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.
Warning and Disclaimer

This book is designed to provide information about the Accessing the WAN course of the Cisco Networking Academy CCNA Exploration curriculum. Every effort has been made to make this book as complete and 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 authors 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

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 of the professional technical community.

Reader feedback is a natural continuation of this process. If you have any comments about 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 be sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.
About the Author

John Rullan has been teaching at Thomas Edison High School in Jamaica, New York for the past 13 years and has been a part of the Cisco Networking Academy since 1998. He is the director of the Cisco Academy for the New York City Department of Education and is the citywide trainer. He provides support to the academy community and has presented at academy conferences throughout the country while working on the Instructional Support and Curriculum Maintenance teams. He also has taught CCNA, CCNP, and network security for the Borough of Manhattan Community College since 2000. He currently holds the Network+, CCNA, CCNP, and CCAI certifications.

About the Contributing Author

Sonya Coker received her undergraduate degree in secondary education from the University of South Alabama. She worked in the public school system for five years as a Title 1 Project Coordinator serving at-risk students. She joined the Cisco Academy program in 1998 when she started a local CCNA Academy at Murphy High School in Mobile, Alabama. She now works as a full-time developer in the Cisco Networking Academy program. She has worked on a variety of Academy curriculum projects, including CCNA, CCNP, Fundamentals of Wireless LANs, and Network Security. She has taught instructor training classes throughout the world.
About the Technical Reviewers

**Roderick Douglas**, Senior Lecturer with the IT Foundry at Sheffield Hallam University in the UK, has been an active Cisco Certified Academy Instructor since 2002. He is committed to delivering high-quality, flexible, and innovative training through the Cisco Academy Program. He has an MSc in computing from Sheffield Hallam University, Sheffield, UK. He holds CCNA and Wireless certifications from Cisco, as well as Microsoft MCSE/MCT, Novell CNE/CNI/Linux, CompTIA Linux+, and Security+, CWNA, Wireless# certifications.

**Lee Hilliard** is a professor and department chair for Computer Networking at College of the Canyons in Santa Clarita, California. He has been involved in the Cisco Networking Academy program since 2000 and is a CCAI and CATC instructor for CREATE CATC. He has structured the Computer Networking department to foster a spirit of community involvement by having students work with local businesses and nonprofit organizations. These efforts include soliciting surplus equipment from local businesses when they upgrade, having the students in the program refurbish the equipment as part of their hands-on lab activities, and then redistributing the equipment to nonprofit organizations. This is a win-win-win situation in which the students get practical application of the skills learned, the distribution of the equipment to underprivileged youth helps address the —digital divide,— and keeping usable equipment in service supports a sustainability effort. Hilliard has a master of science degree in industrial technology from California State University, Fresno.

**Wayne Jarvimaki** is a Main Contact/Lead Instructor for North Seattle Cisco Area Training Center (CATC) and has been training instructors in North America and Asia/Pac since 1998. Wayne serves on the Board of SeaKay, a nonprofit organization that helps Cisco Academies and low-income housing. He is the Senior Network Designer for CNS, a provider of bridged wireless campus networks for Digital Divide communities, and currently holds CCNA and CCAI certifications.
Dedications

I would like to dedicate this book to all my past and present students, whose dedication has inspired me to make this book the best that it can be. I would like to give special thanks to Emil Prysak, Alroy Lam, and Nabil El Bakhar, my current students, and Jalil Khan, a graduate, who still lends a hand and is always around to help.

—John Rullan

For all the students and instructors who have challenged and inspired me throughout my career in the Cisco Networking Academy Program. Your enthusiasm and curiosity remind me that there’s always something new to learn.

—Sonya Coker
Acknowledgments

Sonya Coker, coauthor, for giving me the pleasure of working with her on various support teams. I couldn’t think of anyone else I would like to write this book with. Her input and lab activities are sure to make this Study Guide much more educational and challenging.

Mary Beth Ray, executive editor, for allowing me to share my thoughts and ideas and putting them in this book. She is always there for me and helps keep me on track and on time!

Christopher Cleveland, development editor, for his patience, creativity, and support in making this book possible.

—John Rullan

Thanks to the Exploration development team for making me a part of the process of creating, editing, and improving the course that this book has been written to support. Knowing what you wanted for our students helped set the focus for this Study Guide.

Thanks to Mary Beth Ray and the whole team at Cisco Press for their patience and encouragement. Thanks Chris Cleveland for bearing with me during my learning curve.

