commands can be used to verify that automatic summarization is off.

Task 7: Examine the Routing Tables

The LANs connected to R1 and R3 should now be included in all three routing tables.

```
R2# show ip route
```

Output omitted

```

      10.0.0.0/16 is subnetted, 1 subnets
C       10.1.0.0 is directly connected, FastEthernet0/0
      172.30.0.0/16 is variably subnetted, 7 subnets, 3 masks
R       172.30.0.0/16 [120/1] via 209.165.200.230, 00:01:28, Serial0/0/0
          [120/1] via 209.165.200.234, 00:01:56, Serial0/0/1
R       172.30.1.0/24 [120/1] via 209.165.200.230, 00:00:08, Serial0/0/0
R       172.30.2.0/24 [120/1] via 209.165.200.230, 00:00:08, Serial0/0/0
R       172.30.100.0/24 [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
R       172.30.110.0/24 [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
R       172.30.200.16/28 [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
R       172.30.200.32/28 [120/1] via 209.165.200.234, 00:00:08, Serial0/0/1
      209.165.200.0/30 is subnetted, 2 subnets
C       209.165.200.228 is directly connected, Serial0/0/0
C       209.165.200.232 is directly connected, Serial0/0/1R2#
```

```
R1# show ip route
```

Output omitted

```

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R       10.0.0.0/8 [120/1] via 209.165.200.229, 00:02:13, Serial0/0/0
R       10.1.0.0/16 [120/1] via 209.165.200.229, 00:00:21, Serial0/0/0
```

```

172.30.0.0/16 is variably subnetted, 6 subnets, 2 masks
C    172.30.1.0/24 is directly connected, FastEthernet0/0
C    172.30.2.0/24 is directly connected, FastEthernet0/1
R    172.30.100.0/24 [120/2] via 209.165.200.229, 00:00:21, Serial0/0/0
R    172.30.110.0/24 [120/2] via 209.165.200.229, 00:00:21, Serial0/0/0
R    172.30.200.16/28 [120/2] via 209.165.200.229, 00:00:21, Serial0/0/0
R    172.30.200.32/28 [120/2] via 209.165.200.229, 00:00:21, Serial0/0/0
    209.165.200.0/30 is subnetted, 2 subnets
C    209.165.200.228 is directly connected, Serial0/0/0
R    209.165.200.232 [120/1] via 209.165.200.229, 00:00:21, Serial0/0/0

```

R3# **show ip route**

Output omitted

```

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R    10.0.0.0/8 [120/1] via 209.165.200.233, 00:02:28, Serial0/0/1
R    10.1.0.0/16 [120/1] via 209.165.200.233, 00:00:08, Serial0/0/1
172.30.0.0/16 is variably subnetted, 6 subnets, 2 masks
R    172.30.1.0/24 [120/2] via 209.165.200.233, 00:00:08, Serial0/0/1
R    172.30.2.0/24 [120/2] via 209.165.200.233, 00:00:08, Serial0/0/1
C    172.30.100.0/24 is directly connected, FastEthernet0/0
C    172.30.110.0/24 is directly connected, Loopback0
C    172.30.200.16/28 is directly connected, Loopback1
C    172.30.200.32/28 is directly connected, Loopback2
    209.165.200.0/30 is subnetted, 2 subnets
R    209.165.200.228 [120/1] via 209.165.200.233, 00:00:08, Serial0/0/1
C    209.165.200.232 is directly connected, Serial0/0/1

```

Use the output from the **debug ip rip** command to answer the following questions.

What entries are included in the RIP updates sent out from R1 to R2?

[172.30.1.0/24](#)

[172.30.2.0/24](#)

On R2, what routes are in the RIP updates that are received from R1?

[172.30.1.0/24](#)

[172.30.1.0/24](#)

Are the subnet masks now included in the routing updates? [yes](#)

Task 8: Verify Network Connectivity

Step 1. Check connectivity between the R2 router and PCs.

From R2, how many ICMP messages are successful when pinging PC1? 100% (5/5)

From R2, how many ICMP messages are successful when pinging PC4? 100% (5/5)

Step 2. Check the connectivity between the PCs.

From PC1, is it possible to ping PC2? yes

What is the success rate? 100%

From PC1, is it possible to ping PC3? yes

What is the success rate? 100%

From PC1, is it possible to ping PC4? yes

What is the success rate? 100%

From PC4, is it possible to ping PC2? yes

What is the success rate? 100%

From PC4, is it possible to ping PC3? yes

What is the success rate? 100%

Task 9: Documentation

On each router, capture the following command output to a text (.txt) file and save for future reference.

```
show running-config
```

```
show ip route
```

```
show ip interface brief
```

```
show ip protocols
```

If you need to review the procedures for capturing command output, refer to “Lab 1-1: Cabling a Network and Basic Router Configuration.”

Task 10: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.



Packet Tracer Companion: RIPv2 Basic Configuration (7.5.1)

You can now open the file LSG02-Lab751.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.



Lab 7-2: RIPv2 Challenge Configuration (7.5.2)

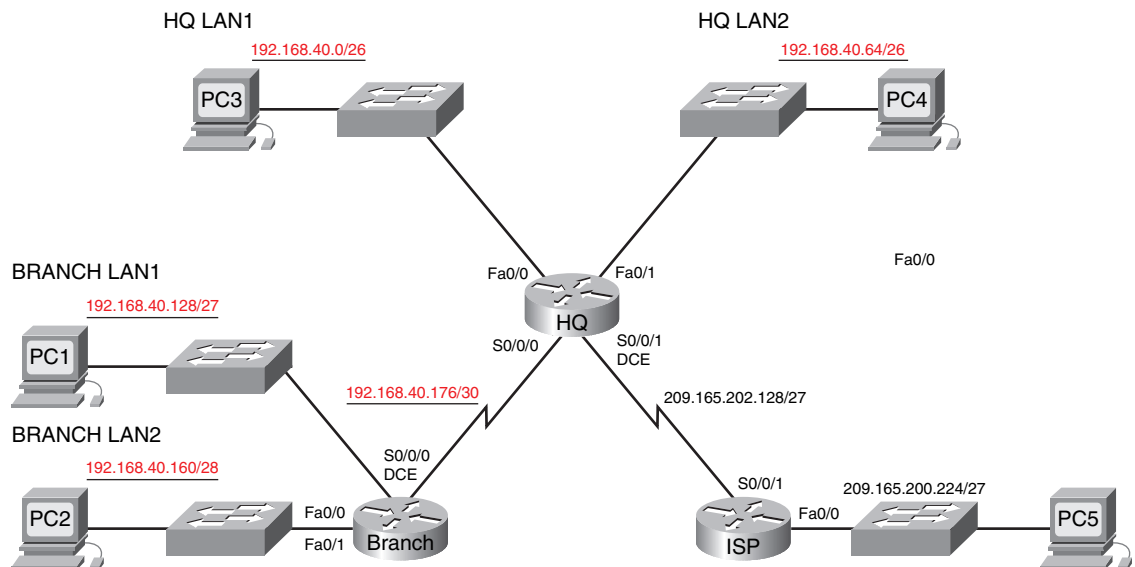
Upon completion of this lab, you will be able to

- Create an efficient VLSM design given the requirements
- Assign appropriate addresses to interfaces and document the addresses
- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Configure routers including RIP version 2
- Configure and propagate a static default route
- Verify RIP version 2 operation
- Test and verify full connectivity
- Reflect on and document the network implementation

Scenario

In this lab activity, you will be given a network address that must be subnetted using VLSM to complete the addressing of the network shown in the topology diagram in Figure 7-4. A combination of RIP version 2 and static routing will be required so that hosts on networks that are not directly connected will be able to communicate with each other.

Figure 7-4 Topology Diagram for Lab 7-2 (Answer)



Task 1: Subnet the Address Space

Step 1. Examine the network requirements.

The addressing for the network has the following requirements:

- The ISP LAN will use the 209.165.200.224/27 network.
- The link between ISP and HQ will use the 209.165.202.128/27 network.

- The 192.168.40.0/24 network must be subnetted using VLSM for all other addresses in the network:
 - The HQ LAN1 will require 50 host IP addresses.
 - The HQ LAN2 will require 50 host IP addresses.
 - The BRANCH LAN1 will require 30 host IP addresses.
 - The BRANCH LAN2 will require 12 host IP addresses.
 - The link between HQ and BRANCH will require an IP address at each end.

Step 2. Consider the following questions when creating your network design.

How many subnets need to be created from the 192.168.40.0/24 network? [5](#)

How many total IP addresses are required from the 192.168.40.0/24 network? [144, or 148 if you count the Fast Ethernet interfaces](#)

What subnet mask will be used for the HQ LAN1 subnet? [255.255.255.192 or /26](#)

What is the maximum number of host addresses that could be used on this subnet? [62](#)

What subnet mask will be used for the HQ LAN2 subnet? [255.255.255.192 or /26](#)

What is the maximum number of host addresses that could be used on this subnet? [62](#)

What subnet mask will be used for the BRANCH LAN1 subnet? [255.255.255.224 or /27](#)

What is the maximum number of host addresses that could be used on this subnet? [30](#)

What subnet mask will be used for the BRANCH LAN2 subnet? [255.255.255.240 or /28](#)

What is the maximum number of host addresses that could be used on this subnet? [14](#)

What subnet mask will be used for the link between the HQ and BRANCH routers? [255.255.255.252 or /30](#)

What is the maximum number of host addresses that could be used on this subnet? [2](#)

Step 3. Assign subnetwork addresses to the topology diagram in Figure 7-4.

- Assign subnet 0 of the 192.168.40.0 network to the HQ LAN1 subnet. What is the network address of this subnet? [192.168.40.0/26](#)
- Assign subnet 1 of the 192.168.40.0 network to the HQ LAN2 subnet. What is the network address of this subnet? [192.168.40.64/26](#)
- Assign subnet 2 of the 192.168.40.0 network to the BRANCH LAN1 subnet. What is the network address of this subnet? [192.168.40.128 /27](#)
- Assign subnet 3 of the 192.168.40.0 network to the BRANCH LAN2 subnet. What is the network address of this subnet? [192.168.40.160 /28](#)
- Assign subnet 4 of the 192.168.40.0 network to the link between the HQ and BRANCH routers. What is the network address of this subnet? [192.168.40.176 /30](#)

Task 2: Determine Interface Addresses

Step 1. Assign appropriate addresses to the device interfaces.

- Assign the first valid host address in the 209.165.200.224/27 network to the LAN interface on the ISP router.

- Assign the last valid host address in the 209.165.200.224/27 network to PC5.
- Assign the first valid host address in the 209.165.202.128/27 network to the WAN interface of ISP.
- Assign the last valid host address in the 209.165.202.128/27 network to the Serial 0/0/1 interface of HQ.
- Assign the first valid host address in the HQ LAN1 network to the LAN1 interface of HQ.
- Assign the last valid host address in the HQ LAN1 network to PC 3.
- Assign the first valid host address in the HQ LAN2 network to the LAN2 interface of HQ.
- Assign the last valid host address in the HQ LAN2 network to PC 4.
- Assign the first valid host address in the HQ/BRANCH WAN link to the Serial 0/0/0 interface of HQ.
- Assign the last valid host address in the HQ/BRANCH WAN link to the Serial 0/0/0 interface of BRANCH.
- Assign the first valid host address in the BRANCH LAN1 network to the LAN1 interface of HQ.
- Assign the last valid host address in the BRANCH LAN1 network to PC 1.
- Assign the first valid host address in the BRANCH LAN2 network to the LAN2 interface of HQ.
- Assign the last valid host address in the BRANCH LAN2 network to PC 2.

Step 2. Document the addresses to be used in Table 7-6.

Table 7-6 Addressing Table for Lab 7-2

Device	Interface	IP Address	Subnet Mask	Default Gateway
BRANCH	Fa0/0	192.168.40.129	255.255.255.224	—
	Fa0/1	192.168.40.161	255.255.255.240	—
	S0/0/0	192.168.40.178	255.255.255.252	—
HQ	Fa0/0	192.168.40.1	255.255.255.192	—
	Fa0/1	192.168.40.65	255.255.255.192	—
	S0/0/0	192.168.40.177	255.255.255.252	—
	S0/0/1	209.165.202.158	255.255.255.224	—
ISP	Fa0/0	209.165.200.225	255.255.255.224	—
	S0/0/1	209.165.202.129	255.255.255.224	—
PC1	NIC	192.168.40.158	255.255.255.224	192.168.40.129
PC2	NIC	192.168.40.174	255.255.255.240	192.168.40.161
PC3	NIC	192.168.40.62	255.255.255.192	192.168.40.1
PC4	NIC	192.168.40.126	255.255.255.192	192.168.40.65
PC5	NIC	209.165.200.254	255.255.255.224	209.165.200.225

Task 3: Prepare the Network

Step 1. Cable a network that is similar to the topology diagram in Figure 7-4.

You can use any current router in your lab as long as it has the required interfaces as shown in the topology.

Note: If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions will appear different.

Step 2. Clear any existing configurations on the routers.

Task 4: Perform Basic Router Configurations

Perform basic configuration of the BRANCH, HQ, and ISP routers according to the following guidelines:

1. Configure the router host name.
2. Disable Domain Name System (DNS) lookup.
3. Configure an EXEC mode password.
4. Configure a message-of-the-day banner.
5. Configure a password for console connections.
6. Configure a password for VTY connections.
7. Synchronize unsolicited messages and debug output with solicited output and prompts for the console and virtual terminal lines.
8. Configure an EXEC timeout of 15 minutes.

Task 5: Configure and Activate Serial and Ethernet Addresses

Step 1. Configure the BRANCH, HQ, and ISP routers.

Configure the interfaces on BRANCH, HQ, and ISP with the IP addresses from the addressing table provided under the topology diagram.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 2. Configure the Ethernet interfaces of PC1, PC2, PC3, PC4, and PC5.

Configure these Ethernet interfaces with the IP addresses from the completed Table 7-6.

Task 6: Verify Connectivity to the Next-Hop Device

You should *not* have connectivity between end devices yet. However, you can test connectivity between two routers and between an end device and its default gateway.

Step 1. Verify BRANCH connectivity by ensuring that BRANCH can ping across the WAN link to HQ and that HQ can ping across the WAN link it shares with ISP.

Step 2. Verify that PC1, PC2, PC3, PC4, and PC5 can ping their respective default gateways.

Task 7: Configure RIPv2 Routing on the BRANCH Router

Consider the networks that need to be included in the RIP updates that are sent out by BRANCH.

What networks are present in the BRANCH routing table? List the networks with slash notation.

[192.168.40.128/27](#)

[192.168.40.160/28](#)

[192.168.40.176/30](#)

What commands are required to enable RIP version 2 and include the connected networks in the routing updates?

[router rip](#)

[version 2](#)

[network 192.168.40.0](#)

Are there any router interfaces that do not need to have RIP updates sent out? [yes](#)

What commands are used to disable RIP updates on these interfaces?

[passive-interface FastEthernet0/0](#)

[passive-interface FastEthernet0/1](#)

Task 8: Configure RIPv2 and Static Routing on HQ

Consider the type of static routing that is needed on HQ.

What networks are present in the HQ routing table? List the networks with slash notation.

[192.168.40.0/26](#)

[209.165.200.0/27](#)

A static default route will need to be configured to send all packets with destination addresses that are not in the routing table to ISP. What command is needed to accomplish this? Use the appropriate exit interface on HQ in the command.

[ip route 0.0.0.0 0.0.0.0 Serial0/0/1](#)

What commands are required to enable RIP version 2 and include the LAN1 and LAN2 networks as well as the link between HQ and BRANCH in the routing updates?

[router rip](#)

[version 2](#)

[network 192.168.40.0](#)

Are there any router interfaces that do not need to have RIP updates sent out? [yes](#)

What commands are used to disable RIP updates on these interfaces?

[passive-interface FastEthernet0/0](#)

[passive-interface FastEthernet0/1](#)

[passive-interface Serial0/0/1](#)

HQ needs to send the default route information to BRANCH in the RIP updates. What command is used to configure this?

[default-information originate](#)

Task 9: Configure Static Routing on the ISP Router

Note: In a real-world implementation of this topology, you would not be configuring the ISP router. However, your service provider is an active partner in solving your connectivity needs. Service provider administrators are human, too, and make mistakes. Therefore, it is important that you understand the types of errors an ISP could make that would cause your networks to lose connectivity.

Static routes will need to be configured on ISP for all traffic that is destined for the RFC 1918 addresses that are used on the BRANCH LANs, HQ LANs, and the link between the BRANCH and HQ routers.

What are the commands that will need to be configured on the ISP router to accomplish this?

[ip route 192.168.40.0 255.255.255.0 Serial10/0/1](#)

Task 10: Verify the Configurations

Answer the following questions to verify that the network is operating as expected.

From PC1, is it possible to ping PC3? [yes](#)

From PC1, is it possible to ping the PC5? [yes](#)

From PC4, is it possible to ping the PC5? [yes](#)

The answer to these questions should be **yes**. If any of the pings failed, check your physical connections and configurations. Refer to your basic troubleshooting techniques used in the Chapter 1 labs.

What routes are present in the routing table of the BRANCH router?

[192.168.40.0/26](#)

[192.168.40.64/26](#)

[192.168.40.128/27](#)

[192.168.40.160/28](#)

[192.168.40.176/30](#)

[0.0.0.0/0](#)

What is the gateway of last resort in the routing table of BRANCH?

[192.168.40.177 to network 0.0.0.0](#)

What routes are present in the routing table of the HQ router?

[192.168.40.0/26](#)

[192.168.40.64/26](#)

[192.168.40.128/27](#)

[192.168.40.160/28](#)

[192.168.40.176/30](#)

[209.165.202.0/27](#)

[0.0.0.0/0](#)

What networks are present in the routing table of ISP?

[192.168.40.0/24](#)

[209.165.200.0/27](#)

[209.165.202.0/27](#)

What networks are present in the RIP updates sent from HQ?

[0.0.0.0/0](#)

[192.168.40.0/26](#)

[192.168.40.64/26](#)

What networks are present in the RIP updates sent from BRANCH?

[192.168.40.128/27](#)

[192.168.40.160/28](#)

Task 11: Reflection

Why is it necessary to use RIPv2 instead of RIPv1 with this network design?

RIPv1 is a classful routing protocol. Classful routing protocols do not include subnet masks. Classful routing protocols summarize networks at major network boundaries. RIPv1 does not support VLSM.

Task 12: Document the Router Configurations

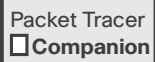
On each router, capture the following command output to a text (.txt) file and save for future reference.

- Running configuration
- Routing table
- Interface summarization

If you need to review the procedures for capturing command output, refer to “Lab 1-1: Cabling a Network and Basic Router Configuration.”

Task 13: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.



Packet Tracer Companion: RIPv2 Challenge Configuration (7.5.2)

You can now open the file LSG02-Lab752.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment.



Lab 7-3: RIPv2 Troubleshooting (7.5.3)

Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram in Figure 7-5
- Erase the startup configuration and reload a router to the default state
- Load the routers with supplied scripts
- Gather information about the nonconverged portion of the network along with any other errors
- Analyze information to determine why convergence is not complete
- Propose solutions to network errors
- Implement solutions to network errors
- Document the corrected network

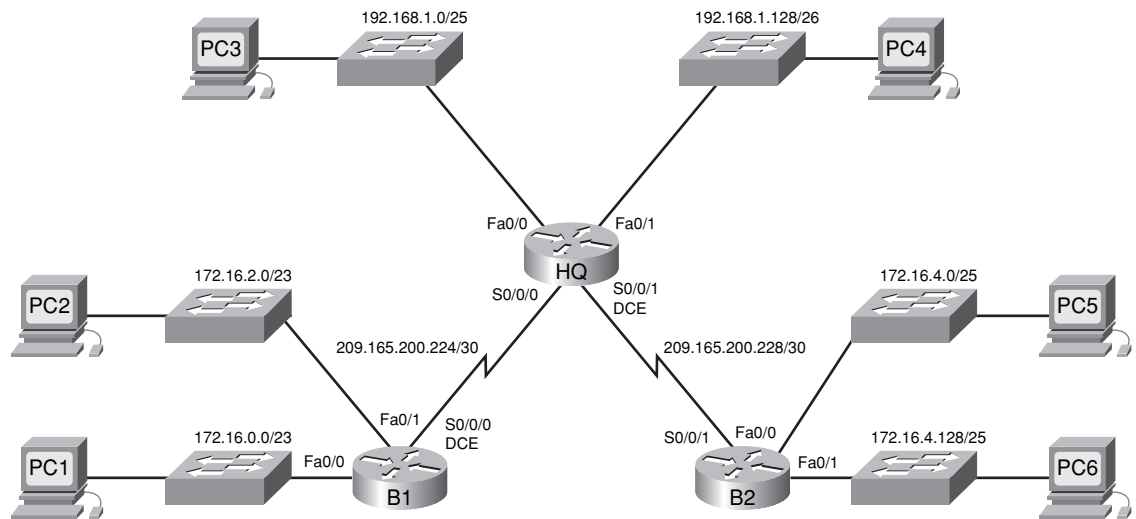
Scenario

In this lab, you will begin by loading configuration scripts on each of the routers. These scripts contain errors that will prevent end-to-end communication across the network. You will need to troubleshoot each router to determine the configuration errors, and then use the appropriate commands to correct the configurations. When you have corrected all the configuration errors, all the hosts on the network should be able to communicate with each other.

The network should also have met the following requirements:

- RIPv2 routing is configured on the BRANCH1 router.
- RIPv2 routing is configured on the BRANCH2 router.
- RIPv2 routing is configured on the HQ router.
- RIP updates must be disabled on the BRANCH1, BRANCH2, and HQ LAN interfaces.

Table 7-7 documents the interface IP address, subnet masks, and default gateways (where applicable) for all the network devices in the topology diagram in Figure 7-5.

Figure 7-5 Topology Diagram for Lab 7-3**Table 7-7 Addressing Table for Lab 7-3**

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	Fa0/0	192.168.1.1	255.255.255.128	—
	Fa0/1	192.168.1.129	255.255.255.192	—
	S0/0/0	209.165.200.225	255.255.255.252	—
	S0/0/1	209.165.200.229	255.255.255.252	—
BRANCH1	Fa0/0	172.16.0.1	255.255.254.0	—
	Fa0/1	172.16.2.1	255.255.254.0	—
	S0/0/0	209.165.200.226	255.255.255.252	—
BRANCH2	Fa0/0	172.16.4.1	255.255.255.128	—
	Fa0/1	172.16.4.129	255.255.255.128	—
	S0/0/1	209.165.200.230	255.255.255.252	—
PC1	NIC	172.16.0.10	255.255.254.0	172.16.0.1
PC2	NIC	172.16.2.10	255.255.254.0	172.16.2.1
PC3	NIC	192.168.1.10	255.255.255.128	192.168.1.1
PC4	NIC	192.168.1.138	255.255.255.192	192.168.1.129
PC5	NIC	172.16.4.10	255.255.255.128	172.16.4.1
PC6	NIC	172.16.4.138	255.255.255.128	172.16.4.129

Task 1: Cable, Erase, and Reload the Routers

- Step 1.** Cable a network that is similar to the one in the topology diagram shown in Figure 7-5.
- Step 2.** Clear the configuration on each router using the **erase startup-config** command and then reload the routers. Answer **no** if asked to save changes.

Task 2: Load Routers with the Supplied Scripts

- Step 1.** Load the following script onto the BRANCH1 router.

```
hostname BRANCH1
!
!
!
interface FastEthernet0/0
 ip address 172.16.0.1 255.255.254.0
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1
 ip address 172.16.2.1 255.255.254.0
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 ip address 209.165.200.226 255.255.255.252
 clock rate 64000
 no shutdown
!
router rip
```

!The version 2 command is missing.

```
passive-interface FastEthernet0/0
passive-interface FastEthernet0/1
network 172.16.0.0
network 209.165.200.0
```

The no auto-summary command is missing.

```
!
ip classless
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end
```

Corrected script:

```

hostname BRANCH1
!
!
!
interface FastEthernet0/0
 ip address 172.16.0.1 255.255.254.0
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1
 ip address 172.16.2.1 255.255.254.0
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 ip address 209.165.200.226 255.255.255.252
 clock rate 64000
 no shutdown
!
router rip
 version 2
 passive-interface FastEthernet0/0
 passive-interface FastEthernet0/1
 network 172.16.0.0
 network 209.165.200.0
 no auto-summary
!
ip classless
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end

```

The errors in the student scripts are as follows:

- The **version 2** command is missing from the RIP configuration.
- The **no auto-summary** command is missing from the RIP configuration.

Step 2. Load the following script onto the BRANCH2 router.

```

hostname BRANCH2
!
!

```

```
!  
interface FastEthernet0/0  
  ip address 172.16.4.129 255.255.255.128  
!The IP address should be 172.16.4.1.  
  duplex auto  
  speed auto  
  no shutdown  
!  
interface FastEthernet0/1  
  ip address 172.16.4.1 255.255.255.128  
!The IP address should be 172.16.4.129.  
  duplex auto  
  speed auto  
  no shutdown  
!  
interface Serial0/0/1  
  ip address 209.165.200.230 255.255.255.252  
  no shutdown  
!  
router rip  
  version 2  
  passive-interface FastEthernet0/0  
  passive-interface FastEthernet0/1  
!The network 172.16.0.0 command is missing.  
  network 209.165.200.0  
!The no auto-summary command is missing.  
!  
ip classless  
!  
!  
!  
!  
line con 0  
line vty 0 4  
  login  
!  
!  
end
```

Corrected script:

```
hostname BRANCH2  
!  
!  
!  
interface FastEthernet0/0  
  ip address 172.16.4.1 255.255.255.128  
  duplex auto  
  speed auto
```

```

    no shutdown
    !
interface FastEthernet0/1
    ip address 172.16.4.129 255.255.255.128
    duplex auto
    speed auto
    no shutdown
    !
interface Serial0/0/1
    ip address 209.165.200.230 255.255.255.252
    no shutdown
    !
router rip
    version 2
    passive-interface FastEthernet0/0
    passive-interface FastEthernet0/1
    network 172.16.0.0
    network 209.165.200.0
    no auto-summary
    !
ip classless
    !
    !
    !
    !
line con 0
line vty 0 4
    login
    !
    !
end

```

The errors in the student scripts are as follows:

- The IP addresses for Fa0/0 and Fa0/1 are reversed:
 - The Fa0/0 interface should be configured with the **ip address 172.16.4.1 255.255.255.128** command.
 - The Fa0/1 interface should be configured with the **ip address 172.16.4.129 255.255.255.128** command.
- The **network 172.16.0.0** command is missing from the RIP configuration.
- The **no auto-summary** command is missing from the RIP configuration.

Step 3. Load the following script onto the HQ router.

```

hostname HQ
    !
    !
    !
interface FastEthernet0/0
    ip address 192.168.1.1 255.255.255.128
    duplex auto

```

```
speed auto
no shutdown
!
interface FastEthernet0/1
ip address 192.168.1.129 255.255.255.192
duplex auto
speed auto
no shutdown
!
interface Serial0/0/0
ip address 209.165.200.225 255.255.255.252
no shutdown
!
interface Serial0/0/1
ip address 209.165.200.229 255.255.255.252
!The clock rate 64000 command is missing.
no shutdown
!
router rip
version 2
passive-interface FastEthernet0/0
passive-interface FastEthernet0/1
network 192.168.1.0
network 209.165.200.0
!The no auto-summary command is missing.
!
ip classless
!
!
!
!
line con 0
line vty 0 4
login
!
!
end
```

Corrected script:

```
hostname HQ
!
!
!
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.128
duplex auto
speed auto
no shutdown
!
```

```

interface FastEthernet0/1
 ip address 192.168.1.129 255.255.255.192
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 ip address 209.165.200.225 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 209.165.200.229 255.255.255.252
 clock rate 64000
 no shutdown
!
router rip
 version 2
 passive-interface FastEthernet0/0
 passive-interface FastEthernet0/1
 network 192.168.1.0
 network 209.165.200.0
 no auto-summary
!
ip classless
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end

```

The errors in the student scripts are as follows:

- The **clock rate 64000** command is missing from the Serial 0/0/1 interface.
- The **no auto-summary** command is missing from the RIP configuration.

Task 3: Troubleshoot the BRANCH1 Router

Step 1. Begin troubleshooting at the host connected to BRANCH1.

From the host PC1, is it possible to ping PC2? yes

From the host PC1, is it possible to ping PC3? no

From the host PC1, is it possible to ping PC5? no

From the host PC1, is it possible to ping the default gateway? yes

Step 2. Examine BRANCH1 to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the configuration of the interfaces? **no**

If there are any problems with the configuration of the interfaces, record any commands that will be necessary to correct the configuration errors.

Step 3. If you have recorded any commands in the previous step, apply them to the router configuration now.

Step 4. View a summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors? **no**

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

Step 5. Troubleshoot the routing configuration on BRANCH1.

What networks and routes are shown in the routing table?

172.16.0.0/23

172.16.0.0 is directly connected

172.16.2.0 is directly connected

192.168.1.0/24 [120/1] via 209.165.200.225

209.165.200.0/30

209.165.200.224 is directly connected

Are there any problems with the routing table? **yes**

If there are any problems with the routing configuration, record any commands that will be necessary to correct the configuration errors.

Are there any problems with the routing table that could be because of errors on other parts of the network?

The routing table is missing routes to the BRANCH2 LANs. This is because of incorrect configuration of one of the other devices.

What networks are included in the RIP updates being sent from BRANCH1?

172.16.0.0/23

172.16.2.0/23

Are there any problems with the RIP updates that are being sent out from the router?

The BRANCH1 router is sending out v1 updates.

If there are any additional problems with the RIP configuration, record any commands that will be necessary to correct the configuration errors.

configure terminal

router rip

version 2

Step 6. If you have recorded any commands, apply them to the router configuration now.

Step 7. View the routing information.

If any changes were made to the configuration in the previous steps, view the routing information again.

Does the information in routing table indicate any configuration errors? no

Does the information included in the RIP updates that are sent out indicate any configuration errors? no

If the answer to either of these questions is **yes**, troubleshoot the routing configuration again.

What networks and routes are shown in the routing table?

172.16.0.0/23

172.16.0.0 is directly connected

172.16.2.0 is directly connected

192.168.1.0/24 [120/1] via 209.165.200.225

209.165.200.0/30

209.165.200.224 is directly connected

Step 8. Attempt to ping between the hosts again.

From the host PC1, is it possible to ping PC3? yes

From the host PC1, is it possible to ping PC4? yes

From the host PC1, is it possible to ping the Serial 0/0/1 interface of the HQ router? no

Task 4: Troubleshoot HQ

Step 1. Begin troubleshooting at the host PC3.

From the host PC3, is it possible to ping PC1? yes

From the host PC3, is it possible to ping PC5? no

From the host PC3, is it possible to ping the default gateway? yes

Step 2. Examine the HQ router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the configuration of the interfaces?

Yes, protocol is down on interface Serial 0/0/1.

If there are any problems with the configuration of the interfaces, record any commands that will be necessary to correct the configuration errors.

configure terminal

interface serial 0/0/1

clock rate 64000

Step 3. If you have recorded any commands in Step 2, apply them to the router configuration now.

Step 4. View the summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors? **no**

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

Step 5. Troubleshoot the routing configuration on HQ.

What networks and routes are shown in the routing table?

172.16.0.0/16 [120/1] via 209.165.200.226

192.168.1.0/24

192.168.1.0/25 is directly connected

192.168.1.128/25 is directly connected

209.165.200.0/30

209.165.200.224 is directly connected

209.165.200.228 is directly connected

Are there any problems with the routing table?

Yes, the routes for the BRANCH2 LANs are missing from the routing table.

If there are any problems with the routing table, record any commands that will be necessary to correct the configuration errors.

There is nothing wrong with the configuration of the HQ router that would cause this.

What networks are included in the RIP updates to BRANCH2?

172.16.0.0/16

192.168.1.0/24

209.165.200.224/30

Are there any problems with the RIP updates that are being sent out from HQ? **no**

If there are any problems with the RIP configuration, record any commands that will be necessary to correct the configuration errors.

Step 6. If you have recorded any commands in the previous step, apply them to the router configuration now.

Step 7. View the routing information.

If any changes were made to the configuration in the previous steps, view the routing information again.

Does the information in routing table indicate any configuration errors on HQ? **no**

Does the information included in the RIP updates that are sent out indicate any configuration errors on HQ? **no**

If the answer to either of these questions is **yes**, troubleshoot the routing configuration again.

- Step 8.** Attempt to ping between the hosts again.
- From the host PC3, is it possible to ping PC1? yes
- From the host PC3, is it possible to ping PC5? no
- From the host PC3, is it possible to ping the default gateway? yes

Task 5: Troubleshoot BRANCH2

- Step 1.** Begin troubleshooting at the host PC5.
- From the host PC5, is it possible to ping PC6? no
- From the host PC5, is it possible to ping PC1? no
- From the host PC3, is it possible to ping the default gateway? no
- Step 2.** Examine BRANCH2 to find possible configuration errors.
- Begin by viewing the summary of status information for each interface on the router.
- Are there any problems with the configuration of the interfaces?
- Yes, the IP addresses for the Fa0/0 and Fa0/1 interfaces are reversed.
- If there are any problems with the configuration of the interfaces, record any commands that will be necessary to correct the configuration errors.
- ```
configure terminal
interface FastEthernet0/0
no ip address
interface FastEthernet0/1
no ip address
interface FastEthernet0/0
ip address 172.16.4.1 255.255.255.128
no shutdown
interface FastEthernet0/1
ip address 172.16.4.129 255.255.255.128
no shutdown
```
- Step 3.** If you have recorded any commands, apply them to the router configuration now.
- Step 4.** View the summary of the status information.
- If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.
- Does the information in the interface status summary indicate any configuration errors? no
- If the answer is **yes**, troubleshoot the interface status of the interfaces again.

**Step 5.** Troubleshoot the routing configuration on BRANCH2.

Begin by viewing the routing table.

What networks and routes are shown in the routing table?

172.16.0.0/16

172.16.0.0/16 [120/2] via 209.165.200.229

172.16.4.0/25 is directly connected

172.16.4.128/25 is directly connected

192.168.1.0/24 [120/1] via 209.165.200.229

209.165.200.0/30

209.165.200.224 [120/1] via 209.165.200.229

209.165.200.228 is directly connected

**Step 6.** Examine the routes that are being sent out in the routing updates from BRANCH2.

Are there any problems with these routing updates?

The BRANCH2 LANs are missing from the routing updates.

If there are any problems with the routing configuration, record any commands that will be necessary to correct the configuration errors.

configure terminal

router rip

network 172.16.0.0

**Step 7.** If you have recorded any commands in the previous step, apply them to the router configuration now.

**Step 8.** Attempt to ping the hosts again.

From the host PC5, is it possible to ping PC6? yes

From the host PC5, is it possible to ping PC1? no

From the host PC3, is it possible to ping the default gateway? yes

From the HQ router, is it possible to ping PC1?

Yes, but not all the pings are successful.

From the HQ router, is it possible to ping PC5?

Yes, but not all the pings are successful.

**Step 9.** Examine the routing updates that are being received on BRANCH2.

What networks are being received in the RIP updates?

172.16.0.0/16

192.168.1.0/24

209.165.200.224/30

Are there any problems with these routing updates?

In the routing updates, the routes for the individual networks on the BRANCH1 LANs are not being received. Because the router is receiving summarized routes, packets destined for the BRANCH1 and BRANCH2 routers might not be routed properly.

If there are any problems with the routing configuration, record any commands that will be necessary to correct the configuration errors.

configure terminal

router rip

no auto-summary

Do these commands need to be applied only to BRANCH2, or do they also need to be applied to any other routers in the network?

Auto-summary should be turned off on all three of the routers.

**Step 10.** If you have recorded any commands in the previous step, apply them to the router configuration now.

**Step 11.** View the routing information.

If any changes were made to the configuration in the previous step, view routing table again.

Does the information in routing table or routing updates indicate any configuration errors?

no

If the answer is **yes**, troubleshoot the routing configuration again.

**Step 12.** Attempt to ping between the hosts again.

From the host PC5, is it possible to ping PC6? yes

From the host PC5, is it possible to ping PC1? yes

From the host PC5, is it possible to ping PC3? yes

From the host PC1, is it possible to ping PC3? yes

From the HQ router, is it possible to ping PC1? yes

From the HQ router, is it possible to ping PC5? yes

## Task 6: Reflection

There were a number of configuration errors in the scripts that were provided for this lab. Use the space below to write a brief description of the errors that you found.

---

---

---

---

---

---

---

---

## Task 7: Documentation

On each router, capture the following command output to a text (.txt) file and save for future reference.

**show running-config**

**show ip route**

**show ip interface brief**

**show ip protocols**

If you need to review the procedures for capturing command output, refer to “Lab 1-1: Cabling a Network and Basic Router Configuration.”

## Task 8: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.



## Packet Tracer Companion: Troubleshooting RIPv2 Configuration (7.5.3)

You can now open the file LSG02-Lab753.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment.



## Packet Tracer Skills Integration Challenge: Configuring and Troubleshooting RIPv2

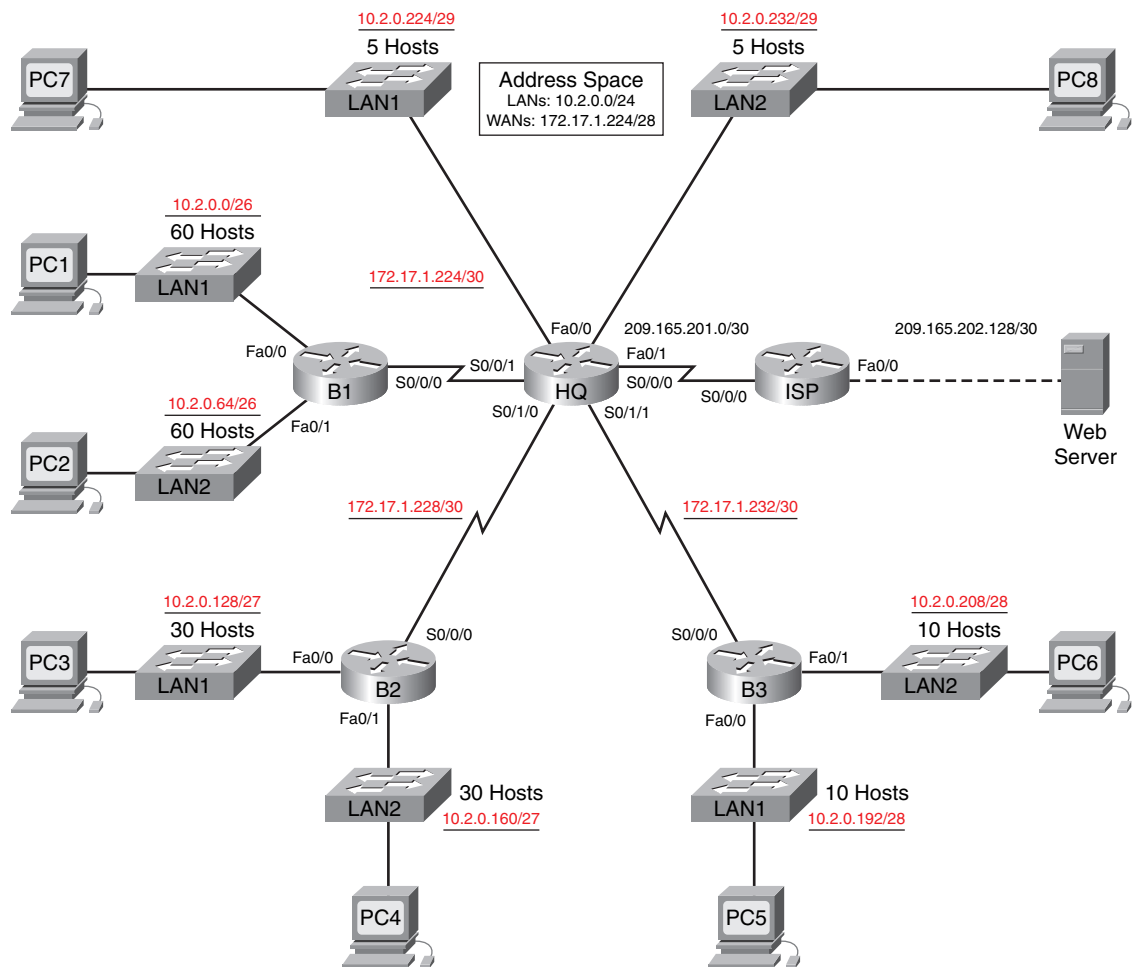
Upon completion of this lab, you will be able to

- Design and document an addressing scheme based on requirements
- Select appropriate equipment and cable the devices

- Apply a basic configuration to the devices
- Test connectivity between directly connected devices
- Configure RIPv2 routing
- Configure static and default routing for Internet access
- Verify full connectivity between all devices in the topology

Open the file LSG02-PTSkills7.pka on the CD-ROM that accompanies this book. You will use the topology in Figure 7-6 and the addressing table in Table 7-8 to document your design.

**Figure 7-6 Packet Tracer Skills Topology Diagram (Answer)**



**Table 7-8 Packet Tracer Skills Addressing Table**

| Device | Interface | IP Address    | Subnet Mask     | Default Gateway |
|--------|-----------|---------------|-----------------|-----------------|
| HQ     | Fa0/0     | 10.2.0.225    | 255.255.255.248 | —               |
|        | Fa0/1     | 10.2.0.233    | 255.255.255.248 | —               |
|        | S0/0/0    | 209.165.201.2 | 255.255.255.252 | —               |
|        | S0/0/1    | 172.17.1.225  | 255.255.255.252 | —               |

*continues*

**Table 7-8 Packet Tracer Skills Addressing Table** *continued*

| Device     | Interface | IP Address      | Subnet Mask     | Default Gateway |
|------------|-----------|-----------------|-----------------|-----------------|
|            | S0/1/0    | 172.17.1.229    | 255.255.255.252 | —               |
|            | S0/1/1    | 172.17.1.233    | 255.255.255.252 | —               |
| B1         | Fa0/0     | 10.2.0.1        | 255.255.255.192 | —               |
|            | Fa0/1     | 10.2.0.65       | 255.255.255.192 | —               |
|            | S0/0/0    | 172.17.1.226    | 255.255.255.252 | —               |
| B2         | Fa0/0     | 10.2.0.129      | 255.255.255.224 | —               |
|            | Fa0/1     | 10.2.0.161      | 255.255.255.224 | —               |
|            | S0/0/0    | 172.17.1.230    | 255.255.255.252 | —               |
| B3         | Fa0/0     | 10.2.0.193      | 255.255.255.240 | —               |
|            | Fa0/1     | 10.2.0.209      | 255.255.255.240 | —               |
|            | S0/0/0    | 172.17.1.234    | 255.255.255.252 | —               |
| ISP        | Fa0/0     | 209.165.202.129 | 255.255.255.252 | —               |
|            | S0/0/0    | 209.165.201.1   | 255.255.255.252 | —               |
| Web Server | NIC       | 209.165.202.130 | 255.255.255.252 | 209.165.202.129 |
| PC1        | NIC       | 10.2.0.62       | 255.255.255.192 | 10.2.0.1        |
| PC2        | NIC       | 10.2.0.126      | 255.255.255.192 | 10.2.0.64       |
| PC3        | NIC       | 10.2.0.158      | 255.255.255.224 | 10.2.0.129      |
| PC4        | NIC       | 10.2.0.190      | 255.255.255.224 | 10.2.0.161      |
| PC5        | NIC       | 10.2.0.206      | 255.255.255.240 | 10.2.0.193      |
| PC6        | NIC       | 10.2.0.222      | 255.255.255.240 | 10.2.0.209      |
| PC7        | NIC       | 10.2.0.230      | 255.255.255.248 | 10.2.0.225      |
| PC8        | NIC       | 10.2.0.238      | 255.255.255.248 | 10.2.0.233      |

## Task 1: Design and Document an Addressing Scheme

**Step 1.** Design an addressing scheme.

Based on the network requirements shown in the topology diagram of Figure 7-6, design an appropriate addressing scheme.

**Step 2.** Document the addressing scheme.

Use the blank spaces in the topology diagram of Figure 7-6 to record the network addresses in dotted decimal/slash format.

Use Table 7-8 to document the IP addresses, subnet masks, and default gateway addresses.



## Task 2: Select Equipment and Cable Devices

**Step 1.** Select the necessary equipment.

Select the remaining devices you will need, and add them to the working space inside Packet Tracer.

**Step 2.** Finish cabling the devices.

Cable the networks according to the topology diagram in Figure 7-6, taking care that interfaces match your documentation in Task 1.

## Task 3: Apply a Basic Configuration

**Step 1.** Configure the routers.

Using your documentation, configure the routers with basic configurations

**Step 2.** Configure the PCs.

Using your documentation, configure the PCs with an IP address, subnet mask, and default gateways.

## Task 4: Test Connectivity

Before continuing, make sure that each device can ping its directly connected neighbor.

## Task 5: Configure and Verify RIPv2 Routing

**Step 1.** Configure RIPv2.

Configure all devices with RIPv2 routing. In your configuration, make sure that you include the following:

- Disable automatic summarization.
- Stop routing updates on interfaces that are not connected to RIP neighbors.

**Step 2.** Verify RIPv2.

Use verification commands to check your configuration. All routers should be converged on all the 10.2.0.0/24 and 172.17.1.224/28 subnets.

## Task 6: Configure Static and Default Routing

Your configuration is not complete until all PCs can ping the web server. Use static and default routing to finish the configuration.

## Task 7: Test Connectivity and Examine the Configuration

All devices should have end-to-end connectivity, and the routing tables should be complete.



# The Routing Table: A Closer Look

The Study Guide portion of this chapter uses a combination of matching, fill-in-the-blank, multiple-choice, and open-ended question exercises to test your knowledge of the routing table lookup process for both classful and classless routing behavior.

The Labs and Activities portion of this chapter includes all the online curriculum labs to ensure that you have mastered the practical, hands-on skills needed to understand the routing table lookup process.

As you work through this chapter, use Chapter 8 in *Routing Protocols and Concepts, CCNA Exploration Companion Guide* or use the corresponding Chapter 8 in the Exploration Routing Protocols and Concepts online curriculum for assistance.

## Study Guide

### Routing Table Structure

The structure or format of the routing table might seem obvious until you take a closer look. Understanding the structure of the routing table will help you verify and troubleshoot routing issues because you will understand the routing table lookup process. You will know exactly what the Cisco IOS does when it searches for a route. The exercises in the following sections focus on the concepts of level 1 and level 2 routes.

### Level 1 and Level 2 Routes

The Cisco IP routing [table](#) is not a flat database, but a [hierarchical](#) structure that is used to speed the lookup process when locating routes and forwarding packets. This structure includes several levels. For simplicity, we will discuss all routes as one of two levels: level 1 or level 2.

Briefly describe a level 1 route.

[A level 1 route is a route with a subnet mask equal to or less than the classful mask of the network address.](#)

List the three types of level 1 routes.

[Default route, supernet route, and network route](#)

List the three sources of level 1 routes.

[Directly connected network, static route, and dynamic routing protocol](#)

The level 1 route can be further defined as an ultimate route.

An ultimate route is a route that includes one or both of the following:

- A [next-hop](#) IP address
- An [exit](#) interface

Indicate which of the following routes are level 1 routes by writing “yes” or “no” in the blank in front of the route.

Level 1 route?

[yes](#) 192.168.1.0/24

[no](#) 192.168.1.32/27

[yes](#) 192.168.4.0/22

[yes](#) 172.16.0.0/14

[yes](#) 172.16.0.0/16

[no](#) 172.16.1.0/24

[no](#) 10.1.0.0/16

[yes](#) 10.0.0.0/8

## Parent and Child Routes

What is the main difference between a parent route and an ultimate route?

A parent route does not have a next-hop IP address or an exit interface. Although a parent route is a level 1 route, the ultimate route is derived from a child route of the parent.

What is the relationship between parent and child routes?

A child route is a level 2 route that provides the next-hop IP address or exit interface for routing traffic to the destination.

In the partial output of the routing table in Example 8-1, indicate whether each route is a parent route or a child route by checking the appropriate column.

### Example 8-1 Parent and Child Routes: Classful

```

10.0.0.0/30 is subnetted, 2 subnets
R 10.10.10.0 [120/1] via 10.10.10.5, 00:00:28, Serial0/0/0
C 10.10.10.4 is directly connected, Serial0/0/0

```

| Route      | Parent | Child |
|------------|--------|-------|
| 10.0.0.0   | X      |       |
| 10.10.10.0 |        | X     |
| 10.10.10.4 |        | X     |

In Table 8-1, describe each part of the partial output shown in Example 8-1.

**Table 8-1 Command Output Description**

| Command Output          | Description                              |
|-------------------------|------------------------------------------|
| 10.0.0.0                | Classful network                         |
| /30                     | Subnet mask for child routes             |
| is subnetted, 2 subnets | Parent route with two child routes       |
| R                       | Route source is RIP                      |
| 10.10.10.0              | First child route                        |
| 120                     | AD value for RIP routes                  |
| 1                       | RIP metric, 1 hop                        |
| via 10.10.10.5          | Next-hop IP address for this child route |
| 00:00:28                | Time since last update from neighbor     |
| Serial0/0/0             | Exit interface for first child route     |
| C                       | Source is connected route                |
| 10.10.10.4              | Second child route                       |
| Serial0/0/0             | Exit interface for second child route    |

In Example 8-2, notice that the child routes do not share the same subnet mask, as was the case in the classful example. In this case, we are implementing a network addressing scheme with VLSM.

In the partial output of the routing table in Example 8-2, indicate whether each route is a parent route or a child route by checking the appropriate column.

**Example 8-2 Parent and Child Routes: Classless**

|   |                                                             |
|---|-------------------------------------------------------------|
|   | 172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks     |
| R | 172.16.0.0/18 [120/1] via 10.10.10.5, 00:00:28, Serial0/0/0 |
| C | 172.16.68.0/22 is directly connected, FastEthernet0/0       |
| C | 172.16.72.0/23 is directly connected, FastEthernet0/1       |

| Route       | Parent | Child |
|-------------|--------|-------|
| 172.16.0.0  | X      |       |
| 172.16.0.0  |        | X     |
| 172.16.68.0 |        | X     |
| 172.16.72.0 |        | X     |

In Table 8-2, describe each part of the partial output shown in Example 8-2.

**Table 8-2 Command Output Description: Classless Routes**

| Command Output         | Description                                       |
|------------------------|---------------------------------------------------|
| 172.16.0.0             | Classful parent route                             |
| /16                    | Classful mask                                     |
| is variably subnetted, | Child routes have different masks                 |
| 3 subnets, 3 masks     | Number of subnets and masks for this parent route |
| R                      | Route source is RIP                               |
| 172.16.0.0             | First child route                                 |
| /18                    | Mask for first child route                        |
| 120                    | AD value for RIP routes                           |
| 1                      | RIP metric, 1 hop                                 |
| via 10.10.10.5         | Next-hop IP address for this child route          |
| 00:00:28               | Time since last update from neighbor              |
| Serial0/0/0            | Exit interface for first child route              |
| C                      | Source is connected route                         |
| 172.16.68.0            | Second child route                                |
| /22                    | Mask for second child route                       |
| FastEthernet0/0        | Exit interface for second child route             |

| Command Output  | Description                           |
|-----------------|---------------------------------------|
| C               | Source is connected route             |
| 172.16.72.0     | Third child route                     |
| /23             | Mask for third child route            |
| FastEthernet0/0 | Exit interface for second child route |

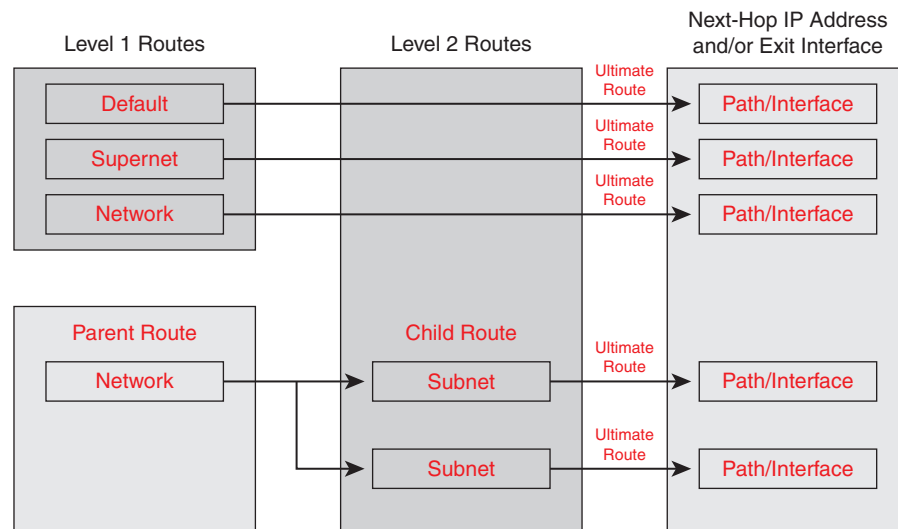
## Routing Table Lookup Process

When a router receives a packet on one of its interfaces, the routing table lookup process compares the destination IP address of the packet with the entries in the routing table. The best match between the packet's destination IP address and the route in the routing table is used to determine out which interface to forward the packet. Just exactly how that happens is the focus of the exercises in the following section.

## Complete the Chart

Figure 8-1 shows an incomplete version of the chart used to explain the routing table lookup process. Write in the correct labels for the chart.

**Figure 8-1 Routing Table: Parent/Child Relationship (Answer)**



## Routing Table Lookup Exercise

The routing table shown in Example 8-3 will be used in this exercise.

### Example 8-3 Routing Table for B2

```
B2# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
```

```
<output omitted>
```

*continues*

*continued*

Gateway of last resort is not set

10.0.0.0/30 is subnetted, 3 subnets

R 10.10.10.0 [120/1] via 10.10.10.5, 00:00:21, Serial0/0/0

C 10.10.10.4 is directly connected, Serial0/0/0

R 10.10.10.8 [120/1] via 10.10.10.5, 00:00:21, Serial0/0/0

172.16.0.0/16 is variably subnetted, 8 subnets, 6 masks

R 172.16.0.0/18 [120/1] via 10.10.10.5, 00:00:21, Serial0/0/0

C 172.16.68.0/22 is directly connected, FastEthernet0/0

C 172.16.72.0/23 is directly connected, FastEthernet0/1

R 172.16.128.0/20 [120/1] via 10.10.10.5, 00:00:21, Serial0/0/0

R 172.16.160.0/21 [120/2] via 10.10.10.5, 00:00:21, Serial0/0/0

R 172.16.176.0/22 [120/2] via 10.10.10.5, 00:00:21, Serial0/0/0

R 172.16.188.0/23 [120/2] via 10.10.10.5, 00:00:21, Serial0/0/0

R 172.16.190.0/24 [120/2] via 10.10.10.5, 00:00:21, Serial0/0/0

The router, B2, receives a packet from 172.16.68.10 destined for 172.16.142.10. Use binary to prove which route in Example 8-3 is the longest match. Make sure that you designate the bits that must match between the IP address and the longest match route. If no route matches, simply state “No match.”

Route 172.16.128.0/20 is the longest match

10101100.00010000.10001110.00001010

10101100.00010000.10000000.00000000

The router, B2, receives a packet from 172.16.72.10 destined for 172.16.179.10. Use binary to prove which route in Example 8-3 is the longest match. Make sure that you designate the bits that must match between the IP address and the longest match route. If no route matches, simply state “No match.”

Route 172.16.176.0/22 is the longest match

10101100.00010000.10110011.00001010

10101100.00010000.10110000.00000000

The router, B2, receives a packet from 172.16.69.10 destined for 172.16.65.10. Use binary to prove which route in Example 8-3 is the longest match. Make sure that you designate the bits that must match between the IP address and the longest match route. If no route matches, simply state “No match.”

No routes matches. The first child route, 172.16.0.0/18, is the closest to a longest match. The bits match through the 17th bit. However, the destination’s 18th bit is “on” whereas the 18th bit in 172.16.0.0/18 is “off.”



## Routing Behavior

What happens when there is a match between the packet's destination IP address and a level 1 parent route, but there is not a match with any of the level 2 child routes? You might assume that the routing table lookup process continues looking for a less specific match in the routing table. However, you will see that this might or might not be the case, depending on the configuration of the router.

## Classful and Classless Routing Behavior

Routing behavior influences the process of searching for the preferred route using the **no ip classless** or **ip classless** commands. Classless and classful routing behaviors are not the same as classless and classful routing protocols. Classful and classless routing protocols affect how the routing table is populated. Classful and classless routing behaviors determine how the routing table is searched after it is populated.

In Table 8-3, the routing protocols are listed. Indicate which are classful and which are classless.

**Table 8-3 Classful and Classless Routing Protocols**

Routing Protocol	Classful or Classless?
RIPv1	Classful
RIPv2	Classless
IGRP	Classful
EIGRP	Classless
OSPF	Classless
IS-IS	Classless

In contrast to classful and classless routing protocols, what determines whether the router operates with classful or classless routing behavior?

The commands **no ip classless** and **ip classless**

Is it possible to have a classless routing protocol configured, yet a classful routing behavior implemented? If yes, give an example. If no, explain why not.

Yes. The routing table could be populated with routes from a classless routing protocol like RIPv2, yet implement classful routing behavior because the **no ip classless** command is configured.

Explanation:

**Building the routing table:** The router learns about remote networks through RIPv2, a classless routing protocol. This means that the routing updates included a subnet mask and therefore support discontinuous networks and VLSM. The routing protocol is only used to populate the routing table. The routing protocol has no effect on the routing table lookup process.

**Lookup process:** The router has been configured with classful routing behavior (**no ip classless**). If there is a match with the parent route, such as 172.16.0.0 (a 16-bit match), but not a match with any of the child routes, the router will drop the packet. Even if a lesser match exists in the routing table (less than the 16 bits of the parent route) such as a default route, that route will not be used.

Is it possible to have a classful routing protocol configured yet a classless routing behavior implemented? If yes, give an example. If no, explain why not.

Yes. The routing table could be populated with routes from a classful routing protocol like RIPv1, yet implement classless routing behavior because the **ip classless** command is configured.

Explanation:

**Building the routing table:** The router learns about remote networks through RIPv1, a classful routing protocol. This means that the routing updates do not include a subnet mask and therefore cannot support discontinuous networks or VLSM. The routing protocol is only used to populate the routing table. The routing protocol has no effect on the routing table lookup process.

**Lookup process:** The router has been configured with classless routing behavior (**ip classless**). If there is a match with the parent route, such as 172.16.0.0 (a 16-bit match), but not a match with any of the child routes, the router will continue to search the routing table for a lesser match.

This could include the default route. If a lesser match is found, the router will forward the packet using that router. Otherwise, it will drop the packet.

## Determine the Route

Using Example 8-4, determine the route used to forward the packet based on the following scenarios.

### Example 8-4 Routing Table for B3

```

B3> show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
<output omitted>
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is 10.10.10.9 to network 0.0.0.0

 10.0.0.0/30 is subnetted, 3 subnets
R 10.10.10.0 [120/1] via 10.10.10.9, 00:00:22, Serial0/0/0
R 10.10.10.4 [120/1] via 10.10.10.9, 00:00:22, Serial0/0/0
C 10.10.10.8 is directly connected, Serial0/0/0
 172.16.0.0/16 is variably subnetted, 8 subnets, 6 masks
R 172.16.0.0/18 [120/1] via 10.10.10.9, 00:00:22, Serial0/0/0
R 172.16.68.0/22 [120/2] via 10.10.10.9, 00:00:22, Serial0/0/0
R 172.16.72.0/23 [120/2] via 10.10.10.9, 00:00:22, Serial0/0/0
R 172.16.128.0/20 [120/1] via 10.10.10.9, 00:00:22, Serial0/0/0
R 172.16.160.0/21 [120/2] via 10.10.10.9, 00:00:22, Serial0/0/0
R 172.16.176.0/22 [120/2] via 10.10.10.9, 00:00:22, Serial0/0/0
C 172.16.188.0/23 is directly connected, FastEthernet0/0
C 172.16.190.0/24 is directly connected, FastEthernet0/1
R* 0.0.0.0/0 [120/1] via 10.10.10.9, 00:00:22, Serial0/0/0

```

The router, B3, receives a packet from 172.16.189.10 destined for 172.16.179.10. The router is running IOS Release 11.1 and RIPv2. No other configuration changes have been made. Use binary to prove which route in Example 8-4 is the longest match. Make sure that you designate the bits that must match between the IP address and the longest match route. If no route matches, simply state “No match.”

Route 172.16.176.0/22 is the longest match.

10101100.00010000.10110011.00001010

10101100.00010000.10110000.00000000

The router, B3, receives a packet from 172.16.190.10 destined for 172.16.74.10. The router is running IOS Release 11.1 and RIPv2. No other configuration changes have been made. Use binary to prove which route in Example 8-4 is the longest match. Make sure that you designate the bits that must match between the IP address and the longest match route. If no route matches, simply state “No match.”

No match. Because Release 11.1 operates with classful routing behavior by default, B3 does not use the default route. It discards the packet because it assumes that it has access to all available subnets of the classful 172.16.0.0 network.

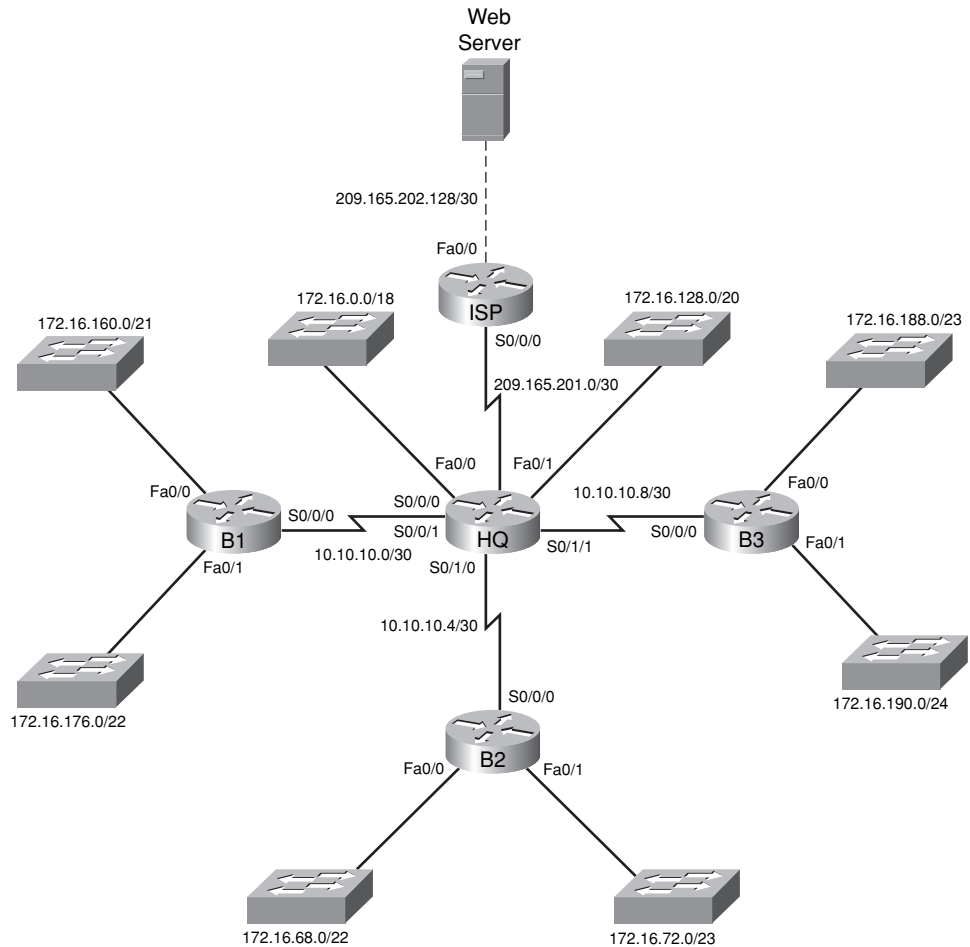
The router, B3, receives a packet from 172.16.190.10 destined for 172.16.192.10. The router is running Cisco IOS Software Release 12.0 and RIPv2. No other configuration changes have been made. Use binary to prove which route in Example 8-4 is the longest match. Make sure that you designate the bits that must match between the IP address and the longest match route. If no route matches, simply state “No match.”

Only the default route matches. Because Cisco IOS Software Release 12.0 operates with classless routing behavior by default (ip classless), the router continues to check all available routes. Because none match, the router will use the default route if available. B3 forwards the packet using the default route.

## Determine the Topology

Using only the partial topology in Figure 8-2 and the output from the **show ip route** command in Examples 8-5 through 8-9, complete the topology using the following guidelines:

- Add necessary devices. Each LAN has a switch as is shown for HQ.
- Connect the devices with the appropriate cables.
- Label the interfaces.
- Label the networks.

**Figure 8-2 Determine the Topology (Answer)****Example 8-5 ISP Routing Table**

```

ISP# show ip route
<output omitted>

Gateway of last resort is not set

 10.0.0.0/28 is subnetted, 1 subnets
S 10.10.10.0 is directly connected, Serial0/0/0
S 172.16.0.0/16 is directly connected, Serial0/0/0
 209.165.201.0/30 is subnetted, 1 subnets
C 209.165.201.0 is directly connected, Serial0/0/0
 209.165.202.0/30 is subnetted, 1 subnets
C 209.165.202.128 is directly connected, FastEthernet0/0

```

**Example 8-6 HQ Routing Table**

```

HQ# show ip route
<output omitted>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

 10.0.0.0/30 is subnetted, 3 subnets
C 10.10.10.0 is directly connected, Serial0/0/1
C 10.10.10.4 is directly connected, Serial0/1/0
C 10.10.10.8 is directly connected, Serial0/1/1
 172.16.0.0/16 is variably subnetted, 8 subnets, 5 masks
C 172.16.128.0/20 is directly connected, FastEthernet0/0
R 172.16.68.0/22 [120/1] via 10.10.10.6, 00:00:02, Serial0/1/0
R 172.16.72.0/23 [120/1] via 10.10.10.6, 00:00:02, Serial0/1/0
C 172.16.0.0/18 is directly connected, FastEthernet0/1
R 172.16.160.0/21 [120/1] via 10.10.10.2, 00:00:05, Serial0/0/1
R 172.16.176.0/22 [120/1] via 10.10.10.2, 00:00:05, Serial0/0/1
R 172.16.188.0/23 [120/1] via 10.10.10.10, 00:00:02, Serial0/1/1
R 172.16.190.0/24 [120/1] via 10.10.10.10, 00:00:02, Serial0/1/1
 209.165.201.0/30 is subnetted, 1 subnets
C 209.165.201.0 is directly connected, Serial0/0/0
S* 0.0.0.0/0 is directly connected, Serial0/0/0

```

**Example 8-7 B1 Routing Table**

```

B1# show ip route
<output omitted>

Gateway of last resort is 10.10.10.1 to network 0.0.0.0

 10.0.0.0/30 is subnetted, 3 subnets
C 10.10.10.0 is directly connected, Serial0/0/0
R 10.10.10.4 [120/1] via 10.10.10.1, 00:00:19, Serial0/0/0
R 10.10.10.8 [120/1] via 10.10.10.1, 00:00:19, Serial0/0/0
 172.16.0.0/16 is variably subnetted, 8 subnets, 5 masks
R 172.16.64.0/20 [120/1] via 10.10.10.1, 00:00:19, Serial0/0/0
R 172.16.68.0/22 [120/2] via 10.10.10.1, 00:00:19, Serial0/0/0
R 172.16.72.0/23 [120/2] via 10.10.10.1, 00:00:19, Serial0/0/0
R 172.16.128.0/20 [120/1] via 10.10.10.1, 00:00:19, Serial0/0/0
C 172.16.160.0/21 is directly connected, FastEthernet0/0
C 172.16.176.0/22 is directly connected, FastEthernet0/1

```

*continues*

*continued*

```
R 172.16.188.0/23 [120/2] via 10.10.10.1, 00:00:19, Serial0/0/0
R 172.16.190.0/24 [120/2] via 10.10.10.1, 00:00:19, Serial0/0/0
R* 0.0.0.0/0 [120/1] via 10.10.10.1, 00:00:19, Serial0/0/0
```

#### Example 8-8 B2 Routing Table

B2# **show ip route**

*<output omitted>*

Gateway of last resort is 10.10.10.5 to network 0.0.0.0

10.0.0.0/30 is subnetted, 3 subnets

```
R 10.10.10.0 [120/1] via 10.10.10.5, 00:00:23, Serial0/0/0
C 10.10.10.4 is directly connected, Serial0/0/0
R 10.10.10.8 [120/1] via 10.10.10.5, 00:00:23, Serial0/0/0
172.16.0.0/16 is variably subnetted, 8 subnets, 5 masks
R 172.16.64.0/20 [120/1] via 10.10.10.5, 00:00:23, Serial0/0/0
C 172.16.68.0/22 is directly connected, FastEthernet0/0
C 172.16.72.0/23 is directly connected, FastEthernet0/1
R 172.16.128.0/20 [120/1] via 10.10.10.5, 00:00:23, Serial0/0/0
R 172.16.160.0/21 [120/2] via 10.10.10.5, 00:00:23, Serial0/0/0
R 172.16.176.0/22 [120/2] via 10.10.10.5, 00:00:23, Serial0/0/0
R 172.16.188.0/23 [120/2] via 10.10.10.5, 00:00:23, Serial0/0/0
R 172.16.190.0/24 [120/2] via 10.10.10.5, 00:00:23, Serial0/0/0
R* 0.0.0.0/0 [120/1] via 10.10.10.5, 00:00:23, Serial0/0/0
```

#### Example 8-9 B3 Routing Table

B3# **show ip route**

*<output omitted>*

Gateway of last resort is 10.10.10.9 to network 0.0.0.0

10.0.0.0/30 is subnetted, 3 subnets

```
R 10.10.10.0 [120/1] via 10.10.10.9, 00:00:06, Serial0/0/0
R 10.10.10.4 [120/1] via 10.10.10.9, 00:00:06, Serial0/0/0
C 10.10.10.8 is directly connected, Serial0/0/0
172.16.0.0/16 is variably subnetted, 8 subnets, 5 masks
R 172.16.64.0/20 [120/1] via 10.10.10.9, 00:00:06, Serial0/0/0
R 172.16.68.0/22 [120/2] via 10.10.10.9, 00:00:06, Serial0/0/0
```

```
R 172.16.72.0/23 [120/2] via 10.10.10.9, 00:00:06, Serial0/0/0
R 172.16.128.0/20 [120/1] via 10.10.10.9, 00:00:06, Serial0/0/0
R 172.16.160.0/21 [120/2] via 10.10.10.9, 00:00:06, Serial0/0/0
R 172.16.176.0/22 [120/2] via 10.10.10.9, 00:00:06, Serial0/0/0
C 172.16.188.0/23 is directly connected, FastEthernet0/0
C 172.16.190.0/24 is directly connected, FastEthernet0/1
R* 0.0.0.0/0 [120/1] via 10.10.10.9, 00:00:06, Serial0/0/0
```

## Labs and Activities

### Command Reference

In Table 8-4, record the command, *including the correct router prompt*, that fits the description.

**Table 8-4** Commands for Chapter 8, The Routing Table: A Closer Look

Command	Description
<code>Router(config)# no ip classless</code>	Configures the routing behavior as classful. On by default in versions of Cisco IOS Software prior to Release 11.3.
<code>Router(config)# ip classless</code>	Configures the routing behavior as classless. On by default in Cisco IOS Software Release 11.3 and later.



### Lab 8-1: Investigating the Routing Table Lookup Process (8.4.1)

Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Perform basic configuration tasks on a router
- Determine level 1 and level 2 routes
- Modify the configuration to reflect static and default routing
- Enable classful routing and investigate classful routing behavior
- Enable classless routing and investigate classless routing behavior

#### Scenarios

In this lab activity, there are two separate scenarios:

- **Scenario A: Level 1 and Level 2 Routes**—In this scenario, you will examine level 1 and level 2 routes in the routing table.
- **Scenario B: Classful and Classless Routing Behavior**—In this scenario, you will examine classful and classless routing behavior.



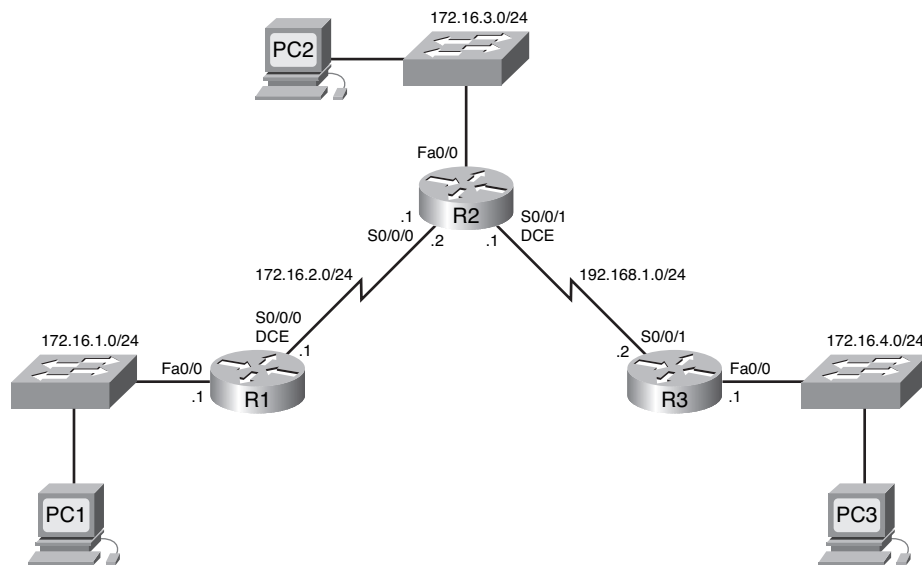
## Scenario A: Level 1 and Level 2 Routes

### Task 1: Prepare the Network

**Step 1.** Cable a network that is similar to the one in the topology diagram shown in Figure 8-3.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

**Figure 8-3 Scenario A Topology for Lab 8-1**



**Note:** If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions will appear different.

**Step 2.** Clear any existing configurations on the routers.

### Task 2: Perform Basic Router Configurations

Perform basic configuration of the R1, R2, and R3 routers according to the following guidelines:

- Configure the router host name.
- Disable Domain Name System (DNS) lookup.
- Configure an EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for console connections.
- Configure a password for VTY connections.

### Task 3: Configure and Activate Serial and Ethernet Addresses

**Step 1.** Configure interfaces on R1, R2, and R3.

Configure the interfaces on the R1, R2, and R3 routers with the IP addresses from Table 8-5.

**Table 8-5 Scenario A Addressing Table for Lab 8-1**

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.16.1.1	255.255.255.0	—
	S0/0/0	172.16.2.1	255.255.255.0	—
R2	Fa0/0	172.16.3.1	255.255.255.0	—
	S0/0/0	172.16.2.2	255.255.255.0	—
	S0/0/1	192.168.1.1	255.255.255.0	—
R3	Fa0/0	172.16.4.1	255.255.255.0	—
	S0/0/1	192.168.1.2	255.255.255.0	—
PC1	NIC	172.16.1.10	255.255.255.0	172.16.1.1
PC2	NIC	172.16.3.10	255.255.255.0	172.16.3.1
PC3	NIC	172.16.4.10	255.255.255.0	172.16.4.1

**Step 2.** Verify IP addressing and interfaces.

Use the **show ip interface brief** command to verify that the IP addressing is correct and that the interfaces are active.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

**Step 3.** Configure Ethernet interfaces of PC1, PC2, and PC3.

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses and default gateways from Table 8-5.

**Step 4.** Test the PC configuration by pinging the default gateway from the PC.

#### Task 4: Configure RIP

Configure RIP version 1 routing on each of the routers. Include **network** statements for each of the directly connected networks.

#### Task 5: Observe Routes Being Deleted and Added to the Routing Table

**Step 1.** View the routing table on the R1 router.

What networks are shown in the routing table?

[172.16.0.0/24 \(Level 1 Parent Route\)](#)

[172.16.1.0 \(Child Route\)](#)

[172.16.2.0 \(Child Route\)](#)

[172.16.3.0 \(Child Route\)](#)

[192.168.1.0/24 \(Level 1 Ultimate Route\)](#)

**Step 2.** Use the **debug ip routing** command to observe changes in the routing table as they occur on the R1 router.

```
R1# debug ip routing
```

```
IP routing debugging is on
```

**Step 3.** Shut down the Serial 0/0/0 interface and observe the debug output.

```
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to administratively
down
RT: interface Serial0/0/0 removed from routing table
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to down
RT: del 172.16.2.0 via 0.0.0.0, connected metric [0/0]
RT: delete network route to 172.16.2.0
RT: NET-RED 172.16.2.0/24
RT: del 172.16.3.0 via 172.16.2.2, rip metric [120/1]
RT: delete network route to 172.16.3.0
RT: NET-RED 172.16.3.0/24
RT: del 192.168.1.0 via 172.16.2.2, rip metric [120/1]
RT: delete network route to 192.168.1.0
RT: NET-RED 192.168.1.0/24
```

**Step 4.** View the routing table on the R1 router and observe the changes that occurred when the Serial 0/0/0 interface was disabled.

```
R1# show ip route
```

```
<Output omitted>
```

```
Gateway of last resort is not set
```

```

 172.16.0.0/24 is subnetted, 1 subnets
C 172.16.1.0 is directly connected, FastEthernet0/0
R1#
```

**Step 5.** Enable the Serial 0/0/0 interface and observe the debug output.

```
R1(config-if)# no shutdown
RT: SETLASTRDB for 172.16.2.0/24
NEW rdb: is directly connected
RT: add 172.16.2.0/24 via 0.0.0.0, connected metric [0/0]
RT: NET-RED 172.16.2.0/24RT: SETLASTRDB for 172.16.0.0/16
NEW rdb: via 172.16.2.2
RT: add 172.16.3.0/24 via 172.16.2.2, rip metric [120/1]
RT: NET-RED 172.16.3.0/24RT: SETLASTRDB for 192.168.1.0/24
NEW rdb: via 172.16.2.2
RT: add 192.168.1.0/24 via 172.16.2.2, rip metric [120/1]
RT: NET-RED 192.168.1.0/24
```

Why is the route to 172.16.2.0/24 added first?

It is a directly connected network.

Why is there a delay before the other routes are added?

RIP updates are sent every 30 seconds.

- Step 6.** Disable the debug output with either the **no debug ip routing** or the **undebug all** command.

## Task 6: Determine Level 1 and Level 2 Routes

- Step 1.** Examine the R1 routing table.

```
R1# show ip route
```

```
<Output omitted>
```

```
Gateway of last resort is not set
```

```
 172.16.0.0/24 is subnetted, 3 subnets
C 172.16.1.0 is directly connected, FastEthernet0/0
C 172.16.2.0 is directly connected, Serial0/0/0
R 172.16.3.0 [120/1] via 172.16.2.2, 00:00:11, Serial0/0/0
R 192.168.1.0/24 [120/1] via 172.16.2.2, 00:00:11, Serial0/0/0
R1#
```

Which of these routes are level 1 routes?

172.16.0.0/24

192.168.1.0/24

Why are these routes level 1 routes?

172.16.0.0/24 is a parent route with more specific child routes. The other is a level 1 route because its subnet mask is equal to the classful mask.

Are any of the level 1 routes ultimate routes?

Yes, 192.168.1.0/24

Why is this route an ultimate route?

The 192.168.1.0/24 route is an ultimate route because the route contains the exit interface Serial 0/0/0.

Are any of the level 1 routes parent routes?

Yes, 172.16.0.0/24

Why is this route a level 1 parent route?

This is a level 1 parent route because it is a level 1 route that does not contain a next-hop IP address or exit interface for any network.

Which of the routes are level 2 routes?

172.16.1.0

172.16.2.0

172.16.3.0

Why are these routes level 2 routes?

These are level 2 routes because they are subnets of the level 1 parent route 172.16.0.0/24.

Packet Tracer  
Companion

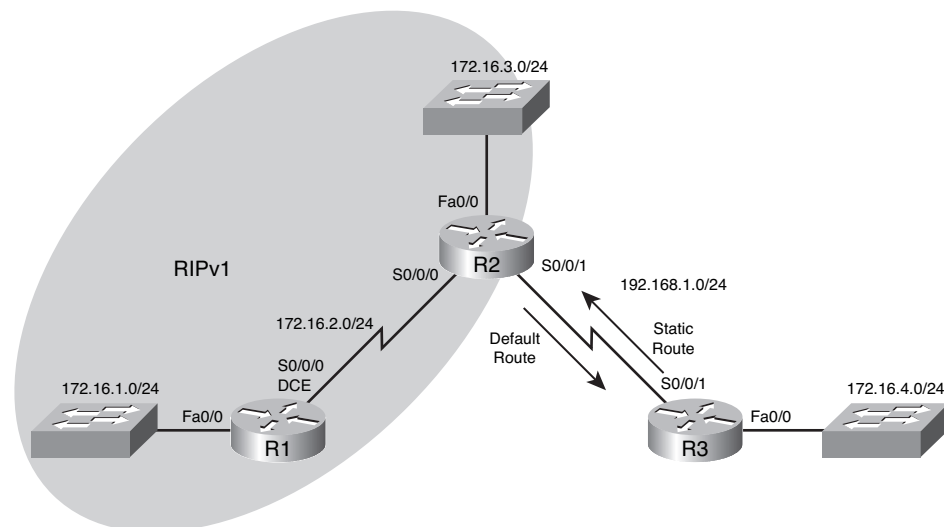
## Packet Tracer Companion: Investigating the Routing Table Lookup Process (8.4.1)

You can now open the file LSG02-Lab841.pka on the CD-ROM that accompanies this book to repeat this portion of the hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.

## Scenario B: Classful and Classless Routing Behavior

Refer to Figure 8-4 to complete the tasks for this scenario.

Figure 8-4 Scenario B Topology Diagram for Lab 8-1



### Task 1: Make Changes Between Scenario A and Scenario B

**Step 1.** Remove the RIP configuration from R3 and configure a static route to 172.16.0.0/16.

```
R3(config)# no router rip
R3(config)# ip route 172.16.0.0 255.255.0.0 Serial0/0/1
```

**Step 2.** Remove the 192.168.1.0 network from the R2 RIP configuration.

```
R2(config)# router rip
R2(config-router)#no network 192.168.1.0
```

**Step 3.** Add a static default route to R3 on the R2 router.

Include the **default-information originate** command in the configuration so that the default static route is included in the RIP updates.

```
R2(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/1
R2(config)# router rip
R2(config-router)# default-information originate
```

## Task 2: Enable Classful Routing Behavior on the Routers

**Step 1.** Use the **no ip classless** command to configure the route lookup process to use classful route lookups.

```
R1(config)# no ip classless
```

```
R2(config)# no ip classless
```

```
R3(config)# no ip classless
```

**Step 2.** Examine the routing table on the R2 router.

```
R2# show ip route
```

```
<output omitted>
```

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
 172.16.0.0/24 is subnetted, 4 subnets
R 172.16.1.0 [120/1] via 172.16.2.1, 00:00:00, Serial0/0/0
C 172.16.2.0 is directly connected, Serial0/0/0
C 172.16.3.0 is directly connected, FastEthernet0/0
C 192.168.1.0/24 is directly connected, Serial0/0/1
S* 0.0.0.0/0 is directly connected, Serial0/0/1
```

**Step 3.** Ping from R2 to PC3 and observe the results.

```
R2# ping 172.16.4.10
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.4.10, timeout is 2 seconds:
```

```
.....
```

```
Success rate is 0 percent (0/5)
```

The ping is unsuccessful because the router is using classful routing behavior.

The route lookup process on the R2 router searches the routing table and finds that the first 16 bits of the destination address are a match with the parent route 172.16.0.0/16. Because the destination address matches the parent route, the child routes are checked.

What are the child routes of the 172.16.0.0/16 parent network?

[172.16.1.0/24](#)

[172.16.2.0/24](#)

[172.16.3.0/24](#)

How many bits in the destination address must match for a packet to be forwarded using one of the child routes? [24](#)

Does the destination address of the ping packets match any of the child routes of 172.16.0.0/16? [no](#)

Because the **no ip classless** command has been used to configure the R2 router to use classful routing behavior, when a level 1 match is found, the router will not search beyond the child routes for a lesser match. Even though there is a default static route configured, it will not be used, and the packet will be dropped.

### Task 3: Enable Classless Routing Behavior on the Routers

**Step 1.** Use the **ip classless** command to reenable classless routing.

```
R1(config)# ip classless

R2(config)# ip classless

R3(config)# ip classless
```

**Step 2.** Examine the routing table on R2.

Notice that the routing table is still the same, even though the router configuration has been changed to use classless routing behavior.

```
R2# show ip route
```

```
<output omitted>
```

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
 172.16.0.0/24 is subnetted, 4 subnets
 R 172.16.1.0 [120/1] via 172.16.2.1, 00:00:00, Serial0/0/0
 C 172.16.2.0 is directly connected, Serial0/0/0
 C 172.16.3.0 is directly connected, FastEthernet0/0
 C 192.168.1.0/24 is directly connected, Serial0/0/1
 S* 0.0.0.0/0 is directly connected, Serial0/0/1
```

**Step 3.** Repeat the ping from R2 to PC3 and observe results.

```
R2# ping 172.16.4.10
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.4.10, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent, round-trip min/avg/max = 28/28/28 ms
```

The ping is successful this time because the router is using classless routing behavior.

The destination address of the packet is a match with the level 1 parent route 172.16.0.0/16, but there is not a match with any of the child routes of this parent route.

Because classless routing behavior is configured, the router will now continue to search the routing table for a route where there might be fewer bits that match, but the route is still a match. The mask of a default route is /0, which means that no bits need to match. In classless routing behavior, if no other route matches, the default route will always match.

```
S* 0.0.0.0/0 is directly connected, Serial0/0/1
```

Because there is a default route configured on the R2 router, this route is used to forward the packets to PC3.

**Step 4.** Examine the routing table on R3 to determine how the traffic generated by the **ping** command is returned to R2.

```
R3# show ip route
```

```
<output omitted>
```

```
Gateway of last resort is not set
```

```

172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
S 172.16.0.0/16 is directly connected, Serial0/0/1
C 172.16.4.0/24 is directly connected, FastEthernet0/0
C 192.168.1.0/24 is directly connected, Serial0/0/1

```

Notice that in the routing table for R3, both the 172.16.4.0/24 subnet route and the 172.16.0.0/16 classful network route are level 2 child routes of the 172.16.0.0/16 parent route. In this case, R3 uses the 172.16.0.0/16 child route and forwards the return traffic out Serial 0/0/1 back to R2.



## Lab 8-2: show ip route Challenge (8.4.2)

Upon completion of this lab, you will be able to

- Determine network topology based on the outputs from the **show ip route** command
- Cable a network according to the topology diagram in Figure 8-5
- Determine router interface addressing based on outputs
- Perform basic configuration tasks on a router
- Determine level 1 and level 2 routes

### Scenario

In this lab activity, you will derive the topology of a network from the output of the **show ip route command**. You must draw a topology diagram and determine the interface addressing on each router. Then you must build and configure the network based on the **show ip route** output. The DTE and DCE assignment is at your discretion. When complete, the output from your network must match those given in Task 1.

## Task 1: Examine the Router Outputs

**Step 1.** Examine the output from the R1 router.

```

R1# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
<output omitted>
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

```

```

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

 10.0.0.0/30 is subnetted, 4 subnets
R 10.10.10.0 [120/1] via 10.10.10.6, 00:00:09, Serial0/0/0
C 10.10.10.4 is directly connected, Serial0/0/0
C 10.10.10.8 is directly connected, Serial0/0/1
R 10.10.10.12 [120/1] via 10.10.10.10, 00:00:09, Serial0/0/1
 172.16.0.0/16 is variably subnetted, 10 subnets, 5 masks
C 172.16.1.0/27 is directly connected, FastEthernet0/0
R 172.16.1.32/28 [120/2] via 10.10.10.10, 00:00:09, Serial0/0/1
R 172.16.1.192/26 [120/1] via 10.10.10.6, 00:00:09, Serial0/0/0

```



```

R 172.16.2.0/26 [120/2] via 10.10.10.6, 00:00:09, Serial0/0/0
R 172.16.2.64/27 [120/1] via 10.10.10.10, 00:00:09, Serial0/0/1
C 172.16.3.0/25 is directly connected, FastEthernet0/1
R 172.16.3.128/26 [120/1] via 10.10.10.6, 00:00:09, Serial0/0/0
R 172.16.3.192/29 [120/2] via 10.10.10.6, 00:00:09, Serial0/0/0
R 172.16.4.0/27 [120/1] via 10.10.10.10, 00:00:09, Serial0/0/1
R 172.16.4.128/25 [120/2] via 10.10.10.10, 00:00:09, Serial0/0/1
C 192.168.1.0/24 is directly connected, Loopback0
S* 0.0.0.0/0 is directly connected, Loopback0

```

**Step 2.** Examine the output from the R2 router.

```

R2# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
<output omitted>
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is 10.10.10.2 to network 0.0.0.0

 10.0.0.0/30 is subnetted, 4 subnets
C 10.10.10.0 is directly connected, Serial0/0/0
R 10.10.10.4 [120/1] via 10.10.10.2, 00:00:04, Serial0/0/0
R 10.10.10.8 [120/2] via 10.10.10.2, 00:00:04, Serial0/0/0
R 10.10.10.12 [120/3] via 10.10.10.2, 00:00:04, Serial0/0/0
 172.16.0.0/16 is variably subnetted, 10 subnets, 5 masks
R 172.16.1.0/27 [120/2] via 10.10.10.2, 00:00:04, Serial0/0/0
R 172.16.1.32/28 [120/4] via 10.10.10.2, 00:00:04, Serial0/0/0
R 172.16.1.192/26 [120/1] via 10.10.10.2, 00:00:04, Serial0/0/0
C 172.16.2.0/26 is directly connected, FastEthernet0/0
R 172.16.2.64/27 [120/3] via 10.10.10.2, 00:00:04, Serial0/0/0
R 172.16.3.0/25 [120/2] via 10.10.10.2, 00:00:04, Serial0/0/0
R 172.16.3.128/26 [120/1] via 10.10.10.2, 00:00:04, Serial0/0/0
C 172.16.3.192/29 is directly connected, FastEthernet0/1
R 172.16.4.0/27 [120/3] via 10.10.10.2, 00:00:04, Serial0/0/0
R 172.16.4.128/25 [120/4] via 10.10.10.2, 00:00:04, Serial0/0/0
R 192.168.1.0/24 [120/2] via 10.10.10.2, 00:00:04, Serial0/0/0
R* 0.0.0.0/0 [120/2] via 10.10.10.2, 00:00:04, Serial0/0/0

```

**Step 3.** Examine the output from the R3 router.

```

R3# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
<output omitted>
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is 10.10.10.5 to network 0.0.0.0

```

```

10.0.0.0/30 is subnetted, 4 subnets
C 10.10.10.0 is directly connected, Serial0/0/1
C 10.10.10.4 is directly connected, Serial0/0/0
R 10.10.10.8 [120/1] via 10.10.10.5, 00:00:04, Serial0/0/0
R 10.10.10.12 [120/2] via 10.10.10.5, 00:00:04, Serial0/0/0
172.16.0.0/16 is variably subnetted, 10 subnets, 5 masks
R 172.16.1.0/27 [120/1] via 10.10.10.5, 00:00:04, Serial0/0/0
R 172.16.1.32/28 [120/3] via 10.10.10.5, 00:00:04, Serial0/0/0
C 172.16.1.192/26 is directly connected, FastEthernet0/1
R 172.16.2.0/26 [120/1] via 10.10.10.1, 00:00:03, Serial0/0/1
R 172.16.2.64/27 [120/2] via 10.10.10.5, 00:00:04, Serial0/0/0
R 172.16.3.0/25 [120/1] via 10.10.10.5, 00:00:04, Serial0/0/0
C 172.16.3.128/26 is directly connected, FastEthernet0/0
R 172.16.3.192/29 [120/1] via 10.10.10.1, 00:00:03, Serial0/0/1
R 172.16.4.0/27 [120/2] via 10.10.10.5, 00:00:04, Serial0/0/0
R 172.16.4.128/25 [120/3] via 10.10.10.5, 00:00:04, Serial0/0/0
R 192.168.1.0/24 [120/1] via 10.10.10.5, 00:00:04, Serial0/0/0
R* 0.0.0.0/0 [120/1] via 10.10.10.5, 00:00:04, Serial0/0/0

```

**Step 4.** Examine the output from the R4 router.

```

R4# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
<output omitted>
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

```

Gateway of last resort is 10.10.10.9 to network 0.0.0.0

```

10.0.0.0/30 is subnetted, 4 subnets
R 10.10.10.0 [120/2] via 10.10.10.9, 00:00:14, Serial0/0/0
R 10.10.10.4 [120/1] via 10.10.10.9, 00:00:14, Serial0/0/0
C 10.10.10.8 is directly connected, Serial0/0/0
C 10.10.10.12 is directly connected, Serial0/0/1
172.16.0.0/16 is variably subnetted, 10 subnets, 5 masks
R 172.16.1.0/27 [120/1] via 10.10.10.9, 00:00:14, Serial0/0/0
R 172.16.1.32/28 [120/1] via 10.10.10.14, 00:00:17, Serial0/0/1
R 172.16.1.192/26 [120/2] via 10.10.10.9, 00:00:14, Serial0/0/0
R 172.16.2.0/26 [120/3] via 10.10.10.9, 00:00:14, Serial0/0/0
C 172.16.2.64/27 is directly connected, FastEthernet0/1
R 172.16.3.0/25 [120/1] via 10.10.10.9, 00:00:14, Serial0/0/0
R 172.16.3.128/26 [120/2] via 10.10.10.9, 00:00:14, Serial0/0/0
R 172.16.3.192/29 [120/3] via 10.10.10.9, 00:00:14, Serial0/0/0
C 172.16.4.0/27 is directly connected, FastEthernet0/0
R 172.16.4.128/25 [120/1] via 10.10.10.14, 00:00:17, Serial0/0/1
R 192.168.1.0/24 [120/1] via 10.10.10.9, 00:00:14, Serial0/0/0
R* 0.0.0.0/0 [120/1] via 10.10.10.9, 00:00:14, Serial0/0/0

```

**Step 5.** Examine the output from the R5 router.

R5# show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP  
<output omitted>

\* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route

Gateway of last resort is 10.10.10.13 to network 0.0.0.0

```

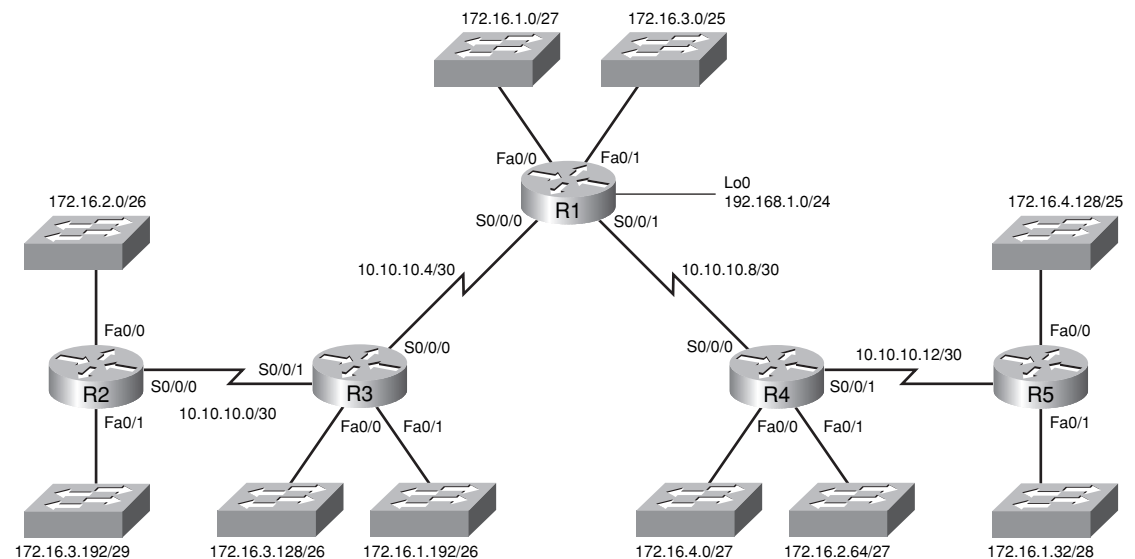
10.0.0.0/30 is subnetted, 4 subnets
R 10.10.10.0 [120/3] via 10.10.10.13, 00:00:21, Serial0/0/0
R 10.10.10.4 [120/2] via 10.10.10.13, 00:00:21, Serial0/0/0
R 10.10.10.8 [120/1] via 10.10.10.13, 00:00:21, Serial0/0/0
C 10.10.10.12 is directly connected, Serial0/0/0
172.16.0.0/16 is variably subnetted, 10 subnets, 5 masks
R 172.16.1.0/27 [120/2] via 10.10.10.13, 00:00:21, Serial0/0/0
C 172.16.1.32/28 is directly connected, FastEthernet0/1
R 172.16.1.192/26 [120/3] via 10.10.10.13, 00:00:21, Serial0/0/0
R 172.16.2.0/26 [120/4] via 10.10.10.13, 00:00:21, Serial0/0/0
R 172.16.2.64/27 [120/1] via 10.10.10.13, 00:00:21, Serial0/0/0
R 172.16.3.0/25 [120/2] via 10.10.10.13, 00:00:21, Serial0/0/0
R 172.16.3.128/26 [120/3] via 10.10.10.13, 00:00:21, Serial0/0/0
R 172.16.3.192/29 [120/4] via 10.10.10.13, 00:00:21, Serial0/0/0
R 172.16.4.0/27 [120/1] via 10.10.10.13, 00:00:21, Serial0/0/0
C 172.16.4.128/25 is directly connected, FastEthernet0/0
R 192.168.1.0/24 [120/2] via 10.10.10.13, 00:00:21, Serial0/0/0
R* 0.0.0.0/0 [120/2] via 10.10.10.13, 00:00:21, Serial0/0/0

```

## Task 2: Create a Diagram of the Network Based on the show ip route Output on Routers R1–R5

**Step 1.** Draw a diagram of the network based on your interpretation of the router outputs in the following space provided in Figure 8-5.

**Figure 8-5** Topology Diagram for Lab 8-2 (Answer)



**Step 2.** Document the interface addresses in Table 8-6.

**Table 8-6 Addressing Table for Lab 8-2**

Device	Interface	IP Address	Subnet Mask
R1	Loopback 0	192.168.1.1	255.255.255.0
	FastEthernet 0/0	172.16.1.1	255.255.255.224
	FastEthernet 0/1	172.16.3.1	255.255.255.128
	Serial 0/0/0	10.10.10.5	255.255.255.252
	Serial 0/0/1	10.10.10.9	255.255.255.252
R2	Serial 0/0/0	10.10.10.1	255.255.255.252
	FastEthernet 0/0	172.16.2.1	255.255.255.192
	FastEthernet 0/1	172.16.3.193	255.255.255.248
R3	Serial 0/0/0	10.10.10.6	255.255.255.252
	Serial 0/0/1	10.10.10.2	255.255.255.252
	FastEthernet 0/0	172.16.3.129	255.255.255.192
	FastEthernet 0/1	172.16.1.193	255.255.255.248
R4	Serial 0/0/0	10.10.10.10	255.255.255.252
	Serial 0/0/1	10.10.10.13	255.255.255.252
	FastEthernet 0/0	172.16.4.1	255.255.255.224
	FastEthernet 0/1	172.16.2.65	255.255.255.224
R5	Serial 0/0/0	10.10.10.14	255.255.255.252
	FastEthernet 0/0	172.16.4.129	255.255.255.128
	FastEthernet 0/1	172.16.1.33	255.255.255.240

### Task 3: Build and Configure the Diagram Using Packet Tracer

- Step 1.** Build the topology diagram you drew in Figure 8-5 in Packet Tracer. 1841 or 2811 routers can be used.
- Step 2.** Configure the interfaces with the appropriate IP address and subnet mask.
- Step 3.** Configure the appropriate routing protocol for each router and advertise all directly connected networks.
- Step 4.** Verify that configurations match the **show ip route** output on routers R1–R5 from Task 1.

## Task 4: Identify Routing Processes

**Step 1.** Examine the R1 routing table.

What are the IP addresses of the directly connected neighbors of the R1 router?

[10.10.10.4](#)

[10.10.10.8](#)

[172.16.1.0/27](#)

[172.16.3.0/25](#)

[192.168.1.0/24](#)

Which routes did R1 learn from the directly connected neighbors?

[10.10.10.0](#)

[10.10.10.12](#)

[172.16.1.32/28](#)

[172.16.1.192/26](#)

[172.16.2.0/26](#)

[172.16.2.64/27](#)

[172.16.3.128/26](#)

[172.16.3.192/29](#)

[172.16.4.0/27](#)

[172.16.4.128/25](#)

**Step 2.** Examine the R2 routing table.

How many total networks/subnets did R2 learn from its neighbors? [13](#)

Where would R2 send packets to networks not currently in its routing table? Why?

[The packets would be sent to the R3 router at the IP address 10.10.10.2. This is the IP address that is the default route in the R2 routing table.](#)

What does the statement **R\* 0.0.0.0 [120/2] via 10.10.10.2, 00:00:04, Serial0/0/0** at the end of the R2 routing table represent?

[Default route to 10.10.10.2](#)

**Step 3.** Examine the R3 routing table.

Which level 2 routes did R3 learn about from its neighbors?

[10.10.10.8](#)

[10.10.10.12](#)

[172.16.1.0/27](#)

[172.16.1.32/28](#)

[172.16.2.0/26](#)

[172.16.2.64/27](#)

[172.16.3.0/25](#)

[172.16.3.192/29](#)

[172.16.4.0/27](#)

[172.16.4.128/25](#)

[192.168.1.0/24](#)

Which networks are directly connected to R3?

[10.10.10.0](#)

[10.10.10.4](#)

[172.16.1.192/26](#)

[172.16.3.128/26](#)

**Step 4.** Examine the R4 routing table.

Which networks are the farthest distance from R4, and how many hops away are they?

[The 172.16.2.0/26 and 172.16.3.192/29 networks are three hops away.](#)

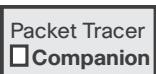
How many usable host addresses are on the networks farthest from R4? [62 and 6](#)

**Step 5.** Examine the R5 routing table.

How many routers must a packet pass through to get from R5 to network 172.16.2.0/26? [4](#)

Why is the gateway of last resort for R5 listed as 10.10.10.13?

[It is the next-hop address on the way to the gateway of last resort.](#)



## **Packet Tracer Companion: show ip route Challenge Lab (8.4.2)**

You can now open the file LSG02-Lab842.pka on the CD-ROM that accompanies this book to repeat this portion of the hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment. A summary of the instructions is provided within the activity.