—Sonya Coker
## Contents at a Glance

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>xxi</td>
</tr>
<tr>
<td>Chapter 1 Introduction to WANs</td>
<td>1</td>
</tr>
<tr>
<td>Chapter 2 PPP</td>
<td>49</td>
</tr>
<tr>
<td>Chapter 3 Frame Relay</td>
<td>115</td>
</tr>
<tr>
<td>Chapter 4 Network Security</td>
<td>183</td>
</tr>
<tr>
<td>Chapter 5 ACLs</td>
<td>285</td>
</tr>
<tr>
<td>Chapter 6 Teleworker Services</td>
<td>331</td>
</tr>
<tr>
<td>Chapter 7 IP Addressing Services</td>
<td>341</td>
</tr>
<tr>
<td>Chapter 8 Network Troubleshooting</td>
<td>407</td>
</tr>
<tr>
<td>Appendix How to Install SDM</td>
<td>543</td>
</tr>
</tbody>
</table>
Contents

Introduction xxii

Chapter 1 Introduction to WANs 1
Providing Integrated Services to the Enterprise 2
Review Question 2
Exercise 1-1: Browsing Through Internet Routing Tables 2
Exercise 1-2: Tracing a Path Through the Internet 4

WAN Technology Concepts 6
Review Question 6

WAN Connection Options 6
Review Questions 7

Chapter Review Vocabulary Exercise: Matching 8
Chapter Review Multiple-Choice Questions 9

Lab 1-1: Challenge Review Lab (1.4.1) 13
Scenario 14
Task 1: Prepare the Network 14
Task 2: Perform Basic Device Configurations 15
Task 3: Configure and Activate Serial and Ethernet Addresses 15
Task 4: Configure STP 18
Task 5: Configure VTP 18
Task 6: Configure VLANs 20
Task 7: Configure RIP Routing 23
Task 8: Configure OSPF Routing 29
Task 9: Configure EIGRP Routing 31
Task 10: Document the Router Configurations 34
Task 11: Clean Up 42

Packet Tracer Exercise: Comprehensive WAN Fundamentals 42
Packet Tracer Skills Integration Challenge 42

Task 1: Configure Static and Default Routing 44
Task 2: Add and Connect the BRANCH Router 45
Task 3: Add and Connect the Switches 45
Task 4: Add and Connect the PCs 45
Task 5: Perform Basic Device Configuration 46
Task 6: Configure OSPF Routing 46
Task 7: Configure STP 47
Task 8: Configure VTP 47
Task 9: Configure Trunking 47
Task 10: Configure VLANs 47
Task 11: Verify End-to-End Connectivity 48
Chapter 2  PPP 49
  Serial Point-to-Point Links  50
  Review Questions 51

PPP Concepts 51
  Vocabulary Exercise: Matching 52

Configuring PPP 53
  Review Questions 53

Configuring PPP with Authentication 53
  Review Questions 54

Chapter Review: Multiple-Choice Questions 54

Chapter Review Exercise 58

Lab 2-1: Basic PPP Configuration Lab (2.5.1) 59
  Scenario 60
  Task 1: Prepare the Network 60
  Task 2: Perform Basic Router Configuration 60
  Task 3: Configure and Activate Serial and Ethernet Addresses 61
  Task 4: Configure OSPF on the Routers 63
  Task 5: Configure PPP Encapsulation on Serial Interfaces 65
  Task 6: Break and Restore PPP Encapsulation 71
  Task 7: Configure PPP Authentication 72
  Task 8: Intentionally Break and Restore PPP CHAP Authentication 76
  Task 9: Document the Router Configurations 78
  Task 10: Clean Up 81
  Packet Tracer Companion: Basic PPP Configuration (2.5.1) 81

Lab 2-2: Challenge PPP Configuration (2.5.2) 82
  Scenario 83
  Task 1: Prepare the Network 83
  Task 2: Perform Basic Router Configuration 83
  Task 3: Configure and Activate Serial and Ethernet Addresses 84
  Task 4: Configure OSPF on Routers 86
  Task 5: Configure PPP Encapsulation on Serial Interfaces 88
  Task 6: Intentionally Break and Restore PPP Encapsulation 90
  Task 7: Configure PPP CHAP Authentication 91
  Task 8: Intentionally Break and Restore PPP CHAP Authentication 92
  Task 9: Document the Router Configurations 93
  Task 10: Clean Up 97
  Packet Tracer Companion: Challenge PPP Configuration (2.5.2) 97