## Packet Tracer Skills Integration Challenge

### Introduction

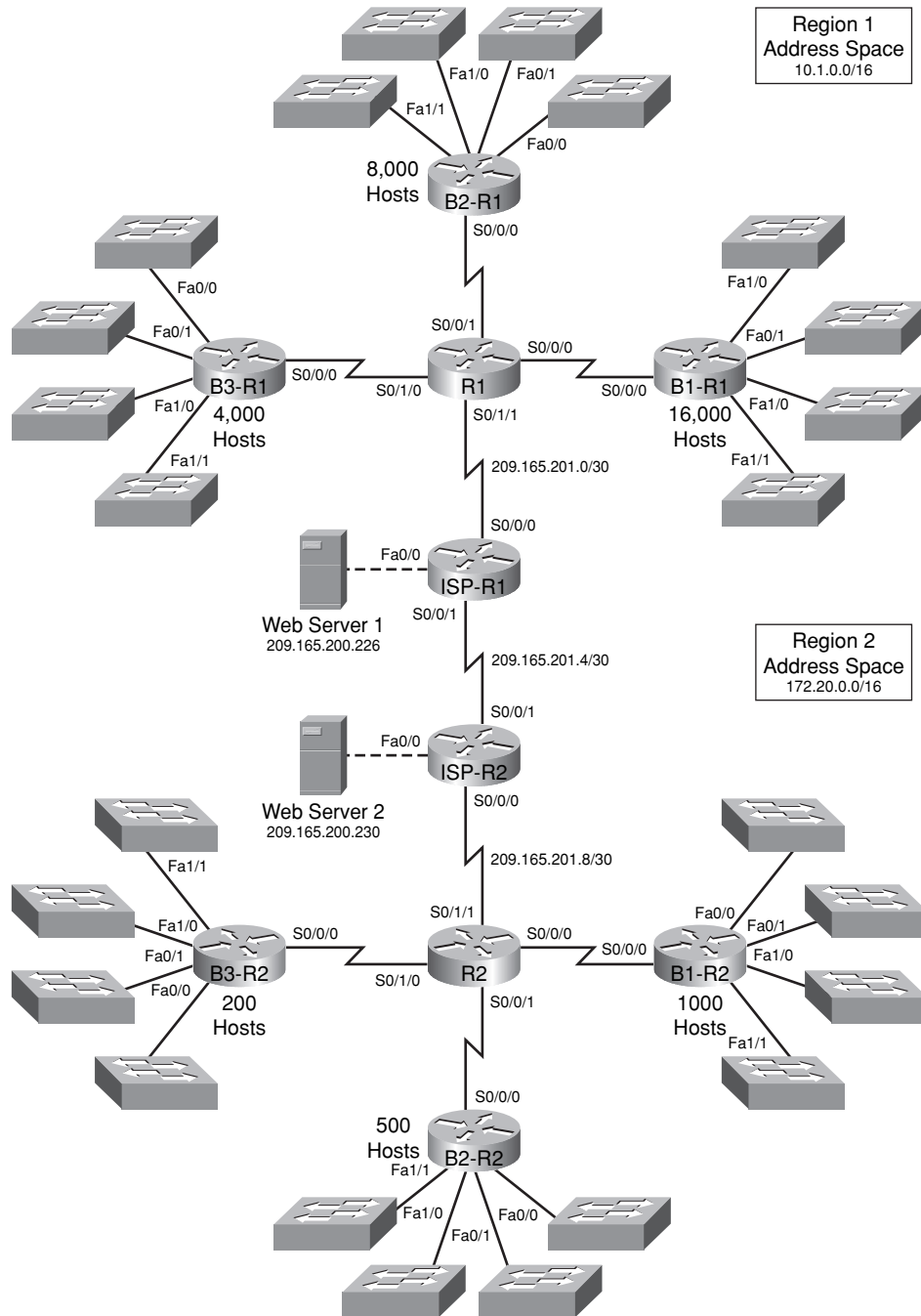
This activity focuses on subnetting skills with VLSM, basic device configurations, RIPv2 routing and static routing. After you configure all devices, test for end-to-end connectivity and examine your configuration. Open the file LSG02-PTSkills8.pka on the CD-ROM that accompanies this book. Use the topology in Figure 8-6 and the addressing tables in Table 8-7 and 8-8 to document your design.

Upon completion of this challenge, you will be able to

- Design and document an addressing scheme based on requirements
- Apply a basic configuration to the devices
- Configure static routing between ISP routers
- Configure RIPv2 routing in both regions
- Disable RIP updates on appropriate interfaces
- Configure default routes and redistribute through RIP
- Verify full connectivity between all devices in the topology

Open the file LSG02-PTSkills8.pka on the CD-ROM that accompanies this book. You will use the topology in Figure 8-6 and the addressing tables in Table 8-7 and 8-8 to document your design.

**Figure 8-6 Packet Tracer Skills Integration Challenge Topology**





**Table 8-7 Addressing Table for R1**

<b>Device</b>	<b>Interface</b>	<b>IP Address</b>	<b>Subnet Mask</b>
R1	S0/0/0	10.1.128.1	255.255.255.252
	S0/0/1	10.1.128.5	255.255.255.252
	S0/1/0	10.1.128.9	255.255.255.252
	S0/1/1	209.165.201.2	255.255.255.252
B1-R1	Fa0/0	10.1.0.1	255.255.240.0
	Fa0/1	10.1.16.1	255.255.240.0
	Fa1/0	10.1.32.1	255.255.240.0
	Fa1/1	10.1.48.1	255.255.240.0
	S0/0/0	10.1.128.2	255.255.255.252
B2-R1	Fa0/0	10.1.64.1	255.255.248.0
	Fa0/1	10.1.72.1	255.255.248.0
	Fa1/0	10.1.80.1	255.255.248.0
	Fa1/1	10.1.88.1	255.255.248.0
	S0/0/0	10.1.128.6	255.255.255.252
B3-R1	Fa0/0	10.1.96.1	255.255.252.0
	Fa0/1	10.1.100.1	255.255.252.0
	Fa1/0	10.1.104.1	255.255.252.0
	Fa1/1	10.1.108.1	255.255.252.0
	S0/0/0	10.1.128.10	255.255.255.252
ISP-R1	S0/0/0	209.165.201.1	255.255.255.252
	S0/0/1	209.165.201.5	255.255.255.252
	Fa0/0	209.165.200.225	255.255.255.252
Web Server 1	NIC	209.165.200.226	255.255.255.252

**Table 8-8 Addressing Table for R2**

<b>Device</b>	<b>Interface</b>	<b>IP Address</b>	<b>Subnet Mask</b>
R2	S0/0/0	172.20.8.1	255.255.255.252
	S0/0/1	172.20.8.5	255.255.255.252
	S0/1/0	172.20.8.9	255.255.255.252
	S0/1/1	209.165.201.10	255.255.255.252

Device	Interface	IP Address	Subnet Mask
B1-R2	Fa0/0	172.20.0.1	255.255.255.0
	Fa0/1	172.20.1.1	255.255.255.0
	Fa1/0	172.20.2.1	255.255.255.0
	Fa1/1	172.20.3.1	255.255.255.0
	S0/0/0	172.20.8.2	255.255.255.252
B2-R2	Fa0/0	172.20.4.1	255.255.255.128
	Fa0/1	172.20.4.129	255.255.255.128
	Fa1/0	172.20.5.1	255.255.255.128
	Fa1/1	172.20.5.129	255.255.255.128
	S0/0/0	172.20.8.6	255.255.255.252
B3-R2	Fa0/0	172.20.6.1	255.255.255.192
	Fa0/1	172.20.6.65	255.255.255.192
	Fa1/0	172.20.6.129	255.255.255.192
	Fa1/1	172.20.6.193	255.255.255.192
	S0/0/0	172.20.8.10	255.255.255.252
ISP-R2	S0/0/0	209.165.201.6	255.255.255.252
	S0/0/1	209.165.201.9	255.255.255.252
	Fa0/0	209.165.200.229	255.255.255.252
Web Server 2	NIC	209.165.200.230	255.255.255.252

## Task 1: Design and Document an Addressing Scheme

**Step 1.** Design an addressing scheme.

Using the topology provided in Figure 8-6 and the following requirements, design an addressing scheme:

- The WAN links between R1 and R2 and their respective ISP routers are already configured. Also, the links between the ISPs and the web servers are already configured.
- The address space for Region 1 is 10.1.0.0/16. Each branch router (B1-R1, B2-R1, and B3-R1) should be allotted address space based on the following requirements. Starting with the largest requirement, assign address space to each router:
  - B1-R1 needs space for 16,000 hosts [10.1.0.0/18](#)
  - B2-R1 needs space for 8000 hosts [10.1.64.0/19](#)
  - B3-R1 needs space for 4000 hosts [10.1.96.0/20](#)
- Divide the address space for each branch router into four equal subnets. Record the subnets in the following tables.

Router B1-R1 Interface	Subnet Number	Subnet Address
Fa0/0	0	10.1.0.0/20
Fa0/1	1	10.1.16.0/20
Fa1/0	2	10.1.32.0/20
Fa1/1	3	10.1.48.0/20

Router B2-R1 Interface	Subnet Number	Subnet Address
Fa0/0	0	10.1.64.0/21
Fa0/1	1	10.1.72.0/21
Fa1/0	2	10.1.80.0/21
Fa1/1	3	10.1.88.0/21

Router B3-R1 Interface	Subnet Number	Subnet Address
Fa0/0	0	10.1.96.0/22
Fa0/1	1	10.1.100.0/22
Fa1/0	2	10.1.104.0/22
Fa1/1	3	10.1.108.0/22

- For the WANs in Region 1, subnet the address space 10.1.128.0/28. Record the subnets in the following table.

Router	Subnet Number	Subnet Address
B1-R1 <—> R1	0	10.1.128.0/30
B2-R1 <—> R1	1	10.1.128.4/30
B3-R1 <—> R1	2	10.1.128.8/30

- The address space for Region 2 is 172.20.0.0/16. Each branch router (B1-R2, B2-R2, and B3-R2) should be allotted address space based on the following requirements. Starting with the largest requirement, assign address space to each router:
  - B1-R2 needs space for 1000 hosts [172.20.0.0/22](#)
  - B2-R2 needs space for 500 hosts [172.20.4.0/23](#)
  - B3-R2 needs space for 200 hosts [172.20.6.0/24](#)
- Divide the address space for each branch router into four equal subnets. Record the subnets in the following tables.

Router B1-R2 Interface	Subnet Number	Subnet Address
Fa0/0	0	172.20.0.0/24
Fa0/1	1	172.20.1.0/24
Fa1/0	2	172.20.2.0/24
Fa1/1	3	172.20.3.0/24

Router B2-R2 Interface	Subnet Number	Subnet Address
Fa0/0	0	172.20.4.0/25
Fa0/1	1	172.20.4.128/25
Fa1/0	2	172.20.5.0/25
Fa1/1	3	172.20.5.128/25

Router B3-R2 Interface	Subnet Number	Subnet Address
Fa0/0	0	172.20.6.0/26
Fa0/1	1	172.20.6.64/26
Fa1/0	2	172.20.6.128/26
Fa1/1	3	172.20.6.192/26

- For the WANs in Region 2, subnet the address space 172.20.255.240/28. Record the subnets in the following table.

Router	Subnet Number	Subnet Address
B1-R2 <—> R2	0	172.20.8.0/30
B2-R2 <—> R2	1	172.20.8.4/30
B3-R2 <—> R2	2	172.20.8.8/30

**Step 2.** Document the addressing scheme.

- (Optional) On the topology shown in Figure 8-6, label each subnet. To save space, use only the last two octets because only these octets change.
- Use Table 8-7 to document the IP addresses and subnet masks. Assign the first IP address to the router interface.
- For the WAN links, assign the first IP address to R1 and R2 for links to each router's respective B1, B2, and B3 routers.

## Task 2: Apply a Basic Configuration

Using your documentation, configure the routers with basic configurations including addressing. Use **cisco** as the line passwords and **class** as the secret password. Use **64000** as the clock rate.

## Task 3: Configure Static Routing Between ISP Routers

Each ISP router already has two static routes to the other ISP router's directly connected WANs. Implement static routing on each ISP router to ensure connectivity between the two regions.

## Task 4: Configure RIPv2 Routing in Both Regions

Configure all routers in both regions with RIPv2 as the dynamic routing protocol. Disable automatic summarization.

## Task 5: Disable RIP Updates on Appropriate Interfaces

RIP updates do not need to be sent out all the router interfaces. Disable RIP updates on appropriate interfaces.

## Task 6: Configure Default Routes and Redistribute Through RIP

- In Region 1, determine which router needs a default route. Configure a default route on that router, and then configure that router to redistribute the default route to other routers in the region.
- In Region 2, determine which router needs a default route. Configure a default route on that router, and then configure that router to redistribute the default route to other routers in the region.

## Task 7: Verify Full Connectivity Between All Devices in the Topology

**Step 1.** Test connectivity.

You should now have end-to-end connectivity. Use **ping** to test connectivity across the network. Each router should be able to ping all other router interfaces and both web servers.

Troubleshoot until pings are successful.

**Step 2.** Examine the configuration.

Use verification commands to make sure that your configurations are complete.



The Study Guide portion of this chapter uses a combination of matching, fill-in-the blank, multiple-choice, and open-ended question exercises to test your knowledge of EIGRP concepts and configurations.

The Labs and Activities portion of this chapter includes all the online curriculum labs, an additional comprehensive lab, and an additional challenge lab to ensure that you have mastered the practical, hands-on skills needed to configure and verify EIGRP routing.

As you work through this chapter, use Chapter 9 in *Routing Protocols and Concepts, CCNA Exploration Companion Guide* or use the corresponding Chapter 9 in the Exploration Routing Protocols and Concepts online curriculum for assistance.

## Study Guide

### Introduction to EIGRP

The main purpose in the Cisco development of Enhanced Interior Gateway Routing Protocol (EIGRP) was to create a classless version of IGRP. EIGRP includes several features that are not commonly found in other distance vector routing protocols like RIP (RIPv1 and RIPv2) and IGRP. Although EIGRP can act like a link-state routing protocol, it is still a distance vector routing protocol. In the following sections of the Study Guide, you will review basic EIGRP concepts and packet types.



## Vocabulary Exercise: Matching

Match the definition on the left with a term on the right. This exercise is not necessarily a one-to-one matching. Some definitions might be used more than once, and some terms might have multiple definitions. However, all terms and definitions are used.

### Definitions

- a. Table that includes route entries for all destinations that the router has learned
- b. A route selected as the primary route to reach a destination
- c. Shows directly connected routers with which the local router has established adjacency
- d. A backup route kept in the topology table in case the primary route goes down
- e. Used by EIGRP to discover, verify, and rediscover neighbor routers
- f. Describes a route that is in a reachable and operational status
- g. Guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize at the same time
- h. Table in which EIGRP places the routes it chooses from the topology table as the best (successor) routes to a destination
- i. Status of a route that has no feasible successors yet; router is waiting on replies from EIGRP routers
- j. Used by EIGRP to guarantee ordered delivery of both reliable and unreliable EIGRP packets to EIGRP neighbors
- k. Used when a router discovers a new neighbor
- l. Used when a router needs specific information from one or all of its neighbors
- m. A relationship formed between neighboring routers using a common media segment for the purpose of exchanging routing information
- n. The metric that a neighbor router advertises to the local router about its own cost to a destination network
- o. Used to respond to EIGRP packets sent reliably
- p. A neighbor's reported distance (RD) to a network is less than the local router's feasible distance to the same destination network.
- q. Lowest calculated metric to reach the destination network
- r. Used to respond to an EIGRP query packet
- s. Data field of an EIGRP packet with type, length, and value specified
- t. For EIGRP routing configuration, simply the inverse of the subnet mask

### Terms

- o acknowledgment packet
- i active state
- m adjacency
- n advertised distance
- g Diffusing Update Algorithm
- p feasibility condition
- q feasible distance
- d, p feasible successor
- e Hello packets
- c neighbor table
- f passive state
- l query packet
- j Reliable Transport Protocol
- r reply packet
- n reported distance
- h routing table
- b successor
- s TLV
- a topology database
- a topology table
- k update packet
- t wildcard mask

## EIGRP Concepts Exercise

### *Roots of EIGRP: IGRP*

Cisco developed the proprietary IGRP in 1985 in response to some of the limitations of [RIPv1](#), including the use of the [hop count](#) metric and the maximum network size of [15 hops](#).

Instead of [hop count](#), both IGRP and EIGRP use metrics composed of [bandwidth](#), [delay](#), [reliability](#), and [load](#). By default, both routing protocols use only [bandwidth](#) and [delay](#). However, because IGRP is a classful routing protocol, its usefulness is limited in many of today's networks.

Therefore, Cisco enhanced IGRP with a new algorithm, [DUAL](#), and other features.

Table 9-1 summarizes the main differences between a traditional distance vector routing protocol, such as RIP, and the enhanced distance vector routing protocol, EIGRP. Fill in the missing words and phrases.

**Table 9-1 Comparing Traditional Distance Vector and EIGRP**

<b>Traditional Distance Vector Routing Protocols</b>	<b>Enhanced Distance Vector Routing Protocol: EIGRP</b>
Uses the <a href="#">Bellman-Ford</a> or Ford-Fulkerson algorithm.	Uses the <a href="#">Diffusing Update Algorithm</a> (DUAL).
Ages out routing entries and uses <a href="#">periodic</a> updates	Does not age out routing entries nor use <a href="#">periodic</a> updates.
Keeps track of only the best routes, the best path to a destination network	Maintains a <a href="#">topology</a> table separate from the routing table, which includes the best path and any <a href="#">loop-free</a> backup paths.
When a route becomes unavailable, the router must wait for a new routing update.	When a route becomes unavailable, DUAL will use a <a href="#">backup</a> path if one exists in the topology table.
Slower <a href="#">convergence</a> because of <a href="#">hold-down</a> timers.	Faster <a href="#">convergence</a> because of the absence of <a href="#">hold-down</a> timers and a system of coordinated route calculations.

### *Algorithm*

Traditional distance vector routing protocols all use some variant of the [Bellman-Ford](#) or Ford-Fulkerson algorithm. These protocols, such as [RIP](#) and [IGRP](#), age out individual routing entries and therefore need to periodically send routing table updates.

EIGRP uses the [Diffusing Update Algorithm](#) (DUAL). EIGRP uses a lightweight [Hello](#) protocol to monitor connection status with its neighbors. Only [changes](#) in the routing information, such as a new link or a link becoming unavailable, cause a routing update to occur.

### *Path Determination*

DUAL maintains a [topology](#) table separate from the routing table, which includes both the best path to a destination network and any [backup](#) paths that DUAL has determined to be [loop-free](#). In EIGRP, [loop-free](#) means that a route has met a requirement known as the feasibility [condition](#).

### Convergence

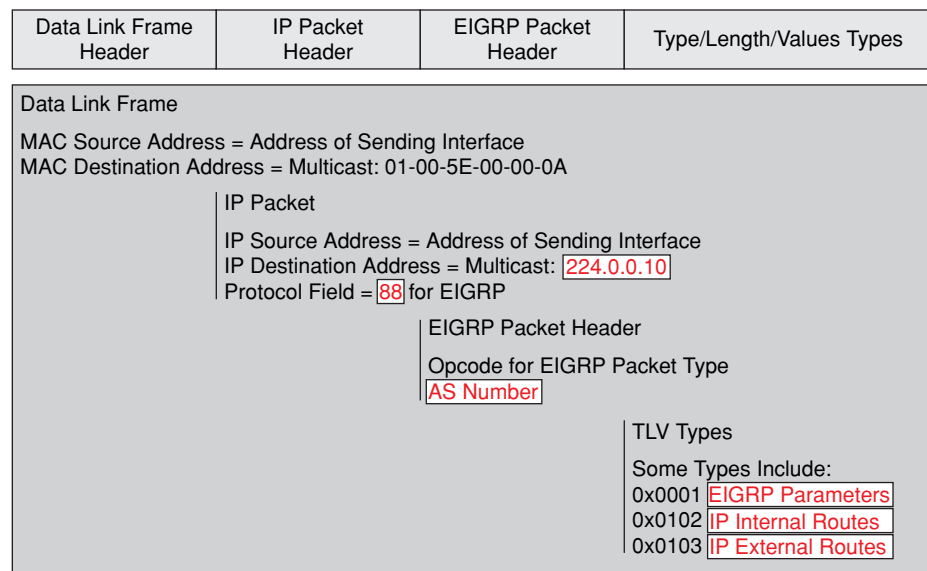
Because of the unreliable nature of **periodic** updates, traditional distance vector routing protocols are prone to routing **loops** and the count-to-**infinity** problem. RIP and IGRP use several mechanisms to help avoid these problems including **hold-down** timers, which cause long convergence times.

EIGRP does not use **hold-down** timers. Instead, loop-free paths are achieved through a system of route calculations (diffusing computations) that result in faster convergence than traditional distance vector routing protocols.

### EIGRP Message Format

Figure 9-1 shows an example of an encapsulated EIGRP message. Fill in the missing field contents.

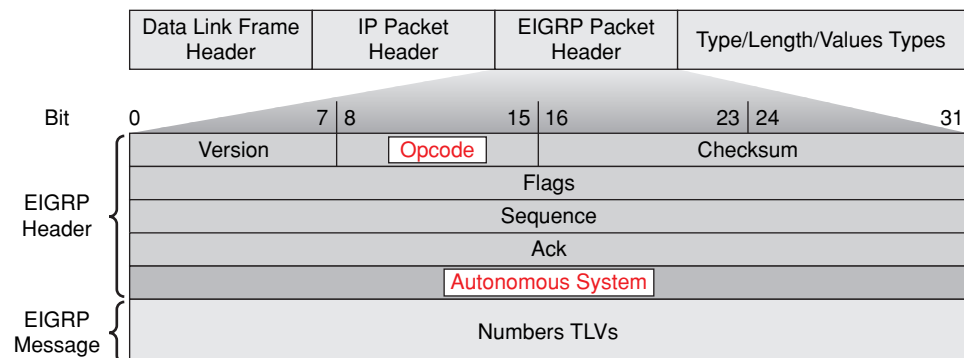
**Figure 9-1 Encapsulated EIGRP Message (Answer)**



The EIGRP packet **header** is included with every EIGRP packet, regardless of its type. In the IP packet header, the protocol field is set to **88** to indicate EIGRP, and the destination address is set to the multicast **224.0.0.10**.

Every EIGRP message includes the header, as shown in Figure 9-2. Fill in the missing field contents.

**Figure 9-2 EIGRP Packet Header (Answer)**



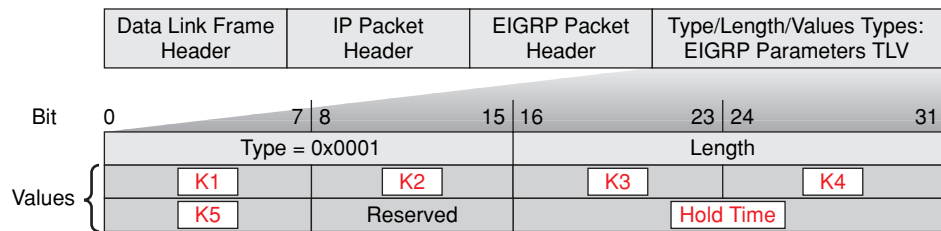
Important fields for our discussion include the Opcode field and the Autonomous System (AS) field. Opcode specifies the EIGRP packet type, which includes

- Update
- Query
- Reply
- Hello

The number in the AS field is used to track multiple instances of EIGRP.

Encapsulated in the EIGRP packet header is the TLV (Type/Length/Value), shown in Figure 9-3. Fill in the missing field contents.

**Figure 9-3 EIGRP Parameters TLV (Answer)**

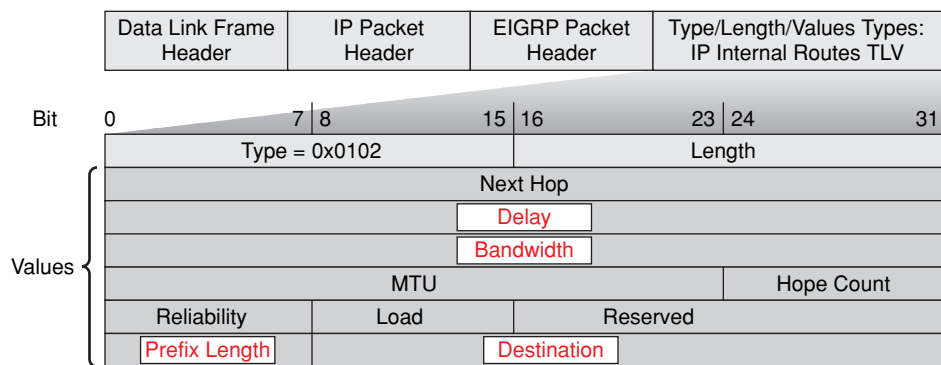


This EIGRP Parameters message includes the weights that EIGRP uses for its composite metric. By default, only bandwidth and delay are weighted. Both are equally weighted; therefore, the K1 field for bandwidth and the K3 field for delay are both set to 1. The other K values are set to 0.

The hold time is the amount of time the EIGRP neighbor receiving this message should wait before considering the advertising router to be down.

Figure 9-4 shows the IP Internal message that is used to advertise EIGRP routes within an autonomous system. Fill in the missing field contents.

**Figure 9-4 IP Internal Routes TLV (Answer)**



Important fields include the metric fields (Delay and Bandwidth), the subnet mask field (Prefix Length), and the Destination field.

Explain how the delay value is calculated.

Delay is calculated as the sum of delays from source to destination in units of 10 microseconds.

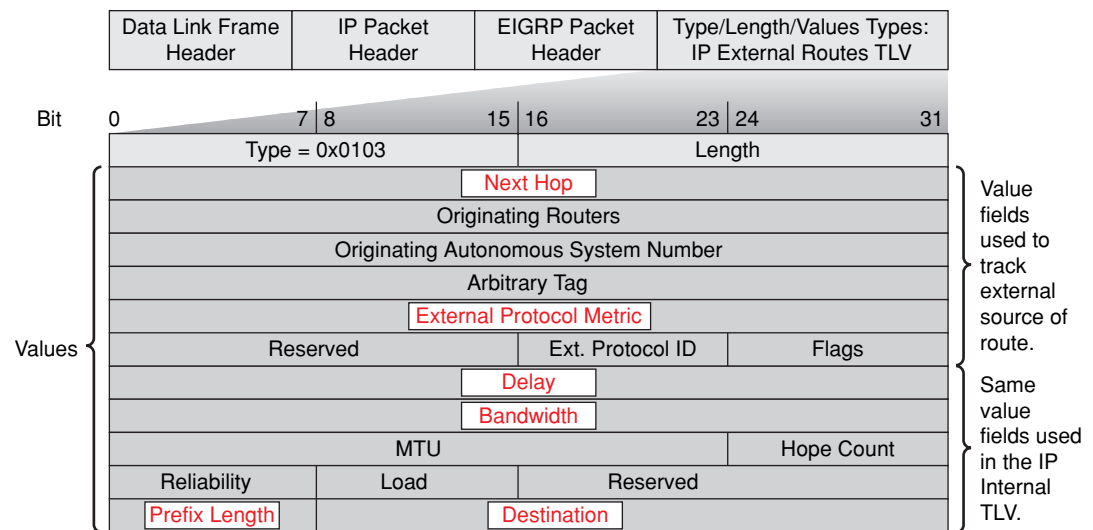
Explain how the bandwidth value is determined.

Bandwidth is the lowest configured bandwidth of any interface along the route.

The subnet mask is specified as the prefix length or the number of network bits in the subnet mask. For example, the subnet mask 255.255.255.0 has a prefix length of 24.

Figure 9-5 shows the IP External message that is used when external routes are imported into the EIGRP routing process. Notice that the bottom half of the IP External TLV includes all the fields used by the IP Internal TLV. Fill in the missing field contents.

**Figure 9-5 IP External Routes TLV (Answer)**



### Protocol-Dependent Modules (PDM)

EIGRP has the capability to route several different protocols, including IP, IPX, and AppleTalk, using protocol-dependent modules (PDM).

### RTP

Reliable Transport Protocol (RTP) is the protocol used by EIGRP for the delivery and reception of EIGRP packets. EIGRP was designed as a network layer independent routing protocol; therefore, RTP includes both reliable delivery and unreliable delivery of EIGRP packets, similar to TCP and UDP, respectively. Reliable RTP requires an acknowledgment to be returned by the receiver to the sender. An unreliable RTP packet does not require an acknowledgment.

RTP can send packets either as a unicast or a multicast. Multicast EIGRP packets use the reserved multicast address of 224.0.0.10.

### EIGRP Packet Types

EIGRP relies on different types of packets to maintain its tables and establish relationships with neighbor routers. Complete the missing elements below by filling in appropriate words or phrases. When encountered, circle whether the packet is reliable or unreliable and whether it is unicast or multicast.

### Hello packets:

- (Reliable/unreliable) (unicast/multicast) sent to the address 224.0.0.10 to discover and maintain neighbors; contains the router's neighbor table

- Default **Hello** interval depends on the bandwidth:
  - ≤ 1.544 Mbps = **60** sec. **Hello** interval (**180** hold time)
  - > 1.544 Mbps = **5** sec. **Hello** interval (**15** hold time)

**Update packets:** Sent (**reliably/unreliably**), there are 2 types:

- (**Unicast/multicast**) to new neighbor discovered; contains routing table
- (**Unicast/multicast**) to all neighbors when topology changes

**Query packets:** Queries are (**unicast/multicast**) (**reliably/unreliably**) during route recomputation, asking neighbors for a new successor to a lost route.

**Reply packets:** Neighbors (**unicast/multicast**) a reply to a query whether or not they have a route.

**Acknowledgment packets:** “Dataless” (**unicast/multicast**) packets that acknowledge the receipt of packets that were sent reliably. This type is actually a Hello packet with a nonzero value in the acknowledgment field.

### *Hello Protocol*

An EIGRP router assumes that as long as it is receiving Hello packets from a neighbor, the neighbor and its routes remain viable. **Hold time** tells the router the maximum time the router should wait to receive the next Hello before declaring that neighbor as **unreachable**. By default, this waiting period is **three** times the **Hello** interval, or **15** seconds on most networks and **180** seconds on networks with speeds of T1 or slower. If the time expires, EIGRP will declare the route as down and DUAL will search for a new path by sending out queries.

### *EIGRP Bounded Updates*

Unlike RIP, EIGRP does not send periodic updates. Instead, EIGRP sends its updates only when the metric for a route changes.

The term **partial** means that the update only includes information about the route changes.

The term **bounded** refers to the propagation of partial updates sent only to those routers that are affected by the change.

### *DUAL: An Introduction*

**Diffusing Update Algorithm** (DUAL) is the convergence algorithm used by EIGRP to calculate best routes and prevent routing loops.

The decision process for all route computations is done by the DUAL **Finite State Machine** (FSM). The DUAL FSM tracks all routes; uses its metric to select efficient, loop-free paths; and selects the routes with the least-cost path to insert into the routing table.

### *Administrative Distance*

EIGRP has a default administrative distance of **90** for internal routes and **170** for routes imported from an external source, such as default routes. EIGRP has a third AD value of **5** for summary routes.

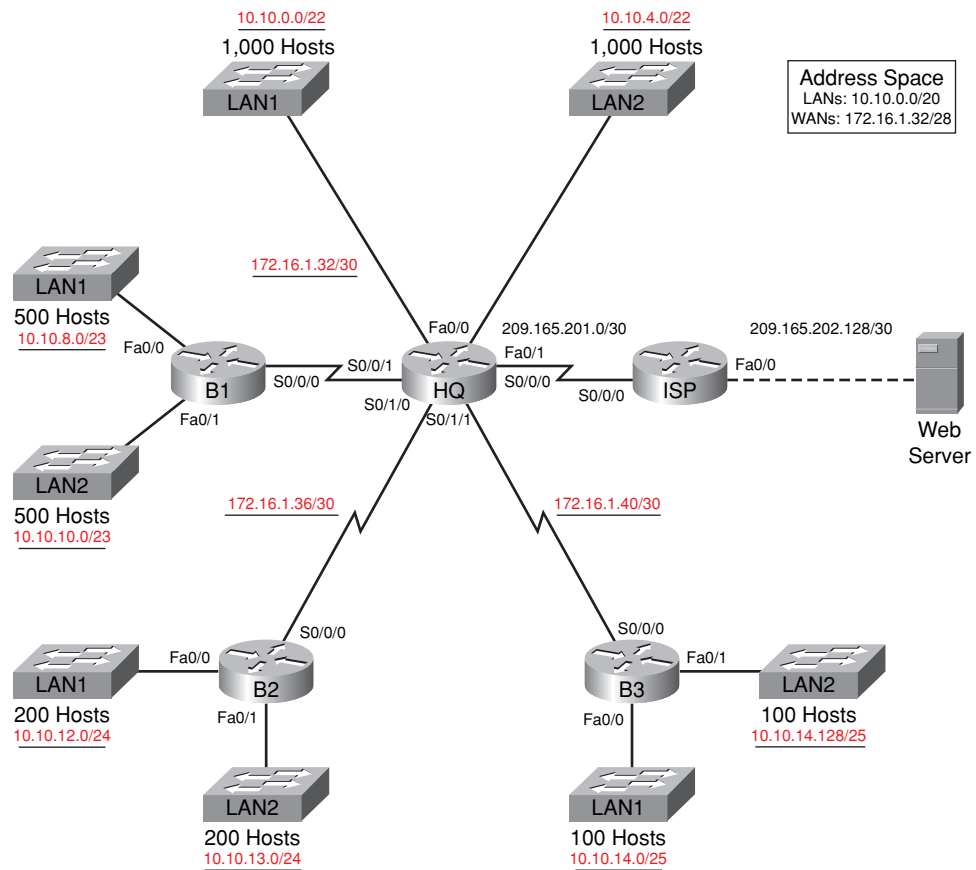
## **Basic EIGRP Configuration**

The following sections review the basics of EIGRP configuration. There are many similarities with the commands used in configuring other routing protocols such as RIP. In these sections of the Study Guide, you will design an addressing scheme and answer questions related to its implementation using EIGRP as the routing protocol.

## Documenting the Addressing Scheme

Refer to the topology shown in Figure 9-6. Using the 10.10.0.0/20 address space for LANs and the 172.16.1.32/28 address space for WANs, you will design an appropriate addressing scheme, which you will document in Table 9-2.

**Figure 9-6 EIGRP Study Guide Topology (Answer)**



**Table 9-2 Addressing Table for EIGRP Study Guide Topology**

Device	Interface	IP Address	Subnet Mask
HQ	Fa0/0	10.10.0.1	255.255.252.0
	Fa0/1	10.10.4.1	255.255.252.0
	S0/0/0	209.165.201.2	255.255.255.252
	S0/0/1	172.16.1.33	255.255.255.252
	S0/1/0	172.16.1.37	255.255.255.252
	S0/1/1	172.16.1.41	255.255.255.252

*continues*

**Table 9-2 Addressing Table for EIGRP Study Guide Topology** *continued*

Device	Interface	IP Address	Subnet Mask
B1	Fa0/0	10.10.8.1	255.255.254.0
	Fa0/1	10.10.10.1	255.255.254.0
	S0/0/0	172.16.1.34	255.255.255.252
B2	Fa0/0	10.10.12.1	255.255.255.0
	Fa0/1	10.10.13.1	255.255.255.0
	S0/0/0	172.16.1.38	255.255.255.252
B3	Fa0/0	10.10.14.1	255.255.255.128
	Fa0/1	10.10.14.129	255.255.255.128
	S0/0/0	172.16.1.42	255.255.255.252
ISP	Fa0/0	209.165.202.129	255.255.255.252
	S0/0/0	209.165.201.1	255.255.255.252
Web Server	NIC	209.165.202.130	255.255.255.252

## LAN Subnets

To begin your design, you will need to determine the subnets that you will use. To use the available address space most efficiently, start with your largest host requirement and work your way to the smallest host requirement. Starting with the LAN subnets, answer the following questions.

For HQ, begin with the 10.10.0.0 address as the subnet for FastEthernet 0/0. What subnet mask would you use to provide enough space for 1000 users while maximizing the number of subnets?

255.255.252.0 or /22

Starting with 10.10.0.0, contiguously assign subnets to the LANs on HQ. List the subnets here.

LAN	Subnet Address/CIDR
HQ LAN1	10.10.0.0/22
HQ LAN2	10.10.4.0/22

For B1, begin with 10.10.8.0 as the subnet for FastEthernet 0/0. What subnet mask would you use to provide enough space 500 users while maximizing the number of subnets?

255.255.254.0 or /23

Starting with 10.10.8.0, contiguously assign subnets to the LANs on B1. List the subnets here.

LAN	Subnet Address/CIDR
B1 LAN1	10.10.8.0/23
B1 LANs	10.10.10.0/23



For B2, begin with 10.10.12.0 as the subnet for FastEthernet 0/0. What subnet mask would you use to provide enough space 250 users while maximizing the number of subnets?

[255.255.255.0 or /24](#)

Starting with 10.10.12.0, contiguously assign subnets to the LANs on B2. List the subnets here.

LAN	Subnet Address/CIDR
B2 LAN1	10.10.12.0/24
B2 LANs	10.10.13.0/24

For B3, begin with 10.10.14.0 as the subnet for FastEthernet 0/0. What subnet mask would you use to provide enough space 100 users while maximizing the number of subnets?

[255.255.255.128 or /25](#)

Starting with 10.10.14.0, contiguously assign subnets to the LANs on B3. List the subnets here.

LAN	Subnet Address/CIDR
B3 LAN1	10.10.14.0/25
B3 LANs	10.10.14.128/25

Use your documentation of the LAN subnet address to label the LANs in the topology shown earlier in Figure 9-6. Use CIDR notation.

## WAN Subnets

For the WAN links, you have been assigned the 172.16.1.32/28 address space. Create subnets for the WANs between HQ and the Branch routers. Use Table 9-3 to document your WAN subnets.

**Table 9-3 WAN Subnets Between HQ and Branch Routers**

Subnet No.	Assign To	Subnet Address	Subnet Mask
0	B1/HQ WAN	172.16.1.32	255.255.255.252
1	B2/HQ WAN	172.16.1.36	255.255.255.252
2	B3/HQ WAN	172.16.1.40	255.255.255.252

Use your documentation of the WAN subnet addresses to label the LANS in the topology shown earlier in Figure 9-6. Use CIDR notation.

## Document Interface Addresses

Use Table 9-2 to document the IP addresses for all the interfaces. Use the following guidelines to ensure that your addresses will work with Packet Tracer Exercise 9-1.

1. Assign the first IP address for all LANs to the router interface.
2. Assign HQ the first IP address for all WAN links to Branch routers.



## Packet Tracer Exercise 9-1

Now you are ready to use Packet Tracer to apply your documented addressing scheme. Open file LSG02-0901.pka on the CD-ROM that accompanies this book to perform this exercise using Packet Tracer.

### Task 1: Basic Router Configuration

**Step 1.** ISP is already configured. Use the following guidelines to configure the host name, banner, enable secret password, and lines for HQ, B1, B2, and B3. Packet Tracer will grade only the host name configurations.

- To avoid incorrect grading, make sure that the router names are configured in ALL CAPS.
- Use the following text for the banner: **Authorized Access Only**.
- For the secret password, use **class**.
- For the console and Telnet lines, configure login access with the password **cisco**.

**Step 2.** Configure the interfaces according to the following guidelines.

- Use the IP address and subnet mask according to the addressing table in the “Documenting the Addressing Scheme” exercise.
- Configure a description for each interface (Packet Tracer will not grade this configuration).
- Configure clocking signals at 64000 bps where necessary.
- Activate the interfaces.

Your completion percentage should be 53%. If not, review the previous steps to see what part of the task you left incomplete.

**Step 3.** Save your configurations for H1, B1, B2, and B3.

After completing the basic configurations, be sure to test for connectivity with directly connected neighbors. Save your Packet Tracer file to use again in the next section. Save the file as LSG02-0901-task1.pkt.

## Configuring EIGRP as the Routing Protocol

By default, when using the **network** command and a classful network address such as 172.16.0.0, all interfaces on the router that belong to that classful network address will be enabled for EIGRP. However, for the topology shown in Figure 9-6, we only want to advertise the subnets that each router belongs to.

List the commands you will use to configure EIGRP on HQ, B1, B2, and B3. Be sure to summarize the LANs into one **network** command. The configuration for HQ is shown as an example.

HQ EIGRP routing configuration:

```
HQ(config)# router eigrp 1
HQ(config-router)# network 172.16.1.32 0.0.0.15
HQ(config-router)# network 10.10.0.0 0.0.7.255
```

B1 EIGRP routing configuration:

```
B1(config)# router eigrp 1
B1(config-router)# network 172.16.1.32 0.0.0.3
B1(config-router)# network 10.10.8.0 0.0.3.255
```

B2 EIGRP routing configuration:

```
B2(config)# router eigrp 1
B2(config-router)# network 172.16.1.36 0.0.0.3
B2(config-router)# network 10.10.12.0 0.0.1.255
```

B3 EIGRP routing configuration:

```
B3(config)# router eigrp 1
B3(config-router)# network 172.16.1.40 0.0.0.3
B3(config-router)# network 10.10.14.0 0.0.0.255
```

In addition to the **network** commands for each router, disable unnecessary EIGRP packets from being sent out interfaces that do not have an EIGRP neighbor. For example, HQ should neither send EIGRP Hello packets to ISP nor to the two LANs.

What command will disable unnecessary EIGRP packets from being sent out an interface? (Hint: The command for RIP is exactly the same.)

```
Router(config-route)# passive-interface interface
```

By default, EIGRP automatically summarizes routes at the major network boundary. Because the topology is discontinuous, you must disable this automatic summarization with the **no auto-summary** command, just as you did in RIPv2.

## Verifying EIGRP

Before any updates can be sent or received by EIGRP, routers must establish adjacencies with their neighbors. EIGRP routers establish adjacencies with neighbor routers by exchanging EIGRP Hello packets.

Use the **show ip eigrp neighbors** command to view the neighbor table and verify that EIGRP has established an adjacency with its neighbors. This command is useful for verifying and troubleshooting EIGRP. Example 9-1 shows the neighbor table for HQ.

**Example 9-1 EIGRP Neighbor Table for HQ**

```
HQ# show ip eigrp neighbors
IP-EIGRP neighbors for process 1
```

H	Address	Interface	Hold	Uptime	SRTT	RTO	Q	Seq
			(sec)		(ms)		Cnt	Num
0	172.16.1.38	Ser0/1/0	14	00:01:15	40	500	0	17
1	172.16.1.42	Ser0/1/1	14	00:01:15	40	500	0	17
2	172.16.1.34	Ser0/0/1	14	00:01:15	40	500	0	17

As with RIP, the **show ip protocols** command shown in Example 9-2 can be used to verify that EIGRP is enabled.

### Example 9-2 Verifying That EIGRP Is Enabled on HQ

```
HQ# show ip protocols
Routing Protocol is "eigrp 1 "
 Outgoing update filter list for all interfaces is not set
 Incoming update filter list for all interfaces is not set
 Default networks flagged in outgoing updates
 Default networks accepted from incoming updates
 EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
 EIGRP maximum hopcount 100
 EIGRP maximum metric variance 1
 Redistributing: eigrp 1
 Automatic network summarization is in effect
 Maximum path: 4
 Routing for Networks:
 172.16.1.32/28
 10.10.0.0/21
 Routing Information Sources:
 Gateway Distance Last Update
 172.16.1.38 90 6
 172.16.1.42 90 7
 172.16.1.34 90 49
 Distance: internal 90 external 170
```

Another way to verify that EIGRP and other functions of the router are configured properly is to examine the routing tables with the **show ip route** command. EIGRP routes are denoted in the routing table with a **D**, which stands for DUAL.

Example 9-3 shows partial output from the routing table for B1 with the Null0 routes highlighted.

### Example 9-3 B1 Routing Table with Null0 Routes

```
10.0.0.0/8 is variably subnetted, 9 subnets, 5 masks
D 10.0.0.0/8 is a summary, 00:01:50, Null0
D 10.10.0.0/22 [90/2172416] via 172.16.1.33, 00:01:45, Serial0/0/0
<remaining child routes omitted>
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
D 172.16.0.0/16 is a summary, 00:01:50, Null0
C 172.16.1.32/30 is directly connected, Serial0/0/0
<remaining child routes omitted>
```

Briefly explain the purpose of the Null0 route.

The 10.0.0.0/8 and 172.16.0.0/16 routes do not actually represent a path to reach the parent networks. If a packet does not match one of the level 2 child routes, it is sent to the Null0 interface. In other words, if the packet matches the level 1 parent—the classful network address—but none of the subnets, the packet is discarded.

Packet Tracer  
Activity

## Packet Tracer Exercise 9-1 (Continued)

Open your LSG02-0901-task1.pka saved version of this Packet Tracer Exercise. According to your answers to the questions in the “Configuring EIGRP as the Routing Protocol” exercise, complete the steps in Task 2.

### Task 2: Configure and Verify EIGRP Routing

- Step 1.** Configure EIGRP routing on HQ and the Branch routers (B1, B2, B3). Include the commands to disable automatic summarization and to stop unnecessary EIGRP updates.
- Step 2.** View the neighbor tables, protocol configuration, and routing tables for all routers. Answer the following questions.
1. How many EIGRP neighbors does HQ have? 3
  2. How many EIGRP neighbors do B1, B2, and B3 have? 1
  3. What are the values for K1 and K3? 1
  4. What are the internal distance and external distance for EIGRP? 90 and 170
  5. How many routes did HQ learn through EIGRP? 8

Your completion percentage should be 76%. If not, review the previous steps to see what part of the task you left incomplete.

After completing the routing configurations, save your Packet Tracer file to use again in the next section. Save the file as LSG02-0701-task2.pkt. Keep the file open to use for the next section.

## EIGRP Metric Calculation

Although EIGRP includes hop count in its routing updates, hop count is not used as part of the EIGRP composite metric. The following sections review the values of the EIGRP metric and describe how EIGRP performs the calculation to arrive at the metric displayed in the routing table.

### EIGRP Metric Concepts

List the values EIGRP uses in its composite metric to calculate the preferred path to a network.

- Bandwidth
- Delay
- Reliability
- Load

Record the formula used to calculate the *default* EIGRP composite metric.

Default metric = [K1\*bandwidth + K3\*delay] \* 256

What command do you use to verify the K values used by EIGRP?

show ip protocols

What command do you use to verify the actual values of the EIGRP metric?

show interface

The bandwidth metric is displayed in Kbit (kilobits). Most serial interfaces use the default value of 1,544,000 bps, which is the value for a T1 connection. The value might or might not reflect the actual physical bandwidth of the interface. If the actual bandwidth of the link differs from the default value, you should modify the value.

Delay is a measure of the time it takes for a packet to traverse a route. This metric is a static value and is expressed in microseconds.

Reliability is a measure of the probability that the link will fail or how often the link has experienced errors. Unlike delay, it is measured dynamically with a value between 0 and 255, with 1 being a minimally reliable link and 255 being 100 percent reliable. Reliability is calculated on a 5-minute weighted average to avoid the sudden impact of high (or low) error rates.

Load reflects the amount of traffic utilizing the link. It is measured dynamically with a value between 0 and 255. A lower value is more desirable because it indicates a less saturated link.

## Modifying the Bandwidth

On most serial links, the bandwidth metric will default to 1544 Kbits. This is the case with all the serial interfaces in Packet Tracer Exercise 9-1. However, notice in the chapter topology shown earlier in Figure 9-6 that the links between HQ and the Branch routers each have an actual bandwidth that is not the same as the default value on the interfaces.

Record the commands necessary on each router to change the bandwidth metric to match the actual bandwidth. Remember: HQ will have to modify the bandwidth on all interfaces connected to Branch routers.

HQ commands to change bandwidth:

```
HQ(config)# int s0/0/1
HQ(config-if)# bandwidth 768
HQ(config-if)# int s0/1/0
HQ(config-if)# bandwidth 512
HQ(config-if)# int s0/1/1
HQ(config-if)# bandwidth 384
```

B1 commands to change bandwidth:

```
B1(config)# int s0/0/0
B1(config-if)# bandwidth 768
```

B2 commands to change bandwidth:

```
B2(config)# int s0/0/0
B2(config-if)# bandwidth 512
```

B3 commands to change bandwidth:

```
B3(config)# int s0/0/0
```

```
B3(config-if)# bandwidth 384
```

Packet Tracer  
Activity

## Packet Tracer Exercise 9-1 (Continued)

Open your LSG02-0903-task2.pka saved version of this Packet Tracer Exercise. According to your answers to the questions in the “Modifying the Bandwidth” exercise, complete the steps in Task 3.

### Task 3: Modify the EIGRP Metric

**Step 1.** Modify the bandwidth on interfaces HQ shares with Branch routers.

**Step 2.** Modify the bandwidth on the interface B1 shares with HQ.

**Step 3.** Modify the bandwidth on the interface B2 shares with HQ.

**Step 4.** Modify the bandwidth on the interface B3 shares with HQ.

Your completion percentage should be 83%. If not, review the previous steps to see what part of the task you left incomplete.

## DUAL

The following sections review the concepts of how DUAL determines the best loop-free path and loop-free backup paths.

### DUAL Concepts Exercise

DUAL provides

- Loop-free paths
- Loop-free backup paths, which can be used immediately
- Fast convergence
- Minimum bandwidth usage with bounded updates

*Successor and Feasible Distance*

Briefly explain the term *successor*.

A successor is a neighboring router that is used for packet forwarding and is the least-cost route to the destination network.

Briefly explain what is meant by *feasible distance*.

Feasible distance (FD) is the lowest calculated metric to reach the destination network.

Examine the routing table for HQ in Example 9-4 and answer the questions that follow.

**Example 9-4 Feasible Distance and Successors in the HQ Routing Table**

```

HQ# show ip route
<output omitted>

Gateway of last resort is not set

 10.0.0.0/8 is variably subnetted, 9 subnets, 5 masks
D 10.0.0.0/8 is a summary, 00:31:59, Null0
C 10.10.0.0/22 is directly connected, FastEthernet0/0
C 10.10.4.0/22 is directly connected, FastEthernet0/1
D 10.10.8.0/23 [90/3847680] via 172.16.1.34, 00:04:30, Serial0/0/1
D 10.10.10.0/23 [90/3847680] via 172.16.1.34, 00:04:30, Serial0/0/1
D 10.10.12.0/24 [90/5514496] via 172.16.1.38, 00:04:25, Serial0/1/0
D 10.10.13.0/24 [90/5514496] via 172.16.1.38, 00:04:25, Serial0/1/0
D 10.10.14.0/25 [90/7181056] via 172.16.1.42, 00:04:25, Serial0/1/1
D 10.10.14.128/25 [90/7181056] via 172.16.1.42, 00:04:25, Serial0/1/1
 172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
D 172.16.0.0/16 is a summary, 00:31:59, Null0
C 172.16.1.32/30 is directly connected, Serial0/0/1
C 172.16.1.36/30 is directly connected, Serial0/1/0
C 172.16.1.40/30 is directly connected, Serial0/1/1
 209.165.201.0/30 is subnetted, 1 subnets
C 209.165.201.0 is directly connected, Serial0/0/0

```

What is the IP address of the successor for network 10.10.8.0/23? [172.16.1.34, which is B1](#)

What is the feasible distance to 10.10.8.0/23? [3847680](#)

What is the IP address of the successor for network 10.10.14.128/25? [172.16.1.42, which is B3](#)

What is the feasible distance to 10.10.14.128/25? [7181056](#)

What is the IP address of the successor for network 10.10.12.0/24? [172.16.1.38, which is B2](#)

What is the feasible distance to 10.10.12.0/24? [5514496](#)

*Feasible Successors, Feasibility Condition, and Reported Distance*

Briefly explain the term *feasible successor*.

A feasible successor is a backup path to other routers maintained in a separate table so that DUAL does not have to be recomputed when the successor becomes unavailable. A feasible successor satisfies the feasibility condition.



Briefly explain *feasibility condition*.

The feasibility condition (FC) is met when a neighbor's reported distance (RD) to a network is less than the local router's feasible distance to the same destination network.

Briefly explain *reported distance*.

The reported distance or advertised distance is simply an EIGRP neighbor's feasible distance to the same destination network. The reported distance is the metric that a router reports to a neighbor about its own cost to that network.

*Topology Table: Successor and Feasible Successor*

The successor, feasible distance, and any feasible successors with their reported distances are kept by a router in its EIGRP topology table or topology database. This table can be viewed using the **show ip eigrp topology** command, as shown in Example 9-5.

---

**Note:** The following table has been modified and does not completely relate to Packet Tracer Exercise 9-1.

---

#### Example 9-5 EIGRP Topology Table Command

```
Router# show ip eigrp topology
IP-EIGRP Topology Table for AS 1

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - Reply status

<output omitted>
P 10.10.12.0/24, 1 successors, FD is 5514496
 via 172.16.1.38 (5514496/28160), Serial0/1/0
 via 172.16.1.42 (7693056/2172416), Serial0/1/1
<output omitted>
P 10.10.14.128/25, 1 successors, FD is 6026496
 via 172.16.1.38 (6026496/2172416), Serial0/1/0
 via 172.16.1.42 (7181056/28160), Serial0/1/1
<output omitted>
```

The topology table lists all successors and feasible successors that DUAL has calculated to destination networks. Use the partial output in Example 9-5 to answer the following questions.

For route 10.10.12.0/24 . . .

What is the IP address of the successor? [172.16.1.38](#)

What is the reported distance of the successor? [28160](#)

What is the feasible distance of the successor? [5514496](#)

What is the IP address of the feasible successor? [172.16.1.42](#)

What is the reported distance of the feasible successor? [2172416](#)

What is the feasible distance of the feasible successor? [7693056](#)

Notice that the reported distance of the feasible successor is less than the feasible distance of the successor.

For route 10.10.14.128/25 . . .

What is the IP address of the successor? [172.16.1.38](#)

What is the reported distance of the successor? [2172416](#)

What is the feasible distance of the successor? [6026496](#)

What is the IP address of the feasible successor? [172.16.1.42](#)

What is the reported distance of the feasible successor? [28160](#)

What is the feasible distance of the feasible successor? [7181056](#)

Notice that the reported distance of the feasible successor is less than the feasible distance of the successor.

What happens if an EIGRP router doesn't have a feasible successor in the topology table and the router loses connection to the successor?

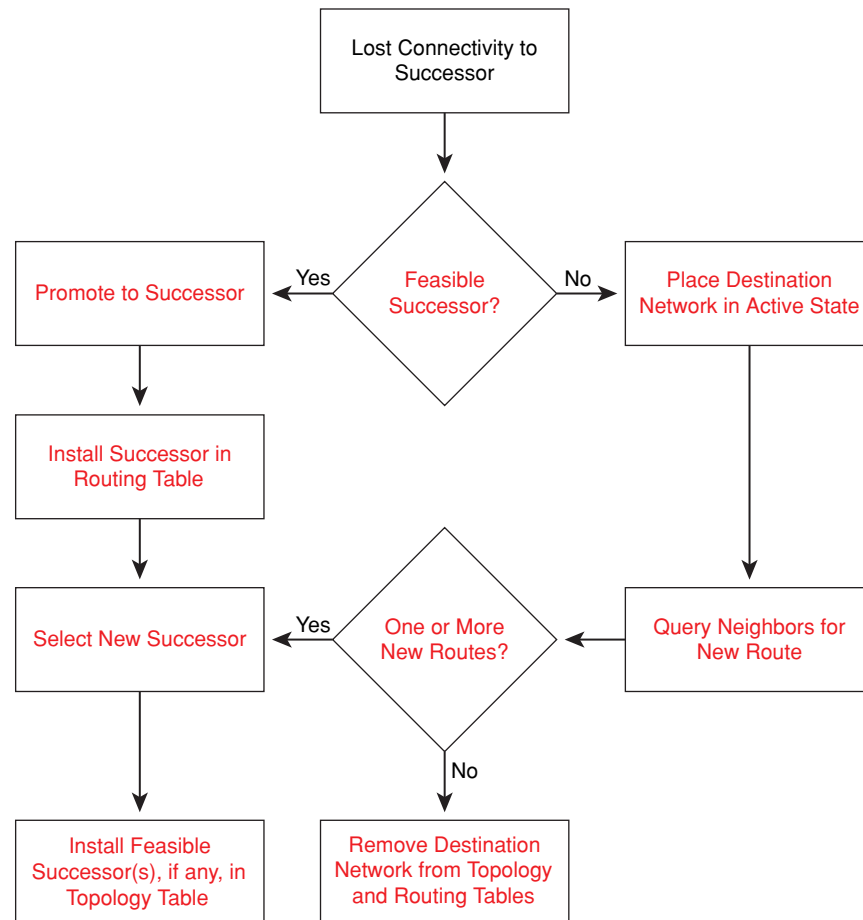
[DUAL must be recomputed and neighbors queried for a possible backup route.](#)

## DUAL FSM Completion Exercise

A Finite State Machine (FSM) is an abstract machine, not a mechanical device with moving parts. FSMs define a set of possible states that something can go through, what events cause those states, and what events result from those states. Designers use FSMs to describe how a device, computer program, or routing algorithm will react to a set of input events.

Figure 9-7 is a simplified flow chart of DUAL's FSM. Fill in the flow chart with the states EIGRP moves through when it loses connectivity with a successor. The flow chart should serve as a visual study aid to help you remember how DUAL converges on new routes.

Figure 9-7 DUAL FSM Flow Chart (Answer)



## More EIGRP Configurations

The following sections review the commands used for EIGRP route summarization, default route propagation, and fine tuning.

### Manual Summarization Exercise

EIGRP can be configured to summarize routes. Record the command syntax to manually configure an EIGRP route summary.

```
Router(config-if)# ip summary-address eigrp as-number network-address subnet-mask
```

In the chapter topology shown earlier in Figure 9-6, HQ and the Branch routers can manually summarize the LANs that are directly connected to each router.

Because HQ has three EIGRP neighbors, the EIGRP manual summarization is configured on each of the serial interfaces shared with Branch routers. Record the commands necessary to configure HQ to advertise its LANs in one route.

```
HQ(config)# interface s0/0/1
```

```
HQ(config-if)# ip summary-address eigrp 1 10.10.0.0 255.255.248.0
```

```
HQ(config-if)# interface s0/1/0
```

```
HQ(config-if)# ip summary-address eigrp 1 10.10.0.0 255.255.248.0
HQ(config-if)# interface s0/1/1
HQ(config-if)# ip summary-address eigrp 1 10.10.0.0 255.255.248.0
```

Record the commands necessary to configure B1 to advertise its LANs in one route.

```
B1(config)# interface s0/0/0
B1(config-if)# ip summary-address eigrp 1 10.10.8.0 255.255.252.0
```

Record the commands necessary to configure B2 to advertise its LANs in one route.

```
B2(config)# interface s0/0/0
B2(config-if)# ip summary-address eigrp 1 10.10.12.0 255.255.254.0
```

Record the commands necessary to configure B3 to advertise its LANs in one route.

```
B3(config)# interface s0/0/0
B3(config-if)# ip summary-address eigrp 1 10.10.14.0 255.255.255.0
```

## EIGRP Default Route Exercise

Using a static route to 0.0.0.0/0 as a default route is not routing protocol dependent. The “quad zero” static default route can be used with any currently supported routing protocols. The static default route is usually configured on the router that has a connection to a network outside the EIGRP routing domain, for example, to an Internet service provider (ISP).

Record the command to configure HQ with a default route. Use the exit interface argument.

```
HQ(config)# ip route 0.0.0.0 0.0.0.0 serial0/0/0
```

EIGRP requires the use of the **redistribute static** command to include this static default route with its EIGRP routing updates. Unfortunately, Packet Tracer v4.1 does not support this command. So, you will need to configure default routes on B1, B2, and B3 using the exit interface argument. Record the commands you will use to configure these default routes on the Branch routers.

```
B1(config)# ip route 0.0.0.0 0.0.0.0 serial0/0/0
B2(config)# ip route 0.0.0.0 0.0.0.0 serial0/0/0
B3(config)# ip route 0.0.0.0 0.0.0.0 serial0/0/0
```

## Fine-Tuning EIGRP Exercise

The last two topics of this chapter review two fundamental ways to fine-tune EIGRP operations. First, we will discuss EIGRP bandwidth utilization. Next, we will discuss how to change the default Hello and hold time values.

### *EIGRP Bandwidth Utilization*

By default, EIGRP will use only up to **50** percent of the bandwidth of an interface for EIGRP information. This prevents the EIGRP process from overutilizing a link and not allowing enough bandwidth for the routing of normal traffic.

The **ip bandwidth-percent eigrp** command can be used to configure the percentage of bandwidth that can be used by EIGRP on an interface. Record the full syntax for this command.

```
Router(config-if)# ip bandwidth-percent eigrp as-number percent
```

This command uses the amount of configured bandwidth (or the default bandwidth) when calculating the percent that EIGRP can use.

#### *Configuring Hello Intervals and Hold Times*

Hello intervals and hold times are configurable on a per-interface basis and do not have to match with other EIGRP routers to establish adjacencies.

Record the command to configure a different Hello interval.

```
Router(config-if)# ip hello-interval eigrp as-number seconds
```

If you change the Hello interval, make sure that you also change the hold time to a value equal to or greater than the Hello interval. Otherwise, neighbor adjacency will go down after the hold time expires and before the next Hello interval.

Record the command to configure a different hold time.

```
Router(config-if)# ip hold-time eigrp as-number seconds
```



## Packet Tracer Exercise 9-1 (Continued)

Open your LSG02-0903-task3.pka saved version of this Packet Tracer Exercise. According to your answers to the questions in the “Manual Summarization Exercise” section, complete the steps in Tasks 4–8.

### Task 4: Configure Manual Summarization

- Step 1.** Configure HQ with a summary route that advertises its LANs in one route. Don't forget to enter this command on all necessary interfaces.
- Step 2.** Configure B1 with a summary route that advertises its LANs in one route.
- Step 3.** Configure B2 with a summary route that advertises its LANs in one route.
- Step 4.** Configure B3 with a summary route that advertises its LANs in one route.

Your completion percentage should be 89%. If not, review the previous steps to see what part of the task you left incomplete.

---

**Note:** Packet Tracer v4.1 does not accurately simulate the manual summary route. Although you configured it, the routing tables will still show all the subnets.

---

### Task 5: Configure Default Routing

According to your answers to the questions in the “EIGRP Default Route Exercise” section, configure HQ, B1, B2, and B3 with a default route.

Your completion percentage should be 93%. If not, review the previous steps to see what part of the task you left incomplete.

### Task 6: Configure Hello Intervals

Configure HQ, B1, B2, and B3 to use a 60-second Hello interval.

Your completion percentage should be 100%. If not, review the previous steps to see what part of the task you left incomplete.

### Task 7: Verify Connectivity

All routers should have end-to-end connectivity. Pinging from any source to any destination should be successful. You can also click **Check Results** and then click the **Connectivity Tests** tab to see whether all the connectivity tests are successful.

### Task 8: Save the Packet Tracer File

Save your Packet Tracer file as LSG02-0901-end.pka.

## Labs and Activities

### Command Reference

In the table that follows, record the command, *including the correct router prompt*, that fits the description. Fill in any blanks with the appropriate missing information.

Command	Description
Router(config)# <b>router eigrp 100</b>	Turns on the EIGRP process. 100 is the <a href="#">autonomous system</a> (AS) number, which can be a number between <a href="#">1</a> and <a href="#">65535</a> . All routers in the same AS must use the same AS number.
Router(config-router)# <b>network 192.168.1.32 0.0.0.31</b>	Enables EIGRP routing for the 192.168.1.32/27 subnet.
Router# <b>show ip eigrp neighbors</b>	Displays a neighbor table.
Router# <b>show interface serial 0/0/0</b>	Verifies the current EIGRP metrics used for the Serial 0/0/0 interface.
Router(config-if)# <b>bandwidth 128</b>	Changes the bandwidth of an interface to 128 kbps.
Router# <b>show ip eigrp topology</b>	Displays the topology table. This command will show you where your feasible successors are.
Router# <b>show ip eigrp topology all-links</b>	Displays the topology table as well as routes that do not match the feasibility condition.
Router# <b>debug eigrp fsm</b>	Displays events/actions related to the DUAL FSM.
Router(config)# <b>ip classless</b>	Enables classless routing behavior.
Router(config-router)# <b>no auto-summary</b>	Turns off the automatic summarization of networks at <a href="#">classful</a> boundaries.
Router(config-router)# <b>eigrp log-neighbor-changes</b>	Logs any changes to an EIGRP neighbor adjacency.
Router(config-if)# <b>ip summary-address eigrp 100 10.10.0.0 255.255.0.0</b>	Enables manual summarization on this specific interface for the 10.10.0.0/16 address space.
Router(config-router)# <b>redistribute static</b>	Configures EIGRP to include static routes in EIGRP routing updates.



### Lab 9-1: Basic EIGRP Configuration (9.6.1)

Upon completion of this lab, you will be able to

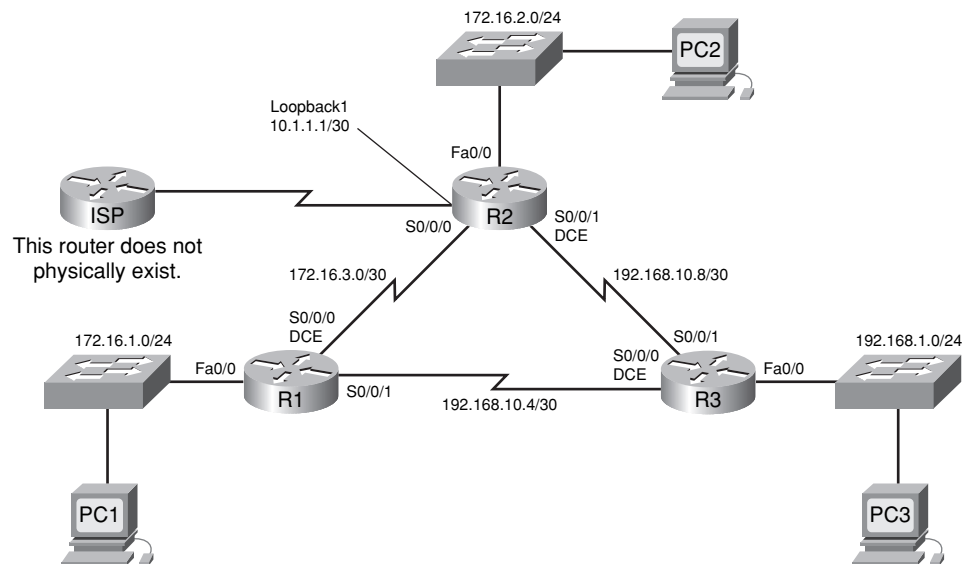
- Cable a network according to the topology diagram in Figure 9-8
- Erase the startup configuration and reload a router to the default state

- Perform basic configuration tasks on a router
- Configure and activate interfaces
- Configure EIGRP routing on all routers
- Verify EIGRP routing using **show** commands
- Disable automatic summarization
- Configure manual summarization
- Configure a static default route
- Propagate default routes to EIGRP neighbors
- Document the EIGRP configuration

### Scenario

In this lab activity, you will learn how to configure the routing protocol EIGRP using the network shown in the topology diagram in Figure 9-8. As you can see in Table 9-4, a loopback address will be used on the R2 router to simulate a connection to an ISP, where all traffic that is not destined for the local network will be sent. Some segments of the network have been subnetted using VLSM. EIGRP is a classless routing protocol that can be used to provide subnet mask information in the routing updates. This will allow VLSM subnet information to be propagated throughout the network.

**Figure 9-8 Topology Diagram for Lab 9-1**



**Table 9-4 Addressing Table for Lab 9-1**

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.16.1.1	255.255.255.0	—
	S0/0/0	172.16.3.1	255.255.255.252	—
	S0/0/1	192.168.10.5	255.255.255.252	—



Device	Interface	IP Address	Subnet Mask	Default Gateway
R2	Fa0/0	172.16.2.1	255.255.255.0	—
	S0/0/0	172.16.3.2	255.255.255.252	—
	S0/0/1	192.168.10.9	255.255.255.252	—
	Lo1	10.1.1.1	255.255.255.252	—
R3	Fa0/0	192.168.1.1	255.255.255.0	—
	S0/0/0	192.168.10.6	255.255.255.252	—
	S0/0/1	192.168.10.10	255.255.255.252	—
PC1	NIC	172.16.1.10	255.255.255.0	172.16.1.1
PC2	NIC	172.16.2.10	255.255.255.0	172.16.2.1
PC3	NIC	192.168.1.10	255.255.255.0	192.168.1.1

## Task 1: Prepare the Network

**Step 1.** Cable a network that is similar to the one in the topology diagram of Figure 9-8.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

**Step 2.** Clear any existing configurations on the routers.

## Task 2: Perform Basic Router Configurations

Perform basic configuration of the R1, R2, and R3 routers according to the following guidelines:

- Configure the router host name.
- Disable Domain Name System (DNS) lookup.
- Configure an EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for console connections.
- Configure a password for VTY connections.

## Task 3: Configure and Activate Serial and Ethernet Addresses

**Step 1.** Configure the interfaces on the R1, R2, and R3 routers.

Configure the interfaces with the IP addresses from Table 9-4.

**Step 2.** Verify IP addressing and interfaces.

Use the **show ip interface brief** command to verify that the IP addressing is correct and that the interfaces are active.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

**Step 3.** Configure the Ethernet interfaces of PC1, PC2, and PC3.

Configure these interfaces with the IP addresses and default gateways from Table 9-4.

## Task 4: Configure EIGRP on the R1 Router

**Step 1.** Enable EIGRP.

Use the **router eigrp** command in global configuration mode to enable EIGRP on the R1 router. Enter a process ID of 1 for the *autonomous-system* parameter:

```
R1(config)# router eigrp 1
R1(config-router)#
```

**Step 2.** Configure the classful network 172.16.0.0.

When you are in the Router EIGRP configuration submode, configure the classful network 172.16.0.0 to be included in the EIGRP updates that are sent out of R1:

```
R1(config-router)# network 172.16.0.0
R1(config-router)#
```

The router will begin to send EIGRP update messages out each interface belonging to the 172.16.0.0 network. EIGRP updates will be sent out of the FastEthernet 0/0 and Serial 0/0/0 interfaces because they are both on subnets of the 172.16.0.0 network.

**Step 3.** Configure the router to advertise the 192.168.10.4/30 network attached to the Serial 0/0/1 interface.

Use the *wildcard-mask* option with the **network** command to advertise only the subnet and not the entire 192.168.10.0 classful network:

```
R1(config-router)# network 192.168.10.4 0.0.0.3
R1(config-router)#
```

---

**Note:** Think of a wildcard mask as the inverse of a subnet mask. The inverse of the subnet mask 255.255.255.252 is 0.0.0.3. To calculate the inverse of the subnet mask, subtract the subnet mask from 255.255.255.255:

```
 255.255.255.255
- 255.255.255.252 Subtract the subnet mask

 0. 0. 0. 3 Wildcard mask
```

---

When you are finished with the EIGRP configuration for R1, return to privileged EXEC mode and save the current configuration to NVRAM:

```
R1(config-router)# end
%SYS-5-CONFIGI: Configured from console by console
R1#
```

## Task 5: Configure EIGRP on the R2 and R3 Routers

**Step 1.** Enable EIGRP routing on the R2 router using the **router eigrp** command. Use a process ID of 1.

```
R2(config)# router eigrp 1
R2(config-router)#
```

**Step 2.** Use the classful address 172.16.0.0 to include the network for the FastEthernet 0/0 interface.

```
R2(config-router)# network 172.16.0.0
R2(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.3.1 (Serial0/0/0) is up: new adjacency
```

Notice that DUAL sends a notification message to the console stating that a neighbor relationship with another EIGRP router has been established.

What is the IP address of the EIGRP neighbor router?

[172.16.3.1](#)

What interface on the R2 router is the neighbor adjacent to?

[Serial0/0/0](#)

**Step 3.** Configure the R2 router to advertise the 192.168.10.8/30 network attached to the Serial 0/0/1 interface.

1. Use the *wildcard-mask* option with the **network** command to advertise only the subnet and not the entire 192.168.10.0 classful network.

2. When you are finished, return to privileged EXEC mode:

```
R2(config-router)# network 192.168.10.8 0.0.0.3
R2(config-router)# end
```

```
%SYS-5-CONFIGI: Configured from console by console
```

```
R2#
```

**Step 4.** Configure EIGRP on the R3 router using the **router eigrp** and **network** commands:

1. Use a process ID of 1.
2. Use the classful network address for the network attached to the FastEthernet 0/0 interface.
3. Include the wildcard masks for the subnets attached to the Serial 0/0/0 and Serial 0/0/1 interfaces.
4. When you are finished, return to privileged EXEC mode.

```
R3(config)# router eigrp 1
R3(config-router)# network 192.168.1.0
R3(config-router)# network 192.168.10.4 0.0.0.3
```

```

R3(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.5 (Serial0/0/0) is up: new adjacency
R3(config-router)# network 192.168.10.8 0.0.0.3
R3(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.9 (Serial0/0/1) is up: new adjacency
R3(config-router)# end
%SYS-5-CONFIGI: Configured from console by console
R3#

```

Notice that when the networks for the serial links from R3 to R1 and R3 to R2 are added to the EIGRP configuration, DUAL sends a notification message to the console stating that a neighbor relationship with another EIGRP router has been established.

## Task 6: Verify EIGRP Operation

### Step 1. View neighbors.

On the R1 router, use the **show ip eigrp neighbors** command to view the neighbor table and verify that EIGRP has established an adjacency with the R2 and R3 routers. You should be able to see the IP address of each adjacent router and the interface that R1 uses to reach that EIGRP neighbor.

```

R1# show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H Address Interface Hold Uptime SRTT RT0 Q Seq
 (sec) (ms) Cnt Num
0 172.16.3.2 Ser0/0/0 10 00:36:51 40 500 0 13
1 192.168.10.6 Ser0/0/1 11 00:26:51 40 500 0 4
R1#

```

### Step 2. View the routing protocol information.

On the R1 router, use the **show ip protocols** command to view information about the routing protocol operation. Notice that the information that was configured in Task 5, such as protocol, process ID, and networks, is shown in the output. The IP addresses of the adjacent neighbors are also shown:

```

R1# show ip protocols
Routing Protocol is "eigrp 1"
 Outgoing update filter list for all interfaces is not set
 Incoming update filter list for all interfaces is not set
 Default networks flagged in outgoing updates
 Default networks accepted from incoming updates
 EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
 EIGRP maximum hopcount 100
 EIGRP maximum metric variance 1

```

```

Redistributing: eigrp 1
Automatic network summarization is in effect
Automatic address summarization:
Maximum path: 4
Routing for Networks:
 172.16.0.0
 192.168.10.4/30
Routing Information Sources:
 Gateway Distance Last Update
 172.16.3.2 90 4811399
 192.168.10.6 90 5411677
Distance: internal 90 external 170

```

Notice that the output specifies the process ID used by EIGRP. Remember, the process ID must be the same on all routers for EIGRP to establish neighbor adjacencies and share routing information.

## Task 7: Examine EIGRP Routes in the Routing Tables

**Step 1.** View the routing table on the R1 router.

EIGRP routes are denoted in the routing table with a **D**, which stands for DUAL (Diffusing Update Algorithm), which is the routing algorithm used by EIGRP.

```
R1# show ip route
```

```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
 area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

```

```
Gateway of last resort is not set
```

```

 172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D 172.16.0.0/16 is a summary, 01:16:19, Null0
C 172.16.1.0/24 is directly connected, FastEthernet0/0
D 172.16.2.0/24 [90/2172416] via 172.16.3.2, 01:16:20, Serial0/0/0
C 172.16.3.0/30 is directly connected, Serial0/0/0
D 192.168.1.0/24 [90/2172416] via 192.168.10.6, 01:06:18, Serial0/0/1
 192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D 192.168.10.0/24 is a summary, 01:06:07, Null0
C 192.168.10.4/30 is directly connected, Serial0/0/1
D 192.168.10.8/30 [90/2681856] via 192.168.10.6, 01:06:07, Serial0/0/1
R1#

```

Notice that the 172.16.0.0/16 parent network is variably subnetted with three child routes using either a /24 or /30 mask. Also notice that EIGRP has automatically included a summary route to Null0 for the 172.16.0.0/16 network. The 172.16.0.0/16 route does not actually

represent a path to reach the parent network, 172.16.0.0/16. If a packet destined for 172.16.0.0/16 does not match one of the level 2 child routes, it is sent to the Null0 interface:

```

172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D 172.16.0.0/16 is a summary, 01:16:19, Null0
C 172.16.1.0/24 is directly connected, FastEthernet0/0
D 172.16.2.0/24 [90/2172416] via 172.16.3.2, 01:16:20, Serial0/0/0
C 172.16.3.0/30 is directly connected, Serial0/0/0

```

The 192.168.10.0/24 network is also variably subnetted and includes a Null0 route:

```

192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D 192.168.10.0/24 is a summary, 01:06:07, Null0
C 192.168.10.4/30 is directly connected, Serial0/0/1
D 192.168.10.8/30 [90/2681856] via 192.168.10.6, 01:06:07,
Serial0/0/1

```

**Step 2.** View the routing table on the R3 router.

The routing table for R3 shows that both R1 and R2 are automatically summarizing the 172.16.0.0/16 network and sending it as a single routing update. Because of automatic summarization, R1 and R2 are not propagating the individual subnets. Because R3 is getting two equal-cost routes for 172.16.0.0/16 from both R1 and R2, both routes are included in the routing table.

```
R3# show ip route
```

```
<output omitted>
```

```

D 172.16.0.0/16 [90/2172416] via 192.168.10.5, 01:15:35, Serial0/0/0
 [90/2172416] via 192.168.10.9, 01:15:22, Serial0/0/1
C 192.168.1.0/24 is directly connected, FastEthernet0/0
 192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D 192.168.10.0/24 is a summary, 01:15:22, Null0
C 192.168.10.4/30 is directly connected, Serial0/0/0
C 192.168.10.8/30 is directly connected, Serial0/0/1
R3#

```

## Task 8: Configure EIGRP Metrics

**Step 1.** View the EIGRP metric information.

Use the **show ip interface** command to view the EIGRP metric information for the Serial 0/0/0 interface on the R1 router. Notice the values that are shown for the bandwidth, delay, reliability, and load.

```
R1# show interface serial0/0/0
```

```

Serial0/0/0 is up, line protocol is up (connected)
 Hardware is HD64570
 Internet address is 172.16.3.1/30
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
 Encapsulation HDLC, loopback not set, keepalive set (10 sec)

```

```
<output omitted>
```

**Step 2.** Modify the bandwidth of the serial interfaces.

On most serial links, the bandwidth metric will default to 1544 Kbits. If this is not the actual bandwidth of the serial link, the bandwidth will need to be changed so that the EIGRP metric can be calculated correctly.

For this lab, the link between R1 and R2 will be configured with a bandwidth of 64 kbps, and the link between R2 and R3 will be configured with a bandwidth of 1024 kbps. Use the **bandwidth** command to modify the bandwidth of the serial interfaces of each router:

```
R1(config)# interface serial0/0/0
R1(config-if)# bandwidth 64

R2(config)# interface serial0/0/0
R2(config-if)# bandwidth 64
R2(config)# interface serial0/0/1
R2(config-if)# bandwidth 1024

R3(config)# interface serial0/0/1
R3(config-if)# bandwidth 1024
```

**Note:** The **bandwidth** command modifies only the bandwidth metric used by routing protocols, not the physical bandwidth of the link.

**Step 3.** Verify the bandwidth modifications.

Use the **show ip interface** command to verify that the bandwidth value of each link has been changed.

```
R1# show interface serial0/0/0
Serial0/0/0 is up, line protocol is up (connected)
 Hardware is HD64570
 Internet address is 172.16.3.1/30
 MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
 Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

*<output omitted>*

```
R2# show interface serial0/0/0
Serial0/0/0 is up, line protocol is up (connected)
 Hardware is HD64570
 Internet address is 172.16.3.2/30
 MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
 Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

*<output omitted>*

```
R3# show interface serial0/0/1
Serial0/0/1 is up, line protocol is up (connected)
 Hardware is HD64570
 Internet address is 192.168.10.9/30
 MTU 1500 bytes, BW 1024 Kbit, DLY 20000 usec, rely 255/255, load 1/255
 Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

*<output omitted>*

---

**Note:** Use the interface configuration command **no bandwidth** to return the bandwidth to its default value.

---

## Task 9: Examine Successors and Feasible Distances

**Step 1.** Examine the successors and feasible distances in the routing table on R2.

```
R2# show ip route
```

```
<output omitted>
```

```
 10.0.0.0/30 is subnetted, 1 subnets
C 10.1.1.0 is directly connected, Loopback1
 172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D 172.16.0.0/16 is a summary, 00:00:52, Null0
D 172.16.1.0/24 [90/40514560] via 172.16.3.1, 00:00:52, Serial0/0/0
C 172.16.2.0/24 is directly connected, FastEthernet0/0
C 172.16.3.0/30 is directly connected, Serial0/0/0
D 192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:11, Serial0/0/1
 192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D 192.168.10.0/24 is a summary, 00:00:11, Null0
D 192.168.10.4/30 [90/3523840] via 192.168.10.10, 00:00:11,
Serial0/0/1
C 192.168.10.8/30 is directly connected, Serial0/0/1
```

**Step 2.** Answer the following questions.

What is the best path to PC1?

[172.16.1.0/24 \[90/40514560\] via 172.16.3.1, 00:00:52, Serial0/0/0](#)

A successor is a neighboring router that is currently being used for packet forwarding. A successor is the least-cost route to the destination network. The IP address of a successor is shown in a routing table entry right after the word *via*.

What is the IP address and name of the successor router in this route?

[172.16.3.1, R1](#)

Feasible distance (FD) is the lowest calculated metric to reach that destination. FD is the metric listed in the routing table entry as the second number inside the brackets.

What is the feasible distance to the network that PC1 is on?

[40514560](#)



## Task 10: Determine Whether R1 Is a Feasible Successor for the Route from R2 to the 192.168.1.0 Network

A feasible successor is a neighbor who has a viable backup path to the same network as the successor. To be a feasible successor, R1 must satisfy the feasibility condition. The feasibility condition (FC) is met when a neighbor's reported distance (RD) to a network is less than the local router's feasible distance to the same destination network.

**Step 1.** Examine the routing table on R1.

```
R1# show ip route
```

```
<output omitted>
```

```

 172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D 172.16.0.0/16 is a summary, 00:42:59, Null0
C 172.16.1.0/24 is directly connected, FastEthernet0/0
D 172.16.2.0/24 [90/40514560] via 172.16.3.2, 00:43:00, Serial0/0/0
C 172.16.3.0/30 is directly connected, Serial0/0/0
D 192.168.1.0/24 [90/2172416] via 192.168.10.6, 00:42:26, Serial0/0/1
 192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D 192.168.10.0/24 is a summary, 00:42:20, Null0
C 192.168.10.4/30 is directly connected, Serial0/0/1
D 192.168.10.8/30 [90/3523840] via 192.168.10.6, 00:42:20,
 Serial0/0/1

```

What is the feasible distance to the 192.168.1.0 network?

2172416

**Step 2.** Examine the routing table on R2.

```
R2# show ip route
```

```
<output omitted>
```

```

10.0.0.0/30 is subnetted, 1 subnets
C 10.1.1.0 is directly connected, Loopback1
 172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D 172.16.0.0/16 is a summary, 00:00:52, Null0
D 172.16.1.0/24 [90/40514560] via 172.16.3.1, 00:00:52, Serial0/0/0
C 172.16.2.0/24 is directly connected, FastEthernet0/0
C 172.16.3.0/30 is directly connected, Serial0/0/0
D 192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:11, Serial0/0/1
 192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D 192.168.10.0/24 is a summary, 00:00:11, Null0
D 192.168.10.4/30 [90/3523840] via 192.168.10.10, 00:00:11,
 Serial0/0/1
C 192.168.10.8/30 is directly connected, Serial0/0/1

```

What is the feasible distance to the 192.168.1.0 network?

3014400

Would R2 consider R1 to be a feasible successor to the 192.168.1.0 network? yes

## Task 11: Examine the EIGRP Topology Table

**Step 1.** View the EIGRP topology table.

Use the **show ip eigrp topology** command to view the EIGRP topology table on R2:

```
R2# show ip eigrp topology
```

```
IP-EIGRP Topology Table for AS 1
```

```
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - Reply status
```

```
P 172.16.2.0/24, 1 successors, FD is 28160
 via Connected, FastEthernet0/0
P 172.16.3.0/30, 1 successors, FD is 40512000
 via Connected, Serial0/0/0
P 192.168.10.8/30, 1 successors, FD is 3011840
 via Connected, Serial0/0/1
P 172.16.0.0/16, 1 successors, FD is 28160
 via Summary (28160/0), Null0
P 192.168.10.0/24, 1 successors, FD is 3011840
 via Summary (3011840/0), Null0
P 172.16.1.0/24, 1 successors, FD is 40514560
 via 172.16.3.1 (40514560/28160), Serial0/0/0
P 192.168.1.0/24, 1 successors, FD is 3014400
 via 192.168.10.10 (3014400/28160), Serial0/0/1
 via 172.16.3.1 (41026560/2172416), Serial0/0/0
P 192.168.10.4/30, 1 successors, FD is 3523840
 via 192.168.10.10 (3523840/2169856), Serial0/0/1
```

**Step 2.** View detailed EIGRP topology information.

Use the *network* parameter of the **show ip eigrp topology** command to view detailed EIGRP topology information for the 192.16.1.0 network.

```
R2# show ip eigrp topology 192.168.1.0
```

```
IP-EIGRP (AS 1): Topology entry for 192.168.1.0/24
```

```
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 3014400
```

```
Routing Descriptor Blocks:
```

```
192.168.10.10 (Serial0/0/1), from 192.168.10.10, Send flag is 0x0
```

```
Composite metric is (3014400/28160), Route is Internal
```

```
Vector metric:
```

```
Minimum bandwidth is 1024 Kbit
```

```
Total delay is 20100 microseconds
```

```
Reliability is 255/255
```

```
Load is 1/255
```

```
Minimum MTU is 1500
```

```
Hop count is 1
```

```
172.16.3.1 (Serial0/0/0), from 172.16.3.1, Send flag is 0x0
```

```
Composite metric is (41026560/2172416), Route is Internal
```

```
Vector metric:
```

```

Minimum bandwidth is 64 Kbit
Total delay is 40100 microseconds
Reliability is 255/255
Load is 1/255
Minimum MTU is 1500
Hop count is 2

```

How many successors are there for this network? 1

What is the feasible distance to this network? 3014400

What is the IP address of the feasible successor? 172.16.3.1

What is the reported distance for 192.168.1.0 from the feasible successor? 2172416

What would be the feasible distance to 192.168.1.0 if R1 became the successor? 41026560

## Task 12: Disable EIGRP Automatic Summarization

**Step 1.** Examine the routing table of the R3 router.

Notice that R3 is not receiving individual routes for the 172.16.1.0/24, 172.16.2.0/24, and 172.16.3.0/24 subnets. Instead, the routing table only has a summary route to the classful network address of 172.16.0.0/16 through the R1 router. This will cause packets that are destined for the 172.16.2.0/24 network to be sent through the R1 router instead of being sent straight to the R2 router:

R3# **show ip route**

*<output omitted>*

```

D 172.16.0.0/16 [90/2172416] via 192.168.10.5, 01:21:54, Serial0/0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
 192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D 192.168.10.0/24 is a summary, 01:21:47, Null0
C 192.168.10.4/30 is directly connected, Serial0/0/0
C 192.168.10.8/30 is directly connected, Serial0/0/1

```

Why is the R1 router (192.168.10.5) the only successor for the route to the 172.16.0.0/16 network?

The R1 router has a better metric (feasible distance) to 172.16.0.0/16. The feasible distance for the path to the R1 router is better because the bandwidth for this path is higher than the path through the R2 router.

**Step 2.** Examine the EIGRP topology table on R3.

Notice that the reported distance from R2 is higher than the feasible distance from R1:

```

R3# show ip eigrp topology
IP-EIGRP Topology Table for AS 1

```

```

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - Reply status

```

```

P 192.168.1.0/24, 1 successors, FD is 28160
 via Connected, FastEthernet0/0
P 192.168.10.4/30, 1 successors, FD is 2169856
 via Connected, Serial0/0/0
P 192.168.10.0/24, 1 successors, FD is 2169856
 via Summary (2169856/0), Null0
P 172.16.0.0/16, 1 successors, FD is 2172416
 via 192.168.10.5 (2172416/28160), Serial0/0/0
 via 192.168.10.9 (3014400/28160), Serial0/0/1
P 192.168.10.8/30, 1 successors, FD is 3011840
 via Connected, Serial0/0/1

```

- Step 3.** Disable automatic summarization on all three routers with the **no auto-summary** command.

```

R1(config)# router eigrp 1
R1(config-router)# no auto-summary
R2(config)# router eigrp 1
R2(config-router)# no auto-summary
R3(config)# router eigrp 1
R3(config-router)# no auto-summary

```

- Step 4.** View the routing table on R1 again.

Notice that individual routes for the 172.16.1.0/24, 172.16.2.0/24, and 172.16.3.0/24 subnets are now present, and the summary Null route is no longer listed:

```
R3# show ip route
```

```
<output omitted>
```

```

 172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D 172.16.1.0/24 [90/2172416] via 192.168.10.5, 00:02:37, Serial0/0/0
D 172.16.2.0/24 [90/3014400] via 192.168.10.9, 00:02:39, Serial0/0/1
D 172.16.3.0/30 [90/41024000] via 192.168.10.9, 00:02:39, Serial0/0/1
 [90/41024000] via 192.168.10.5, 00:02:37,
Serial0/0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
 192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C 192.168.10.4/30 is directly connected, Serial0/0/0
C 192.168.10.8/30 is directly connected, Serial0/0/1

```

## Task 13: Configure Manual Summarization

- Step 1.** Add loopback addresses to the R3 router.

Add two loopback addresses, 192.168.2.1/24 and 192.168.3.1/24, to the R3 router. These virtual interfaces will be used to represent networks to be manually summarized along with the 192.168.1.0/24 LAN:

```
R3(config)# interface loopback1
```

```
%LINK-5-CHANGED: Interface Loopback1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
```

```
R3(config-if)# ip address 192.168.2.1 255.255.255.0
R3(config-if)# interface loopback2
```

```
%LINK-5-CHANGED: Interface Loopback2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2, changed state to
up
R3(config-if)# ip address 192.168.3.1 255.255.255.0
```

**Step 2.** Add the 192.168.2.0 and 192.168.3.0 networks to the EIGRP configuration on R3.

```
R3(config)# router eigrp 1
R3(config-router)# network 192.168.2.0
R3(config-router)# network 192.168.3.0
```

**Step 3.** Verify the new routes.

View the routing table on the R1 router to verify that the new routes are being sent out in the EIGRP updates sent by R3.

```
R1# show ip route
```

```
<output omitted>
```

```

 172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C 172.16.1.0/24 is directly connected, FastEthernet0/0
D 172.16.2.0/24 [90/3526400] via 192.168.10.6, 00:15:07, Serial0/0/1
C 172.16.3.0/30 is directly connected, Serial0/0/0
D 192.168.1.0/24 [90/2172416] via 192.168.10.6, 00:15:07, Serial0/0/1
D 192.168.2.0/24 [90/2297856] via 192.168.10.6, 00:01:07, Serial0/0/1
D 192.168.3.0/24 [90/2297856] via 192.168.10.6, 00:00:57, Serial0/0/1
 192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C 192.168.10.4/30 is directly connected, Serial0/0/1
D 192.168.10.8/30 [90/3523840] via 192.168.10.6, 00:15:07,
Serial0/0/1
```

**Step 4.** Apply manual summarization to the outbound interfaces.

The routes to the 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24 networks can be summarized in the single network 192.168.0.0/22. Use the **ip summary-address eigrp as-number network-address subnet-mask** command to configure manual summarization on each of the outbound interfaces connected to EIGRP neighbors:

```
R3(config)# interface serial0/0/0
R3(config-if)# ip summary-address eigrp 1 192.168.0.0 255.255.252.0
R3(config-if)# interface serial0/0/1
R3(config-if)# ip summary-address eigrp 1 192.168.0.0 255.255.252.0
```

**Step 5.** Verify the summary route.

View the routing table on the R1 router to verify that the summary route is being sent out in the EIGRP updates sent by R3.

```
R1# show ip route
```

```
<output omitted>
```

```

172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C 172.16.1.0/24 is directly connected, FastEthernet0/0
D 172.16.2.0/24 [90/3526400] via 192.168.10.6, 00:15:07, Serial0/0/1
C 172.16.3.0/30 is directly connected, Serial0/0/0
D 192.168.0.0/22 [90/2172416] via 192.168.10.6, 00:01:11, Serial0/0/1
 192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C 192.168.10.4/30 is directly connected, Serial0/0/1
D 192.168.10.8/30 [90/3523840] via 192.168.10.6, 00:15:07,
Serial0/0/1

```

## Task 14: Configure and Distribute a Static Default Route

**Step 1.** Configure a static default route on the R2 router.

Use the loopback address that has been configured to simulate a link to an ISP as the exit interface:

```
R2(config)# ip route 0.0.0.0 0.0.0.0 loopback1
```

**Step 2.** Include the static route in EIGRP updates.

Use the **redistribute static** command to include the static route in the EIGRP updates that are sent from the R2 router:

```
R2(config)# router eigrp 1
R2(config-router)# redistribute static
```

**Step 3.** Verify the static default route.

View the routing table on the R1 router to verify that the static default route is being redistributed through EIGRP.

```
R1# show ip route
```

```
<output omitted>
```

```
Gateway of last resort is 192.168.10.6 to network 0.0.0.0
```

```

192.168.10.0/30 is subnetted, 2 subnets
C 192.168.10.4 is directly connected, Serial0/0/1
D 192.168.10.8 [90/3523840] via 192.168.10.6, 01:06:01, Serial0/0/1
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C 172.16.1.0/24 is directly connected, FastEthernet0/0
D 172.16.2.0/24 [90/3526400] via 192.168.10.6, 01:05:39, Serial0/0/1
C 172.16.3.0/30 is directly connected, Serial0/0/0
D*EX 0.0.0.0/0 [170/3651840] via 192.168.10.6, 00:02:14, Serial0/0/1
D 192.168.0.0/22 [90/2172416] via 192.168.10.6, 01:05:38, Serial0/0/1

```

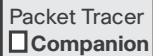
## Task 15: Documentation

On each router, capture the following command output to a text (.txt) file and save for future reference:

- **show running-config**
- **show ip route**
- **show ip interface brief**
- **show ip protocols**

## Task 16: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.



## Packet Tracer Companion: Basic EIGRP Configuration (9.6.1)

You can now open the file LSG02-Lab961.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment.



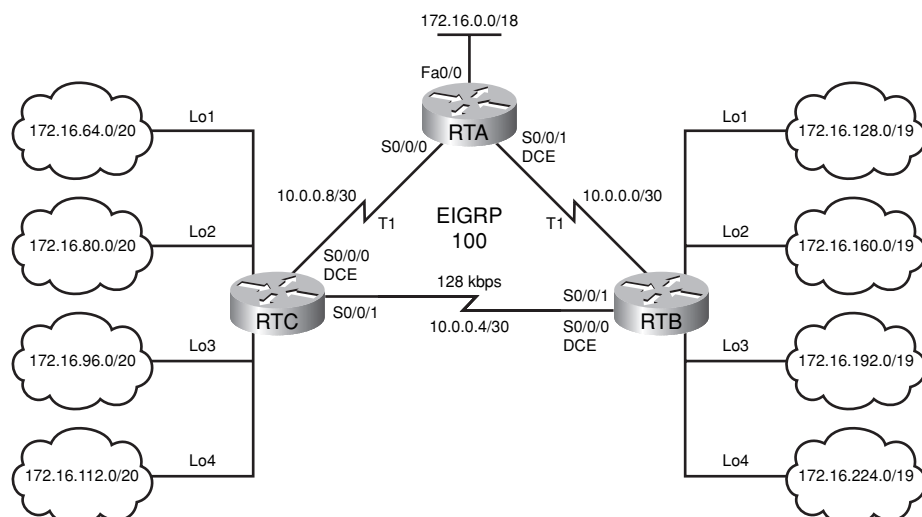
## Lab 9-2: Comprehensive EIGRP Configuration

Upon completion of this lab, you will be able to

- Configure EIGRP routing
- Configure bandwidth and turn off automatic summarization
- Configure manual summarization

Figure 9-9 shows the topology diagram for this lab and Table 9-5 provides the interface, IP address, and subnet mask information for the networking devices in this lab.

**Figure 9-9** Topology Diagram for Lab 9-2



**Table 9-5 Addressing Table for Lab 9-2**

Device	Interface	IP Address	Subnet Mask
RTA	S0/0/1	10.0.0.1	255.255.255.252
	S0/0/0	10.0.0.10	255.255.255.252
	Fa0/0	172.16.0.1	255.255.192.0
RTB	S0/0/1	10.0.0.2	255.255.255.252
	S0/0/0	10.0.0.5	255.255.255.252
	Lo1	172.16.128.1	255.255.224.0
	Lo2	172.16.160.1	255.255.224.0
	Lo3	172.16.192.1	255.255.224.0
RTC	S0/0/1	10.0.0.6	255.255.255.252
	S0/0/0	10.0.0.9	255.255.255.252
	Lo1	172.16.64.1	255.255.240.0
	Lo2	172.16.80.1	255.255.240.0
	Lo3	172.16.96.1	255.255.240.0
	Lo4	172.16.112.1	255.255.240.0

## Task 1: Cable the Topology and Basic Configurations

**Step 1.** Cable the topology as shown in Figure 9-9. If data communications equipment/data terminal equipment (DCE/DTE) connections and interfaces are different than shown in Figure 9-9 and the table, relabel the figure to match your connections.

**Step 2.** Configure the routers as follows.

- Configure the router host name.
- Disable DNS lookup.
- Configure an EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for console connections.
- Configure a password for VTY connections.

**Step 3.** The following is a basic configuration for RTA.

```
Router(config)# hostname RTA
RTA(config)# ip subnet-zero
RTA(config)# no ip domain-lookup
RTA(config)# ip host RTC 10.0.0.9 10.0.0.6
RTA(config)# ip host RTB 10.0.0.2 10.0.0.5
RTA(config)# banner motd &
!!!AUTHORIZED ACCESS ONLY!!!&
```



```

RTA(config)# line con 0
RTA(config-line)# exec-timeout 30 0
RTA(config-line)# password cisco
RTA(config-line)# logging synchronous
RTA(config-line)# login
RTA(config-line)# ine aux 0
RTA(config-line)# exec-timeout 30 0
RTA(config-line)# password cisco
RTA(config-line)# logging synchronous
RTA(config-line)# login
RTA(config-line)# line vty 0 4
RTA(config-line)# exec-timeout 30 0
RTA(config-line)# password cisco
RTA(config-line)# logging synchronous
RTA(config-line)# login
RTA(config-line)# end
RTA# copy run start

```

---

**Instructor note:** This basic configuration can be used on all three routers with changes to the host name and the host table. At this level in their studies, your students should be able to do this with little or no help from you.

---

## Task 2: Configure Interfaces and EIGRP Routing

**Step 1.** Use Table 9-5 and the topology shown in Figure 9-9 to configure each router with the correct interface addresses. The interface configuration for RTA is as follows.

```

RTA(config)# interface FastEthernet0/0
RTA(config-if)# description Link to RTA LAN
RTA(config-if)# ip address 172.16.0.1 255.255.192.0
RTA(config-if)# no shutdown
RTA(config-if)# interface Serial0/0/0
RTA(config-if)# description Link to RTC
RTA(config-if)# ip address 10.0.0.10 255.255.255.252
RTA(config-if)# clockrate 64000
RTA(config-if)# no shutdown
RTA(config-if)# interface Serial0/0/1
RTA(config-if)# description Link to RTB
RTA(config-if)# ip address 10.0.0.1 255.255.255.252
RTA(config-if)# clockrate 64000
RTA(config-if)# no shutdown

```

**RTB:**

```

RTB(config)# interface Loopback1
RTB(config-if)# ip address 172.16.128.1 255.255.224.0
RTB(config-if)# interface Loopback2
RTB(config-if)# ip address 172.16.160.1 255.255.224.0
RTB(config-if)# interface Loopback3
RTB(config-if)# ip address 172.16.192.1 255.255.224.0
RTB(config-if)# interface Loopback4

```

```
RTB(config-if)# ip address 172.16.224.1 255.255.224.0
RTB(config-if)# interface Serial0/0/0
RTB(config-if)# description Link to RTC
RTB(config-if)# ip address 10.0.0.5 255.255.255.252
RTB(config-if)# clockrate 64000
RTB(config-if)# no shutdown
RTB(config-if)# interface Serial0/0/1
RTB(config-if)# description Link to RTA
RTB(config-if)# ip address 10.0.0.2 255.255.255.252
RTB(config-if)# no shutdown
```

RTC:

```
RTC(config)# interface Loopback1
RTC(config-if)# ip address 172.16.64.1 255.255.240.0
RTC(config-if)# interface Loopback2
RTC(config-if)# ip address 172.16.80.1 255.255.240.0
RTC(config-if)# interface Loopback3
RTC(config-if)# ip address 172.16.96.1 255.255.240.0
RTC(config-if)# interface Loopback4
RTC(config-if)# ip address 172.16.112.1 255.255.240.0
RTC(config-if)# interface Serial0/0/0
RTC(config-if)# description Link to RTA
RTC(config-if)# ip address 10.0.0.9 255.255.255.252
RTC(config-if)# no shutdown
RTC(config-if)# interface Serial0/0/1
RTC(config-if)# description Link to RTB
RTC(config-if)# ip address 10.0.0.6 255.255.255.252
RTC(config-if)# no shutdown
```

- Step 2.** Configure each router with EIGRP routing. The configuration for RTA follows. All routers have the same basic EIGRP configuration.

```
RTA(config)# router eigrp 100
RTA(config-router)# network 10.0.0.0
RTA(config-router)# network 172.16.0.0
```

### Task 3: Configure Bandwidth and Automatic Summarization

- Step 1.** According to the topology shown in Figure 9-9, RTB and RTC are connected with a 128-kbps link. Enter the commands on both routers necessary to adjust the default bandwidth to match the actual speed.

```
RTB(config)# interface Serial0/0/0
RTB(config-if)# bandwidth 128
```

```
RTC(config)# interface Serial0/0/1
RTC(config-if)# bandwidth 128
```

**Step 2.** Display the routing table on RTA.

```
RTA# show ip route
(output omitted)
Gateway of last resort is not set

 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D 172.16.0.0/16 is a summary, 00:23:16, Null0
C 172.16.0.0/18 is directly connected, FastEthernet0/0
 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D 10.0.0.0/8 is a summary, 00:23:20, Null0
C 10.0.0.0/30 is directly connected, Serial0/0/1
```

**Step 3.** Notice that RTA does not have routes to the simulated LANs on RTB and RTC. Enter the command to disable automatic summarization on all three routers.

Each router should have the **no auto-summary** command configured within the EIGRP routing process.

## Task 4: Configure Manual Summarization

**Step 1.** Display the routing table on RTA.

```
RTA# show ip route
(output omitted)
Gateway of last resort is not set

 172.16.0.0/16 is variably subnetted, 9 subnets, 3 masks
D 172.16.160.0/19 [90/2297856] via 10.0.0.2, 00:00:16, Serial0/0/1
D 172.16.128.0/19 [90/2297856] via 10.0.0.2, 00:00:16, Serial0/0/1
D 172.16.224.0/19 [90/2297856] via 10.0.0.2, 00:00:16, Serial0/0/1
D 172.16.192.0/19 [90/2297856] via 10.0.0.2, 00:00:16, Serial0/0/1
C 172.16.0.0/18 is directly connected, FastEthernet0/0
D 172.16.112.0/20 [90/2297856] via 10.0.0.9, 00:00:29, Serial0/0/0
D 172.16.96.0/20 [90/2297856] via 10.0.0.9, 00:00:30, Serial0/0/0
D 172.16.80.0/20 [90/2297856] via 10.0.0.9, 00:00:30, Serial0/0/0
D 172.16.64.0/20 [90/2297856] via 10.0.0.9, 00:00:30, Serial0/0/0
 10.0.0.0/30 is subnetted, 3 subnets
C 10.0.0.8 is directly connected, Serial0/0/0
C 10.0.0.0 is directly connected, Serial0/0/1
D 10.0.0.4 [90/21024000] via 10.0.0.9, 00:00:30, Serial0/0/0
 [90/21024000] via 10.0.0.2, 00:00:30, Serial0/0/1
```

**Step 2.** Notice that RTA has 12 routes. Some of these routes can be summarized to reduce the size of the routing table. On RTB and RTC, enter the command to summarize the simulated LANs into one summary route.

The simulated LANs on RTB share the same bit pattern for the first 21 bits of the network prefix 172.16.128.0.

The simulated LANs on RTC share the same bit pattern for the first 18 bits of the network prefix 172.16.64.0.

What command would you configure on both serial interfaces for RTB?