Lab 2-3: Troubleshooting PPP Configuration (2.5.3) 98
  Scenario 99
  Task 1: Load Routers with the Supplied Scripts 99
  Task 2: Find and Correct Network Errors 105
Task 3: Document the Corrected Network 105
Task 4: Clean Up 109
Packet Tracer Companion: Troubleshooting PPP Configuration (2.5.3) 109

Packet Tracer Exercise 2-1: PPP 109
Packet Tracer Exercise 2-2: PPP Troubleshooting 109
Packet Tracer Skills Integration Challenge 109
Task 1: Configure Static and Default Routing 111
Task 2: Add and Connect a Router 111
Task 3: Design and Document an Addressing Scheme 111
Task 4: Add and Connect the Devices in the Address Space 112
Task 5: Configure Basic Device Settings 112
Task 6: Configure PPP Encapsulation with CHAP Authentication 113
Task 7: Configure OSPF Routing 113
Task 8: Configure VLANs 114
Task 9: Verify Connectivity 114

Chapter 3 Frame Relay 115
Basic Frame Relay Concepts 116
Review Questions 117
Configuring Frame Relay 117
Vocabulary Exercise: Matching Terms 118

Advanced Frame Relay Concepts 118
Fill-in-the-Blank Exercise 119

Configuring Advanced Frame Relay 119
Vocabulary Exercise: Matching Commands 120

Chapter Review Multiple-Choice Questions 122
Lab 3-1: Basic Frame Relay (3.5.1) 126
Scenario 127
Task 1: Prepare the Network 127
Task 2: Perform Basic Router Configuration 128
Task 3: Configure Frame Relay 129
Task 4: Verify the Configuration 134
Task 5: Troubleshoot Frame Relay 138
Task 6: Configure a Frame Relay Subinterface 143
Final Configurations 149

Lab 3-2: Challenge Frame Relay Configuration (3.5.2) 152
Scenario 153
Task 1: Prepare the Network 153
Task 2: Perform Basic Router Configuration 153
Task 3: Configure IP Addresses 153
Task 4: Configure EIGRP on Routers R1 and R2 154
Task 5: Configure Frame Relay PVC Between R1 and R2 154
Task 6: Intentionally Break the PVC, and Then Restore It 155
Task 7: Configure Frame Relay Subinterfaces 155
Task 8: Intentionally Break the PVC, and Then Restore It 156
Task 9: Document the Router Configurations 156
Task 10: Clean Up 156

**Lab 3-3: Troubleshooting Frame Relay (3.5.3)** 156
Scenario 157
Task 1: Prepare the Network 157
Task 2: Troubleshoot and Repair the Frame Relay Connection Between R1 and R2 162
Task 3: Document the Router Configurations 162
Task 4: Clean Up 162

**Lab 3-4: Frame Relay with Subinterfaces** 162
Scenario 164
Task 1: Configure the HQ Router 164
Task 2: Configure Subinterfaces on the HQ Router 164
Task 3: Configure the Serial Interface on the Branch 1 Router 165
Task 4: Configure the Serial Interface on the Branch 2 Router 165
Task 5: Configure the Serial Interface on the Branch 3 Router 165
Task 6: Configure the FastEthernet Interface on the Branch 1 LAN 166
Task 7: Configure the FastEthernet Interface on the Branch 2 LAN 166
Task 8: Configure the FastEthernet Interface on the Branch 3 LAN 166
Task 9: Configure EIGRP 166
Task 10: Verify the Configurations 167
Packet Tracer Companion: Frame Relay Full Mesh 174

**Packet Tracer Skills Integration Challenge** 174
Task 1: Configure PPP with CHAP Between Devices 176
Task 2: Configure Full-Mesh Frame Relay 177
Task 3: Configure Static and Default Routing 178
Task 4: Configure and Test Inter-VLAN Routing 179
Task 5: Configure VTP and Trunking on the Switches 179
Task 6: Configure VLANs on the Switch 180
Task 7: Configure and Verify VLAN 99 181
Task 8: Configure S1 as Root for All Spanning Trees 181
Task 9: Assign Ports to VLANs 182
Task 10: Test End-to-End Connectivity 182
Chapter 4  
Network Security 183

Introduction to Network Security 184
Vocabulary Exercise: Matching 184
Vocabulary Exercise: Completion 185