```
RTB(config-if)# ip summary-address eigrp 100 172.16.128.0 255.255.128.0
```

What command would you configure on both serial interfaces for RTC?

```
RTC(config-if)# ip summary-address eigrp 100 172.16.64.0 255.255.192.0
```

**Step 3.** Display the routing table for RTA. You should only have six routes.

```
RTA# show ip route
```

```
(output omitted)
```

```
Gateway of last resort is not set
```

```

 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D 172.16.128.0/17 [90/2297856] via 10.0.0.2, 01:36:05, Serial0/0/1
C 172.16.0.0/18 is directly connected, FastEthernet0/0
D 172.16.64.0/18 [90/2297856] via 10.0.0.9, 01:38:11, Serial0/0/0
 10.0.0.0/30 is subnetted, 3 subnets
C 10.0.0.8 is directly connected, Serial0/0/0
C 10.0.0.0 is directly connected, Serial0/0/1
D 10.0.0.4 [90/21024000] via 10.0.0.9, 01:36:05, Serial0/0/0
 [90/21024000] via 10.0.0.2, 01:36:05, Serial0/0/1

```



## Lab 9-3: Challenge EIGRP Configuration (9.6.2)

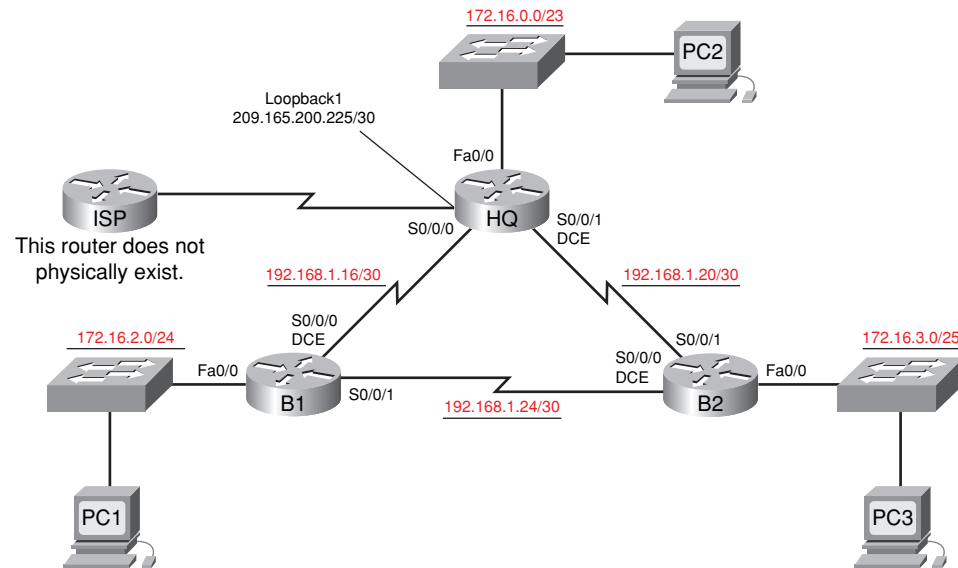
Upon completion of this lab, you will be able to

- Create an efficient VLSM design given requirements
- Assign appropriate addresses to interfaces and document
- Cable a network according to the topology diagram in Figure 9-10
- Erase the startup configuration and reload a router to the default state
- Configure routers including EIGRP
- Configure and propagate a static default route
- Verify EIGRP operation
- Test and verify full connectivity
- Reflect on and document the network implementation

### Scenario

In this lab activity, you will be given a network address that must be subnetted using VLSM to complete the addressing of the network shown in the topology diagram in Figure 9-10. A combination of EIGRP routing and static routing will be required so that hosts on networks that are not directly connected will be able to communicate with each other. EIGRP must be configured so that all IP traffic takes the shortest path to the destination address.

Figure 9-10 Topology Diagram for Lab 9-3 (Answer)



## Task 1: Subnet the Address Space

**Step 1.** Examine the network requirements.

The addressing for the network has the following requirements:

- The 172.16.0.0/16 network must be subnetted to provide addresses for the three LANs.
  - The HQ LAN will require 500 addresses.
  - The BRANCH1 LAN will require 200 addresses.
  - The BRANCH2 LAN will require 100 addresses.
- The loopback address representing the link between the HQ router and the ISP will use the 209.165.200.224/30 network.
- The 192.168.1.16/28 address space must be subnetted to obtain the addresses for the links between the three routers.

**Step 2.** Consider the following questions when creating your network design.

How many subnets need to be created from the 172.16.0.0/16 network? 3

How many total IP addresses are required from the 172.16.0.0/16 network? 800

What subnet mask will be used for the HQ LAN subnet? 255.255.254.0 or /23

What is the maximum number of host addresses that could be used on this subnet? 510

What subnet mask will be used for the BRANCH1 LAN subnet? 255.255.255.0 or /24

What is the maximum number of host addresses that could be used on this subnet? 254

What subnet mask will be used for the BRANCH2 LAN subnet? 255.255.255.128 or /25

What is the maximum number of host addresses that could be used on this subnet? 126

What subnet mask will be used for the links between the three routers? [255.255.255.252](#) or [/30](#)

What is the maximum number of host addresses that could be used on each of these subnets? [2](#)

**Step 3.** Assign subnetwork addresses to the topology diagram.

1. Assign subnet 0 of the 172.16.0.0/16 network to the HQ LAN subnet. What is the network address of this subnet? [172.16.0.0/23](#)
2. Assign the next available address space of the 172.16.0.0/16 network to the BRANCH1 LAN subnet. What is the network address of this subnet? [172.16.2.0/24](#)
3. Assign the next available address space of the 172.16.0.0/16 network to the BRANCH2 LAN subnet. What is the network address of this subnet? [172.16.3.0/25](#)
4. Assign subnet 0 of the 192.168.1.16/28 network to the link between the HQ and BRANCH1 routers. What is the network address of this subnet? [192.168.1.16 /30](#)
5. Assign subnet 1 of the 192.168.1.16/28 network to the link between the HQ and BRANCH2 routers. What is the network address of this subnet? [192.168.1.20 /30](#)
6. Assign subnet 2 of the 192.168.1.16/28 network to the link between the BRANCH1 and BRANCH2 routers. What is the network address of this subnet? [192.168.1.24 /30](#)

## Task 2: Determine Interface Addresses

**Step 1.** Assign appropriate addresses to the device interfaces.

- Assign the first valid host address of the 209.165.200.224/30 network to the loopback interface on the HQ router.
- Assign the first valid IP address of the HQ LAN network to the LAN interface of the HQ router.
- Assign the last valid IP address of the HQ LAN network to PC2.
- Assign the first valid IP address of the BRANCH1 LAN network to the LAN interface of the BRANCH1 router.
- Assign the last valid IP address of the BRANCH1 LAN network to PC1.
- Assign the first valid IP address of the BRANCH2 LAN network to the LAN interface of the BRANCH2 router.
- Assign the last valid IP address of the BRANCH2 LAN network to PC3.
- Assign the first valid IP address of the HQ-to-BRANCH1 link network to the Serial 0/0/0 interface of the HQ router.
- Assign the last valid IP address of the HQ-to-BRANCH1 link network to the Serial 0/0/0 interface of the Branch router.
- Assign the first valid IP address of the HQ-to-BRANCH2 link network to the Serial 0/0/1 interface of the HQ router.
- Assign the last valid IP address of the HQ-to-BRANCH2 link network to the Serial 0/0/1 interface of the Branch router.

- Assign the first valid IP address of the BRANCH1-to-BRANCH2 link network to the Serial 0/0/1 interface of the BRANCH1 router.
- Assign the last valid IP address of the BRANCH1-to-BRANCH2 link network to the Serial 0/0/0 interface of the BRANCH2 router.

**Step 2.** Document the addresses to be used in Table 9-6.

**Table 9-6 Addressing Table for Lab 9-3**

Device Gateway	Interface	IP Address	Subnet Mask	Default
HQ	Fa0/0	172.16.0.1	255.255.254.0	—
	S0/0/0	192.168.1.17	255.255.255.252	—
	S0/0/1	192.168.1.21	255.255.255.252	—
	Lo1	209.165.200.225	255.255.255.252	—
BRANCH1	Fa0/0	172.16.2.1	255.255.255.0	—
	S0/0/0	192.168.1.18	255.255.255.252	—
	S0/0/1	192.168.1.25	255.255.255.252	—
BRANCH2	Fa0/0	172.16.3.1	255.255.255.128	—
	S0/0/0	192.168.1.26	255.255.255.252	—
	S0/0/1	192.168.1.22	255.255.255.252	—
PC1	NIC	172.16.2.254	255.255.255.0	172.16.2.1
PC2	NIC	172.16.1.254	255.255.254.0	172.16.0.1
PC3	NIC	172.16.3.126	255.255.255.128	172.16.3.1

### Task 3: Prepare the Network

**Step 1.** Cable a network that is similar to the one in the topology diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

**Step 2.** Clear any existing configurations on the routers.

### Task 4: Perform Basic Router Configurations

Perform basic configuration of the BRANCH1, BRANCH2, HQ, and ISP routers according to the following guidelines:

- Configure the router host name.
- Disable DNS lookup.
- Configure an EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for console connections.

- Configure a password for VTY connections.
- Synchronize unsolicited messages and debug output with solicited output and prompts for the console and virtual terminal lines.
- Configure an EXEC timeout of 15 minutes.

## Task 5: Configure and Activate Serial and Ethernet Addresses

**Step 1.** Configure the interfaces on the HQ, BRANCH1, and BRANCH2 routers.

Configure the interfaces with the IP addresses from Table 9-6.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

**Step 2.** Configure the Ethernet interfaces.

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses from Table 9-6.

## Task 6: Verify Connectivity to the Next-Hop Device

You should *not* have connectivity between end devices yet. However, you can test connectivity between two routers and between an end device and its default gateway.

**Step 1.** Verify connectivity of routers.

Verify that the HQ, BRANCH1, and BRANCH2 routers can ping each of the neighboring routers across the WAN links.

**Step 2.** Verify connectivity of PCs.

Verify that PC1, PC2, and PC3 can ping their respective default gateways.

## Task 7: Configure EIGRP Routing on the BRANCH1 Router

Consider the networks that need to be included in the EIGRP updates that are sent out by the BRANCH1 router.

What directly connected networks are present in the BRANCH1 routing table?

172.16.2.0

192.168.1.16

192.168.1.24

Will these networks need to have the subnet mask information included in the network statements?

yes

What commands are required to enable EIGRP and include the connected networks in the routing updates?

```
router eigrp 1
network 172.16.2.0 0.0.0.255
network 192.168.1.16 0.0.0.3
network 192.168.1.24 0.0.0.3
```



What command is required to enable EIGRP to include the VLSM information instead of summarizing routes at the classful boundary?

`no auto summary`

Are there any router interfaces that do not need to have EIGRP updates sent out? [yes](#)

What command is used to disable EIGRP updates on these interfaces?

`passive-interface FastEthernet0/0`

## Task 8: Configure EIGRP and Static Routing on the HQ Router

Consider the type of static routing that is needed on HQ.

A static default route will need to be configured to send all packets with destination addresses that are not in the routing table to the loopback address representing the link between the HQ router and the ISP. What command is needed to accomplish this?

`ip route 0.0.0.0 0.0.0.0 loopback1`

What directly connected networks are present in the HQ routing table?

[172.16.0.0](#)

[192.168.1.16](#)

[192.168.1.20](#)

[209.165.200.224](#)

Will the networks of the HQ LAN and the links between the BRANCH1 and BRANCH2 routers need to have the subnet mask information included in the network statements? [yes](#)

What commands are required to enable EIGRP and include the appropriate networks in the routing updates?

`router eigrp 1`

`network 172.16.0.0 0.0.1.255`

`network 192.168.1.16 0.0.0.3`

`network 192.168.1.20 0.0.0.3`

What command is required to enable EIGRP to include the VLSM information instead of summarizing routes at the classful boundary?

`no auto summary`

Are there any router interfaces that do not need to have EIGRP updates sent out? [yes](#)

What command is used to disable EIGRP updates on this interface?

`passive-interface FastEthernet0/0`

The HQ router needs to send the default route information to the BRANCH1 and BRANCH2 routers in the EIGRP updates. What command is used to configure this?

`redistribute static`

## Task 9: Configure EIGRP Routing on the BRANCH2 Router

Consider the networks that need to be included in the EIGRP updates that are sent out by the BRANCH2 router.

What directly connected networks are present in the BRANCH2 routing table?

172.16.3.0

192.168.1.20

192.168.1.24

Will these networks need to have the subnet mask information included in the network statements?

yes

What commands are required to enable EIGRP and include the connected networks in the routing updates?

router eigrp 1

network 172.16.3.0 0.0.0.127

network 192.168.1.20 0.0.0.3

network 192.168.1.24 0.0.0.3

What command is required to enable EIGRP to include the VLSM information instead of summarizing routes at the classful boundary?

no auto summary

Are there any router interfaces that do not need to have EIGRP updates sent out? yes

What command is used to disable EIGRP updates on these interfaces?

passive-interface FastEthernet0/0

## Task 10: Verify the Configurations

Answer the following questions to verify that the network is operating as expected.

From PC1, is it possible to ping PC2? yes

From PC1, is it possible to ping PC3? yes

The answer to the above questions should be **yes**. If any of the above pings failed, check your physical connections and configurations. Refer to your basic troubleshooting techniques used in the Chapter 1 labs.

What EIGRP routes are present in the routing table of the BRANCH1 router?

172.16.0.0/16 summary

172.16.0.0/23

172.16.3.0/25

192.168.1.0/24 summary

192.168.1.20/30

0.0.0.0/0

What is the gateway of last resort in the routing table of the BRANCH1 router?

[192.168.1.17 to network 0.0.0.0](#)

What EIGRP routes are present in the routing table of the HQ router?

[172.16.0.0/16 summary](#)

[172.16.2.0/24](#)

[172.16.3.0/25](#)

[192.168.1.0/24 summary](#)

[192.168.1.24/30](#)

What is the gateway of last resort in the routing table of the HQ router?

[0.0.0.0 to network 0.0.0.0](#)

What EIGRP routes are present in the routing table of the BRANCH2 router?

[172.16.0.0/16 summary](#)

[172.16.0.0/23](#)

[172.16.2.0/24](#)

[192.168.1.0/24 summary](#)

[192.168.1.16/30](#)

[0.0.0.0/0](#)

What is the gateway of last resort in the routing table of the BRANCH2 router?

[192.168.1.21 to network 0.0.0.0](#)

## Task 11: Reflection

Why is it necessary to use disable automatic summarization with this network design?

If the routes in the routing table are summarized at the classful network boundary 17.16.0.0, the paths between the three routers will all have an equal cost, and packets might not be sent using the route with the least number of hops.

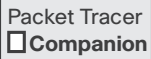
## Task 12: Document the Router Configurations

On each router, capture the following command output to a text (.txt) file and save for future reference:

- Running configuration
- Routing table
- Interface summarization

## Task 13: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.



## Packet Tracer Companion: Challenge EIGRP Configuration (9.6.2)

You can now open the file LSG02-Lab962.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment.



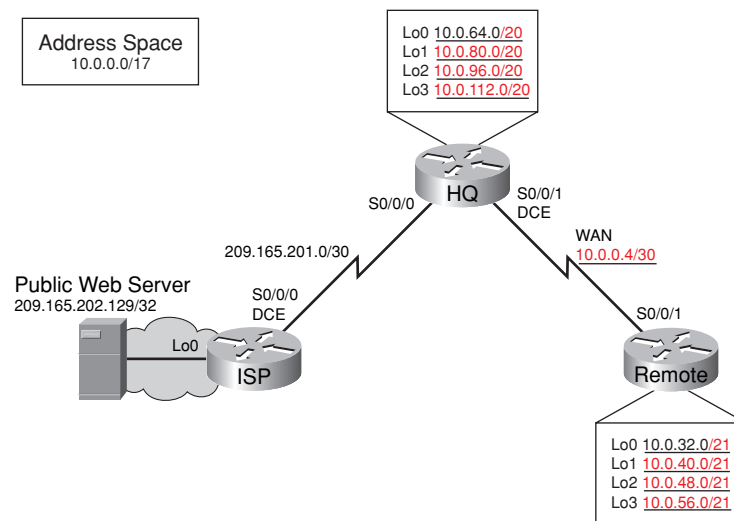
## Challenge Lab 9-4: EIGRP Design and Configuration

Upon completion of this lab, you should be able to

- Design a VLSM addressing scheme
- Configure routers with basic configurations using your addressing scheme
- Configure dynamic, static, and default routing
- Configure manual summarization
- Verify connectivity and troubleshoot problems

Figure 9-11 shows the topology diagram for this lab.

**Figure 9-11 Topology Diagram for Lab 9-4 (Answer)**



### Task 1: Design the Addressing Scheme

You are given the address space 10.0.0.0/17. The four loopback interfaces on HQ and four loopback interfaces on REMOTE are used to simulate different parts of a global network. Use the following specifications to design your addressing scheme.

For HQ, begin with the 10.0.64.0 address as the subnet for loopback 0. What subnet mask would you use to provide enough space for 4000 users while maximizing the number of subnets?

255.255.240.0 or /20

Starting with 10.0.64.0, contiguously assign the next three subnets, all supporting 4000 hosts. List all four subnets here.

[10.0.64.0/20](#)

[10.0.80.0/20](#)

[10.0.96.0/20](#)

[10.0.112.0/20](#)

For REMOTE, begin with the 10.0.32.0 address as the subnet for loopback 0. What subnet mask would you use to provide enough space for 2000 users while maximizing the number of subnets?

[255.255.248.0 or /21](#)

Starting with 10.0.32.0, contiguously assign the next three subnets, all supporting 2000 hosts. List all four subnets here.

[10.0.32.0/21](#)

[10.0.40.0/21](#)

[10.0.48.0/21](#)

[10.0.56.0/21](#)

Now pick a WAN subnet for the link shared by HQ and REMOTE. List the subnet you assigned here.

[Can be any subnet /30 from the 10.0.0.0/21 address space.](#)

Label the topology in Figure 9-11 with the networks and finish filling in the IP address table in Table 9-7 with your chosen addressing scheme. Use the first available IP address in each subnet as the interface address. For the WAN subnet, assign HQ the first address.

**Table 9-7 Addressing Table for Lab 9-4**

Device	Interface	IP Address	Subnet Mask
ISP	Lo0	209.165.202.129	255.255.255.255
	S0/0	209.165.201.1	255.255.255.252
HQ	S0/0	209.165.201.2	255.255.255.252
	S0/0/1	10.0.0.5	255.255.255.252
	Lo0	10.0.64.1	255.255.240.0
	Lo1	10.0.80.1	255.255.240.0
	Lo2	10.0.96.1	255.255.240.0
REMOTE	Lo3	10.0.112.1	255.255.240.0
	S0/0/1	10.0.0.6	255.255.255.252
	Lo0	10.0.32.1	255.255.248.0
	Lo1	10.0.40.1	255.255.248.0
	Lo2	10.0.48.1	255.255.248.0
	Lo3	10.0.56.1	255.255.248.0

## Task 2: Cable the Topology and Basic Configuration

- Step 1.** Choose three routers and cable them according to the topology in Figure 9-11. You will not need any LAN interfaces or switches for this lab.
- Step 2.** Configure the routers' basic configurations including interface addresses.

## Task 3: Configure EIGRP Routing and Default Routing

- Step 1.** Configure both HQ and REMOTE to use EIGRP as the routing protocol. Use 100 as the AS number. Enter the simulated LAN subnets and the WAN link between HQ and REMOTE. *Do not* advertise the 209.165.201.0/30 network. Make sure that you disable automatic summarization.
- Step 2.** Configure ISP with a static route pointing to the 10.0.0.0/17 address space.
- Step 3.** Configure HQ with a default route pointing to ISP.
- Step 4.** Configure HQ to advertise the default route to REMOTE with the **redistribute static** command within the EIGRP routing process.
- Step 5.** Verify HQ and REMOTE routing tables.
- HQ should have six directly connected routes, four EIGRP routes, and one static route.
  - REMOTE should have five directly connected routes, four EIGRP routes, and one EIGRP external route.
  - Verify that REMOTE can ping the Simulated Web Server at 209.165.202.129.

```
REMOTE# ping 209.165.202.129
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 209.165.202.129, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
```

## Task 4: Manual Summarization

- Step 1.** Because the simulated LANs on both HQ and REMOTE were assigned contiguously, you can summarize the routing updates to reduce the size of the routing tables. What commands will summarize the simulated LANs on HQ?

```
HQ(config)# interface serial 0/0/1
```

```
HQ(config-if)# ip summary-address eigrp 100 10.0.64.0 255.255.192.0
```

- Step 2.** What commands will summarize the simulated LANs on REMOTE?

```
REMOTE(config)# interface serial 0/0/1
```

```
REMOTE(config-if)# ip summary-address eigrp 100 10.0.32.0 255.255.224.0
```

## Task 5: Verification and Documentation

- Step 1.** Capture the following verifications to a text file called verify.txt.
- Ping output from REMOTE pinging the simulated web server
  - Capture **show ip route** on all three routers: ISP, HQ, and REMOTE
  - Capture **show ip eigrp neighbor** and **show ip eigrp topology** on HQ and REMOTE
- Step 2.** Capture the running configurations on all three routers to separate text files. Use the host name of the router to name each text file.
- Step 3.** Clean up the verify.txt, HQ.txt, REMOTE.txt, and ISP.txt files. Add appropriate notes to assist in your studies.

Final scripts and **show** command output:

```
HQ
hostname HQ
!
enable secret class
!
ip subnet-zero
no ip domain-lookup
ip host REMOTE 10.0.0.6
ip host WEB 209.165.202.129
ip host ISP 209.165.201.1
!
interface Loopback0
 ip address 10.0.64.1 255.255.240.0
!
interface Loopback1
 ip address 10.0.80.1 255.255.240.0
!
interface Loopback2
 ip address 10.0.96.1 255.255.240.0
!
interface Loopback3
 ip address 10.0.112.1 255.255.240.0
!
interface Serial0/0/0
 description Link to ISP
 ip address 209.165.201.2 255.255.255.252
 clockrate 64000
 no shutdown
!
interface Serial0/0/1
 description Link to REMOTE
 ip address 10.0.0.5 255.255.255.252
```

```
ip summary-address eigrp 100 10.0.64.0 255.255.192.0
clockrate 64000
no shutdown
!
router eigrp 100
 redistribute static
 network 10.0.0.0
 no auto-summary
 eigrp log-neighbor-changes
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
banner motd &

!!!AUTHORIZE ACCESS ONLY!!!

&
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
end
HQ# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
```



P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

```

209.165.201.0/30 is subnetted, 1 subnets
C 209.165.201.0 is directly connected, Serial0/0/0
 10.0.0.0/8 is variably subnetted, 7 subnets, 4 masks
C 10.0.0.4/30 is directly connected, Serial0/0/1
D 10.0.32.0/19 [90/2297856] via 10.0.0.6, 00:04:47, Serial0/0/1
D 10.0.64.0/18 is a summary, 00:05:16, Null0
C 10.0.64.0/20 is directly connected, Loopback0
C 10.0.80.0/20 is directly connected, Loopback1
C 10.0.96.0/20 is directly connected, Loopback2
C 10.0.112.0/20 is directly connected, Loopback3
S* 0.0.0.0/0 is directly connected, Serial0/0/0

```

HQ# **show ip eigrp neighbors**

IP-EIGRP neighbors for process 100

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num	Type
0	10.0.0.6	Se0/0/1	12 00:05:42	384	2304	0	9	

HQ# **show ip eigrp topology**

IP-EIGRP Topology Table for AS(100)/ID(10.0.112.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,  
r - reply Status, s - sia Status

```

P 0.0.0.0/0, 1 successors, FD is 2169856
 via Rstatic (2169856/0)
P 10.0.0.4/30, 1 successors, FD is 2169856
 via Connected, Serial0/0/1
P 10.0.32.0/19, 1 successors, FD is 2297856
 via 10.0.0.6 (2297856/128256), Serial0/0/1
P 10.0.64.0/18, 1 successors, FD is 128256
 via Summary (128256/0), Null0
P 10.0.64.0/20, 1 successors, FD is 128256
 via Connected, Loopback0
P 10.0.80.0/20, 1 successors, FD is 128256
 via Connected, Loopback1
P 10.0.96.0/20, 1 successors, FD is 128256
 via Connected, Loopback2

```

```
P 10.0.112.0/20, 1 successors, FD is 128256
 via Connected, Loopback3
```

---

```
REMOTE
hostname REMOTE
!
enable secret class
!
ip subnet-zero
no ip domain-lookup
ip host WEB 209.165.202.129
ip host ISP 209.165.201.1
ip host HQ 10.0.0.5
!
interface Loopback0
 ip address 10.0.32.1 255.255.248.0
!
interface Loopback1
 ip address 10.0.40.1 255.255.248.0
!
interface Loopback2
 ip address 10.0.48.1 255.255.248.0
!
interface Loopback3
 ip address 10.0.56.1 255.255.248.0
!
interface Serial0/0/1
 description Link to HQ
 ip address 10.0.0.6 255.255.255.252
 ip summary-address eigrp 100 10.0.32.0 255.255.224.0
 no shutdown
!
router eigrp 100
 network 10.0.0.0
 no auto-summary
 eigrp log-neighbor-changes
!
ip classless
!
banner motd &

!!!AUTHORIZES ACCESS ONLY!!!

&
```

```

!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
end

```

REMOTE# **show ip route**

```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

```

Gateway of last resort is 10.0.0.5 to network 0.0.0.0

```

 10.0.0.0/8 is variably subnetted, 7 subnets, 4 masks
C 10.0.0.4/30 is directly connected, Serial0/0/1
C 10.0.40.0/21 is directly connected, Loopback1
D 10.0.32.0/19 is a summary, 00:05:06, Null0
C 10.0.32.0/21 is directly connected, Loopback0
C 10.0.56.0/21 is directly connected, Loopback3
C 10.0.48.0/21 is directly connected, Loopback2
D 10.0.64.0/18 [90/2297856] via 10.0.0.5, 00:04:58, Serial0/0/1
D*EX 0.0.0.0/0 [170/2681856] via 10.0.0.5, 00:04:58, Serial0/0/1

```

REMOTE# **show ip eigrp neighbors**

IP-EIGRP neighbors for process 100

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num	Type
---	---------	-----------	----------------------	--------------	-----	----------	------------	------

```
0 10.0.0.5 Se0/0/1 14 00:05:19 24 200 0 11
```

```
REMOTE# show ip eigrp topology
```

```
IP-EIGRP Topology Table for AS(100)/ID(10.0.56.1)
```

```
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status
```

```
P 0.0.0.0/0, 1 successors, FD is 2681856
 via 10.0.0.5 (2681856/2169856), Serial0/0/1
P 10.0.0.4/30, 1 successors, FD is 2169856
 via Connected, Serial0/0/1
P 10.0.40.0/21, 1 successors, FD is 128256
 via Connected, Loopback1
P 10.0.32.0/19, 1 successors, FD is 128256
 via Summary (128256/0), Null0
P 10.0.32.0/21, 1 successors, FD is 128256
 via Connected, Loopback0
P 10.0.56.0/21, 1 successors, FD is 128256
 via Connected, Loopback3
P 10.0.48.0/21, 1 successors, FD is 128256
 via Connected, Loopback2
P 10.0.64.0/18, 1 successors, FD is 2297856
 via 10.0.0.5 (2297856/128256), Serial0/0/1
```

---

```
ISP
```

```
hostname ISP
```

```
!
```

```
enable secret class
```

```
!
```

```
ip subnet-zero
```

```
no ip domain-lookup
```

```
ip host HQ 209.165.201.2
```

```
!
```

```
interface Loopback0
```

```
 description Simulated Public Web Server
```

```
 ip address 209.165.202.129 255.255.255.255
```

```
!
```

```
interface Serial0/0/0
```

```
 description Link to HQ
```

```
 ip address 209.165.201.1 255.255.255.252
```

```
 no shutdown
```

```
!
```

```
ip classless
```

```
ip route 10.0.0.0 255.255.128.0 Serial0/0/0
!
banner motd &

 !!!AUTHORIZED ACCESS ONLY!!!

&
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
end
```

ISP# **show ip route**

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route
```

Gateway of last resort is not set

```
 209.165.201.0/30 is subnetted, 1 subnets
C 209.165.201.0 is directly connected, Serial0/0/0
 209.165.202.0/32 is subnetted, 1 subnets
C 209.165.202.129 is directly connected, Loopback0
 10.0.0.0/17 is subnetted, 1 subnets
S 10.0.0.0 is directly connected, Serial0/0/0
```



## Lab 9-5: EIGRP Troubleshooting (9.6.3)

Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram in Figure 9-12
- Erase the startup configuration and reload a router to the default state
- Load the routers with supplied scripts
- Discover where communication is not possible
- Gather information about the misconfigured portion of the network along with any other errors
- Analyze information to determine why communication is not possible
- Propose solutions to network errors
- Implement solutions to network errors
- Document the corrected network

### Scenario

In this lab, you will begin by loading configuration scripts on each of the routers. These scripts contain errors that will prevent end-to-end communication across the network. You will need to troubleshoot each router to determine the configuration errors, and then use the appropriate commands to correct the configurations. When you have corrected all the configuration errors, all the hosts on the network should be able to communicate with each other.

The network should also have met the following requirements:

- EIGRP routing is configured on the BRANCH1 router.
- EIGRP routing is configured on the BRANCH2 router.
- EIGRP routing is configured on the HQ router.
- EIGRP updates must be disabled on the BRANCH1, BRANCH2, and HQ LAN interfaces.
- All EIGRP routers must use a process ID of 1.

Figure 9-12 shows the topology diagram and Table 9-8 provides the interface, IP address, subnet mask, and default gateway (where applicable) information for all the network devices depicted in Figure 9-12.

Figure 9-12 Topology Diagram for Lab 9-5 (Answer)

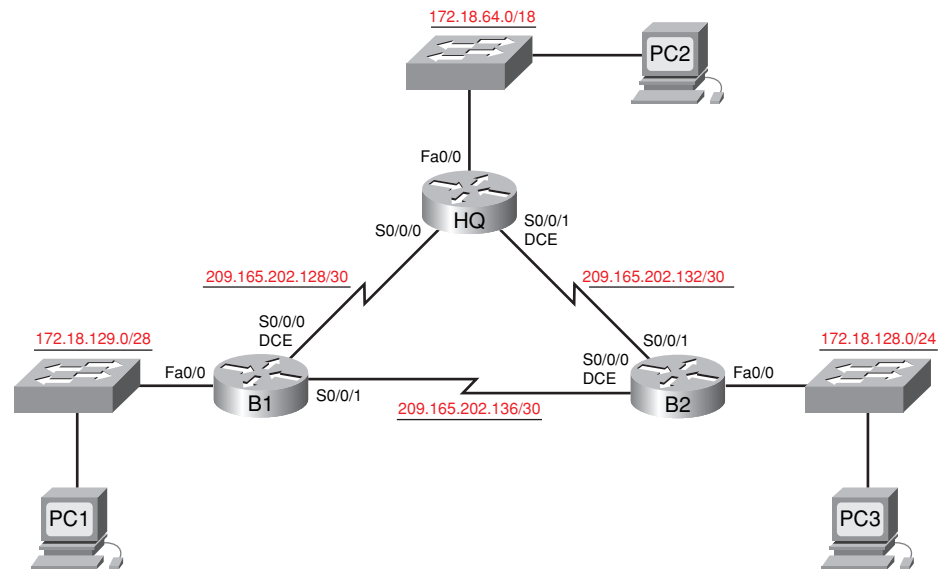


Table 9-8 Addressing Table for Lab 9-5

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	Fa0/0	172.18.64.1	255.255.192.0	—
	S0/0/0	209.165.202.129	255.255.255.252	—
	S0/0/1	209.165.202.133	255.255.255.252	—
BRANCH1	Fa0/0	172.18.129.1	255.255.255.240	—
	S0/0/0	209.165.202.130	255.255.255.252	—
	S0/0/1	209.165.202.137	255.255.255.252	—
BRANCH2	Fa0/0	172.18.128.1	255.255.255.0	—
	S0/0/0	209.165.202.138	255.255.255.252	—
	S0/0/1	209.165.202.134	255.255.255.252	—
PC1	NIC	172.18.129.14	172.18.129.1	255.255.255.240
PC2	NIC	172.18.100.100	172.18.64.1	255.255.192.0
PC3	NIC	172.18.128.10	172.18.128.1	255.255.255.0

## Task 1: Cable, Erase, and Reload the Routers

**Step 1.** Cable a network.

Cable a network that is similar to the one in the topology diagram in Figure 9-12.

**Step 2.** Clear the configuration on each router.

Clear the configuration on each of the routers using the **erase startup-config** command and then **reload** the routers. Answer **no** if asked to save changes.

## Task 2: Load Routers with the Supplied Scripts

**Step 1.** Load the following script onto the BRANCH1 router.

---

**Instructor note:** Missing or misconfigured commands are shown in red.

---

```
hostname BRANCH1
!
!
no ip domain-lookup
!
interface FastEthernet0/0
 ip address 172.18.129.1 255.255.255.240
 duplex auto
 speed auto
 ! the no shutdown command is missing
!
interface Serial0/0/0
 ip address 209.165.202.130 255.255.255.252
 clock rate 64000
 no shutdown
!
interface Serial0/0/1
 ip address 209.165.202.137 255.255.255.252
 no shutdown
!
router eigrp 2
 !The process ID should be 1
 passive-interface FastEthernet0/0
 network 209.165.202.128 0.0.0.3
 network 209.165.202.136 0.0.0.3
 network 172.18.129.0 0.0.0.7
 !The 172.18.129.0 network mask should be 0.0.0.15
 no auto-summary
!
ip classless
!
!
!
!
line con 0
line vty 0 4
 login
!
!
End
```

**Corrected script:**

```
hostname BRANCH1
!
!
```



```

no ip domain-lookup
!
interface FastEthernet0/0
 ip address 172.18.129.1 255.255.255.240
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 ip address 209.165.202.130 255.255.255.252
 clock rate 64000
 no shutdown
!
interface Serial0/0/1
 ip address 209.165.202.137 255.255.255.252
 no shutdown
!
router eigrp 1
 passive-interface FastEthernet0/0
 network 172.18.129.0 0.0.0.15
 network 209.165.202.128 0.0.0.3
 network 209.165.202.136 0.0.0.3
 no auto-summary
!
ip classless
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end!
!
end

```

The errors in the student scripts are as follows:

- The **no shutdown** command is missing from the FastEthernet 0/0 interface.
- The EIGRP process ID is incorrect.
- The network mask for the 172.18.129.0/28 network is incorrect.

**Step 2.** Load the following script onto the BRANCH2 router.

```

hostname BRANCH2
!
!
no ip domain-lookup
!
interface FastEthernet0/0

```

```
ip address 172.18.128.1 255.255.255.0
duplex auto
speed auto
no shutdown
!
interface Serial0/0/0
ip address 209.165.202.138 255.255.255.252
!The clock rate 64000 command is missing
no shutdown
!
interface Serial0/0/1
ip address 209.165.202.134 255.255.255.252
no shutdown
!
router eigrp 1
passive-interface FastEthernet0/0
network 172.18.128.0 0.0.0.255
network 209.165.202.132 0.0.0.3
network 209.165.202.136 0.0.0.3
!The no auto-summary command is missing
!
ip classless
!
!
!
!
line con 0
line vty 0 4
login
!
!
end
```

Corrected script:

```
hostname BRANCH2
!
!
no ip domain-lookup
!
interface FastEthernet0/0
ip address 172.18.128.1 255.255.255.0
duplex auto
speed auto
no shutdown
!
interface Serial0/0/0
ip address 209.165.202.138 255.255.255.252
clock rate 64000
no shutdown
!
```

```

interface Serial0/0/1
 ip address 209.165.202.134 255.255.255.252
 no shutdown
!
router eigrp 1
 passive-interface FastEthernet0/0
 network 172.18.128.0 0.0.0.255
 network 209.165.202.132 0.0.0.3
 network 209.165.202.136 0.0.0.3
 no auto-summary
!
ip classless
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end

```

The errors in the student scripts are as follows:

- The **clock rate 64000** command is missing from Serial 0/0/0 interface.
- The **no auto-summary** command is missing from the EIGRP configuration.

**Step 3.** Load the following script onto the HQ router.

```

hostname HQ
!
!
no ip domain-lookup
!
interface FastEthernet0/0
 ip address 172.18.64.1 255.255.192.0
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 ip address 209.165.202.129 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 209.165.202.133 255.255.255.252
 clock rate 64000
 no shutdown
!
router eigrp 1
 passive-interface Serial0/0/0

```

```
!The passive-interface command should use FastEthernet0/0
network 172.18.64.0
!The mask 0.0.63.255 is missing from the network statement for 172.18.64.0
network 209.165.202.128 0.0.0.3
network 209.165.202.132 0.0.0.3
no auto-summary
!
ip classless
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end
```

Corrected script:

```
hostname HQ
!
!
no ip domain-lookup
!
interface FastEthernet0/0
 ip address 172.18.64.1 255.255.192.0
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 ip address 209.165.202.129 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 209.165.202.133 255.255.255.252
 clock rate 64000
 no shutdown
!
router eigrp 1
 passive-interface FastEthernet0/0
 network 172.18.64.0 0.0.63.255
 network 209.165.202.128 0.0.0.3
 network 209.165.202.132 0.0.0.3
 no auto-summary
!
ip classless
!
!
```

```

!
!
line con 0
line vty 0 4
 login
!
!
end

```

The errors in the student scripts are as follows:

- The **passive-interface** command is configured for the incorrect interface.
- The 0.0.63.255 mask is missing from the **network** statement for the 172.18.64.0/18 network.

### Task 3: Troubleshoot the BRANCH1 Router

**Step 1.** Begin troubleshooting at the host connected to the BRANCH1 router.

From the host PC1, is it possible to ping PC2? no

From the host PC1, is it possible to ping PC3? no

From the host PC1, is it possible to ping the default gateway? no

**Step 2.** Examine the BRANCH1 router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the configuration of the interfaces?

Yes, the FastEthernet 0/0 interface is administratively down.

The protocol is down on the Serial 0/0/1 interface.

If there are any problems with the configuration of the interfaces, record any commands that will be necessary to correct the configuration errors.

**configure terminal**

**interface FastEthernet0/0**

**no shutdown**

**Step 3.** If you have recorded any commands, apply them to the router configuration now.

**Step 4.** View a summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors on the BRANCH1 router? no

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

**Step 5.** Troubleshoot the routing configuration on the BRANCH1 router.

What routes are shown in the routing table?

172.18.129.0 is directly connected

209.165.202.128 is directly connected

Are there any problems with the routing table or the EIGRP configuration?

Yes, there are no EIGRP routes in the routing table.

Verify the routing process with the **show ip protocols** command. Are there any problems with the EIGRP configuration?

The process ID for EIGRP is incorrect.

The 172.18.129.0 network mask is incorrect. It should be 0.0.0.15. Also, BRANCH1 is not advertising the 209.165.202.128/30 network.

If there are any problems with the EIGRP configuration, record any commands that will be necessary to correct the configuration errors.

Because the process ID is incorrect, the entire EIGRP configuration must be redone:

```
no router eigrp 2
router eigrp 1
passive-interface FastEthernet0/0
network 209.165.202.128 0.0.0.3
network 209.165.202.136 0.0.0.3
network 172.18.129.0 0.0.0.15
no auto-summary
```

Are there any connectivity problems that could be due to errors on other parts of the network?

The protocol is down on the Serial 0/0/1 interface. However, the configuration on BRANCH1 is correct. So, the Serial 0/0/0 interface on the BRANCH2 router should be checked.

What connected networks are shown in the EIGRP topology table of the BRANCH1 router?

209.165.202.128/30

172.18.129.0/28

Are there any problems with the connected networks in the EIGRP topology table?

The 209.165.202.136/30 network is not in the table because the protocol is down on Serial 0/0/1.

**Step 6.** If you have recorded any commands in the previous steps, apply them to the router configuration now.

**Step 7.** View the routing information.

If any changes were made to the configuration in the previous steps, view the routing information again.

Does the information in the routing table or other verification commands indicate any configuration errors on the BRANCH1 router? no

Does the information in the EIGRP topology table indicate any configuration errors on the BRANCH1 router? no

If the answer to either of these questions is **yes**, troubleshoot the routing configuration again.

What routes are shown in the routing table?

172.18.0.0/16 is a summary

172.18.129.0/28 is directly connected

209.165.202.0/24 is a summary

209.165.202.128/30 is directly connected

**Step 8.** Attempt to ping between the hosts again.

From the host PC1, is it possible to ping PC2? no

From the host PC1, is it possible to ping PC3? no

From the host PC1, is it possible to ping the Serial 0/0/0 interface of the HQ router? no

From the host PC1, is it possible to ping the Serial 0/0/1 interface of the HQ router? no

## Task 4: Troubleshoot the HQ Router

**Step 1.** Begin troubleshooting at the host PC2.

From the host PC2, is it possible to ping PC1? no

From the host PC2, is it possible to ping PC3? yes

From the host PC2, is it possible to ping the default gateway? yes

**Step 2.** Examine the HQ router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the configuration of the interfaces?

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the configuration of the interfaces? no

---

---

---

---

If there are any problems with the configuration of the interfaces, record any commands that will be necessary to correct the configuration errors.

---

---

---

---

**Step 3.** If you have recorded any commands in the previous step, apply them to the router configuration now.

**Step 4.** View a summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors on the HQ router? no

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

**Step 5.** Troubleshoot the routing configuration on the HQ router.

What routes are shown in the routing table?

172.18.0.0/16 is a summary

172.18.64.0/18 is directly connected

172.18.129.0/28 via 209.165.202.130

209.165.202.0/24 is a summary

209.165.202.128/30 is directly connected

209.165.202.132/30 is directly connected

Are there any problems with the routing table or the EIGRP configuration?

The 209.165.202.136/30 network is missing from the routing table.

The 172.18.128.0/24 network is missing from the routing table.

Only the summary route 172.18.0.0/16 network is being received from the BRANCH2 router.

The mask is missing from the **network** statement for the 172.18.64.0/18 network.

The **passive-interface** command is configured for the wrong interface.

If there are any problems with the EIGRP configuration, record any commands that will be necessary to correct the configuration errors.

**router eigrp 1**

**no network 172.18.0.0**

**network 172.18.64.0.0 0.0.63.255**

**no passive-interface serial0/0/0**

**passive-interface FastEthernet0/0**

Are there any connectivity problems that could be due to errors on other parts of the network?

The link between the BRANCH1 and BRANCH2 routers is not in the routing table.

The Serial 0/0/0 interface on the BRANCH2 router should be checked.

What connected networks are shown in the EIGRP topology table of the HQ router?

209.165.202.128/30

209.165.202.132/30

172.18.64.0/18



---

Are there any problems with the connected networks in the EIGRP topology table? no

---

---

---

---

**Step 6.** If you have recorded any commands in the previous steps, apply them to the router configuration now.

**Step 7.** View the routing information.

If any changes were made to the configuration in the previous steps, view the routing information again.

Does the information in routing table indicate any configuration errors on the HQ router? no

Does the information in the EIGRP topology table indicate any configuration errors on the HQ router? no

If the answer to either of these questions is **yes**, troubleshoot the routing configuration again.

What EIGRP routes are shown in the routing table?

172.18.0.0/16 via 209.165.202.134

172.18.64.0/18 is directly connected

209.165.202.128 is directly connected

209.165.202.132 is directly connected

**Step 8.** Attempt to ping between the hosts again.

From the host PC2, is it possible to ping PC1? yes

From the host PC2, is it possible to ping PC3? yes

From the host PC2, is it possible to ping the Serial 0/0/0 interface of the BRANCH2 router? no

From the host PC2, is it possible to ping the Serial 0/0/1 interface of the BRANCH2 router? yes

## Task 5: Troubleshoot the BRANCH2 Router

**Step 1.** Begin troubleshooting at the host PC3.

From the host PC3, is it possible to ping PC1? yes

From the host PC3, is it possible to ping PC2? yes

From the host PC3, is it possible to ping the default gateway? yes

**Step 2.** Examine the BRANCH2 router to find possible configuration errors.

Are there any problems with the configuration of the interfaces?

The protocol is down on the Serial 0/0/0 interface.

The clock rate is missing from the interface.

If there are any problems with the configuration of the interfaces, record any commands that will be necessary to correct the configuration errors.

**interface serial0/0/0**

**clock rate 64000**

**Step 3.** If you have recorded any commands in the previous step, apply them to the router configuration now.

**Step 4.** View a summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors on the BRANCH2 router? no

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

**Step 5.** Troubleshoot the routing configuration on the BRANCH2 router.

What routes are shown in the routing table?

172.18.0.0/16 is a summary

172.18.64.0/18 via 209.165.202.133

172.18.128.0/24 is directly connected

172.18.129.0/28 via 209.165.202.137

209.165.202.0/24 is a summary

209.165.202.128/30 via 209.165.202.133

209.165.202.128/30 via 209.165.202.137

209.165.202.132/30 is directly connected

209.165.202.136/30 is directly connected

Are there any problems with the routing table or the EIGRP configuration?

---

---

---

---

---

The **no auto-summary** command is missing.

If there are any problems with the EIGRP configuration, record any commands that will be necessary to correct the configuration errors.

**router eigrp 1****no auto-summary**

Are there any connectivity problems that could be due to errors on other parts of the network? no

---

---

---

---

---

What connected networks are shown in the EIGRP topology table of the BRANCH2 router?

172.18.128.0/24

209.165.202.132/30

209.165.202.136/30

Are there any problems with the connected networks in the EIGRP topology table? no

---

---

---

---

---

**Step 6.** If you have recorded any commands in the previous steps, apply them to the router configuration now.

**Step 7.** View the routing information.

If any changes were made to the configuration in the previous steps, view the routing information again.

Does the information in routing table indicate any configuration errors on the BRANCH2 router? no

Does the information in the EIGRP topology table indicate any configuration errors on the BRANCH2 router? no

If the answer to either of these questions is **yes**, troubleshoot the routing configuration again.

What routes are shown in the routing table?

172.18.0.0/16 is a summary

172.18.64.0/18 via 209.165.202.133

172.18.128.0/24 is directly connected

172.18.129.0/28 via 209.165.202.137

209.165.202.0/24 is a summary

209.165.202.128/30 via 209.165.202.133

209.165.202.128/30 via 209.165.202.137

209.165.202.132/30 is directly connected

209.165.202.136/30 is directly connected

**Step 8.** Attempt to ping between the hosts again.

From the host PC3, is it possible to ping PC1? yes

From the host PC3, is it possible to ping PC2? yes

From the host PC3, is it possible to ping the Serial 0/0/0 interface of the BRANCH1 router? yes

From the host PC3, is it possible to ping the Serial 0/0/1 interface of the BRANCH1 router? yes

## Task 6: Reflection

There were a number of configuration errors in the scripts that were provided for this lab. Use the space to write a brief description of the errors that you found.

---

---

---

---

---

## Task 7: Documentation

On each router, capture the following command output to a text (.txt) file and save for future reference:

- **show running-config**
- **show ip route**
- **show ip interface brief**
- **show ip protocols**

If you need to review the procedures for capturing command output, refer to “Lab 1-1: Cabling a Network and Basic Router Configuration (1.5.1).”

## Task 8: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Packet Tracer  
□ Companion

## Packet Tracer Companion: EIGRP Troubleshooting (9.6.3)

You can now open the file LSG02-Lab963.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment.

Packet Tracer  
□ Challenge

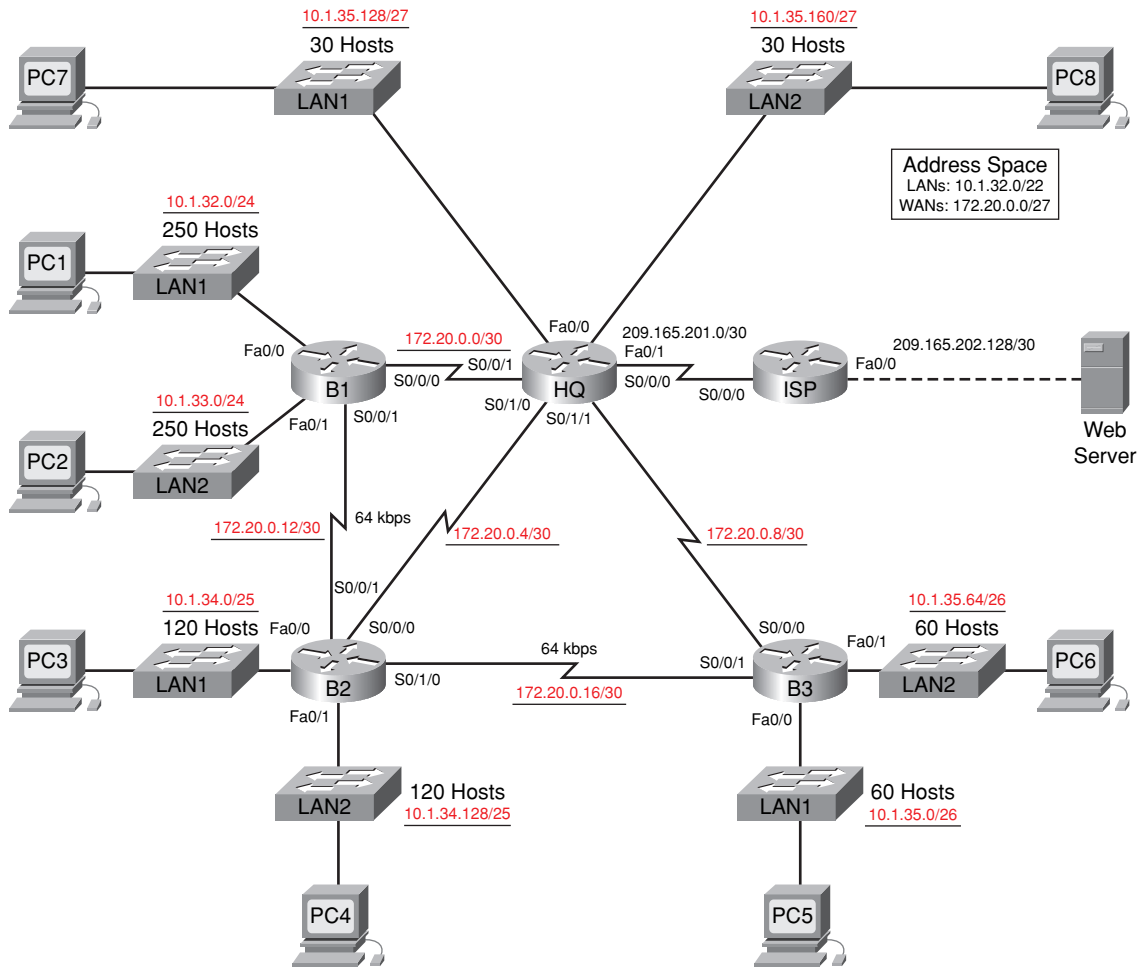
## Packet Tracer Skills Integration Challenge: EIGRP Configuration

Upon completion of this challenge, you should be able to do the following:

- Design and document an addressing scheme based on requirements
- Apply a basic configuration to the devices
- Test connectivity between directly connected devices
- Configure and verify EIGRP routing
- Configure EIGRP summary routes
- Fine-tune EIGRP
- Configure static and default routing for Internet access
- Verify full connectivity between all devices in the topology

Open the file LSG02-PTSkills9.pka on the CD-ROM that accompanies this book. You will use the topology in Figure 9-13 and the addressing table in Table 9-9 to document your design.

**Figure 9-13 Packet Tracer Skills Integration Challenge Topology (Answer)**



**Table 9-9 Addressing Table**

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	Fa0/0	10.1.35.129	255.255.255.224	—
	Fa0/1	10.1.35.161	255.255.255.224	—
	S0/0/0	209.165.201.2	255.255.255.252	—
	S0/0/1	172.20.0.1	255.255.255.252	—
	S0/1/0	172.20.0.5	255.255.255.252	—
	S0/1/1	172.20.0.9	255.255.255.252	—
B1	Fa0/0	10.1.32.1	255.255.255.0	—
	Fa0/1	10.1.33.1	255.255.255.0	—
	S0/0/0	172.20.0.2	255.255.255.252	—
	S0/0/1	172.20.0.13	255.255.255.252	—
B2	Fa0/0	10.1.34.1	255.255.255.128	—
	Fa0/1	10.1.34.129	255.255.255.128	—
	S0/0/0	172.20.0.6	255.255.255.252	—
	S0/0/1	172.20.0.14	255.255.255.252	—
	S0/1/0	172.20.0.17	255.255.255.252	—
B3	Fa0/0	10.1.35.1	255.255.255.192	—
	Fa0/1	10.1.35.65	255.255.255.192	—
	S0/0/0	172.20.0.10	255.255.255.252	—
	S0/0/1	172.20.0.18	255.255.255.252	—
ISP	Fa0/0	209.165.202.129	255.255.255.252	—
	S0/0/0	209.165.201.1	255.255.255.252	—
Web Server	NIC	209.165.202.130	255.255.255.252	209.165.202.129
PC1	NIC	10.1.32.254	255.255.255.0	10.1.32.1
PC2	NIC	10.1.33.254	255.255.255.0	10.1.33.1
PC3	NIC	10.1.34.126	255.255.255.128	10.1.34.1
PC4	NIC	10.1.34.254	255.255.255.128	10.1.34.129
PC5	NIC	10.1.35.62	255.255.255.192	10.1.35.1
PC6	NIC	10.1.35.126	255.255.255.192	10.1.35.65
PC7	NIC	10.1.35.158	255.255.255.224	10.1.35.129
PC8	NIC	10.1.35.190	255.255.255.224	10.1.35.161

## Task 1: Design and Document an Addressing Scheme

### Step 1. Design an addressing scheme.

Based on the network requirements shown in the topology in Figure 9-13, design an appropriate addressing scheme.

- For the LANs, use the address space 10.1.32.0/22. Starting with the largest subnets' requirements on B1, assign subnets in order throughout the topology.
- For the WANs, use the address space 172.20.0.0/27. Assign WAN subnets according to the following specifications:
  - Subnet 0 to the WAN link between HQ and B1
  - Subnet 1 to the WAN link between HQ and B2
  - Subnet 2 to the WAN link between HQ and B3
  - Subnet 3 to the WAN link between B1 and B2
  - Subnet 4 to the WAN link between B2 and B3

### Step 2. Document the addressing scheme.

- Use the blank spaces on the topology to record the network addresses in dotted decimal/slash format.
- Use Table 9-9 to document the IP addresses, subnet masks, and default gateway addresses:
  - For LANs, assign the first address to the router interface. Assign the last address to the PC.
  - For WAN links to HQ, assign the first address to the HQ router.
  - For WAN links between branch routers:
    - Assign the first address to B1 for the link between B1 and B2.
    - Assign the first address to B2 for the link between B2 and B3.

## Task 2: Apply a Basic Configuration

### Step 1. Configure the routers.

Using your documentation, configure the routers with basic configurations.

### Step 2. Configure the PCs.

Using your documentation, configure the PCs with an IP address, subnet mask, and default gateway.

## Task 3: Test Connectivity

Before continuing, make sure that each device can ping its directly connected neighbor.



## Task 4: Configure and Verify EIGRP Routing

### Step 1. Configure EIGRP.

Configure all devices with EIGRP routing using 1 as the process ID. In your configuration, make sure that you include the following:

- Disable automatic summarization.
- Stop routing updates on interfaces that are not connected to EIGRP neighbors.
- All LANs should be summarized into one advertisement to neighbors. For example, HQ should summarize its two LANs when advertising to B1, B2, and B3.

### Step 2. Verify EIGRP.

Use verification commands to check your configuration. All routers should be converged on all the 10.1.32.0/22 and 172.20.0.0/27 subnets.

## Task 5: Fine-Tune EIGRP

### Step 1. Adjust bandwidth values used to calculate metrics.

The links between the branch routers (B1 to B2 and B2 to B3) are for backup purposes only. Configure the bandwidth values to match the actual bandwidth so that EIGRP does not equal-cost load across the T1 links to HQ and the backup links to the neighboring branch router.

### Step 2. Adjust Hello intervals for the slower links.

Change the Hello intervals for the 64-kbps links to 60 seconds.

## Task 6: Configure Static and Default Routing

Because Packet Tracer does not support redistribution of default routes, all routers except ISP will need a default route.

## Task 7: Test Connectivity and Examine the Configuration

Test connectivity and examine the configuration.



# Link-State Routing Protocols

The Study Guide portion of this chapter uses a combination of matching, fill-in-the-blank, multiple-choice, and open-ended question exercises to test your knowledge of link-state routing protocols.

There are no hands-on labs in this chapter. However, the Labs and Activities portion does include a Packet Tracer Skills Integration Challenge Activity.

As you work through this chapter, use Chapter 10 in *Routing Protocols and Concepts, CCNA Exploration Companion Guide* or use the corresponding Chapter 10 in the Exploration Routing Protocols and Concepts online curriculum for assistance.

## Study Guide

### Link-State Routing

Distance vector routing protocols are like road signs because routers must make preferred path decisions based on a distance or metric to a network. Just as travelers trust a road sign to accurately state the distance to the next town, a distance vector router trusts that another router is advertising the true distance to the destination network.

Link-state routing protocols take a different approach. Link-state routing protocols are more like a road map because they create a topological map of the network, and each router uses this map to determine the shortest path to each network. Just as you refer to a map to find the route to another town, link-state routers use a map to determine the preferred path to reach another destination.

### Link-State Routing Concepts Exercise

#### *Link-State Routing Protocols*

Link-state routing protocols are also known as [shortest path first](#) protocols and are built around Edsger [Dijkstra](#)'s SPF algorithm.

The IP link-state routing protocols include

- [Open Shortest Path First \(OSPF\)](#)
- [Intermediate System-to-Intermediate System \(IS-IS\)](#)

#### *Introduction to the SPF Algorithm*

The SPF algorithm accumulates [costs](#) along each path, from source to destination. Each router calculates the SPF algorithm and determines the [cost](#) from its own perspective. Using Figure 10-1, complete Table 10-1 through 10-5, filling in the appropriate information for each router. As an example, Table 10-1 for R1 is partially complete.

Figure 10-1 Topology of Link-State Routers

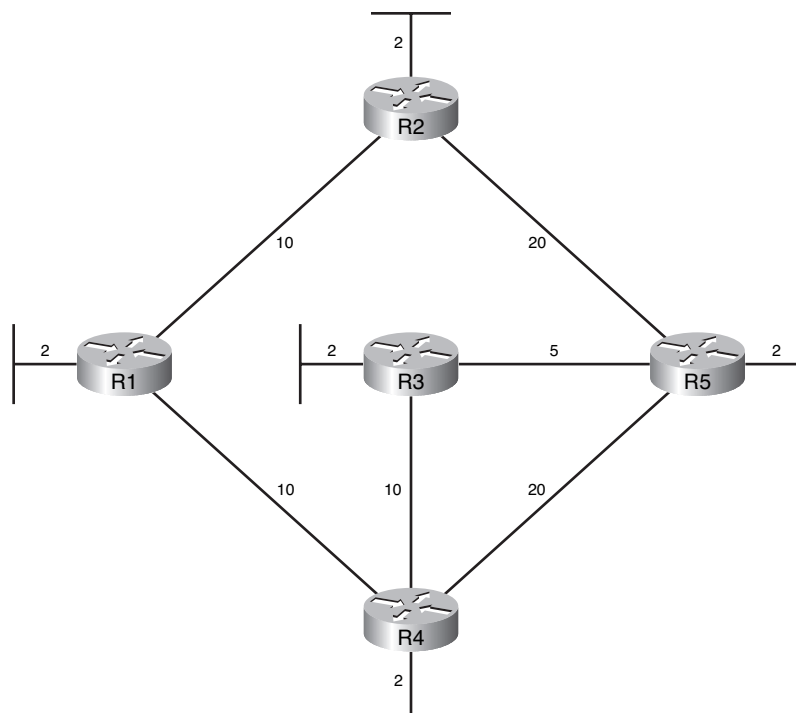


Table 10-1 SPF Tree for R1

Destination	Shortest Path	Cost
R2 LAN	R1 to R2	12
R3 LAN	R1 to R4 to R3	22
R4 LAN	R1 to R4	12
R5 LAN	R1 to R4 to R3 to R5	27

Table 10-2 SPF Tree for R2

Destination	Shortest Path	Cost
R1 LAN	R2 to R1	12
R3 LAN	R2 to R5 to R3	27
R4 LAN	R2 to R1 to R4	22
R5 LAN	R2 to R5	22

**Table 10-3 SPF Tree for R3**

Destination	Shortest Path	Cost
R1 LAN	R3 to R4 to R1	22
R2 LAN	R3 to R5 to R2	27
R4 LAN	R3 to R4	12
R5 LAN	R3 to R5	7

**Table 10-4 SPF Tree for R4**

Destination	Shortest Path	Cost
R1 LAN	R4 to R1	12
R2 LAN	R4 to R1 to R2	22
R3 LAN	R4 to R3	12
R5 LAN	R4 to R3 to R5	17

**Table 10-5 SPF Tree for R5**

Destination	Shortest Path	Cost
R1 LAN	R5 to R3 to R4 to R1	27
R2 LAN	R5 to R2	22
R3 LAN	R5 to R3	7
R4 LAN	R5 to R3 to R4	17

### *Link-State Routing Process*

All routers in our topology will complete the following generic link-state routing process to reach a state of convergence:

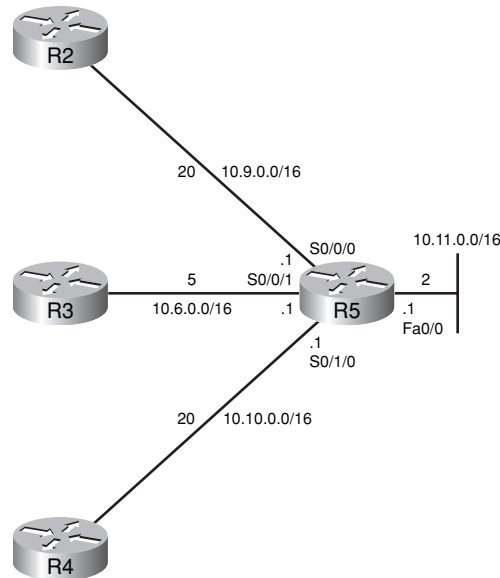
1. Each router learns about its own links, its own directly connected networks. This is done by detecting that an interface is in the **up** state.
2. Each router is responsible for meeting its neighbors on directly connected networks. Similar to Enhanced Interior Gateway Routing Protocol (EIGRP), link-state routers do this by exchanging **Hello** packets with other link-state routers on **directly connected** networks.
3. Each router builds a link-state packet (LSP) containing the state of each **directly connected** link. This is done by recording all the pertinent information about each neighbor, including **neighbor ID**, **link type**, and **bandwidth**.
4. Each router floods the LSP to all neighbors, who then store all LSPs received in a **database**. Neighbors then flood the LSPs to their neighbors until all routers in the area have received the LSPs. Each router stores a copy of each LSP received from its neighbors in a local **database**.
5. Each router uses the **database** to construct a complete map of the **topology** and computes the best path to each destination network.

We will discuss this process in more detail in the following topics.

### *Learning About Directly Connected Networks*

The topology in Figure 10-2 now shows the network addresses and interfaces for R5.

**Figure 10-2 Topology of the Perspective of R5**



The first step in the link-state routing process is *each router learns about its own links, its own directly connected networks*. This occurs when you correctly configure and activate the interfaces.

In Table 10-6, list the link-state information for R5, including the network address, type of interface, address, cost and neighbor.

**Table 10-6 Link-State Information for R5**

Network Address	Interface	IP Address	Cost	Neighbor
10.9.0.0/16	S0/0/0	10.9.0.1	20	R2
10.6.0.0/16	S0/0/1	10.6.0.1	5	R3
10.10.0.0/16	S0/1/0	10.10.0.1	20	R4
10.11.0.0/16	Fa0/0	10.11.0.1	2	None

### *Sending Hello Packets to Neighbors*

The second step in the link-state routing process is *each router is responsible for meeting its neighbors on directly connected networks*.

Routers with link-state routing protocols use a **Hello** protocol to discover any neighbors on its links. In relation to link state routing, what is a neighbor?

A neighbor is any other router that is enabled with the same link-state routing protocol.

Small Hello packets are periodically exchanged between two adjacent neighbors, which serve as a “keepalive” function to monitor the state of the neighbor. If a router stops receiving Hello packets from a neighbor, that neighbor is considered unreachable and the adjacency is broken.

#### *Building the Link-State Packet*

The third step in the link-state routing process is *each router builds a link-state packet (LSP) containing the state of each directly connected link.*

After a router has established its adjacencies, it can build its link-state packets (LSP) that contain the link-state information about its links. The table you filled out previously contains all the information for R5’s LSP.

#### *Flooding Link-State Packets to Neighbors*

The fourth step in the link-state routing process is *each router floods the LSP to all neighbors, who then store all LSPs received in a database.*

What happens when a router receives an LSP from a neighbor?

Whenever a router receives an LSP from a neighboring router, it immediately sends that LSP out all other interfaces except the interface that received the LSP. This process creates a flooding effect of LSPs from all routers throughout the routing area.

With triggered updates, distance vector routing protocols also send out updates when there is a change. What is one reason why link-state routing protocols converge faster?

Unlike distance vector routing protocols, which must first run the Bellman-Ford algorithm to process routing updates before sending them to other routers, link-state routing protocols calculate the SPF algorithm after the flooding is complete. As a result, link-state routing protocols reach convergence much faster than distance vector routing protocols.

#### *Constructing a Link-State Database*

The final step in the link-state routing process is *each router uses the database to construct a complete map of the topology and computes the best path to each destination network.*

After each router has propagated its own LSPs using the link-state flooding process, each router will then have an LSP from every link-state router in the routing area. These LSPs are stored in the link-state database. Each router in the routing area can now use the SPF algorithm to construct the SPF trees that you saw earlier.

Figure 10-3 shows the entire topology, with network addresses.



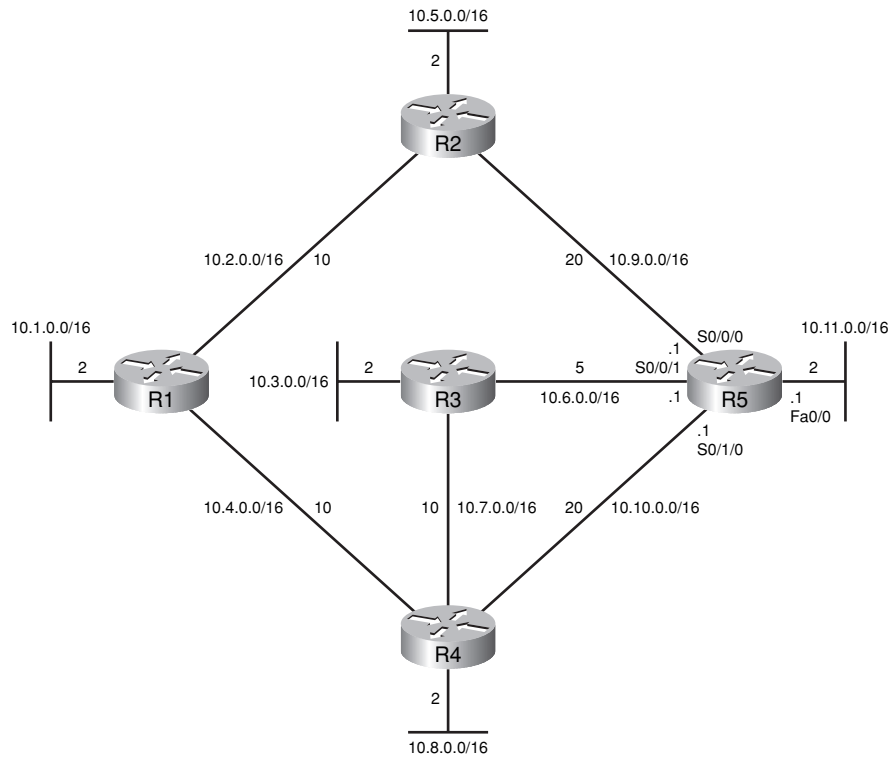
**Figure 10-3 Topology of Link-State Routers with Network Addresses**

Table 10-7 shows partial information in the link-state database for R5 after all LSPs have been received and R5 is ready to calculate the SPF algorithm. Fill in the missing information.

**Table 10-7 Link-State Database for R5****LSPs from R1:**


---



---

Connected to neighbor **R2** on network **10.2.0.0/16**, cost of **10**

---

Connected to neighbor **R4** on network **10.4.0.0/16**, cost of **10**

---

Has a network **10.1.0.0/16**, cost of **2**

**LSPs from R2:**


---

Connected to neighbor **R1** on network **10.2.0.0/16**, cost of **10**

---

Connected to neighbor **R5** on network **10.9.0.0/16**, cost of **20**

---

Has a network **10.5.0.0/16**, cost of **2**

**LSPs from R3:**


---

Connected to neighbor **R5** on network **10.6.0.0/16**, cost of **5**

---

Connected to neighbor **R4** on network **10.7.0.0/16**, cost of **10**

---

Has a network **10.3.0.0/16**, cost of **2**

**LSPs from R4:**


---

Connected to neighbor **R1** on network **10.4.0.0/16**, cost of **10**

---

*continues*

**Table 10-7** Link-State Database for R5 *continued*


---

 Connected to neighbor R3 on network 10.7.0.0/16, cost of 10
 

---

 Connected to neighbor R5 on network 10.10.0.0/16, cost of 20
 

---

 Has a network 10.8.0.0/16, cost of 2
 

---

**R5 Link States:**


---

 Connected to neighbor R2 on network 10.9.0.0/16, cost of 20
 

---

 Connected to neighbor R3 on network 10.6.0.0/16, cost of 5
 

---

 Connected to neighbor R4 on network 10.10.0.0/16, cost of 20
 

---

 Has a network 10.11.0.0/16, cost of 2
 

---

*Shortest Path First (SPF) Tree*

Because all LSPs have been processed using the SPF algorithm, R5 has now constructed the complete SPF tree. Table 10-8 repeats the SPF tree for R5 that you determined earlier. Fill in the table again here.

**Table 10-8** SPF Tree for R5

Destination	Shortest Path	Cost
R1 LAN	R5 to R3 to R4 to R1	27
R2 LAN	R5 to R2	22
R3 LAN	R5 to R3	7
R4 LAN	R5 to R3 to R4	17

Using this tree, the SPF algorithm results indicate the shortest path to each network. Only the LANs are shown in the table, but SPF can also be used to determine the shortest path to each WAN link network shown in Figure 10-3 shown earlier. Complete the missing information in the following list for R5's shortest path to each network:

- Network 10.1.0.0/16 via R5 Serial 0/0/1 at a cost of 27
- Network 10.2.0.0/16 via R2 Serial 0/0/0 at a cost of 30
- Network 10.3.0.0/16 via R3 Serial 0/0/1 at a cost of 7
- Network 10.4.0.0/16 via R3 Serial 0/0/1 at a cost of 25
- Network 10.5.0.0/16 via R2 Serial 0/0/0 at a cost of 22
- Network 10.7.0.0/16 via R3 Serial 0/0/1 at a cost of 15
- Network 10.8.0.0/16 via R3 Serial 0/0/1 at a cost of 17

## Implementing Link-State Routing Protocols

The following sections include exercises covering the advantages and requirements of link-state routing protocols.

## Advantages of a Link-State Routing Protocol Exercise

Explain briefly why each of the following is an advantage of link-state routing protocols over distance vector routing protocols.

---

**Instructor note:** The following answers are direct quotes from the text. The student should be encouraged to answer these question in his or her own words.

---

### *Builds a Topological Map*

Link-state routing protocols create a topological map, or SPF tree, of the network topology. Distance vector routing protocols do not have a topological map of the network. Routers implementing a distance vector routing protocol only have a list of networks, which includes the cost (distance) and next-hop routers (direction) to those networks. Because link-state routing protocols exchange link states, the SPF algorithm can build an SPF tree of the network. Using the SPF tree, each router can independently determine the shortest path to every network.

### *Fast Convergence*

There are several reasons why a link-state routing protocol converges faster than a distance vector routing protocol. When receiving a link-state packet (LSP), link-state routing protocols immediately flood the LSP out all interfaces except for the interface from which the LSP was received. A router using a distance vector routing protocol needs to process each routing update and update its routing table before flooding them out other interfaces, even with triggered updates. Another reason is the lack of a hold-down timer, which is a distance vector routing protocol feature designed to give the network time to converge. Link-state routing protocols do not use a hold-down timer because any changes in the topology are flooded immediately within the entire routing domain using LSPs.

### *Event-Driven Updates*

After the initial flooding of LSPs, link-state routing protocols only send out an LSP when there is a change in the topology. The LSP contains only the information regarding the affected link. Unlike some distance vector routing protocols, link-state routing protocols do not send periodic updates.

### *Hierarchical Design*

Link-state routing protocols such as OSPF and IS-IS use the concept of areas. Multiple areas create a hierarchical design to networks, allowing better route aggregation (summarization) and the isolation of routing issues within an area. Multiarea OSPF and IS-IS are discussed further in CCNP.

## Requirements of a Link-State Routing Protocol Exercise

Explain briefly why each of the following requirements is important when a network administrator is considering implementing a link-state routing protocol.

---

**Instructor note:** The following answers are direct quotes from the text. The student should be encouraged to answer these questions in his or her own words.

---

### *Memory Requirements*

Link-state routing protocols typically require more memory, more CPU processing, and at times more bandwidth than distance vector routing protocols. The memory requirements are because of the use of link-state databases and the creation of the SPF tree.

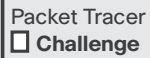
*Processing Requirements*

Link-state protocols can also require more CPU processing than distance vector routing protocols. The SPF algorithm requires more CPU time than distance vector algorithms such as Bellman-Ford because link-state protocols build a complete map of the topology.

*Bandwidth Requirements*

The flooding of link-state packets can adversely affect the available bandwidth on a network. This should only occur during initial startup of routers, but can also be an issue on unstable networks.

## Labs and Activities



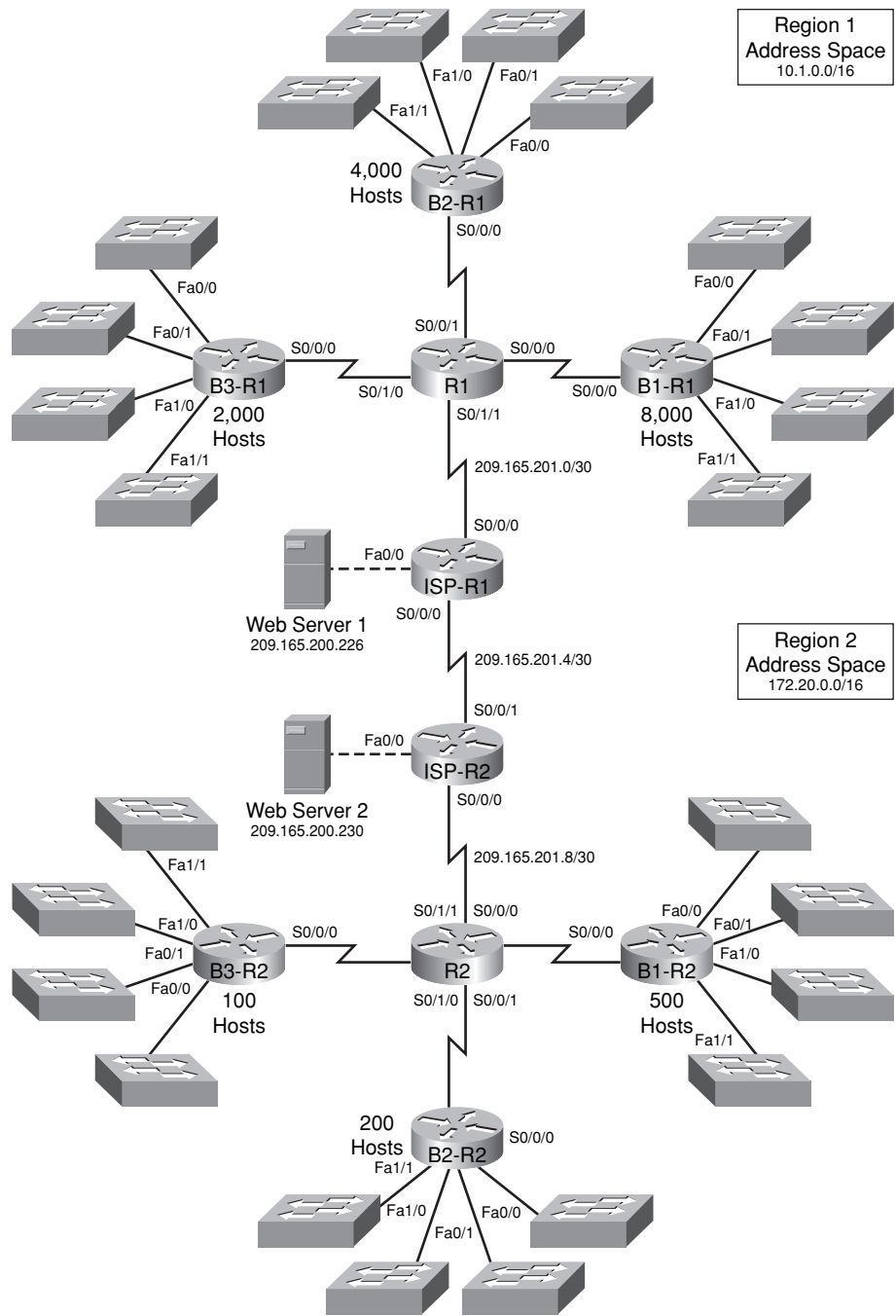
### Packet Tracer Skills Integration Challenge: EIGRP and RIPv2 Configuration

Upon completion of this challenge, you will be able to

- Design and document an addressing scheme based on requirements
- Apply a basic configuration to the devices
- Configure static routing between ISP routers
- Configure EIGRP routing in Region 1 and RIPv2 routing Region 2
- Disable routing updates on appropriate interfaces
- Configure and redistribute default routes
- Verify full connectivity between all devices in the topology

Open the file LSG02-PTSkills10.pka on the CD-ROM that accompanies this book. You will use the topology in Figure 10-4 and the addressing tables in Tables 10-9 and 10-10 to document your design.

Figure 10-4 Packet Tracer Skills Integration Challenge Topology



**Table 10-9 Addressing Table for R1**

<b>Device</b>	<b>Interface</b>	<b>IP Address</b>	<b>Subnet Mask</b>
R1	S0/0/0	10.1.64.1	255.255.255.252
	S0/0/1	10.1.64.5	255.255.255.252
	S0/1/0	10.1.64.9	255.255.255.252
	S0/1/1	209.165.201.2	255.255.255.252
B1-R1	Fa0/0	10.1.0.1	255.255.248.0
	Fa0/1	10.1.8.1	255.255.248.0
	Fa1/0	10.1.16.1	255.255.248.0
	Fa1/1	10.1.24.1	255.255.248.0
	S0/0/0	10.1.64.2	255.255.255.252
B2-R1	Fa0/0	10.1.32.1	255.255.252.0
	Fa0/1	10.1.36.1	255.255.252.0
	Fa1/0	10.1.40.1	255.255.252.0
	Fa1/1	10.1.44.1	255.255.252.0
	S0/0/0	10.1.64.6	255.255.255.252
B3-R1	Fa0/0	10.1.48.1	255.255.254.0
	Fa0/1	10.1.50.1	255.255.254.0
	Fa1/0	10.1.52.1	255.255.254.0
	Fa1/1	10.1.54.1	255.255.254.0
	S0/0/0	10.1.64.10	255.255.255.252
ISP-R1	S0/0/0	209.165.201.1	255.255.255.252
	S0/0/1	209.165.201.5	255.255.255.252
	Fa0/0	209.165.200.225	255.255.255.252
Web Server 1	NIC	209.165.200.226	255.255.255.252

**Table 10-10 Addressing Table for R2**

<b>Device</b>	<b>Interface</b>	<b>IP Address</b>	<b>Subnet Mask</b>
R2	S0/0/0	172.20.4.1	255.255.255.252
	S0/0/1	172.20.4.5	255.255.255.252
	S0/1/0	172.20.4.9	255.255.255.252
	S0/1/1	209.165.201.10	255.255.255.252

*continues*

**Table 10-10 Addressing Table for R2** *continued*

Device	Interface	IP Address	Subnet Mask
B1-R2	Fa0/0	172.20.0.1	255.255.255.128
	Fa0/1	172.20.0.129	255.255.255.128
	Fa1/0	172.20.1.1	255.255.255.128
	Fa1/1	172.20.1.129	255.255.255.128
	S0/0/0	172.20.4.2	255.255.255.252
B2-R2	Fa0/0	172.20.2.1	255.255.255.192
	Fa0/1	172.20.2.65	255.255.255.192
	Fa1/0	172.20.2.129	255.255.255.192
	Fa1/1	172.20.2.193	255.255.255.192
	S0/0/0	172.20.4.6	255.255.255.252
B3-R2	Fa0/0	172.20.3.1	255.255.255.224
	Fa0/1	172.20.3.33	255.255.255.224
	Fa1/0	172.20.3.65	255.255.255.224
	Fa1/1	172.20.3.97	255.255.255.224
	S0/0/0	172.20.4.10	255.255.255.252
ISP-R2	S0/0/0	209.165.201.9	255.255.255.252
	S0/0/1	209.165.201.6	255.255.255.252
	Fa0/0	209.165.200.229	255.255.255.252
Web Server 2	NIC	209.165.200.230	255.255.255.252

## Task 1: Design and Document an Addressing Scheme

**Step 1.** Design an addressing scheme.

Using the topology in Figure 10-4 and the following requirements, design an addressing scheme:

- The WAN links between R1 and R2 and their respective ISP routers are already configured. Also, the links between the ISPs and the web servers are already configured.
- The address space for Region 1 is 10.1.0.0/16. Each branch router (B1-R1, B2-R1, and B3-R1) should be allotted address space based on the following requirements. Starting with the largest requirement, assign address space to each router:
  - B1-R1 needs space for 8000 hosts [10.1.0.0/19](#)
  - B2-R1 needs space for 4000 hosts [10.1.32.0/20](#)
  - B3-R1 needs space for 2000 hosts [10.1.48.0/21](#)
- Divide the address space for each branch router into four equal subnets. Record the subnets in the tables that follow.



Router B1-R1 Interface	Subnet Number	Subnet Address
Fa0/0	0	10.1.0.0/21
Fa0/1	1	10.1.8.0/21
Fa1/0	2	10.1.16.0/21
Fa1/1	3	10.1.24.0/21

Router B2-R1 Interface	Subnet Number	Subnet Address
Fa0/0	0	10.1.32.0/22
Fa0/1	1	10.1.36.0/22
Fa1/0	2	10.1.40.0/22
Fa1/1	3	10.1.44.0/22

Router B3-R1 Interface	Subnet Number	Subnet Address
Fa0/0	0	10.1.48.0/23
Fa0/1	1	10.1.50.0/23
Fa1/0	2	10.1.52.0/23
Fa1/1	3	10.1.54.0/23

- For the WANs in Region 1, subnet the address space 10.1.64.0/28. Record the subnets in the table that follows.

Router	Subnet Number	Subnet Address
B1-R1 <—> R1	0	10.1.64.0/30
B2-R1 <—> R1	1	10.1.64.4/30
B3-R1 <—> R1	2	10.1.64.8/30

- The address space for Region 2 is 172.20.0.0/16. Each branch router (B1-R2, B2-R2, and B3-R2) should be allotted address space based on the following requirements. Starting with the largest requirement, assign address space to each router:
  - B1-R2 needs space for 500 hosts [172.20.0.0/23](#)
  - B2-R2 needs space for 200 hosts [172.20.2.0/24](#)
  - B3-R2 needs space for 100 hosts [172.20.3.0/25](#)
- Divide the address space for each branch router into four equal subnets. Record the subnets in the tables that follow.

Router B1-R2 Interface	Subnet Number	Subnet Address
Fa0/0	0	172.20.0.0/25
Fa0/1	1	172.20.0.128/25
Fa1/0	2	172.20.1.0/25
Fa1/1	3	172.20.1.128/25

Router B2-R2 Interface	Subnet Number	Subnet Address
Fa0/0	0	172.20.2.0/26
Fa0/1	1	172.20.2.64/26
Fa1/0	2	172.20.2.128/26
Fa1/1	3	172.20.2.192/26

Router B3-R2 Interface	Subnet Number	Subnet Address
Fa0/0	0	172.20.3.0/27
Fa0/1	1	172.20.3.32/27
Fa1/0	2	172.20.3.64/27
Fa1/1	3	172.20.3.96/27

- For the WANs in Region 2, subnet the address space 172.20.255.240/28. Record the subnets in the table that follows.

Router	Subnet Number	Subnet Address
B1-R2 <—> R2	0	172.20.4.0/30
B2-R2 <—> R2	1	172.20.4.4/30
B3-R2 <—> R2	2	172.20.4.8/30

**Step 2.** Document the addressing scheme.

- (Optional) On the topology in Figure 10-4, label each subnet. To save space, use only the last two octets because only these octets change.
- Use the table provided in the printed instructions to document the IP addresses and subnet masks. Assign the first IP address to the router interface.
- For the WAN links, assign the first IP address to R1 and R2 for links to each router's respective B1, B2, and B3 routers.

## Task 2: Apply a Basic Configuration

Using your documentation, configure the routers with basic configurations including addressing. Use **cisco** as the line passwords and **class** as the secret password. Use **64000** as the clock rate.

## Task 3: Configure Static Routing Between ISP Routers

Each ISP router already has two static routes to the other ISP router's directly connected WANs. Implement static routing on each ISP router to ensure connectivity between the two regions.

## Task 4: Configure EIGRP Routing in Region 1 and RIPv2 Routing Region 2

**Step 1.** Configure EIGRP routing in Region 1.

Configure all routers in Region 1 (R1, B1-R1, B2-R1, and B3-R1) with EIGRP as the dynamic routing protocol.

- Use 1 as the process ID for EIGRP.
- Disable automatic summarization.
- Manually summarize routes advertised by the branch routers to R1 so that only one route is sent. (Note: The current version of Packet Tracer allows the configuration of the summary command. However, the routing tables will still display as if summarization has not been configured. This is a known bug that will be addressed in a future release.)
- Configure the Hello intervals on the branch routers to 30 seconds.

**Step 2.** Configure RIPv2 routing Region 2.

Configure all routers in Region 2 (R2, B1-R2, B2-R2, and B3-R2) with RIPv2 as the dynamic routing protocol. Disable automatic summarization.

## Task 5: Disable Routing Updates on Appropriate Interfaces

Routing updates do not need to be sent out all the router interfaces. Disable routing updates on appropriate interfaces.

## Task 6: Configure and Redistribute Default Routes

Packet Tracer does not yet support the redistribution of static default routes with EIGRP. Therefore, you must configure all routers in Region 1 with a default route. Use the exit interface argument.

Configure the appropriate router in Region 2 with a default route. Then configure that router to redistribute the default route to all other routers in the region.

## Task 7: Verify Full Connectivity Between All Devices in the Topology

**Step 1.** Test connectivity.

You should now have end-to-end connectivity. Use **ping** to test connectivity across the network. Each router should be able to ping all other router interfaces and both Web Servers.

Troubleshoot until pings are successful.

**Step 2.** Examine the configuration.

Use verification commands to make sure that your configurations are complete.

The Study Guide portion of this chapter uses a combination of matching, fill-in-the-blank, multiple-choice, and open-ended question exercises to test your knowledge of OSPF concepts and configurations.

The Labs and Activities portion of this chapter includes all the online curriculum labs, an additional comprehensive lab, and an additional challenge lab to ensure that you have mastered the practical, hands-on skills needed to configure and verify OSPF routing.

As you work through this chapter, use Chapter 11 in *Routing Protocols and Concepts, CCNA Exploration Companion Guide* or use the corresponding Chapter 11 in the Exploration Routing Protocols and Concepts online curriculum for assistance.

## Study Guide

### Introduction to OSPF

Open Shortest Path First (OSPF) is a link-state routing protocol that was developed as a replacement for the distance vector Routing Information Protocol (RIP). RIP was an acceptable routing protocol in the early days of networking and the Internet, but its reliance on hop count as the only measure for choosing the best route quickly became unacceptable in larger networks that needed a more robust routing solution. OSPF is a classless routing protocol that uses the concept of areas for scalability. RFC 2328 defines the OSPF metric as an arbitrary value called cost. Cisco IOS Software uses bandwidth as the OSPF cost metric. In the following sections of the Study Guide, you will review basic OSPF concepts and protocols.

## Vocabulary Exercise: Matching

Match the definition on the left with a term on the right.

### Definitions

- a. Responsible for updating all other OSPF routers when a change occurs in the multiaccess network
- b. OSPF packet used to reply to LSRs as well as to announce new information
- c. Attaches to multiple areas, maintains separate link-state databases for each area it is connected to, and routes traffic destined for or arriving from other areas
- d. Describes the details of OSPF link-state concepts and operations
- e. Sent by an OSPF router to confirm receipt of an LSU
- f. Monitors the DR and takes over as DR if the current DR fails
- g. When a failure occurs in the network, such as when a neighbor becomes unreachable, these are flooded throughout an area
- h. An open standard, link-state routing protocol designed to address the limitations of RIP
- i. An OSPF router that is neither DR or BDR but participates in the OSPF process on a multiaccess network
- j. A network that cycles between an up state and a down state
- k. Connects to an external routing domain that uses a different routing policy
- l. Contains an abbreviated list of the sending router's link-state database and is used by receiving routers to check against the local link-state database
- m. When this is *not* equal, the router with the highest number will be the DR regardless of router ID values
- n. This is the router ID for an OSPF router if no loopbacks are configured
- o. Asks for more information about any entry in the DBD

### Terms

- c area border router (ABR)
- k Autonomous System Boundary Router (ASBR)
- f backup designated router (BDR)
- l database description (DBD)
- a designated router (DR)
- i DRothers
- j flapping link
- n highest IP address
- e link-state acknowledgment (LSAck)
- g link-state advertisements (LSA)
- o link-state request (LSR)
- b link-state update (LSU)
- h Open Shortest Path First (OSPF)
- d RFC 2328
- m router priority

## OSPF Concepts Exercise

### Background of OSPF

The initial development of OSPF began in 1987 by the [Internet Engineering Task Force \(IETF\)](#) OSPF Working Group. At that time, the Internet was largely an academic and research network funded by the U.S. government.

In 1998, the OSPFv2 specification was updated to the current version reflected in RFC [2328](#). Because OSPF is an open standard, you can easily find the RFC online. List one website where the OSPF RFC can be found:

<http://www.ietf.org/rfc/rfc2328>

### OSPF Message Encapsulation

The data portion of an OSPF message is encapsulated in a packet. This data field can include one of five OSPF packet types. Each packet type is briefly discussed in the next topic.

Figure 11-1 shows an example of an encapsulated OSPF message. Fill in the missing field contents.

**Figure 11-1 Encapsulated OSPF Message (Answer)**

Data Link Frame Header	IP Packet Header	OSPF Packet Header	OSPF Packet Type-Specific Data																																																												
Data Link Frame (Ethernet Fields Shown Here)																																																															
MAC Source Address = Address of Sending Interface																																																															
MAC Destination Address = Multicast: 01-00-5E-00-00-05 or 01-00-5E-00-00-06																																																															
<table border="1"> <tr> <td colspan="4">IP Packet</td> </tr> <tr> <td colspan="4">IP Source Address = Address of Sending Interface</td> </tr> <tr> <td colspan="4">IP Destination Address = Multicast: <a href="#">224.0.0.5</a> or <a href="#">224.0.0.6</a></td> </tr> <tr> <td colspan="4">Protocol Field = <a href="#">89 for OSPF</a></td> </tr> <tr> <td colspan="4"> <table border="1"> <tr> <td colspan="4">OSPF Packet Header</td> </tr> <tr> <td colspan="4">Type Code for OSPF Packet Type</td> </tr> <tr> <td colspan="4">Router ID and Area ID</td> </tr> <tr> <td colspan="4"> <table border="1"> <tr> <td colspan="4">OSPF Packet Types</td> </tr> <tr> <td>0x01</td> <td><a href="#">Hello</a></td> <td colspan="2"></td> </tr> <tr> <td>0x02</td> <td><a href="#">Database Description (DD)</a></td> <td colspan="2"></td> </tr> <tr> <td>0x03</td> <td><a href="#">Link State Request</a></td> <td colspan="2"></td> </tr> <tr> <td>0x04</td> <td><a href="#">Link State Update</a></td> <td colspan="2"></td> </tr> <tr> <td>0x05</td> <td><a href="#">Link State Acknowledgment</a></td> <td colspan="2"></td> </tr> </table> </td> </tr> </table> </td> </tr> </table>				IP Packet				IP Source Address = Address of Sending Interface				IP Destination Address = Multicast: <a href="#">224.0.0.5</a> or <a href="#">224.0.0.6</a>				Protocol Field = <a href="#">89 for OSPF</a>				<table border="1"> <tr> <td colspan="4">OSPF Packet Header</td> </tr> <tr> <td colspan="4">Type Code for OSPF Packet Type</td> </tr> <tr> <td colspan="4">Router ID and Area ID</td> </tr> <tr> <td colspan="4"> <table border="1"> <tr> <td colspan="4">OSPF Packet Types</td> </tr> <tr> <td>0x01</td> <td><a href="#">Hello</a></td> <td colspan="2"></td> </tr> <tr> <td>0x02</td> <td><a href="#">Database Description (DD)</a></td> <td colspan="2"></td> </tr> <tr> <td>0x03</td> <td><a href="#">Link State Request</a></td> <td colspan="2"></td> </tr> <tr> <td>0x04</td> <td><a href="#">Link State Update</a></td> <td colspan="2"></td> </tr> <tr> <td>0x05</td> <td><a href="#">Link State Acknowledgment</a></td> <td colspan="2"></td> </tr> </table> </td> </tr> </table>				OSPF Packet Header				Type Code for OSPF Packet Type				Router ID and Area ID				<table border="1"> <tr> <td colspan="4">OSPF Packet Types</td> </tr> <tr> <td>0x01</td> <td><a href="#">Hello</a></td> <td colspan="2"></td> </tr> <tr> <td>0x02</td> <td><a href="#">Database Description (DD)</a></td> <td colspan="2"></td> </tr> <tr> <td>0x03</td> <td><a href="#">Link State Request</a></td> <td colspan="2"></td> </tr> <tr> <td>0x04</td> <td><a href="#">Link State Update</a></td> <td colspan="2"></td> </tr> <tr> <td>0x05</td> <td><a href="#">Link State Acknowledgment</a></td> <td colspan="2"></td> </tr> </table>				OSPF Packet Types				0x01	<a href="#">Hello</a>			0x02	<a href="#">Database Description (DD)</a>			0x03	<a href="#">Link State Request</a>			0x04	<a href="#">Link State Update</a>			0x05	<a href="#">Link State Acknowledgment</a>		
IP Packet																																																															
IP Source Address = Address of Sending Interface																																																															
IP Destination Address = Multicast: <a href="#">224.0.0.5</a> or <a href="#">224.0.0.6</a>																																																															
Protocol Field = <a href="#">89 for OSPF</a>																																																															
<table border="1"> <tr> <td colspan="4">OSPF Packet Header</td> </tr> <tr> <td colspan="4">Type Code for OSPF Packet Type</td> </tr> <tr> <td colspan="4">Router ID and Area ID</td> </tr> <tr> <td colspan="4"> <table border="1"> <tr> <td colspan="4">OSPF Packet Types</td> </tr> <tr> <td>0x01</td> <td><a href="#">Hello</a></td> <td colspan="2"></td> </tr> <tr> <td>0x02</td> <td><a href="#">Database Description (DD)</a></td> <td colspan="2"></td> </tr> <tr> <td>0x03</td> <td><a href="#">Link State Request</a></td> <td colspan="2"></td> </tr> <tr> <td>0x04</td> <td><a href="#">Link State Update</a></td> <td colspan="2"></td> </tr> <tr> <td>0x05</td> <td><a href="#">Link State Acknowledgment</a></td> <td colspan="2"></td> </tr> </table> </td> </tr> </table>				OSPF Packet Header				Type Code for OSPF Packet Type				Router ID and Area ID				<table border="1"> <tr> <td colspan="4">OSPF Packet Types</td> </tr> <tr> <td>0x01</td> <td><a href="#">Hello</a></td> <td colspan="2"></td> </tr> <tr> <td>0x02</td> <td><a href="#">Database Description (DD)</a></td> <td colspan="2"></td> </tr> <tr> <td>0x03</td> <td><a href="#">Link State Request</a></td> <td colspan="2"></td> </tr> <tr> <td>0x04</td> <td><a href="#">Link State Update</a></td> <td colspan="2"></td> </tr> <tr> <td>0x05</td> <td><a href="#">Link State Acknowledgment</a></td> <td colspan="2"></td> </tr> </table>				OSPF Packet Types				0x01	<a href="#">Hello</a>			0x02	<a href="#">Database Description (DD)</a>			0x03	<a href="#">Link State Request</a>			0x04	<a href="#">Link State Update</a>			0x05	<a href="#">Link State Acknowledgment</a>																						
OSPF Packet Header																																																															
Type Code for OSPF Packet Type																																																															
Router ID and Area ID																																																															
<table border="1"> <tr> <td colspan="4">OSPF Packet Types</td> </tr> <tr> <td>0x01</td> <td><a href="#">Hello</a></td> <td colspan="2"></td> </tr> <tr> <td>0x02</td> <td><a href="#">Database Description (DD)</a></td> <td colspan="2"></td> </tr> <tr> <td>0x03</td> <td><a href="#">Link State Request</a></td> <td colspan="2"></td> </tr> <tr> <td>0x04</td> <td><a href="#">Link State Update</a></td> <td colspan="2"></td> </tr> <tr> <td>0x05</td> <td><a href="#">Link State Acknowledgment</a></td> <td colspan="2"></td> </tr> </table>				OSPF Packet Types				0x01	<a href="#">Hello</a>			0x02	<a href="#">Database Description (DD)</a>			0x03	<a href="#">Link State Request</a>			0x04	<a href="#">Link State Update</a>			0x05	<a href="#">Link State Acknowledgment</a>																																						
OSPF Packet Types																																																															
0x01	<a href="#">Hello</a>																																																														
0x02	<a href="#">Database Description (DD)</a>																																																														
0x03	<a href="#">Link State Request</a>																																																														
0x04	<a href="#">Link State Update</a>																																																														
0x05	<a href="#">Link State Acknowledgment</a>																																																														

### OSPF Packet Types

The following list describes the five different types of OSPF link-state packets (LSP). Each packet serves a specific purpose in the OSPF routing process. Fill in the name for each packet type.

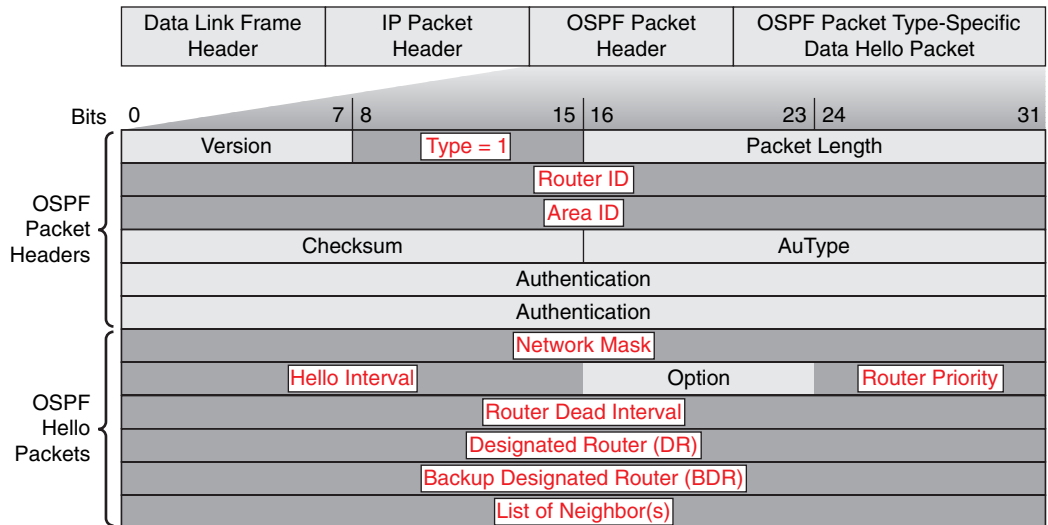
1. [Hello](#): Used to establish and maintain adjacency with other OSPF routers
2. [Database description \(DBD\)](#): Contains an abbreviated list of the sending router's link-state database and is used by receiving routers to check against the local link-state database
3. [Link-state request \(LSR\)](#): A request for more information about an entry in the DBD
4. [Link-state update \(LSU\)](#): Used to reply to LSRs as well as to announce new information
5. [Link-state acknowledgment \(LSAck\)](#): Confirms receipt of an LSU



### Hello Protocol

Every OSPF message includes the header, as shown in Figure 11-2. Also shown in the figure are the fields of the OSPF Hello packet. Fill in the missing field contents.

**Figure 11-2 OSPF Message Format (Answer)**



Receiving a **Hello** packet on an interface confirms for a router that there is another OSPF router on this link. OSPF then establishes **adjacency** with the neighbor.

Before two routers can form an OSPF neighbor **adjacency**, they must agree on three values: **Hello** interval, **Dead** interval, and **network** type. The OSPF **Hello** interval indicates how often an OSPF router transmits its Hello packets. By default, OSPF Hello packets are sent every **10** seconds on multi-access and point-to-point segments and every **30** seconds on nonbroadcast multiaccess (NBMA) segments (Frame Relay, X.25, ATM).

In most cases, OSPF Hello packets are sent as multicast to an address reserved for *ALLSPFRouters* at **224.0.0.5**.

The **Dead** interval is the period, expressed in seconds, that the router will wait to receive a Hello packet before declaring the neighbor “down.” Cisco uses a default of **four** times the Hello interval. For multiaccess and point-to-point segments, this period is **40** seconds. For NBMA networks, the **Dead** interval is **120** seconds.

If the **Dead** interval expires before the routers receive a Hello packet, OSPF will remove that neighbor from its link-state database.

To reduce the amount of OSPF traffic on multiaccess networks, OSPF elects a **designated router (DR)** and **backup designated router (BDR)**. The **DR** is responsible for updating all other OSPF routers (called **DRothers**) when a change occurs in the multiaccess network. The **BDR** monitors the **DR** and takes over as the **DR** if the current **DR** fails.

### OSPF Link-State Updates

Link-state updates (LSU) are the packets used for OSPF routing updates. An LSU packet can contain **11** different types of **link-state advertisements (LSA)**.

### OSPF Algorithm

Each OSPF router maintains a [link-state database](#) containing the [LSAs](#) received from all other routers. After a router has received all [LSAs](#) and built its local [link-state database](#), OSPF uses Dijkstra's [shortest path first \(SPF\)](#) algorithm to create an [SPF](#) tree. The [SPF](#) tree is then used to populate the IP [routing table](#) with the best paths to each network.

### Administrative Distance

With this chapter, you have learned all the administrative distances for the routing protocols covered on the CCNA exam. Fill in the missing route sources and administrative distance (AD) values in Table 11-1.