Securing Cisco Routers 186
Describe Good Password Practices 186
Configuring Router Passwords 186

Secure Router Network Services 187
Vulnerable Router Services Exercise 188
Securing Routing Protocols: Completion 188

Using Cisco Security Device Manager 189
Preparing a Router for SDM 189

Secure Router Management 190
Managing Cisco IOS Images: Identify Commands 190
Managing Cisco IOS Images: Short Answer 190
Password-Recovery Exercise 191

Lab 4-1: Basic Security Configuration (4.6.1) 193
Scenario 193
Task 1: Prepare the Network 195
Task 2: Perform Basic Router Configurations 195
Task 3: Secure the Router from Unauthorized Access 195
Task 4: Secure Access to the Network 198
Task 5: Logging Activity with SNMP (Simple Network Management Protocol) 201
Task 6: Disabling Unused Cisco Network Services 202
Task 7: Managing Cisco IOS and Configuration Files 208
Task 8: Using SDM to Secure a Router 223
Task 9: Document the Router Configurations 230
Task 10: Clean Up 238

Lab 4-2: Challenge Security Configuration (4.6.2) 238
Scenario 238
Task 1: Prepare the Network 240
Task 2: Perform Basic Router Configurations 240
Task 3: Secure Access to Routers 240
Task 4: Secure Access to the Network 242
Task 5: Logging Activity with SNMP (Simple Network Management Protocol) 244
Task 6: Disabling Unused Cisco Network Services 244
Task 7: Managing Cisco IOS and Configuration Files 251
Task 8: Using SDM to Secure R2 252
Task 9: Document the Router Configurations 253
Task 10: Clean Up 261
Lab 4-3: Troubleshooting Security Configuration (4.6.3)  262
  Scenario 262
  Task 1: Load Routers with the Supplied Scripts 263
  Task 2: Find and Correct All Network Errors 274
  Task 3: Document the Corrected Network 274
  Task 4: Clean Up 282

Packet Tracer Skills Integration Challenge 283
  Task 1: Configure Routing 284
  Task 2: Configure OSPF Authentication 284
  Task 3: Upgrade the Cisco IOS Image 284

Chapter 5  ACLs  285

Using ACLs to Secure Networks  286
  Multiple-Choice Questions 287

Configuring Standard ACLs: Command Exercise  289

Configuring Extended ACLs  291
  Vocabulary Exercise: Matching Terms 291
  Extended ACL Command Exercise 292

Configuring Complex ACLs  293
  Review Questions 293
  Vocabulary Exercise: Matching Terms 294

Lab 5-1: Basic Access Control Lists (5.5.1)  295
  Scenario 296
  Task 1: Prepare the Network 296
  Task 2: Perform Basic Router Configurations 296
  Task 3: Configure a Standard ACL 300
  Task 4: Configure an Extended ACL 302
  Task 5: Control Access to the VTY Lines with a Standard ACL 303
  Task 6: Troubleshoot ACLs 304
  Task 7: Document the Router Configurations 305
  Task 8: Clean Up 308
  Packet Tracer Companion: Basic Access Control Lists (5.5.1) 308

Lab 5-2: Access Control Lists Challenge (5.5.2)  309
  Task 1: Prepare the Network 310
  Task 2: Perform Basic Router Configurations 310
  Task 3: Configure Standard ACLs 312
  Task 4: Configure Extended ACLs 313
  Task 5: Verify an ACL 314
  Task 6: Document the Router Configurations 315
  Task 7: Clean Up 318
  Packet Tracer Companion: Challenge Access Control Lists (5.5.2) 318
Lab 5-3: Troubleshooting Access Control Lists (5.5.3) 318
Scenario 319
Task 1: Load Routers with the Supplied Scripts 319
Task 2: Find and Correct Network Errors 322
Task 3: Document the Corrected Network 322
Task 4: Clean Up 324
Packet Tracer Exercise 5.1: Named Access Control Lists 325
Packet Tracer Exercise 5.2: Access Control Lists 325

Packet Tracer Skills Integration Challenge 325
Introduction 326
Task 1: Configure PPP with CHAP Authentication 326
Task 2: Configure Default Routing 327
Task 3: Configure OSPF Routing 327
Task 4: Implement Multiple ACL Security Policies 328

Chapter 6 Teleworker Services 331
Business Requirements for Teleworker Services 332
Review Questions 332

Broadband Services: Fill-in-the-Blank Exercise 333

VPN Technology 334
Vocabulary Exercise: Matching 334
Multiple-Choice Questions 335

Packet Tracer Exercise 6-1: DSL/Cable Configuration 337
Packet Tracer Exercise 6-2: Wireless Configuration 337

Packet Tracer Skills Integration Challenge 337
Task 1: Apply Basic Router Configurations 339
Task 2: Configure Dynamic and Default Routing 339
Task 3: Establish Teleworker Services 339
Task 4: Test Connectivity Before ACL Configuration 340
Task 5: Apply ACL Policies 340
Task 6: Test Connectivity After ACL Configuration 340

Chapter 7 IP Addressing Services 341
DHCP 342
Vocabulary Exercise: Matching 342

Scaling Networks with NAT 343
Fill-in-the-Blank Exercise 343
Vocabulary Exercise: Matching 344

Reasons for Using IPv6 344
Multiple-Choice Questions 345
Concept Questions 348
Lab 7-1: Basic DHCP and NAT Configuration (7.4.1) 349
Scenario 350
Task 1: Prepare the Network 350
Task 2: Perform Basic Router Configurations 350
Task 3: Configure PC1 and PC2 to Receive an IP Address Through DHCP 352
Task 4: Configure a Cisco IOS DHCP Server 353
Task 5: Configure Static and Default Routing 356
Task 6: Configure Static NAT 357
Task 7: Configure Dynamic NAT with a Pool of Addresses 357
Task 8: Configure NAT Overload 359
Task 9: Document the Network 360
Task 10: Clean Up 364
Packet Tracer Companion: Basic DHCP and NAT Configuration (7.4.1) 364

Lab 7-2: Challenge DHCP and NAT Configuration (7.4.2) 365
Scenario 366
Task 1: Prepare the Network 366
Task 2: Perform Basic Router Configurations 366
Task 3: Configure a Cisco IOS DHCP Server 368
Task 4: Configure Static and Default Routing 368
Task 5: Configure Static NAT 369
Task 6: Configure Dynamic NAT with a Pool of Addresses 369
Task 7: Document the Network 369
Task 8: Clean Up 369
Packet Tracer Companion: Challenge DHCP and NAT Configuration (7.4.2) 373

Lab 7-3: Troubleshooting DHCP and NAT (7.4.3) 373
Scenario 374
Task 1: Prepare the Network 374
Task 2: Find and Correct Network Errors 377
Task 3: Document the Router Configurations 378
Task 4: Clean Up 378
Final Configurations 378
Packet Tracer Companion: Troubleshooting DHCP and NAT Configuration (7.4.3) 381

Lab 7-4: IPv6 Basic Configuration Using an Adtran 381
Scenario 381
Task 1: Upgrade IOS to Support IPv6 382
Task 2: Enter Basic Configuration for Each Device 382
Task 3: Enable IPv6 Forwarding 383
Task 4: Configure IPv6 Addresses 384
Task 5: Create and Address Loopbacks 385
Task 6: Configure RIPng Routing 386
Task 7: Test Connectivity 388

Lab 7-5: IPv6 Basic Configuration Using a Frame Switch 389
Scenario 389
Task 1: Upgrade IOS to Support IPv6 389
Task 2: Enter the Basic Configuration for Each Device 390
Task 3: Enable IPv6 Forwarding 391
Task 4: Configure IPv6 Addresses 392
Task 5: Create and Address Loopbacks 393
Task 6: Configure RIPng Routing 395
Task 7: Test Connectivity 399
Task 8: Advertise the Default Route 399

Packet Tracer Exercise 7-1: DHCP 400
Packet Tracer Exercise 7-2: DHCP Troubleshooting 400
Packet Tracer Exercise 7-3: Configuring NAT, PAT, and Static NAT 400
Packet Tracer Exercise 7-4: Double NAT with DHCP

400 Packet Tracer Skills Integration Challenge 400
Task 1: Apply Basic Configurations 402
Task 2: Configure PPP Encapsulation with CHAP 402
Task 3: Configure Dynamic and Default Routing 403
Task 4: Configure Routers Using DHCP 403
Task 5: Verify That PCs Are Automatically Configured with Addressing Details 404
Task 6: Configure a DNS Server with DNS Entries 404
Task 7: Configure an ACL to Permit NAT 404
Task 8: Configure Static NAT 405
Task 9: Configure Dynamic NAT with Overload 405
Task 10: Configure the ISP Router with a Static Route 405
Task 11: Test Connectivity 405