**Table 11-1 Default Administrative Distances**

Route Source	AD
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

## Basic OSPF Configuration

Now that you have a good understanding of how OSPF works, it is time to learn the configuration commands you use for OSPF. The first exercise in the following sections will take you step by step through an OSPF configuration. The second exercise reviews verification commands.

### Learn the OSPF Commands Exercise

1. Document the command syntax, including the router prompt, to configure the OSPF routing process.  
`Router(config)# router ospf process-id`
2. The value for *process-id* can be any number between 1 and 65,535.
3. True or False: All routers in an area must have the same *process-id*.

False. The *process-id* is only significant to the local router and has no meaning to other OSPF neighbors. OSPF neighbors are unaware of what process ID the local router is using. However, it is considered a best practice to maintain a consistent process ID throughout the routing domain.

- Document the command syntax, including the router prompt, for adding network statements to the OSPF routing process.

```
Router(config-router)# network address wildcard-mask area area-id
```

- For single-area OSPF configurations, the *area-id* parameter is normally set to 0.
- The *wildcard-mask* argument is simply the inverse of the subnet mask. List the corresponding wildcard mask for each of the following subnet masks:

255.255.255.0: 0.0.0.255

255.255.255.128: 0.0.0.127

255.255.255.192: 0.0.0.63

255.255.255.240: 0.0.0.15

255.255.0.0: 0.0.255.255

255.255.252.0: 0.0.3.255

255.255.240.0: 0.0.15.255

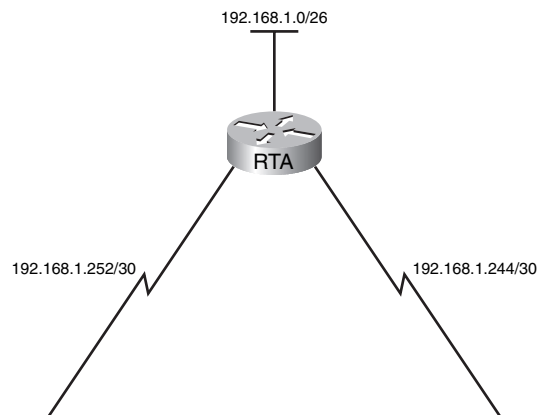
255.0.0.0: 0.255.255.255

255.224.0.0: 0.31.255.255

255.248.0.0: 0.7.255.255

- Refer to Figure 11-3. In the space provided, document the correct commands, including the router prompt, to configure RTA to advertise all directly connected networks in OSPF.

**Figure 11-3 RTA OSPF Configuration**



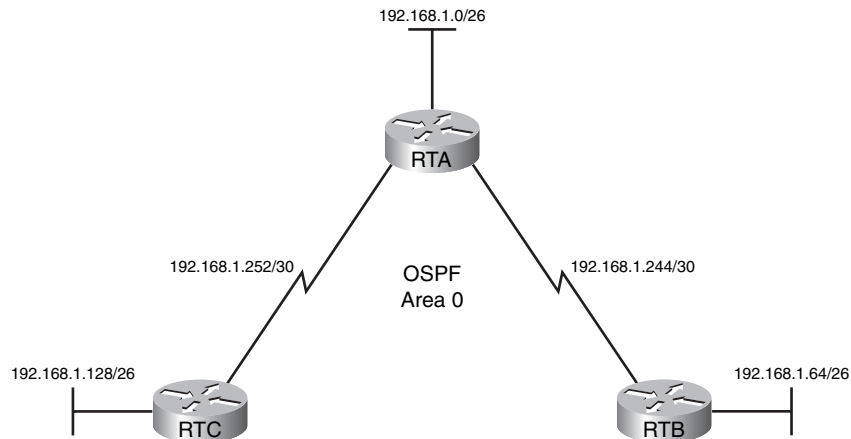
```
RTA(config)# router ospf 1
```

```
RTA(config-router)# network 192.168.1.0 0.0.0.63 area 0
```

```
RTA(config-router)# network 192.168.1.244 0.0.0.3 area 0
```

```
RTA(config-router)# network 192.168.1.252 0.0.0.3 area 0
```

- OSPF routers that share a common link become neighbors on that link. In Figure 11-4, RTB and RTC are neighbors of RTA, but not of each other. These routers send each other OSPF Hello packets to establish adjacency. These packets also act as keepalives so that each router knows that adjacent routers are still functional.

**Figure 11-4 Establishing OSPF Adjacency**

9. Using Figure 11-4, document the correct commands, including the router prompt, to configure RTB and RTC to advertise all directly connected networks in OSPF.

!OSPF Configuration for RTB.

!Note that the process-id does NOT have to match with RTA

RTB(config)# **router ospf 2**

RTB(config-router)# **network 192.168.1.64 0.0.0.63 area 0**

RTB(config-router)# **network 192.168.1.244 0.0.0.3 area 0**

!OSPF Configuration for RTC.

RTC(config)# **router ospf 3**

RTC(config-router)# **network 192.168.1.128 0.0.0.63 area 0**

RTC(config-router)# **network 192.168.1.252 0.0.0.3 area 0**

## Verify OSPF Configuration Exercise

Fill in the missing commands to complete the following sentences.

The **show ip ospf neighbor** command can be used to verify and troubleshoot OSPF neighbor relationships.

The **show ip protocols** command is a quick way to verify vital OSPF configuration information, including the OSPF process ID, router ID, networks the router is advertising, neighbors the router is receiving updates from, and default administrative distance, which is 110 for OSPF.

The **show ip ospf** command can also be used to examine the OSPF process ID and router ID. Additionally, this command displays the OSPF area information as well as the last time the SPF algorithm was calculated.

The quickest way to verify Hello and Dead intervals is to use the **show ip ospf interface** command.

The quickest way to verify OSPF convergence is to use the **show ip route** command to view the routing table for each router in the topology.

## OSPF Metric

The OSPF metric is called cost. From RFC 2328:

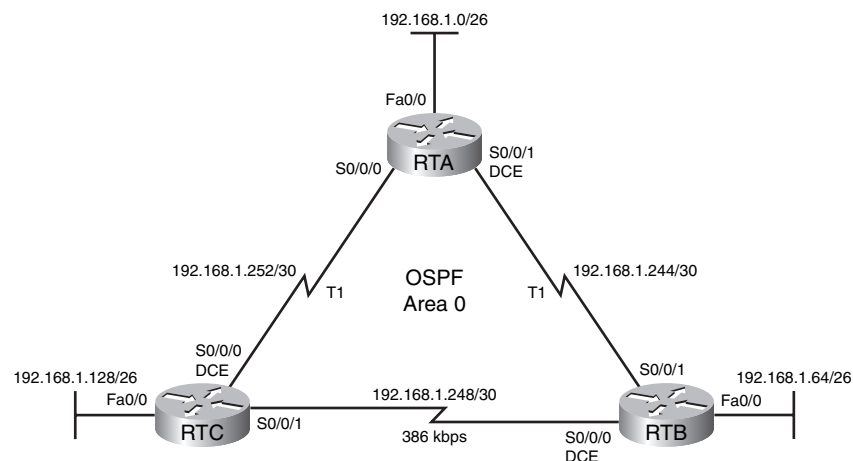
*A cost is associated with the output side of each router interface. This cost is configurable by the system administrator. The lower the cost, the more likely the interface is to be used to forward data traffic.*

Notice that RFC 2328 does not specify which values should be used to determine the cost. The exercises in the following sections cover cost calculation and the two methods for configuring OSPF cost on a Cisco router.

## Calculating the Cost Metric Exercise

In Figure 11-5, note the differences in bandwidth. If OSPF uses the default bandwidth on the serial interfaces to calculate the cost, RTB will send traffic destined for the LAN on RTC directly to RTC, and RTC will send traffic destined for the LAN on RTB directly to RTB. However, the path through RTA is faster.

**Figure 11-5** Configure OSPF Cost Metric



What is the formula that Cisco IOS uses to calculate the cost metric for OSPF?

$\text{Cost} = 10^8 / \text{bandwidth in bps}$

What is the OSPF cost of a T1 link?

$10^8 / 1544000 \text{ bps} = 64.7$ , which is rounded to a cost of 64 by the IOS

What is the OSPF cost of a Fast Ethernet link?

$10^8 / 100,000,000 \text{ bps} = 1$

What is the OSPF cost of a 56K dialup link?

$10^8 / 56000 = 1785.71$ , which is rounded to a cost of 1785 by the IOS

## Modifying the Cost Metric Exercise

Assume that RTB and RTC are both Cisco 2800 series routers. The default bandwidth on serial interfaces for 2800 routers is 1544 kbps (T1). What command would you enter to verify the default or configured bandwidth on an interface? [show interface](#)

Referring to Figure 11-5, document the commands needed to configure the bandwidth correctly so that OSPF uses an accurate cost metric.

```
RTB(config)# interface serial 0/0/0
```

```
RTB(config-if)# bandwidth 386
```

---

```
RTC(config)# interface serial 0/0/1
```

```
RTC(config-if)# bandwidth 386
```

Instead of configuring the bandwidth, you could configure the cost directly. Document the commands for RTB and RTC that would configure the actual OSPF cost?

```
RTB(config)# interface serial 0/0/0
```

```
RTB(config-if)# ip ospf cost 259
```

---

```
RTC(config)# interface serial 0/0/1
```

```
RTC(config-if)# ip ospf cost 259
```

## OSPF and Multiaccess Networks

A multiaccess network is a network with more than two devices on the same shared media. Examples of multiaccess networks include Ethernet, Token Ring, and Frame Relay. Token Ring is LAN technology that is for the most part obsolete. Frame Relay is a WAN technology that is discussed in a later CCNA course. The following exercises cover the concepts of multiaccess networks in OSPF and the DR/BDR election process.

## OSPF and Multiaccess Networks Completion Exercise

Complete the missing words or phrases in the following paragraphs.

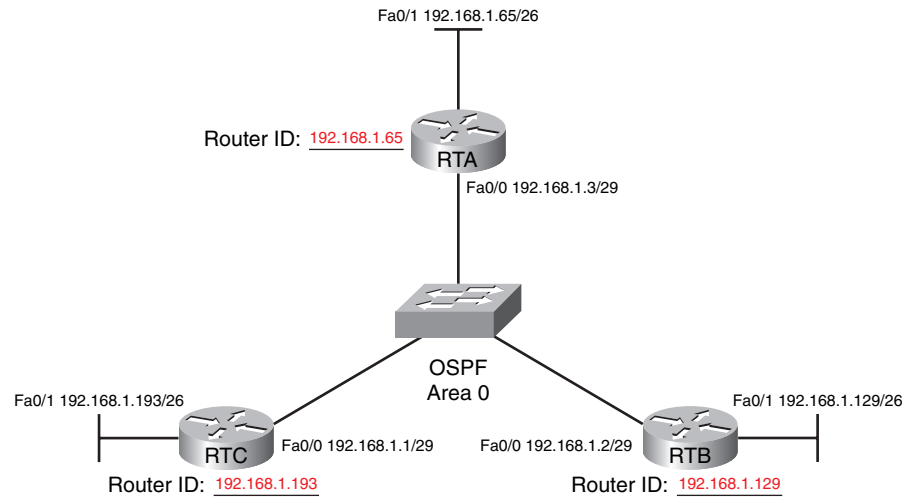
On multiaccess networks (networks supporting more than two routers), such as Ethernet and Frame Relay networks, the Hello protocol elects a [designated router \(DR\)](#) and a [backup designated router \(BDR\)](#). Among other things, the [designated router](#) is responsible for generating LSAs for the entire multiaccess network, which allows a reduction in routing update traffic.

The DR, BDR, and every other router in an OSPF network sends out Hellos using [224.0.0.5](#) as the destination address. If a DRother (a router that is not the DR) needs to send an LSA, it will send it using [224.0.0.6](#) as the destination address. The DR and the BDR will receive LSAs at this address.

The DR/BDR election is based on OSPF [priority](#) and OSPF router [ID](#). By default, all OSPF routers have a [priority](#) of [1](#). If all OSPF routers have the same [priority](#), the highest router [ID](#) determines the DR and BDR.

Unless a loopback interface is configured, the [highest](#) IP address on an active interface at the moment of OSPF process startup is used as the router [ID](#).

In Figure 11-6, label each router with its router ID. Assume that all routers came up simultaneously and that all interfaces are active.

**Figure 11-6 Determine the Router ID (Answer)**

In Figure 11-6, which router would be the DR? **RTC** BDR? **RTB**

You can override the router ID that OSPF chooses by configuring an IP address on a **loopback** interface. This will provide stability to your OSPF network because **loopback** interfaces do not become inactive.

Assume that network policy has determined that RTA is best suited to be the DR. In addition, the policy states that all OSPF routers will be configured with a loopback interface to provide stability to OSPF:

- Loopback for RTA is 10.0.0.3/32
- Loopback for RTB is 10.0.0.2/32
- Loopback for RTC is 10.0.0.1/32

Document the correct commands, including the router prompt, to configure loopback interfaces on each router.

```
RTA(config)# interface loopback 0
RTA(config-if)# ip address 10.0.0.3 255.255.255.255
RTB(config)# interface loopback 0
RTB(config-if)# ip address 10.0.0.2 255.255.255.255
RTC(config)# interface loopback 0
RTC(config-if)# ip address 10.0.0.1 255.255.255.255
```

With loopback interfaces now configured on each router, what must you do to change which router is the DR?

The routers must either be reloaded or the OSPF process has to be removed with the **no router ospf process-id** command and then completely reconfigured before routers will use the loopback addresses as the router ID. However, the first router reconfigured will become the DR regardless of the value of the router ID unless you reload the routers. So, the best way to ensure which router is the DR is by configuring priority.

In addition to configuring loopbacks, it would be a good idea to configure RTA with an OSPF priority that would ensure that it always wins the DR/BDR election. The syntax for configuring OSPF priority is as follows:

```
Router(config-if)# ip ospf priority priority
```

Document the commands you would use to configure RTA to make sure that its priority will always win the DR/BDR election.

```
RTA(config)# interface Fa 0/0
```

```
RTA(config-if)# ip ospf priority 2
```

!Any priority higher than the default of 1 will work.

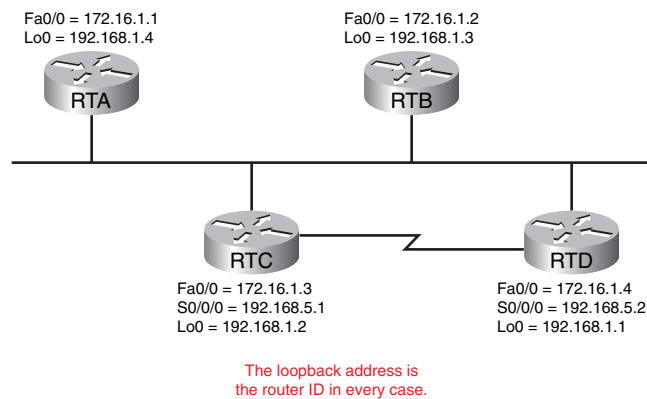
## DR/BDR Election Exercise

In the following exercises, assume that all routers are simultaneously booted. Determine the network type, if applicable, and label which router is elected as the DR and which router is elected as the BDR.

Hint: Remember, if priority is equal, router ID determines the DR and BDR.

Refer to Figure 11-7 and answer the following questions.

**Figure 11-7 DR/BDR Election Exercise 1 Topology (Answer)**



What is the router ID for RTA? 192.168.1.4

What is the router ID for RTB? 192.168.1.3

What is the router ID for RTC? 192.168.1.2

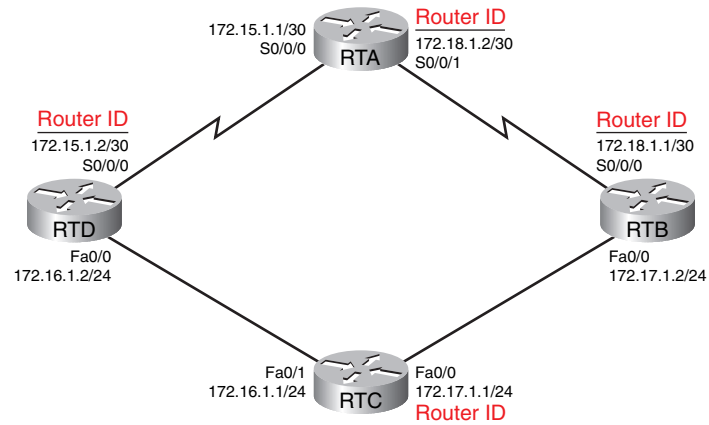
What is the router ID for RTD? 192.168.1.1

Which router will be elected the DR? RTA

Which router will be elected the BDR? RTB

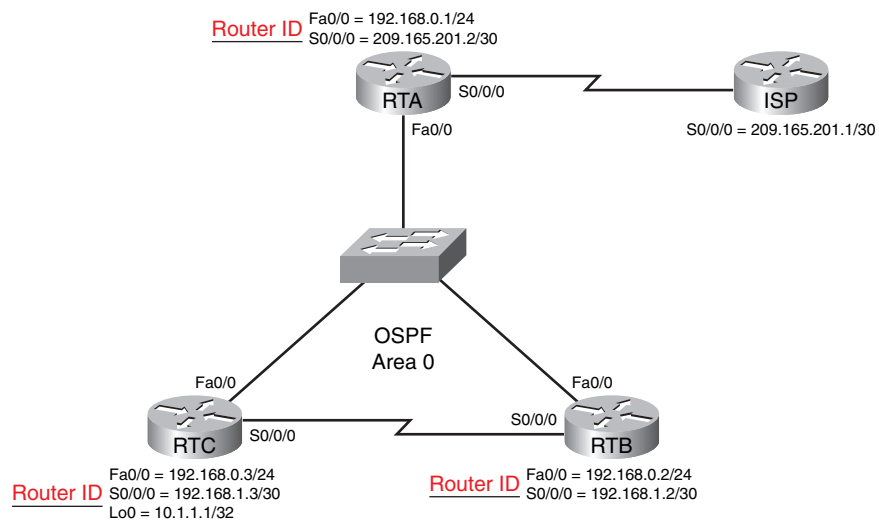
Refer to Figure 11-8 and, in the table that follows, determine whether there will be a DR/BDR election. If applicable, designate which router is the DR and which router is the BDR.



**Figure 11-8 DR/BDR Election Exercise 2 Topology (Answer)**

Network	DR/BDR Election?	Which Router Is the DR?	Which Router Is the BDR?
172.15.1.0/30	No	—	—
172.16.1.0/24	Yes	RTC	RTD
172.17.1.0/24	Yes	RTB	RTC
172.18.1.0/30	No	—	—

Refer to Figure 11-9 and answer the following questions.

**Figure 11-9 DR/BDR Election Exercise 3 Topology (Answer)**

What is the router ID for RTA? 209.165.201.2

What is the router ID for RTB? 192.168.1.2

What is the router ID for RTC? 10.1.1.1

Which router is the DR for the 192.168.0.0/24 network? **RTA**

Which router is the BDR for the 192.168.0.0/24 network? **RTB**

Now assume a priority of 0 on RTA. Which router is the DR for the 192.168.1.0/24 network? **RTB**

What will happen if another router, RTD, joins the 192.168.0.0/24 network with a router ID of 209.165.201.9?

**Nothing. Both the DR and BDR have to go down before RTD can become the DR.**

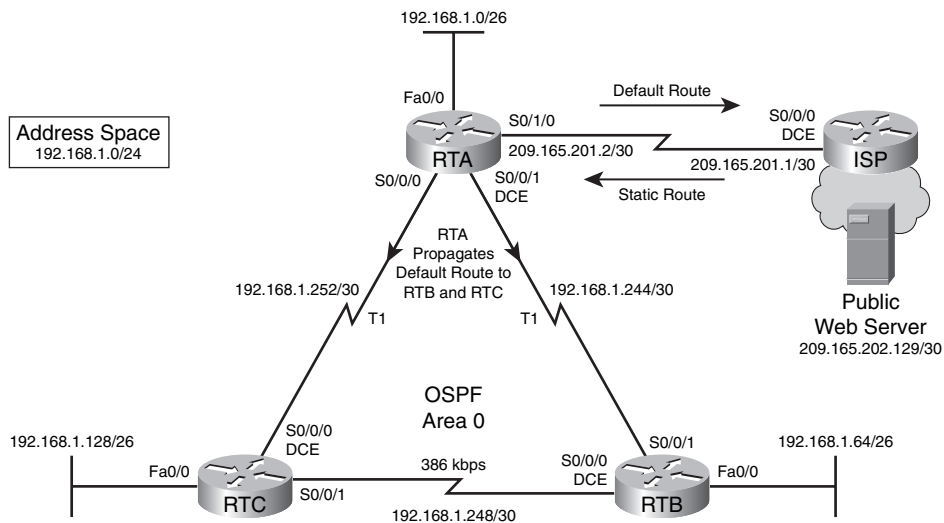
## More OSPF Configuration

The following exercises focus on additional OSPF configurations, including propagating a default route, modifying the reference bandwidth for metric calculations, and modifying the OSPF intervals.

### Redistributing an OSPF Default Route Exercise

In Figure 11-10, notice that RTA is now the gateway router because it provides access outside the area. In OSPF terminology, RTA is called the **Autonomous System Boundary Router (ASBR)**, because it connects to an external routing domain that uses a different routing policy.

**Figure 11-10 Propagating a Default Route**



Each routing protocol handles the propagation of default routing information a little differently. For OSPF, the gateway router must be configured with two commands. First, RTA will need a static default route pointing to ISP. Document the command to configure a static default route on RTA using the *exit-interface* argument.

```
RTA(config)# ip route 0.0.0.0 0.0.0.0 serial 0/1/0
```

Using the *exit-interface* argument, document the command necessary to configure ISP with a static route pointing to the 192.168.1.0/24 address space.

```
ISP(config)# ip route 192.168.1.0 255.255.255.0 serial 0/0/0
```

At this point, any host on the LAN attached to RTA will be able to access ISP and be able to ping the Public Web Server at 209.165.202.129. However, RTB and RTC still cannot ping outside the 192.168.1.0/24 address space. Why?

Because neither router has a default route

Document the command that needs to be configured on RTA to fix this problem.

RTA(config-router)# default-information originate

## Fine-Tuning OSPF Exercise

### *Modifying the Reference Bandwidth*

Cisco OSPF cost uses accumulated bandwidth. The bandwidth value of each interface is calculated using  $100,000,000/\text{bandwidth}$ . The 100,000,000, or  $10^8$ , is known as the reference bandwidth.

As you know from previous studies, we now have link speeds that are much faster than 100,000,000 (the speed of Fast Ethernet), including Gigabit Ethernet and 10GigE. Therefore, 100,000,000 results in interfaces with bandwidth values of 100 Mbps and higher having the same OSPF cost of 1.

For RTA, RTB, and RTC, document the commands to change the reference bandwidth to 10,000.

RTA(config-router)# auto-cost reference-bandwidth 10000

RTB(config-router)# auto-cost reference-bandwidth 10000

RTC(config-router)# auto-cost reference-bandwidth 10000

Make sure that you configure this command on all routers in the OSPF routing domain.

### *Modifying OSPF Intervals*

OSPF routers must use matching Hello intervals and Dead intervals on the same link. The default interval values result in efficient OSPF operation and seldom need to be modified. However, you can change them.

Again, refer to Figure 11-10. Assuming that the current intervals are 10 and 40, document the commands necessary to change these intervals on the link between RTB and RTC to a value four times greater than the current value.

RTB(config)# interface serial 0/0/0

RTB(config-if)# ip ospf hello-interval 40

RTB(config-if)# ip ospf dead-interval 160

RTC(config)# interface serial 0/0/1

RTC(config-if)# ip ospf hello-interval 40

RTC(config-if)# ip ospf dead-interval 160

Note that it is not necessary to configure the Dead interval as long as the desired interval is four times the Hello. The IOS will automatically increase the Dead interval to four times the configured Hello interval.

## Labs and Activities

### Command Reference

In the table that follows, record the command, *including the correct router prompt*, that fits the description. Fill in any blanks with the appropriate missing information.

Command	Description
Router(config)# <b>router ospf 123</b>	Turns on OSPF process number 123. The process ID is any value between <u>1</u> and <u>65,535</u> . The process ID <i>does not equal</i> the OSPF area.
Router(config-router)# <b>network 172.16.10.0 0.0.0.255 area 0</b>	OSPF advertises interfaces, not networks. Uses the wildcard mask to determine which interfaces to advertise. The command shown reads: Any interface with an address of 172.16.10.x is to be put into Area 0.
Router(config-if)# <b>ip ospf priority 50</b>	Changes the OSPF priority for an interface to 50.
Router(config-if)# <b>bandwidth 128</b>	Changes the bandwidth of an interface to 128 kbps.
Router(config-if)# <b>ip ospf cost 1564</b>	Changes the cost to a value of 1564.
Router(config-if)# <b>ip ospf hello-interval 20</b>	Changes the Hello interval timer to 20 seconds.
Router(config-if)# <b>ip ospf dead-interval 80</b>	Changes the Dead interval timer to 80 seconds.
Router(config)# <b>ip route 0.0.0.0 0.0.0.0 s0/0/0</b>	Creates a static default route pointing out the Serial 0/0/0 interface. This route will have an administrative distance of <u>0</u> .
Router(config-router)# <b>default-information originate</b>	Sets the default route to be propagated to all OSPF routers.
Router# <b>show ip protocol</b>	Displays parameters for all routing protocols running on the router.
Router# <b>show ip route</b>	Displays the complete IP routing table.
Router# <b>show ip ospf</b>	Displays basic OSPF information for all OSPF processes running on the router.
Router# <b>show ip ospf interface</b>	Displays OSPF information as it relates to all interfaces.
Router# <b>show ip ospf neighbor</b>	List all the OSPF neighbors and their states.
Router# <b>show ip ospf neighbor detail</b>	Displays a detailed list of neighbors.



## Lab 11-1: Basic OSPF Configuration (11.6.1)

Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Perform basic configuration tasks on a router
- Configure and activate interfaces
- Configure OSPF routing on all routers
- Configure OSPF router IDs
- Verify OSPF routing using **show** commands
- Configure a static default route
- Propagate a default route to OSPF neighbors
- Configure OSPF Hello and Dead timers
- Configure OSPF on a multiaccess network
- Configure OSPF priority
- Understand the OSPF election process
- Document the OSPF configuration

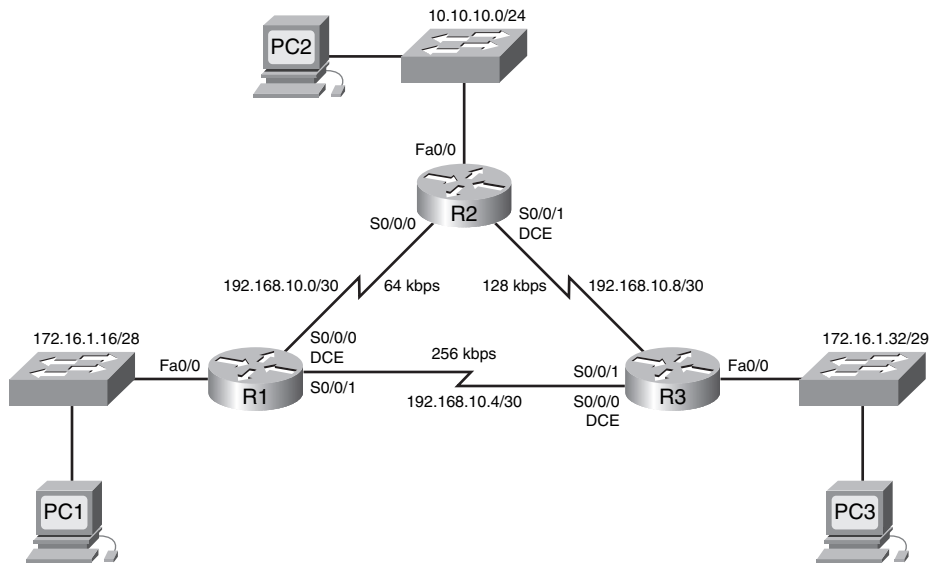
### Scenarios

In this lab activity, there are two separate scenarios. In the first scenario, you will learn how to configure the routing protocol OSPF using the network shown in the topology diagram in Scenario A. The segments of the network have been subnetted using VLSM. OSPF is a classless routing protocol that can be used to provide subnet mask information in the routing updates. This will allow VLSM subnet information to be propagated throughout the network.

In the second scenario, you will learn how to configure OSPF on a multiaccess network. You will also learn how to use the OSPF election process to determine the designated router (DR), backup designated router (BDR), and DRother states.

### Scenario A: Basic OSPF Configuration

Figure 11-11 shows the topology diagram for this scenario, and Table 11-2 provides the interface, IP address, subnet mask, and default gateway (where applicable) information for the routers and PCs shown in Figure 11-11.

**Figure 11-11 Topology for Lab 11-1: Scenario A****Table 11-2 Addressing Table for Lab 11-1: Scenario A**

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	172.16.1.17	255.255.255.240	—
	S0/0/0	192.168.10.1	255.255.255.252	—
	S0/0/1	192.168.10.5	255.255.255.252	—
R2	Fa0/0	10.10.10.1	255.255.255.0	—
	S0/0/0	192.168.10.2	255.255.255.252	—
	S0/0/1	192.168.10.9	255.255.255.252	—
R3	Fa0/0	172.16.1.33	255.255.255.248	—
	S0/0/0	192.168.10.6	255.255.255.252	—
	S0/0/1	192.168.10.10	255.255.255.252	—
PC1	NIC	172.16.1.20	255.255.255.240	172.16.1.17
PC2	NIC	10.10.10.10	255.255.255.0	10.10.10.1
PC3	NIC	172.16.1.35	255.255.255.248	172.16.1.33

## Task 1: Prepare the Network

**Step 1.** Cable a network that is similar to the one shown in the topology diagram of Figure 11-11.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

**Note:** If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions will appear different.

**Step 2.** Clear any existing configurations on the routers.

## Task 2: Perform Basic Router Configurations

Perform basic configuration of the R1, R2, and R3 routers according to the following guidelines:

- Configure the router host name.
- Disable Domain Name System (DNS) lookup.
- Configure a privileged EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for console connections.
- Configure a password for VTY connections.

## Task 3: Configure and Activate Serial and Ethernet Addresses

**Step 1.** Configure interfaces on R1, R2, and R3.

Configure these interfaces with the IP addresses from Table 11-2.

**Step 2.** Verify IP addressing and interfaces.

Use the **show ip interface brief** command to verify that the IP addressing is correct and that the interfaces are active.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

**Step 3.** Configure Ethernet interfaces of PC1, PC2, and PC3.

Configure these interfaces with the IP addresses and default gateways from Table 11-2.

**Step 4.** Test the PC configuration by pinging the default gateway from the PC.

## Task 4: Configure OSPF on the R1 Router

**Step 1.** Use the **router ospf** command in global configuration mode to enable OSPF on the R1 router. Enter a process ID of 1 for the *process-ID* parameter.

```
R1(config)# router ospf 1
R1(config-router)#
```

**Step 2.** Configure the network statement for the LAN network.

When you are in the router OSPF configuration submode, configure the LAN network 172.16.1.16/28 to be included in the OSPF updates that are sent out of R1.

The OSPF **network** command uses a combination of *network-address* and *wildcard-mask* similar to that which can be used by Enhanced Interior Gateway Routing Protocol (EIGRP). Unlike EIGRP, the wildcard mask in OSPF is required.

Use an area ID of 0 for the OSPF *area-id* parameter. 0 will be used for the OSPF area ID in all the **network** statements in this topology:

```
R1(config-router)# network 172.16.1.16 0.0.0.15 area 0
R1(config-router)#
```

- Step 3.** Configure the router to advertise the 192.168.10.0/30 network attached to the Serial 0/0/0 interface.

```
R1(config-router)# network 192.168.10.0 0.0.0.3 area 0
R1(config-router)#
```

- Step 4.** Configure the router to advertise the 192.168.10.4/30 network attached to the Serial 0/0/1 interface.

```
R1(config-router)# network 192.168.10.4 0.0.0.3 area 0
R1(config-router)#
```

- Step 5.** When you are finished with the OSPF configuration for R1, return to privileged EXEC mode.

```
R1(config-router)# end
%SYS-5-CONFIGI: Configured from console by console
R1#
```

## Task 5: Configure OSPF on the R2 and R3 Routers

- Step 1.** Enable OSPF routing on the R2 router using the **router ospf** command and a process ID of 1.

```
R2(config)# router ospf 1
R2(config-router)#
```

- Step 2.** Configure the router to advertise the LAN network 10.10.10.0/24 in the OSPF updates.

```
R2(config-router)# network 10.10.10.0 0.0.0.255 area 0
R2(config-router)#
```

- Step 3.** Configure the router to advertise the 192.168.10.0/30 network attached to the Serial 0/0/0 interface.

```
R2(config-router)# network 192.168.10.0 0.0.0.3 area 0
R2(config-router)#
```

```
00:07:27: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on Serial0/0/0 from
EXCHANGE to FULL, Exchange Done
```

Notice that when the network for the serial link from R1 to R2 is added to the OSPF configuration, the router sends a notification message to the console stating that a neighbor relationship with another OSPF router has been established.



- Step 4.** Configure the router to advertise the 192.168.10.8/30 network attached to the Serial 0/0/1 interface.

When you are finished, return to privileged EXEC mode:

```
R2(config-router)# network 192.168.10.8 0.0.0.3 area 0
R2(config-router)# end
%SYS-5-CONFIGI: Configured from console by console
R2#
```

- Step 5.** Configure OSPF on the R3 router using the **router ospf** and **network** commands.

Use a process ID of 1. Configure the router to advertise the three directly connected networks. When you are finished, return to privileged EXEC mode:

```
R3(config)# router ospf 1
R3(config-router)# network 172.16.1.32 0.0.0.7 area 0
R3(config-router)# network 192.168.10.4 0.0.0.3 area 0
R3(config-router)#
00:17:46: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.5 on Serial0/0/0 from
LOADING to FULL, Loading Done
R3(config-router)# network 192.168.10.8 0.0.0.3 area 0

R3(config-router)#
00:18:01: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.9 on Serial0/0/1 from
EXCHANGE to FULL, Exchange Done
R3(config-router)# end
%SYS-5-CONFIGI: Configured from console by console
R3#
```

Notice that when the networks for the serial links from R3 to R1 and R3 to R2 are added to the OSPF configuration, the router sends a notification message to the console stating that a neighbor relationship with another OSPF router has been established.

## Task 6: Configure OSPF Router IDs

The OSPF router ID is used to uniquely identify the router in the OSPF routing domain. A router ID is an IP address. Cisco routers derive the router ID in one of three ways and with the following precedence:

1. IP address configured with the OSPF **router-id** command
2. Highest IP address of any of the router's loopback addresses
3. Highest active IP address on any of the router's physical interfaces

- Step 1.** Examine the current router IDs in the topology.

Because no router IDs or loopback interfaces have been configured on the three routers, the router ID for each router is determined by the highest IP address of any active interface.

What is the router ID for R1? [192.168.10.5](#)

What is the router ID for R2? [192.168.10.9](#)

What is the router ID for R3? [192.168.10.10](#)

The router ID can also be seen in the output of the **show ip protocols**, **show ip ospf**, and **show ip ospf interfaces** commands:

```
R3# show ip protocols
Routing Protocol is "ospf 1"
 Outgoing update filter list for all interfaces is not set
 Incoming update filter list for all interfaces is not set
 Router ID 192.168.10.10
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Maximum path: 4
<output omitted>
```

---

```
R3# show ip ospf
Routing Process "ospf 1" with ID 192.168.10.10
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
<output omitted>
```

---

```
R3# show ip ospf interface
FastEthernet0/0 is up, line protocol is up
 Internet address is 172.16.1.33/29, Area 0
 Process ID 1, Router ID 192.168.10.10, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 192.168.10.10, Interface address 172.16.1.33
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:00
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
<output omitted>
```

**Step 2.** Use loopback addresses to change the router IDs of the routers in the topology.

```
R1(config)# interface loopback 0
R1(config-if)# ip address 10.1.1.1 255.255.255.255
```

---

```
R2(config)# interface loopback 0
R2(config-if)# ip address 10.2.2.2 255.255.255.255
```

---

```
R3(config)# interface loopback 0
R3(config-if)# ip address 10.3.3.3 255.255.255.255
```

**Step 3.** Reload the routers to force the new router IDs to be used.

When a new router ID is configured, it will not be used until the OSPF process is restarted. Make sure that the current configuration is saved to NRAM, and then use the **reload** command to restart each of the routers.

When the router is reloaded, what is the router ID for R1? [10.1.1.1](#)

When the router is reloaded, what is the router ID for R2? [10.2.2.2](#)

When the router is reloaded, what is the router ID for R3? [10.3.3.3](#)

**Step 4.** Use the **show ip ospf neighbors** command to verify that the router IDs have changed.

```
R1# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.3.3.3	0	FULL/ -	00:00:30	192.168.10.6	Serial0/0/1
10.2.2.2	0	FULL/ -	00:00:33	192.168.10.2	Serial0/0/0

```
R2# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.3.3.3	0	FULL/ -	00:00:36	192.168.10.10	Serial0/0/1
10.1.1.1	0	FULL/ -	00:00:37	192.168.10.1	Serial0/0/0

```
R3# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.2.2.2	0	FULL/ -	00:00:34	192.168.10.9	Serial0/0/1
10.1.1.1	0	FULL/ -	00:00:38	192.168.10.5	Serial0/0/0

**Step 5.** Use the **router-id** command to change the router ID on the R1 router.

**Note:** Some IOS versions do not support the **router-id** command. If this command is not available, continue to Task 7.

```
R1(config)# router ospf 1
```

```
R1(config-router)# router-id 10.4.4.4
```

```
Reload or use "clear ip ospf process" command, for this to take effect
```

If this command is used on an OSPF router process that is already active (has neighbors), the new router ID is used at the next reload or at a manual OSPF process restart. To manually restart the OSPF process, use the **clear ip ospf process** command:

```
R1(config-router)#end
```

```
R1# clear ip ospf process
```

```
Reset ALL OSPF processes? [no]:yes
```

```
R1#
```

**Step 6.** Use the **show ip ospf neighbor** command on router R2 to verify that the router ID of R1 has been changed.

```
R2# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.3.3.3	0	FULL/ -	00:00:36	192.168.10.10	Serial0/0/1
10.4.4.4	0	FULL/ -	00:00:37	192.168.10.1	Serial0/0/0

**Step 7.** Remove the configured router ID with the **no** form of the **router-id** command.

```
R1(config)# router ospf 1
R1(config-router)# no router-id 10.4.4.4
Reload or use "clear ip ospf process" command, for this to take effect
```

**Step 8.** Restart the OSPF process using the **clear ip ospf process** command.

Restarting the OSPF process forces the router to use the IP address configured on the Loopback 0 interface as the router ID:

```
R1(config-router)# end
R1# clear ip ospf process
Reset ALL OSPF processes? [no]:yes
R1#
```

## Task 7: Verify OSPF Operation

**Step 1.** On the R1 router, use the **show ip ospf neighbor** command to view the information about the OSPF neighbor routers R2 and R3.

You should be able to see the neighbor ID and IP address of each adjacent router, and the interface that R1 uses to reach that OSPF neighbor:

```
R1# show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
10.2.2.2 0 FULL/- 00:00:32 192.168.10.2 Serial0/0/0
10.3.3.3 0 FULL/- 00:00:32 192.168.10.6 Serial0/0/1
R1#
```

**Step 2.** On the R1 router, use the **show ip protocols** command to view information about the routing protocol operation.

Notice that the information that was configured in the previous tasks, such as protocol, process ID, neighbor ID, and networks, is shown in the output. The IP addresses of the adjacent neighbors are also shown:

```
R1# show ip protocols
Routing Protocol is "ospf 1"
 Outgoing update filter list for all interfaces is not set
 Incoming update filter list for all interfaces is not set
 Router ID 10.1.1.1
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Maximum path: 4
 Routing for Networks:
 172.16.1.16 0.0.0.15 area 0
 192.168.10.0 0.0.0.3 area 0
 192.168.10.4 0.0.0.3 area 0
 Routing Information Sources:
 Gateway Distance Last Update
 10.2.2.2 110 00:11:43
 10.3.3.3 110 00:11:43
 Distance: (default is 110)
```

Notice that the output specifies the process ID used by OSPF.

## Task 8: Examine OSPF Routes in the Routing Tables

View the routing table on the R1 router. OSPF routes are denoted in the routing table with an **O**.

```
R1# show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```

 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.1.1.1/32 is directly connected, Loopback0
O 10.10.10.0/24 [110/65] via 192.168.10.2, 00:01:02, Serial0/0/0
 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.1.16/28 is directly connected, FastEthernet0/0
O 172.16.1.32/29 [110/65] via 192.168.10.6, 00:01:12, Serial0/0/1
 192.168.10.0/30 is subnetted, 3 subnets
C 192.168.10.0 is directly connected, Serial0/0/0
C 192.168.10.4 is directly connected, Serial0/0/1
O 192.168.10.8 [110/128] via 192.168.10.6, 00:01:12, Serial0/0/1
 [110/128] via 192.168.10.2, 00:01:02, Serial0/0/0
```

Notice that unlike RIPv2 and EIGRP, OSPF does not automatically summarize at major network boundaries.

## Task 9: Configure OSPF Cost

**Step 1.** Use the **show ip route** command on the R1 router to view the OSPF cost to reach the 10.10.10.0/24 network.

```
R1# show ip route
```

```
<output omitted>
```

```

 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.1.1.1/32 is directly connected, Loopback0
O 10.10.10.0/24 [110/65] via 192.168.10.2, 00:16:56, Serial0/0/0
 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.1.16/28 is directly connected, FastEthernet0/0
O 172.16.1.32/29 [110/65] via 192.168.10.6, 00:17:06, Serial0/0/1
 192.168.10.0/30 is subnetted, 3 subnets
C 192.168.10.0 is directly connected, Serial0/0/0
```

```
C 192.168.10.4 is directly connected, Serial0/0/1
O 192.168.10.8 [110/128] via 192.168.10.6, 00:17:06, Serial0/0/1
 [110/128] via 192.168.10.2, 00:16:56, Serial0/0/0
```

- Step 2.** Use the **show interfaces serial0/0/0** command on the R1 router to view the bandwidth of the Serial 0/0/0 interface.

```
R1# show interfaces serial0/0/0
Serial0/0/0 is up, line protocol is up (connected)
 Hardware is HD64570
 Internet address is 192.168.10.1/30
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
 Encapsulation HDLC, loopback not set, keepalive set (10 sec)
 Last input never, output never, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/0 (size/max/drops); Total output drops: 0
<output omitted>
```

On most serial links, the bandwidth metric will default to 1544 Kbits. If this is not the actual bandwidth of the serial link, the bandwidth will need to be changed so that the OSPF cost can be calculated correctly.

- Step 3.** Use the **bandwidth** command to change the bandwidth of the serial interfaces of the R1 and R2 routers to the actual bandwidth.

```
R1(config)# interface serial0/0/0
R1(config-if)# bandwidth 64
R1(config-if)# interface serial0/0/1
R1(config-if)# bandwidth 256

R2(config)# interface serial0/0/0
R2(config-if)# bandwidth 64
R1(config-if)# interface serial0/0/1
R1(config-if)# bandwidth 128
```

- Step 4.** Use the **show ip ospf interface** command on the R1 router to verify the cost of the serial links.

The cost of the serial link between R1 and R2 is now 1562, the result of the calculation 108/64,000 bps. Each router will now also have a new cost for its Serial 0/0/1 interface:

```
R1# show ip ospf interface
```

```
<output omitted>
```

```
Serial0/0/0 is up, line protocol is up
 Internet address is 192.168.10.1/30, Area 0
 Process ID 1, Router ID 10.1.1.1, Network Type POINT-TO-POINT, Cost: 1562
 Transmit Delay is 1 sec, State POINT-TO-POINT,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:05
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)
```

```

Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
 Adjacent with neighbor 10.2.2.2
Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
 Internet address is 192.168.10.5/30, Area 0
 Process ID 1, Router ID 10.1.1.1, Network Type POINT-TO-POINT, Cost: 390
 Transmit Delay is 1 sec, State POINT-TO-POINT,
<output omitted>

```

**Step 5.** Use the **ip ospf cost** command to configure the OSPF cost on the R3 router.

An alternative method to using the **bandwidth** command is to use the **ip ospf cost** command, which allows you to directly configure the cost. Use the **ip ospf cost** command to change the bandwidth of the serial interfaces of R3:

```

R3(config-if)# interface serial0/0/0
R3(config-if)# ip ospf cost 390

```

**Step 6.** Use the **show ip ospf interface** command on the R3 router to verify that the cost of each of the serial links is now 781.

```
R3# show ip ospf interface
```

```
<output omitted>
```

```

Serial0/0/1 is up, line protocol is up
 Internet address is 192.168.10.10/30, Area 0
 Process ID 1, Router ID 10.3.3.3, Network Type POINT-TO-POINT, Cost: 781
 Transmit Delay is 1 sec, State POINT-TO-POINT,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:06
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1 , Adjacent neighbor count is 1
 Adjacent with neighbor 10.2.2.2
 Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
 Internet address is 192.168.10.6/30, Area 0
 Process ID 1, Router ID 10.3.3.3, Network Type POINT-TO-POINT, Cost: 390
 Transmit Delay is 1 sec, State POINT-TO-POINT,
<output omitted>

```

## Task 10: Redistribute an OSPF Default Route

**Step 1.** Configure a loopback address on the R1 router to simulate a link to an ISP.

```
R1(config)# interface loopback1
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to
up
R1(config-if)# ip address 172.30.1.1 255.255.255.252
```

**Step 2.** Configure a static default route on the R1 router.

Use the loopback address that has been configured to simulate a link to an ISP as the exit interface:

```
R1(config)# ip route 0.0.0.0 0.0.0.0 loopback1
R1(config)#
```

**Step 3.** Use the **default-information originate** command to include the static route in the OSPF updates that are sent from the R1 router.

```
R1(config)# router ospf 1
R1(config-router)# default-information originate
R1(config-router)#
```

**Step 4.** View the routing table on the R2 router to verify that the static default route is being redistributed through OSPF.

```
R2# show ip route
```

<output omitted>

```
Gateway of last resort is 192.168.10.1 to network 0.0.0.0

 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.2.2.2/32 is directly connected, Loopback0
C 10.10.10.0/24 is directly connected, FastEthernet0/0
 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O 172.16.1.16/28 [110/1172] via 192.168.10.10, 00:29:28, Serial0/0/1
O 172.16.1.32/29 [110/782] via 192.168.10.10, 00:29:28, Serial0/0/1
 192.168.10.0/30 is subnetted, 3 subnets
C 192.168.10.0 is directly connected, Serial0/0/0
O 192.168.10.4 [110/1171] via 192.168.10.10, 00:25:56, Serial0/0/1
C 192.168.10.8 is directly connected, Serial0/0/1
O*E2 0.0.0.0/0 [110/1] via 192.168.10.10, 00:01:11, Serial0/0/1
```



## Task 11: Configure Additional OSPF Features

**Step 1.** Use the **auto-cost reference-bandwidth** command to adjust the reference bandwidth value.

Increase the reference bandwidth to 10000 to simulate 10GigE speeds. Configure this command on all routers in the OSPF routing domain.

```
R1(config-router)# auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
R2(config-router)# auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
R3(config-router)# auto-cost reference-bandwidth 10000

% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
```

**Step 2.** Examine the routing table on the R1 router to verify the change in the OSPF cost metric.

Notice that the values are much larger cost values for OSPF routes:

```
R1# show ip route
```

```
<output omitted>
```

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.1.1.1/32 is directly connected, Loopback0
O 10.10.10.0/24 [110/39943] via 192.168.10.6, 00:01:01, Serial0/0/1
 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.16.1.16/28 is directly connected, FastEthernet0/0
O 172.16.1.32/29 [110/39162] via 192.168.10.6, 00:00:51, Serial0/0/1
 172.30.0.0/30 is subnetted, 1 subnets
C 172.30.1.0 is directly connected, Loopback1
 192.168.10.0/30 is subnetted, 3 subnets
C 192.168.10.0 is directly connected, Serial0/0/0
C 192.168.10.4 is directly connected, Serial0/0/1
O 192.168.10.8 [110/39843] via 192.168.10.6, 00:01:01, Serial0/0/1
S* 0.0.0.0/0 is directly connected, Loopback1
```

**Step 3.** Use the **show ip ospf neighbor** command on R1 to view the Dead Time counter.

The Dead Time counter is counting down from the default interval of 40 seconds:

```
R1# show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
10.2.2.2 0 FULL/- 00:00:34 192.168.10.2 Serial0/0/0
10.3.3.3 0 FULL/- 00:00:34 192.168.10.6 Serial0/0/1
```

**Step 4.** Configure the OSPF Hello and Dead intervals.

The OSPF Hello and Dead intervals can be modified manually using the **ip ospf hello-interval** and **ip ospf dead-interval** interface commands. Use these commands to change the Hello interval to 5 seconds and the Dead interval to 20 seconds on the Serial 0/0/0 interface of the R1 router:

```
R1(config)# interface serial0/0/0
R1(config-if)# ip ospf hello-interval 5
R1(config-if)# ip ospf dead-interval 20
R1(config-if)#
01:09:04: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/0 from FULL
to DOWN. Neighbor Down: Dead timer expired
01:09:04: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/0 from FULL
to Down: Interface down or detached
```

After 20 seconds, the Dead Timer on R1 expires. R1 and R2 lose adjacency because the Dead Timer and Hello Timer must be configured identically on each side of the serial link between R1 and R2.

**Step 5.** Modify the Dead Timer and Hello Timer intervals.

Modify the Dead Timer and Hello Timer intervals on the Serial 0/0/0 interface of the R2 router to match the intervals configured on the Serial 0/0/0 interface of the R1 router:

```
R2(config)# interface serial0/0/0
R2(config-if)# ip ospf hello-interval 5
R2(config-if)# ip ospf dead-interval 20
R2(config-if)#
01:12:10: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.1 on Serial0/0/0 from
EXCHANGE to FULL, Exchange Done
```

Notice that IOS displays a message when adjacency has been established with a state of Full.

**Step 6.** Use the **show ip ospf interface serial0/0/0** command to verify that the Hello Timer and Dead Timer intervals have been modified.