Chapter 8 Network Troubleshooting 407
Documenting Your Network 408
Concept Questions 408

Troubleshooting Methodologies and Tools 409
Multiple-Choice Questions 410

WAN Communications 411
Fill-in-the-Blank Exercise 412

Network Troubleshooting 412
Vocabulary Exercise: Define 413

Activity 8-1: Troubleshooting Role Play (8.3.7) 414
Scenario 414
Task 1: Build the Network 415
Task 2: Test the Network 415
Task 3: Break the Network 415
Task 4: Troubleshoot the Problem 415
Task 5: Gather Symptoms from Suspect Devices 415
Task 6: Correct the Problem 415
Task 7: Document the Problem and Solution 415
Task 8: Reverse the Roles and Start Over 415
Task 9: Clean Up 415

Lab 8-1: Troubleshooting Enterprise Networks 1 (8.5.1) 416
Scenario 417
Task 1: Load Routers with the Supplied Scripts 418
Task 2: Find and Correct All Network Errors 431
Task 3: Verify That Requirements Are Fully Met 431
Task 4: Document the Corrected Network 432
Task 5: Clean Up 445
Alternate Configurations 445
Packet Tracer Companion: Troubleshooting Enterprise Networks 1 (8.5.1) 457

Lab 8-2: Troubleshooting Enterprise Networks 2 (8.5.2) 458
Scenario 459
Task 1: Load Routers with the Supplied Scripts 460
Task 2: Find and Correct All Network Errors 473
Task 3: Verify That Requirements Are Fully Met 473
Task 4: Document the Corrected Network 474
Task 5: Clean Up 485
Packet Tracer Companion: Troubleshooting Enterprise Networks 2 (8.5.2) 485

Lab 8-3: Troubleshooting Enterprise Networks 3 (8.5.3) 486
Scenario 487
Task 1: Load Routers with the Supplied Scripts 488
Task 2: Find and Correct All Network Errors 500
Task 3: Verify That Requirements Are Fully Met 500
Task 4: Document the Corrected Network 501
Task 5: Clean Up 512
Packet Tracer Companion: Troubleshooting Enterprise Networks 3 (8.5.3) 512

Packet Tracer Exercise 8-1: Comprehensive Network Troubleshooting

513 Packet Tracer Skills Integration Challenge 513
Task 1: Configure Frame Relay in a Hub-and-Spoke Topology 515
Task 2: Configure PPP with CHAP and PAP Authentication 519
Task 3: Configure Static and Dynamic NAT on HQ 520
Task 4: Configure Static and Default Routing 521
Task 5: Configure Inter-VLAN Routing 522
Task 6: Configure and Optimize EIGRP Routing 523
Task 7: Configure VTP, Trunking, the VLAN Interface, and VLANs 526
Task 8: Assign VLANs and Configure Port Security 530
Task 9: Configure STP  532
Task 10: Configure DHCP  533
Task 11: Configure a Firewall ACL 536
Task 12: Configure Wireless Connectivity 537
Task 13: Network Troubleshooting 542

How to Install SDM 543

Step 1: Preparation 543
Step 2: Prepare the Router for SDM 543
Step 3: Configure Addressing 544
Step 4: Extract SDM on the Host 544
Step 5: Install SDM on the PC 544
Step 6: Run SDM from the PC 545
Step 7: Install SDM to the Router 547
Step 8: Run SDM from the Router 549
Icons Used in This Book

![Icons](Image)

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:

- **Bold** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), bold indicates commands that the user enters (such as a `show` command).

- **Italic** indicates arguments for which you supply actual values.

- Vertical bars (|) separate alternative, mutually exclusive elements.

- Square brackets ([ ]) indicate an optional element.

- Braces ({ }) indicate a required choice.

- Braces within brackets ({{ }}) indicate a required choice within an optional element.
Introduction

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

Accessing the WAN, CCNA Exploration Labs and Study Guide is a supplement to your classroom and laboratory experience with the Cisco Networking Academy. To succeed 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 acquire the knowledge and practice the skills associated with the content area of the CCNA Exploration Accessing the WAN course.

Specifically, this book helps you work on these main areas:

- WAN technology concepts
- PPP concepts and configuration
- Frame Relay concepts and configuration
- Network security threats and mitigation techniques
- Access control list operation and configuration
- Broadband services and technologies
- Network Address Translation concepts and configuration
- DHCP operation and configuration
- IPv6 concepts
- Troubleshooting methodologies and tools

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

Audience for This Book

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

Goals and Methods

The most important goal of this book is to help you pass the CCNA exam (640-802). Passing this foundation exam means that you not only have the required knowledge of the technologies covered by the exam, but that you can plan, design, implement, operate, and troubleshoot these technologies. In other words, these exams are rigorously application-based. You can view the exam topics any time at http://www.cisco.com/go/certifications. The topics are divided into eight categories:
- Describe how a network works
- Configure, verify, and troubleshoot a switch with VLANs and 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 Accessing the WAN course focuses on the third, fifth, sixth, seventh, and eighth topics.

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

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

In the configuration chapters, you’ll find many Packet Tracer Activities that work with the Cisco Packet Tracer tool. Packet Tracer allows you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available 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 portion of each chapter includes all the online Curriculum Labs, some additional supplemental labs that you can perform with Packet Tracer, 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 cover implementations and assume that you have a firm-enough grasp on the technologies to — go it alone! These labs often give you only 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 Lab. Avoid the temptation to work through the Challenge Lab by flipping back through the Basic Lab when you are unsure 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 ask you to fix a broken network. These labs include corrupted scripts that you purposely load onto the routers. Then you use troubleshooting techniques to isolate problems and implement the solution. By the end of the lab, you should have a functional network with full end-to-end connectivity.
Most of the Hands-on Labs include Packet Tracer Companion Activities, in which you can use Packet Tracer to complete a simulation of the lab.

Each chapter ends with a 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.

**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 they 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 version 4.x is available only to Cisco Networking Academies through the Academy Connection website.

**How This Book Is Organized**

Because the content of this book and the online curriculum is sequential, you should work through this book 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 Accessing the WAN course. This book has eight chapters with the same numbers and names as the online course chapters.

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

- **Chapter 1, “Introduction to WANs”**: The exercises in the Study Guide portion of this chapter focus on LAN design concepts, including vocabulary and the three-layer hierarchical model. 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 2, “PPP”**: The exercises in the first part of this chapter help you understand basic Ethernet and switching concepts, including building the MAC address table and collision and broadcast domains. Then the Packet Tracer exercises cover, in detail, how to configure a switch, including basic switch management and configuring switch security. The Lab portion of the chapter includes two Basic Labs, a Challenge Lab, and a Packet Tracer Skills Integration Challenge activity.
Chapter 3, “Frame Relay”: The exercises in the first portion of this chapter focus on the concepts of VLANs, including benefits of VLANs and types of VLANs. The exercises then cover VLAN trunking concepts before moving into a section devoted to a VLAN and trunk configuration Packet Tracer exercise. The Lab portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.

Chapter 4, “Network Security”: The exercises in this chapter focus on key network security threats, tools, and mitigation techniques for Cisco routers. Configuration practice is provided for router security tasks. 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 5, “ACLs”: Exercises in this chapter focus on the concept of redundant LAN topologies, using STP and its variants to stop loops, and the commands to manipulate root bridge elections. The 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, “Teleworker Services”: This short chapter focuses on how to configure inter-VLAN routing, including two Packet Tracer exercises. 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 7, “IP Addressing Services”: The exercises in this chapter include several matching term activities, multiple choice questions, fill-in-the-blank exercises, and concept questions that test your knowledge on DHCP and scaling IP addresses with the use of NAT and PAT. It also tests your knowledge of IPv6 and routing using the next generation of RIP. The Lab portion of this chapter includes all the online curriculum labs for DHCP and NAT as well as four additional Packet Tracer activities that test your knowledge and skills in complex configurations using DHCP, Static NAT, PAT, and double NAT. A Packet Tracer Skills Integration Challenge ties all of these concepts together.

Chapter 8, “Network Troubleshooting”: The exercises in this chapter begin with wireless LAN concepts, including standards, operation, and security. The exercises then cover wireless configuration for LAN access using a Linksys WRT300N, including a Packet Tracer exercise. The Lab portion of the chapter includes a Basic Lab, a Challenge Lab, a Troubleshooting Lab, and a Packet Tracer Skills Integration Challenge activity.

Appendix, “How to Install SDM”: Cisco Router and Security Device Manager (SDM) is used in the security labs for this course. This appendix describes and illustrates how to install SDM on a Cisco router or PC.

About the CD-ROM

The CD-ROM included with this book contains 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.