```
R2# show ip ospf interface serial0/0/0
=Serial0/0/0 is up, line protocol is up
 Internet address is 192.168.10.2/30, Area 0
 Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT, Cost: 65535
 Transmit Delay is 1 sec, State POINT-TO-POINT,
 Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
 Hello due in 00:00:00
 Index 3/3, flood queue length 0
```

```

Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
 Adjacent with neighbor 10.1.1.1
Suppress hello for 0 neighbor(s)

```

**Step 7.** Use the **show ip ospf neighbor** command on R1 to verify that the neighbor adjacency with R2 has been restored.

Notice that the Dead Time for Serial 0/0/0 is now much lower because it is counting down from 20 seconds instead of the default 40 seconds. Serial 0/0/1 is still operating with default timers:

```

R1# show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
10.2.2.2 0 FULL/- 00:00:19 192.168.10.2 Serial0/0/0
10.3.3.3 0 FULL/- 00:00:34 192.168.10.6 Serial0/0/1

```

## Task 12: Document the Router Configurations

On each router, capture the following command output to a text file and save for future reference:

- Running configuration
- Routing table
- Interface summarization
- Output from **show ip protocols**

## Task 13: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

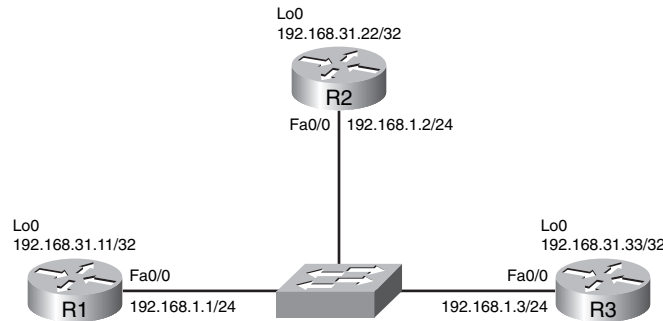


### Packet Tracer Companion: Basic OSPF Configuration (11.6.2)

You can now open the file LSG02-Lab1161a.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment.

## Scenario B: Configure OSPF on a Multiaccess Network

Figure 11-12 shows the topology diagram for this scenario, and Table 11-3 provides the interface, IP address, subnet mask, and default gateway (where applicable) information for the routers shown in Figure 11-12.

**Figure 11-12 Topology for Lab 11-1: Scenario B****Table 11-3 Addressing Table for Lab 11-1: Scenario B**

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	—
	Loopback1	192.168.31.11	255.255.255.255	—
R2	Fa0/0	192.168.1.2	255.255.255.0	—
	Loopback1	192.168.31.22	255.255.255.255	—
R3	Fa0/0	192.168.1.3	255.255.255.0	—
	Loopback1	192.168.31.33	255.255.255.255	—

## Task 1: Prepare the Network

**Step 1.** Cable a network that is similar to the one shown in the topology diagram of Figure 11-12.

You can use any current router in your lab as long as it has the required interfaces shown in the topology.

**Note:** If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions will appear different.

In this topology, we have three routers sharing a common Ethernet multiaccess network, 192.168.1.0/24. Each router will be configured with an IP address on the Fast Ethernet interface and a loopback address for the router ID.

**Step 2.** Clear any existing configurations on the routers.

## Task 2: Perform Basic Router Configurations

Perform basic configuration of the R1, R2, and R3 routers according to the following guidelines:

- Configure the router host name.
- Disable DNS lookup.
- Configure a privileged EXEC mode password.
- Configure a message-of-the-day banner.

- Configure a password for console connections.
- Configure a password for VTY connections.

### Task 3: Configure and Activate Ethernet and Loopback Addresses

**Step 1.** Configure interfaces on R1, R2, and R3.

Configure the Ethernet and Loopback interfaces on the R1, R2, and R3 routers with the IP addresses from the table under the topology diagram. Use the **show ip interface brief** command to verify that the IP addressing is correct. When you have finished, be sure to save the running configuration to the NVRAM of the router.

**Step 2.** Verify IP addressing and interfaces.

Use the **show ip interface brief** command to verify that the IP addressing is correct and that the interfaces are active.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

### Task 4: Configure OSPF on the DR Router

The DR and BDR election process takes place as soon as the first router has its interface enabled on the multiaccess network. This can happen as the routers are powered on or when the OSPF **network** command for that interface is configured. If a new router enters the network after the DR and BDR have already been elected, it will not become the DR or BDR even if it has a higher OSPF interface priority or router ID than the current DR or BDR. Configure the OSPF process on the router with the highest router ID first to ensure that this router becomes the DR.

**Step 1.** Use the **router ospf** command in global configuration mode to enable OSPF on the R3 router.

Enter a process ID of 1 for the *process-ID* parameter. Configure the router to advertise the 192.168.1.0/24 network. Use an area ID of 0 for the OSPF *area-id* parameter in the **network** statement.

```
R3(config)# router ospf 1
R3(config-router)# network 192.168.1.0 0.0.0.255 area 0
R3(config-router)# end
```

**Step 2.** Use the **show ip ospf interface** command to verify that the OSPF has been configured correctly and that R3 is the DR.

```
R3# show ip ospf interface
FastEthernet0/0 is up, line protocol is up
 Internet address is 192.168.1.3/24, Area 0
 Process ID 1, Router ID 192.168.31.33, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 192.168.31.33, Interface address 192.168.1.3
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:07
```

```

Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)

```

## Task 5: Configure OSPF on the BDR

Configure the OSPF process on the router with the second-highest router ID next to ensure that this router becomes the BDR.

- Step 1.** Use the **router ospf** command in global configuration mode to enable OSPF on the R2 router.

Enter a process ID of 1 for the *process-ID* parameter. Configure the router to advertise the 192.168.1.0/24 network. Use an area ID of 0 for the OSPF *area-id* parameter in the **network** statement:

```

R2(config)# router ospf 1
R2(config-router)# network 192.168.1.0 0.0.0.255 area 0
R2(config-router)# end
%SYS-5-CONFIGI: Configured from console by console
R2#
00:08:51: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.33 on FastEthernet0/0
from LOADING to FULL, Loading Done

```

Notice that an adjacency is formed with the R3 router. It can take up to 40 seconds for the R3 router to send a Hello packet. When this packet is received, the neighbor relationship is formed.

- Step 2.** Use the **show ip ospf interface** command to verify that the OSPF has been configured correctly and that R2 is the BDR.

```

R2# show ip ospf interface
FastEthernet0/0 is up, line protocol is up
 Internet address is 192.168.1.2/24, Area 0
 Process ID 1, Router ID 192.168.31.22, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State BDR, Priority 1
 Designated Router (ID) 192.168.31.33, Interface address 192.168.1.3
 Backup Designated Router (ID) 192.168.31.22, Interface address
 192.168.1.2
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:03
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1, Adjacent neighbor count is 1
 Adjacent with neighbor 192.168.1.3 (Designated Router)
 Suppress hello for 0 neighbor(s)

```

- Step 3.** Use the **show ip ospf neighbor** command to view information about the other routers in the OSPF area.

Notice that R3 is the DR:

```
R2# show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
192.168.31.33 1 FULL/DR 00:00:33 192.168.1.3 FastEthernet0/0
```

## Task 6: Configure OSPF on the DRother Router

Configure the OSPF process on the router with the lowest router ID last. This router will be designated as DRother instead of DR or BDR.

- Step 1.** Use the **router ospf** command in global configuration mode to enable OSPF on the R1 router.

Enter a process ID of 1 for the *process-ID* parameter. Configure the router to advertise the 192.168.1.0/24 network. Use an area ID of 0 for the OSPF *area-id* parameter in the **network** statement:

```
R1(config)# router ospf 1
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# end
```

```
%SYS-5-CONFIGI: Configured from console by console
```

```
R1#
```

```
00:16:08: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.22 on FastEthernet0/0
from LOADING to FULL, Loading Done
```

```
00:16:12: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.33 on FastEthernet0/0
from EXCHANGE to FULL, Exchange Done
```

Notice that an adjacency is formed with the R2 and R3 routers. It can take up to 40 seconds for both the R2 and R3 routers to each send a Hello packet.

- Step 2.** Use the **show ip ospf interface** command to verify that OSPF has been configured correctly and that R1 is a DRother.

```
R1# show ip ospf interface
FastEthernet0/0 is up, line protocol is up
 Internet address is 192.168.1.1/24, Area 0
 Process ID 1, Router ID 192.168.31.11, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State DROTHER, Priority 1
 Designated Router (ID) 192.168.31.33, Interface address 192.168.1.3
 Backup Designated Router (ID) 192.168.31.22, Interface address
 192.168.1.2
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:00
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 2, Adjacent neighbor count is 2
```

```
Adjacent with neighbor 192.168.31.33 (Designated Router)
Adjacent with neighbor 192.168.31.22 (Backup Designated Router)
Suppress hello for 0 neighbor(s)
```

- Step 3.** Use the **show ip ospf neighbor** command to view information about the other routers in the OSPF area.

Notice that R3 is the DR and R2 is the BDR:

```
R1# show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
192.168.31.22 1 FULL/BDR 00:00:35 192.168.1.2 FastEthernet0/0
192.168.31.33 1 FULL/DR 00:00:30 192.168.1.3 FastEthernet0/0
```

## Task 7: Use the OSPF Priority to Determine the DR and BDR

- Step 1.** Use the **ip ospf priority** interface command to change the OSPF priority of the R1 router to 255, which is the highest possible priority.

```
R1(config)# interface fastEthernet0/0
R1(config-if)# ip ospf priority 255
R1(config-if)# end
```

- Step 2.** Use the **ip ospf priority** interface command to change the OSPF priority of the R3 router to 100.

```
R3(config)# interface fastEthernet0/0
R3(config-if)# ip ospf priority 100
R3(config-if)# end
```

- Step 3.** Use the **ip ospf priority** interface command to change the OSPF priority of the R2 router to 0.

A priority of 0 causes the router to be ineligible to participate in an OSPF election and become a DR or BDR:

```
R2(config)# interface fastEthernet0/0
R2(config-if)# ip ospf priority 0
R2(config-if)# end
```

- Step 4.** Shut down and reenables the FastEthernet 0/0 interfaces to force an OSPF election.

The FastEthernet 0/0 interfaces of each of the routers can be shut down and reenables to force an OSPF election. Shut down the FastEthernet 0/0 interface on each of the three routers. Notice that as the interfaces are shut down, the OSPF adjacencies are lost:

```
R1(config)# interface fastEthernet0/0
R1(config-if)# shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
```



```
02:17:22: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.22 on FastEthernet0/0
from FULL to Down: Interface down or detached
```

```
02:17:22: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.33 on FastEthernet0/0
from FULL to Down: Interface down or detached
```

```
R2(config)# interface fastethernet0/0
```

```
R2(config-if)# shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administra
tively down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to down
```

```
02:17:06: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.33 on FastEthernet0/0
from FULL to Down: Interface down or detached
```

```
02:17:06: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.11 on FastEthernet0/0
from FULL to Down: Interface down or detached
```

```
R3(config)# interface fastethernet0/0
```

```
R3(config-if)# shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administra
tively down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to down
```

```
02:17:22: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.22 on FastEthernet0/0
from FULL to Down: Interface down or detached
```

```
02:17:22: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.11 on FastEthernet0/0
from FULL to Down: Interface down or detached
```

**Step 5.** Reenable the FastEthernet 0/0 interface on the R2 router.

```
R2(config-if)# no shut
```

```
R2(config-if)# end
```

```
%SYS-5-CONFIGI: Configured from console by console
```

**Step 6.** Reenable the FastEthernet 0/0 interface on the R1 router.

Notice that an adjacency is formed with the R2 router. It can take up to 40 seconds for the R2 router to send a Hello packet:

```
R1(config-if)# no shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
```

```
R1(config-if)# end
```

```
%SYS-5-CONFIGI: Configured from console by console
```

```
R1#
```

```
02:31:43: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.22 on FastEthernet0/0
from EXCHANGE to FULL, Exchange Done
```

**Step 7.** Use the **show ip ospf neighbor** command on the R1 router to view the OSPF neighbor information for that router.

Notice that even though the R2 router has a higher router ID than R1, the R2 router has been set to a state of DROther because the OSPF priority has been set to 0:

```
R1# show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.31.22	0	FULL/DROTHER	00:00:33	192.168.1.2	FastEthernet0/0

**Step 8.** Reenable the FastEthernet 0/0 interface on the R3 router.

Notice that an adjacency is formed with the R1 and R2 routers. It can take up to 40 seconds for both the R1 and R2 routers to each send a Hello packet:

```
R3(config-if)# no shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
R3(config-if)# end
%SYS-5-CONFIGI: Configured from console by console
02:37:32: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.11 on FastEthernet0/0
from LOADING to FULL, Loading Done
02:37:36: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.31.22 on FastEthernet0/0
from EXCHANGE to FULL, Exchange Done
```

**Step 9.** Use the **show ip ospf interface** command on the R3 router to verify that R3 has become the BDR.

```
R3# show ip ospf interface
FastEthernet0/0 is up, line protocol is up
 Internet address is 192.168.1.3/24, Area 0
 Process ID 1, Router ID 192.168.31.33, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State BDR, Priority 100
 Designated Router (ID) 192.168.31.11, Interface address 192.168.1.1
<output omitted>
```

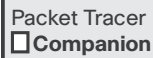
## Task 8: Document the Router Configurations

On each router, capture the following command output to a text file and save for future reference:

- Running configuration
- Routing table
- Interface summarization
- Output from **show ip protocols**

## Task 9: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.



## Packet Tracer Companion: Basic OSPF Configuration (11.6.1)

You can now open the file LSG02-Lab1161b.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment.



## Lab 11-2: Challenge OSPF Configuration (11.6.2)

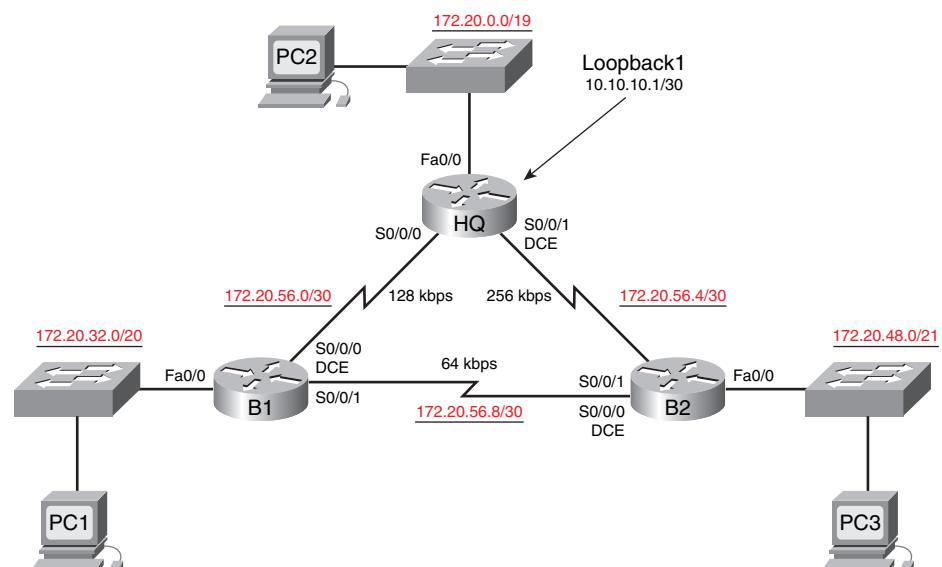
Upon completion of this lab, you will be able to

- Create an efficient VLSM design given requirements
- Assign appropriate addresses to interfaces and document
- Cable a network according to the topology diagram in Figure 11-13
- Erase the startup configuration and reload a router to the default state
- Configure routers including OSPF
- Configure and propagate a static default route
- Verify OSPF operation
- Test and verify full connectivity
- Reflect on and document the network implementation

### Scenario

In this lab activity, you will be given a network address that must be subnetted using VLSM to complete the addressing of the network shown in the topology diagram in Figure 11-13. A combination OSPF routing and static routing will be required so that hosts on networks that are not directly connected will be able to communicate with each other. An OSPF area ID of 0 and process ID of 1 will be used in all OSPF configurations.

**Figure 11-13 Topology Diagram for Lab 11-2 (Answer)**



## Task 1: Subnet the Address Space

**Step 1.** Examine the network requirements.

The addressing for the network has the following requirements:

- The 172.20.0.0/16 network must be subnetted to provide addresses for the LANs and serial links:
  - The HQ LAN will require 8000 addresses
  - The Branch1 LAN will require 4000 addresses
  - The Branch2 LAN will require 2000 addresses
  - The links between the routers will require two addresses for each link
- The loopback address representing the link between the HQ router and the ISP will use the 10.10.10.0/30 network.

**Step 2.** Consider the following questions when creating your network design.

How many subnets need to be created from the 172.20.0.0/16 network? 6

How many total IP addresses are required from the 172.16.0.0/16 network? 14006

What subnet mask will be used for the HQ LAN subnet? 255.255.224.0 or /19

What is the maximum number of host addresses that could be used on this subnet? 8190

What subnet mask will be used for the Branch1 LAN subnet? 255.255.240.0 or /20

What is the maximum number of host addresses that could be used on this subnet? 4094

What subnet mask will be used for the Branch2 LAN subnet? 255.255.248.0 or /21

What is the maximum number of host addresses that could be used on this subnet? 2046

What subnet mask will be used for the links between the three routers?

255.255.255.252 or /30

What is the maximum number of host addresses that could be used on each of these subnets? 2

**Step 3.** Assign subnetwork addresses to the topology diagram in Figure 11-13.

- Assign subnet 0 of the 172.20.0.0/16 network to the HQ LAN subnet. What is the network address of this subnet? 172.20.0.0/19
- Assign the next available address space of the 172.20.0.0/16 network to the Branch1 LAN subnet. What is the network address of this subnet? 172.20.32.0/20
- Assign the next available address space of the 172.20.0.0/16 network to the Branch2 LAN subnet. What is the network address of this subnet? 172.20.48.0/21
- Assign the next available address space of the 172.20.0.0/16 network to the link between the HQ and Branch1 routers. What is the network address of this subnet? 172.20.56.0/30
- Assign the next available address space of the 172.20.0.0/16 network to the link between the HQ and Branch2 routers. What is the network address of this subnet? 172.20.56.4/30

- Assign the next available address space of the 172.20.0.0/16 network to the link between the Branch1 and Branch2 routers. What is the network address of this subnet?  
172.20.56.8 /30

## Task 2: Determine Interface Addresses

Assign appropriate addresses to the device interfaces.

- Assign the first valid host address in the 10.10.10.0/30 network to the Loopback 1 interface on the HQ router.
- Assign the first valid IP address of the HQ LAN network to the LAN interface of the HQ router.
- Assign the last valid IP address of the HQ LAN network to PC2.
- Assign the first valid IP address of the Branch1 LAN network to the LAN interface of the Branch1 router.
- Assign the last valid IP address of the Branch1 LAN network to PC1.
- Assign the first valid IP address of the Branch2 LAN network to the LAN interface of the Branch2 router.
- Assign the last valid IP address of the Branch2 LAN network to PC3.
- Assign the first valid IP address of the HQ-to-Branch1 link network to the Serial 0/0/0 interface of the HQ router.
- Assign the last valid IP address of the HQ-to-Branch1 link network to the Serial 0/0/0 interface of the Branch2 router.
- Assign the first valid IP address of the HQ-to-Branch2 link network to the Serial 0/0/1 interface of the HQ router.
- Assign the last valid IP address of the HQ-to-Branch2 link network to the Serial 0/0/1 interface of the Branch2 router.
- Assign the first valid IP address of the Branch1-to-Branch2 link network to the Serial 0/0/1 interface of the Branch1 router.
- Assign the last valid IP address of the Branch1-to-Branch2 link network to the Serial 0/0/0 interface of the Branch2 router.

Document the addresses to be used in Table 11-4.

**Table 11-4 Addressing Table for Lab 11-2**

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	Fa0/0	172.20.0.1	255.255.224.0	—
	S0/0/0	172.20.56.1	255.255.255.252	—
	S0/0/1	172.20.56.5	255.255.255.252	—
	Lo1	10.10.10.1	255.255.255.252	—

*continues*

**Table 11-4 Addressing Table for Lab 11-2** *continued*

Device	Interface	IP Address	Subnet Mask	Default Gateway
Branch1	Fa0/0	172.20.32.1	255.255.240.0	—
	S0/0/0	172.20.56.2	255.255.255.252	—
	S0/0/1	172.20.56.9	255.255.255.252	—
Branch2	Fa0/0	172.20.48.1	255.255.248.0	—
	S0/0/0	172.20.56.10	255.255.255.252	—
	S0/0/1	172.20.56.6	255.255.255.252	—
PC1	NIC	172.20.47.254	172.20.32.1	255.255.240.0
PC2	NIC	172.20.31.254	172.20.0.1	255.255.224.0
PC3	NIC	172.20.55.254	172.20.48.1	255.255.248.0

### Task 3: Prepare the Network

**Step 1.** Cable a network that is similar to the one shown in the topology diagram of Figure 11-13.

You can use any current router in your lab as long as it has the required interfaces as shown in the topology.

**Step 2.** Clear any existing configurations on the routers.

### Task 4: Perform Basic Router Configurations

Perform basic configuration of the BRANCH, HQ, and ISP routers according to the following guidelines:

- Configure the router host name.
- Disable DNS lookup.
- Configure a privileged EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for console connections.
- Configure a password for VTY connections.
- Synchronize unsolicited messages and debug output with solicited output and prompts for the console and virtual terminal lines.
- Configure an EXEC timeout of 15 minutes.

### Task 5: Configure and Activate Serial and Ethernet Addresses

**Step 1.** Configure the interfaces on the HQ, Branch1, and Branch2 routers with the IP addresses from the table provided under the topology diagram.

When you have finished, be sure to save the running configuration to the NVRAM of the router.

**Step 2.** Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses from the table provided under the topology diagram.

**Step 3.** Configure the correct bandwidth for the serial interfaces on the Branch1 router.

What commands are required to accomplish this?

**configure terminal**

**interface serial0/0/0**

**bandwidth 128**

**interface serial 0/0/1**

**bandwidth 64**

**Step 4.** Configure the correct bandwidth for the serial interfaces on the Branch2 router.

What commands are required to accomplish this?

**configure terminal**

**interface serial0/0/0**

**bandwidth 64**

**interface serial 0/0/1**

**bandwidth 256**

**Step 5.** Configure the correct bandwidth for the serial interfaces on the HQ router.

What commands are required to accomplish this?

**configure terminal**

**interface serial0/0/0**

**bandwidth 128**

**interface serial 0/0/1**

**bandwidth 256**

## Task 6: Verify Connectivity to the Next-Hop Device

You should *not* have connectivity between end devices yet. However, you can test connectivity between the two routers and between an end device and its default gateway.

**Step 1.** Verify that the HQ, Branch1, and Branch2 routers can ping each of the neighboring routers across the WAN links.

**Step 2.** Verify that PC1, PC2, and PC3 can ping their respective default gateway.

## Task 7: Configure OSPF Routing on the Branch1 Router

**Step 1.** Consider the networks that need to be included in the OSPF updates that are sent out by the Branch1 router.

What directly connected networks are present in the Branch1 routing table?

[172.20.32.0/20](#)

[172.20.56.0/30](#)

[172.20.56.8/30](#)

What commands are required to enable OSPF and include the connected networks in the routing updates?

**[router ospf 1](#)**

**[network 172.20.32.0 0.0.15.255 area 0](#)**

**[network 172.20.56.0 0.0.0.3 area 0](#)**

**[network 172.20.56.8 0.0.0.3 area 0](#)**

Are there any router interfaces that do not need to have OSPF updates sent out? [Yes](#)

What command is used to disable OSPF updates on these interfaces?

**[passive-interface FastEthernet0/0](#)**

## Task 8: Configure OSPF and Static Routing on the HQ Router

**Step 1.** Consider the type of static routing that is needed on HQ.

A static default route will need to be configured to send all packets with destination addresses that are not in the routing table to the loopback address representing the link between the HQ router and the ISP. What command is needed to accomplish this?

**[ip route 0.0.0.0 0.0.0.0 loopback1](#)**

What directly connected networks are present in the HQ routing table?

[10.10.10.0](#)

[172.20.0.0/19](#)

[172.20.56.0/30](#)

[172.20.56.4/30](#)

Will the networks of the HQ LAN and the links between the Branch1 and Branch2 routers need to have the subnet mask information included in the network statements? [yes](#)

What commands are required to enable OSPF and include the appropriate networks in the routing updates?

**[router ospf 1](#)**

**[network 172.20.0.0 0.0.31.255 area 0](#)**

**[network 172.20.56.0 0.0.0.3 area 0](#)**

**[network 172.20.56.4 0.0.0.3 area 0](#)**

Are there any router interfaces that do not need to have OSPF updates sent out? [Yes](#)



What commands are used to disable OSPF updates on these interfaces?

**passive-interface FastEthernet0/0**

**passive-interface Loopback1**

The HQ router needs to send the default route information to the Branch1 and Branch2 routers in the OSPF updates. What command is used to configure this?

**default-information originate**

## Task 9: Configure OSPF Routing on the Branch2 Router

Consider the networks that need to be included in the OSPF updates that are sent out by the Branch2 router.

What directly connected networks are present in the Branch2 routing table?

172.20.48.0/21

172.20.56.4/30

172.20.56.8/30

What commands are required to enable OSPF and include the connected networks in the routing updates?

**router ospf 1**

**network 172.20.48.0 0.0.7.255 area 0**

**network 172.20.56.4 0.0.0.3 area 0**

**network 172.20.56.8 0.0.0.3 area 0**

Are there any router interfaces that do not need to have OSPF updates sent out? Yes

What command is used to disable OSPF updates on these interfaces?

**passive-interface FastEthernet0/0**

## Task 10: Verify the Configurations

Answer the following questions to verify that the network is operating as expected.

From PC1, is it possible to ping PC2? Yes

From PC1, is it possible to ping PC3? Yes

The answer to these questions should be **yes**. If any of these pings failed, check your physical connections and configurations. Refer to your basic troubleshooting techniques used in the Chapter 1 labs.

What OSPF routes are present in the routing table of the Branch1 router?

172.20.0.0/19 [110/782] via 172.20.56.1

172.20.48.0/21 [110/1172] via 172.20.56.1

172.20.56.4/30 [110/1171] via 172.20.56.1

What is the gateway of last resort in the routing table of the Branch1 router?

[172.20.56.1 to network 0.0.0.0](#)

What OSPF routes are present in the routing table of the HQ router?

[172.20.32.0/20 \[110/782\] via 172.20.56.2](#)

[172.20.48.0/21 \[110/391\] via 172.20.56.6](#)

[172.20.56.8/30 \[110/1952\] via 172.20.56.6](#)

What is the gateway of last resort in the routing table of the HQ router?

[0.0.0.0 to network 0.0.0.0](#)

What OSPF routes are present in the routing table of the Branch2 router?

[172.20.0.0/19 \[110/391\] via 172.20.56.5](#)

[172.20.32.0/20 \[110/1172\] via 172.20.56.5](#)

[172.20.56.0/30 \[110/1171\] via 172.20.56.5](#)

What is the gateway of last resort in the routing table of the Branch2 router?

[172.20.56.5 to network 0.0.0.0](#)

## Task 11: Reflection

On PC1, use the **tracert** command to examine the route that is used between PC1 and PC3.

What are the hops in the route to PC3?

[172.20.32.1, the FastEthernet 0/0 interface of the Branch1 router](#)

[172.20.56.1, the Serial 0/0/0 interface of the HQ router](#)

[172.20.56.6, the Serial 0/0/1 interface of the Branch2 router](#)

[172.20.55.254, the IP address of PC3](#)

Is this the least number of hops that can be used to reach PC3? No

If the answer is **no**, why is a path with more than the minimum amount of hops used?

[The serial connection between the Branch1 and HQ routers and the connection between the HQ and Branch2 routers have a higher bandwidth than the link between the Branch1 and Branch2 routers. Routes with higher bandwidth values have a lower calculated cost. The route with the lowest cost is chosen as the route to the Branch2 LAN.](#)

## Task 12: Documentation

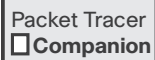
On each router, capture the following command output to a text (.txt) file and save for future reference:

- **show running-config**
- **show ip route**
- **show ip interface brief**
- **show ip protocols**

If you need to review the procedures for capturing command output, refer to “Lab 1-1: Cabling a Network and Basic Router Configuration.”

## Task 13: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.



## Packet Tracer Companion: Challenge OSPF Configuration (11.6.2)

You can now open the file LSG02-Lab1162.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment.



## Lab 11-3: OSPF Troubleshooting Lab (11.6.3)

Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram in Figure 11-14
- Erase the startup configuration and reload a router to the default state
- Load the routers with supplied scripts
- Discover where communication is not possible
- Gather information about the misconfigured portion of the network, along with any other errors
- Analyze information to determine why communication is not possible
- Propose solutions to network errors
- Implement solutions to network errors
- Document the corrected network

### Scenario

In this lab, you will begin by loading configuration scripts on each of the routers. These scripts contain errors that will prevent end-to-end communication across the network. You will need to troubleshoot each router to determine the configuration errors, and then use the appropriate commands to correct the configurations. When you have corrected all the configuration errors, all the hosts on the network should be able to communicate with each other.

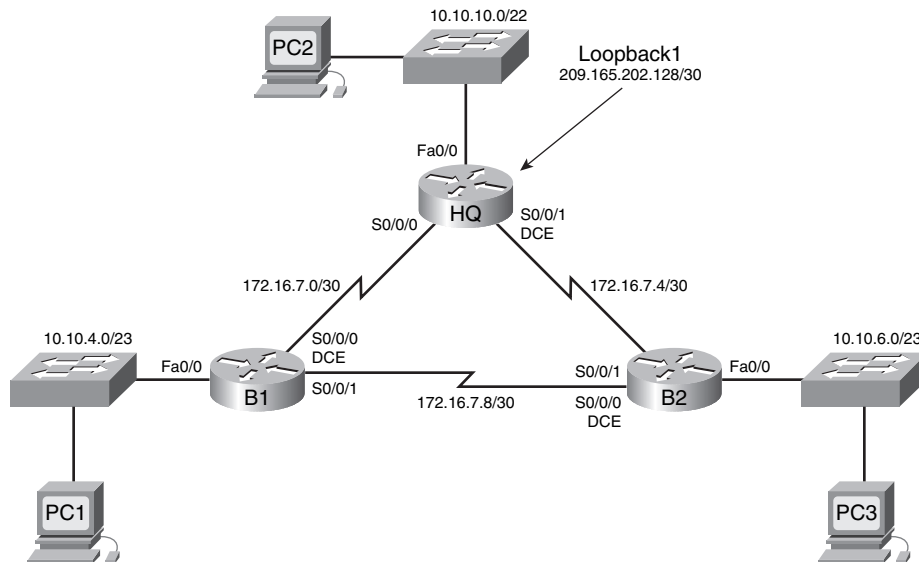
The network should also have met the following requirements:

- OSPF routing is configured on the Branch1 router.
- OSPF routing is configured on the Branch2 router.
- OSPF routing is configured on the HQ router.
- OSPF updates must be disabled on the LAN and loopback interfaces.
- The HQ router must redistribute the default route to the loopback interface in the routing updates.

- All OSPF routers must use a process ID of 1.
- All OSPF routers must be in area 0.

Figure 11-14 shows the topology diagram for this lab, and Table 11-5 provides the interface, IP address, subnet mask, and default gateway (where applicable) information for the routers and PCs in Figure 11-14.

**Figure 11-14 Topology Diagram for Lab 11-3**



**Table 11-5 Addressing Table for Lab 11-3**

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	Fa0/0	10.10.0.1	255.255.252.0	—
	S0/0/0	172.16.7.1	255.255.255.252	—
	S0/0/1	172.16.7.5	255.255.255.252	—
	Lo1	209.165.202.129	255.255.255.252	—
Branch1	Fa0/0	10.10.4.1	255.255.254.0	—
	S0/0/0	172.16.7.2	255.255.255.252	—
	S0/0/1	172.16.7.9	255.255.255.252	—
Branch2	Fa0/0	10.10.6.1	255.255.254.0	—
	S0/0/0	172.16.7.10	255.255.255.252	—
	S0/0/1	172.16.7.6	255.255.255.252	—
PC1	NIC	10.10.5.254	255.255.254.0	10.10.4.1
PC2	NIC	10.10.3.254	255.255.252.0	10.10.0.1
PC3	NIC	10.10.7.254	255.255.254.0	10.10.6.1

## Task 1: Cable, Erase, and Reload the Routers

**Step 1.** Cable a network.

Cable a network that is similar to the one shown in the topology diagram of Figure 11-14.

**Step 2.** Clear the configuration on each router.

Clear the configuration on each of the routers using the **erase startup-config** command and then reload the routers. Answer **no** if asked to save changes.

## Task 2: Load Routers with the Supplied Scripts

**Step 1.** Load the following script onto the Branch1 router.

---

**Instructor note:** Missing or misconfigured commands are shown in red.]

---

```

hostname Branch1
!
!
no ip domain-lookup
!
interface FastEthernet0/0
ip address 10.10.4.1 255.255.254.0
duplex auto
speed auto
no shutdown
!
interface Serial0/0/0
ip address 172.16.7.2 255.255.255.252
! The clock rate 64000 command is missing.
no shutdown
!
interface Serial0/0/1
ip address 172.16.7.9 255.255.255.252
no shutdown
!
router ospf 2
! The command should be router ospf 1.
passive-interface FastEthernet0/0
network 10.10.4.0 0.0.1.255 area 0
network 172.16.7.0 0.0.0.3 area 0
network 172.16.7.8 0.0.0.3 area 0
!
ip classless
!
!
!
line con 0
line vty 0 4
login

```

```
!
!
end
```

Corrected script:

```
hostname Branch1
!
!
no ip domain-lookup
!
interface FastEthernet0/0
 ip address 10.10.4.1 255.255.254.0
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.7.2 255.255.255.252
 clock rate 64000
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.7.9 255.255.255.252
 no shutdown
!
router ospf 1
 passive-interface FastEthernet0/0
 network 10.10.4.0 0.0.1.255 area 0
 network 172.16.7.0 0.0.0.3 area 0
 network 172.16.7.8 0.0.0.3 area 0
!
ip classless
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end
```

The errors in the student scripts are as follows:

- The **clock rate 64000** command is missing from the Serial 0/0/0 interface.
- The OSPF process ID is incorrect.

**Step 2.** Load the following script onto the Branch2 router.

```
hostname Branch2
!
```

```

!
!
interface FastEthernet0/0
 ip address 10.10.6.1 255.255.254.0
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.7.10 255.255.255.252
 clock rate 64000
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.7.6 255.255.255.252

```

**! The no shutdown command is missing.**

```

!
router ospf 1
 log-adjacency-changes
 passive-interface Serial0/0/1

```

**! The passive-interface command should be for the Fa0/0 interface.**

```

 network 172.16.7.4 0.0.0.3 area 0
 network 172.16.7.8 0.0.0.3 area 0
 network 10.10.6.0 0.0.3.255 area 0

```

**! The command for the LAN network should be network 10.10.6.0 0.0.1.255 area 0.**

```

!
ip classless
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end

```

**Corrected script:**

```

hostname Branch2
!
!
!
interface FastEthernet0/0
 ip address 10.10.6.1 255.255.254.0
 duplex auto
 speed auto
 no shutdown
!

```

```
interface Serial0/0/0
 ip address 172.16.7.10 255.255.255.252
 clock rate 64000
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.7.6 255.255.255.252
 no shutdown
!
router ospf 1
 passive-interface FastEthernet0/0
 network 10.10.6.0 0.0.1.255 area 0
 network 172.16.7.4 0.0.0.3 area 0
 network 172.16.7.8 0.0.0.3 area 0
!
ip classless
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end
```

The errors in the student scripts are as follows:

- The **no shutdown** command is missing from the Serial 0/0/1 interface.
- The **passive-interface** command is configured for the Serial 0/0/1 interface instead of the FastEthernet 0/0 interface.
- The **network** statement for the LAN network is incorrect.

**Step 3.** Load the following script onto the HQ router.

```
hostname HQ
!
!
no ip domain-lookup
!
interface FastEthernet0/0
 ip address 10.10.10.1 255.255.252.0
! The IP address should be 10.10.0.1 255.255.252.0.
 duplex auto
 speed auto
 no shutdown
!
!
interface Serial0/0/0
 ip address 172.16.7.1 255.255.255.252
```



```
no shutdown
!
interface Serial0/0/1
 ip address 172.16.7.5 255.255.255.252
 clock rate 64000
 no shutdown
!
interface Loopback1
 ip address 209.165.202.129 255.255.255.252
!
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/0
 passive-interface Loopback1
 network 172.16.7.0 0.0.0.3 area 0
 network 172.16.7.4 0.0.0.3 area 0
 network 10.10.0.0 0.0.7.255 area 0
```

! The mask for the 10.10.0.0 network should be 0.0.3.255.

! The **default-information originate** command is missing.

```
!
ip classless
ip route 0.0.0.0 0.0.0.0 loopback1
!
!
!
!
line con 0
line vty 0 4
 login
!
!
end
```

Corrected script:

```
hostname HQ
!
!
no ip domain-lookup
!
interface FastEthernet0/0
 ip address 10.10.0.1 255.255.252.0
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.7.1 255.255.255.252
 no shutdown
!
interface Serial0/0/1
```

```
ip address 172.16.7.5 255.255.255.252
clock rate 64000
no shutdown
!
interface Loopback1
 ip address 209.165.202.129 255.255.255.252
!
router ospf 1
 passive-interface FastEthernet0/0
 passive-interface Loopback1
 network 10.10.0.0 0.0.3.255 area 0
 network 172.16.7.0 0.0.0.3 area 0
 network 172.16.7.4 0.0.0.3 area 0
 default-information originate
!
ip classless
!
!
ip route 0.0.0.0 0.0.0.0 Loopback1
!
!
line con 0
line vty 0 4
 login
!
!
end
```

The errors in the student scripts are as follows:

- The IP address of the FastEthernet 0/0 interface is incorrect.
- The **default-information originate** command is missing from the OSPF configuration.
- The mask for the 10.10.0.0 **network** statement should be 0.0.3.255.

### Task 3: Troubleshoot the Branch1 Router

**Step 1.** Begin troubleshooting at the host connected to the Branch1 router.

From the host PC1, is it possible to ping PC2? no

From the host PC1, is it possible to ping PC3? yes

From the host PC1, is it possible to ping the default gateway? yes

**Step 2.** Examine the Branch1 router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the status of the interfaces?

The protocol is down on the Serial 0/0/0 interface.

Examine the interface configuration portion of the output of the **show running-configuration** command.

Are there any problems with the configuration of the interfaces?

The clock rate 64000 command is missing from the Serial 0/0/0 interface.

If there are any problems with the configuration of the interfaces, record any commands that will be necessary to correct the configuration errors.

**configure terminal**

**interface serial0/0/0**

**clock rate 64000**

**Step 3.** If you have recorded any commands in the previous step, apply them to the router configuration now.

**Step 4.** View a summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors on the Branch1 router? no

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

**Step 5.** Troubleshoot the routing configuration on the Branch1 router.

What routes are shown in the routing table?

10.10.4.0 is directly connected

10.10.6.0 [110/65] via 172.16.7.10

172.16.7.0 is directly connected

172.16.7.8 is directly connected

Are there any problems with the routing table?

Yes, some of the OSPF routes that should be present are missing.

The missing routes are the links between the HQ and Branch2 routers, the HQ LAN, and the default route on the HQ router.

Does the information in the routing table indicate any configuration errors on the Branch1 router, or will it be necessary to troubleshoot the configurations on the other two routers to correct the errors?

The other routers will need to be checked to find the cause of the missing routes.

Use the **show running-configuration**, **show ip protocols**, and **show ip ospf neighbor** commands to view information about the OSPF configuration on the Branch1 router. Are there any problems with the OSPF configuration?

The process ID for OSPF is incorrect.

If there are any problems with the OSPF configuration, record any commands that will be necessary to correct the configuration errors.

**no router ospf 2**

**router ospf 1**

**passive-interface fastethernet0/0**

network 10.10.4.0 0.0.1.255 area 0

network 172.16.7.0 0.0.0.3 area 0

network 172.16.7.8 0.0.0.3 area 0

**Step 6.** If you have recorded any commands in the previous step, apply them to the router configuration now.

**Step 7.** View the routing information.

If any changes were made to the configuration in the previous steps, view the routing information again.

Does the information in the routing table indicate any configuration errors on the Branch1 router? no

If the answer is **yes**, troubleshoot the routing configuration again.

What routes are shown in the routing table?

10.10.4.0 is directly connected

10.10.6.0 [110/65] via 172.16.7.10

172.16.7.0 is directly connected

172.16.7.8 is directly connected

**Step 8.** Attempt to ping between the hosts again.

From the host PC1, is it possible to ping PC2? no

From the host PC1, is it possible to ping PC3? yes

From the host PC1, is it possible to ping the Serial 0/0/0 interface of the HQ router? yes

From the host PC1, is it possible to ping the Serial 0/0/1 interface of the HQ router? no

## Task 4: Troubleshoot the HQ Router

**Step 1.** Begin troubleshooting at the host PC2.

From the host PC2, is it possible to ping PC1? no

From the host PC2, is it possible to ping PC3? no

From the host PC2, is it possible to ping the default gateway? no

**Step 2.** Examine the HQ router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the status of the interfaces?

The status and protocol of the Serial 0/0/1 interface are both down.

The IP address of the FastEthernet 0/0 interface is incorrect.

Examine the interface configuration portion of the output of the **show running-configuration** command.

Are there any problems with the configuration of the interfaces?

The IP address of the FastEthernet 0/0 interface is incorrect (this might be noted already).

If there are any problems with the configuration of the interfaces, record any commands that will be necessary to correct the configuration errors.

**interface fastethernet0/0**

**ip address 10.10.0.1 255.255.252.0**

Are there any problems with the interface status that could be due to errors on other parts of the network?

The link between the HQ and Branch2 routers is down.

The Serial 0/0/0 interface on the Branch2 router should be checked.

**Step 3.** If you have recorded any commands in the previous step, apply them to the router configuration now.

**Step 4.** View a summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors on the HQ router? no

If the answer is **yes**, troubleshoot the interface status of the interfaces again.

**Step 5.** Troubleshoot the routing configuration on the HQ router.

What routes are shown in the routing table?

10.10.0.0/22 is directly connected

10.10.4.0/23 [110/65] via 172.16.7.2

10.10.6.0/23 [110/129] via 172.16.7.2

172.16.7.0 is directly connected

172.16.7.8 [110/128] via 172.16.7.2

209.165.202.128 is directly connected

0.0.0.0/0 is directly connected

Are there any problems with the routing table?

The link between the HQ and Branch2 routers is missing from the routing table.

The route to the Branch2 LAN is through the Branch1 router.

Use the **show running-configuration**, **show ip protocols**, and **show ip ospf neighbor** commands to view information about the OSPF configuration on the HQ router. Are there any additional problems with the OSPF configuration?

The **default-information originate** command is missing from the OSPF configuration.

The mask for the 10.10.0.0/22 LAN is incorrect.

The Branch2 router is not in the OSPF neighbor table.

If there are any problems with the OSPF configuration, record any commands that will be necessary to correct the configuration errors.

**router OSPF 1**

**no network 10.10.0.0 0.0.7.255 area 0**

**network 10.10.0.0 0.0.3.255 area 0**

**default-information originate**

Are there any problems on the HQ router that could be due to errors on other parts of the network?

The link between the HQ and Branch2 routers is not in the routing table.

The Branch2 router is not in the OSPF neighbor table.

The Serial 0/0/1 interface on the Branch2 router should be checked.

**Step 6.** If you have recorded any commands in the previous step, apply them to the router configuration now.

**Step 7.** View the routing information.

If any changes were made to the configuration in the previous steps, view the routing information again.

Does the information in routing table indicate any configuration errors on the HQ router?

no

If the answer is **yes**, troubleshoot the routing configuration again.

**Step 8.** Attempt to ping between the hosts again.

From the host PC2, is it possible to ping PC1? yes

From the host PC2, is it possible to ping PC3? yes

From the host PC2, is it possible to ping the Serial 0/0/0 interface of the Branch2 router?

yes

From the host PC2, is it possible to ping the Serial 0/0/1 interface of the Branch2 router?

no

## **Task 5: Troubleshoot the Branch2 Router**

**Step 1.** Begin troubleshooting at the host PC3.

From the host PC3, is it possible to ping PC1? yes

From the host PC3, is it possible to ping PC2? yes

From the host PC3, is it possible to ping the default gateway? yes

From the host PC3, is it possible to ping the Serial 0/0/1 interface of the Branch2 router?

no

**Step 2.** Examine the Branch2 router to find possible configuration errors.

Begin by viewing the summary of status information for each interface on the router.

Are there any problems with the status of the interfaces?

The Serial 0/0/1 interface is administratively down.

If there are any problems with the configuration of the interfaces, record any commands that will be necessary to correct the configuration errors.

**interface serial0/0/1**

**no shutdown**

**Step 3.** If you have recorded any commands in the previous step, apply them to the router configuration now.

**Step 4.** View a summary of the status information.

If any changes were made to the configuration in the previous step, view the summary of the status information for the router interfaces again.

Does the information in the interface status summary indicate any configuration errors on the Branch2 router? no

If the answer is yes, troubleshoot the interface status of the interfaces again.

**Step 5.** Troubleshoot the routing configuration on the Branch2 router.

What routes are shown in the routing table?

10.10.0.0/22 [110/129] via 172.16.7.9

10.10.4.0/23 [110/65] via 172.16.7.9

10.10.6.0/23 is directly connected

172.16.7.0 [110/128] via 172.16.7.9

172.16.7.4 is directly connected

172.16.7.8 is directly connected

0.0.0.0/0 [110/1] via 172.16.7.9

Are there any problems with the routing table?

The route to the HQ LAN is through the Branch1 router.

Use the **show running-configuration**, **show ip protocols**, and **show ip ospf neighbor** commands to view information about the OSPF configuration on the Branch2 router. Are there any problems with the OSPF configuration?

The HQ router is not shown in the neighbor table.

The **passive-interface** command is configured to use the wrong interface.

The mask used in the **network** statement for the 10.10.6.0/23 LAN is incorrect.

If there are any problems with the OSPF configuration, record any commands that will be necessary to correct the configuration errors.

**router ospf 1**

**no passive-interface serial0/0/1**

**passive-interface fastethernet0/0**

**no network 10.10.6.0 0.0.3.255 area 0**

**network 10.10.6.0 0.0.1.255 area 0**

**Step 6.** If you have recorded any commands in the previous step, apply them to the router configuration now.

**Step 7.** View the routing information.

If any changes were made to the configuration in the previous steps, view the routing information again.

Does the information in the routing table indicate any configuration errors on the Branch2 router? no

If the answer to this question is **yes**, troubleshoot the routing configuration again.

What routes are shown in the routing table?

10.10.0.0/22 [110/65] via 172.16.7.5

10.10.4.0/23 [110/65] via 172.16.7.9

10.10.6.0/23 is directly connected

172.16.7.0 [110/128] via 172.16.7.9

[110/128] via 172.16.7.5

172.16.7.4 is directly connected

172.16.7.8 is directly connected

0.0.0.0 [110/1] via 172.16.7.5

**Step 8.** Attempt to ping between the hosts again.

From the host PC3, is it possible to ping PC1? yes

From the host PC3, is it possible to ping PC2? yes

From the host PC3, is it possible to ping the Serial 0/0/0 interface of the Branch1 router? yes

From the host PC3, is it possible to ping the Serial 0/0/1 interface of the Branch1 router? yes

## Task 6: Reflection

There were a number of configuration errors in the scripts that were provided for this lab. Use the space to write a brief description of the errors that you found.

---

---

---

---

---

---

---

---



## Task 7: Documentation

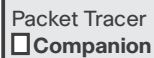
On each router, capture the following command output to a text (.txt) file and save for future reference:

- **show running-config**
- **show ip route**
- **show ip interface brief**
- **show ip protocols**

If you need to review the procedures for capturing command output, refer to “Lab 1-1: Cabling a Network and Basic Router Configuration.”

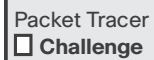
## Task 8: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.



### Packet Tracer Companion: OSPF Troubleshooting (11.6.3)

You can now open the file LSG02-Lab1163.pka on the CD-ROM that accompanies this book to repeat this hands-on lab using Packet Tracer. Remember, however, that Packet Tracer is not a substitute for a hands-on lab experience with real equipment.

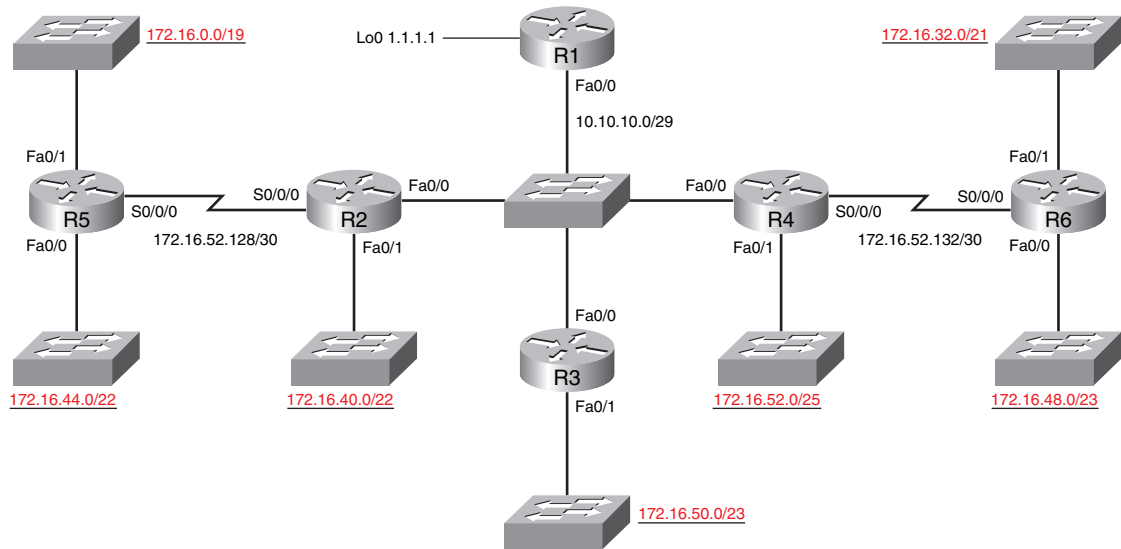


### Packet Tracer Skills Integration Challenge: OSPF Configuration

Upon completion of this challenge, you should be able to

- Design and document an addressing scheme based on requirements
- Apply a basic configuration to the devices
- Configure a router's priority and router ID
- Configure OSPF routing
- Disable routing updates on appropriate interfaces
- Verify full connectivity between all devices in the topology

Open the file LSG02-PTSkills11.pka on the CD-ROM that accompanies this book. You will use the topology in Figure 11-15 and the addressing table in Table 11-6 to document your design.

**Figure 11-15 Packet Tracer Skills Integration Challenge Topology (Answer)****Table 11-6 Addressing Table for the Packet Tracer Skills Integration Challenge Activity**

Device	Interface	IP Address	Subnet Mask
R1	Fa0/0	10.10.10.1	255.255.255.248
	Loopback0	1.1.1.1	255.255.255.255
R2	Fa0/0	10.10.10.2	255.255.255.248
	Fa0/1	172.16.40.1	255.255.252.0
	S0/0/0	172.16.52.130	255.255.255.252
R3	Fa0/0	10.10.10.3	255.255.255.248
	Fa0/1	172.16.50.1	255.255.254.0
R4	Fa0/0	10.10.10.4	255.255.255.248
	Fa0/1	172.16.52.1	255.255.255.128
	S0/0/0	172.16.52.133	255.255.255.252
R5	Fa0/0	172.16.44.1	255.255.252.0
	Fa0/1	172.16.0.1	255.255.224.0
	S0/0/0	172.16.52.129	255.255.255.252
R6	Fa0/0	172.16.48.1	255.255.254.0
	Fa0/1	172.16.32.1	255.255.248.0
	S0/0/0	172.16.52.134	255.255.255.252

## Task 1: Design and Document an Addressing Scheme

Use the 172.16.0.0/16 network to create an efficient addressing scheme that meets the following requirements.

Host Name	Interface	Number of Hosts
R2	Fa0/1	1000
R3	Fa0/1	400
R4	Fa0/1	120
R5	Fa0/1	6000
R5	Fa0/0	800
R6	Fa0/1	2000
R6	Fa0/0	500

**Note:** Interface Fa0/0 has been preconfigured on R1, R2, R3, and R4.

## Task 2: Apply a Basic Configuration

On each router, use the following chart to complete the basic router configurations.

Console Password	VTY Password	Enable Secret Password	Clock Rate (if applicable)
cisco	cisco	cisco	56000

## Task 3: Configure OSPF Routing

**Step 1.** Configure OSPF routing on each router.

**Step 2.** Verify that all routes were learned.

## Task 4: Fine-Tuning OSPF

**Step 1.** Use the following guidelines to complete this task.

- R1 will never participate in a DR/BDR election.
- R2 will always become the DR.
- R3 and R4 will both have the same priority of 100.
- R4 should always become the BDR.

**Note:** All priorities should be set on Fa0/0.

**Step 2.** Force a DR/BDR election.

## **Task 5: Configure a Loopback**

- Step 1.** On R1, configure a loopback with a 1.1.1.1/32 address.
- Step 2.** Create a default route to the loopback.
- Step 3.** Propagate the route within OSPF updates.

## **Task 6: View OSPF Updates**

- Step 1.** Enter simulation mode.
- Step 2.** Select only OSPF in the filter.
- Step 3.** View the updates.