You can find updates to these files on this book’s website at http://www.ciscopress.com/title/9781587132018.
About the Cisco Press Website for This Book

Cisco Press may provide additional content that you can access by registering your book at the cisco-press.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 log into your account, or create a free account if you do not have one already. Then enter this book’s ISBN, located on the back cover.

After you register your book, it appears on your Account page under Registered Products, and you can access any online material from there.
The Study Guide portion of this chapter uses a combination of matching and multiple-choice question exercises to test your knowledge and skills of basic wide-area networks (WAN).

The Labs and Activities portion of this chapter includes all the online curriculum labs. The challenge labs are added to ensure that you have mastered the practical, hands-on skills needed to understand material learned in previous semesters of the Exploration curriculum.

Understanding a router’s place and function in the Internet is necessary for moving further in your studies of WANs. You learned how routers communicate within an autonomous system using interior gateway protocols in the Routing Protocols and Concepts CCNA Exploration curriculum. This section tests your knowledge in WAN concepts, technologies, and connection types.

As you work through this chapter, use Chapter 1 in the Accessing the WAN, CCNA Exploration Companion Guide or use the corresponding Chapter 1 in the Accessing the WAN online curriculum for assistance.
Study Guide

Providing Integrated Services to the Enterprise

Up until now, the curriculum has focused on LANs, their devices, and how communication occurs using various protocols and services. The focal point of this chapter is on WANs, their devices, and how communication occurs using various encapsulation methods and WAN connections. This section discusses the importance of designing a WAN in a hierarchical structure to ensure a reliable network infrastructure. The Cisco Enterprise Architecture was designed to help a business’s network grow as the company grows. This architecture assists network designers with a template to support data centers, branch offices, and teleworkers.

Review Question

You are an engineer in charge of a network that has grown in size from a LAN to a metropolitan-area network (MAN). The network now supports a campus network, multiple offsite offices, data centers, and teleworkers. How can the Cisco Enterprise Architecture help your network to grow parallel to your company? Write an essay of no more than 250 words. Make sure to include WAN connections, wireless mobility, and IP communications. To assist with your answer, use the curriculum and the following URL: http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns477/net_brochure0900aecd802843ce.pdf.

Exercise 1-1: Browsing Through Internet Routing Tables

Lab exercises from previous chapters required you to configure various routing protocols to route traffic within an autonomous system. The size of the routing table varied, depending on the number of routers in each exercise. The number of locations a —real— company has will most often determine the actual size of their routing table. A static default route is used to route traffic to networks not listed in the routing table (autonomous system) and usually points to your ISP. An ISP’s router, which routes traffic to the Internet, may have hundreds of thousands of routes in its routing table. Looking Glass Sites offers publicly available route servers to view current Internet routing tables.

2. Under Routing-Related (Route Servers, etc.), you will notice that there are nine options to choose from. These are companies that allow access to their route servers. In this activity, you access them to view their routing tables.
3. Click the ATT (US) link.
4. HyperTerminal will open or a command box will appear asking you to enter a username (see Figure 1-1). Enter the username reviews. Note that the username is not misspelled.
5. The hostname of route server should appear in User Exec mode.
6. Use the `show ip route` command to display the current routing tables. Use the Enter key or spacebar to scroll through the table. The size of the table is —mind boggling! Can you imagine troubleshooting a network of this magnitude?

7. Open another web browser and log on to http://www.arin.net/index.shtml. This site is the American Registry for Internet Numbers (ARIN). This site serves many important purposes; you are going to use it to determine who owns (leases) a particular network address.

8. The 206.107.185.0 network address was taken from the routing table. Enter this address into the Search WHOIS box in the upper-right corner (see Figure 1-2) and press Enter.

---

**Figure 1-1 HyperTerminal Login**

![HyperTerminal Login Image]

---

**Figure 1-2 Checking the American Registry for Internet Numbers**

![ARIN Image]
9. The company that leases this address happens to be another ISP. In this case, it belongs to Sprint (see Figure 1-3). Sprint then subleases the address to Rocky Mountain Communications, which in turn subleases the address to Pacific Press Publishing. What this means is that ATT and Sprint route Internet traffic through each other’s networks.

Figure 1-3 ARIN WHOIS Results

10. Look through the routing table again, and this time on a piece of paper write down several of the IP addresses listed. Go back to ARIN and place the address in the WHOIS box and see which other companies you will find that ATT routes traffic for.

Exercise 1-2: Tracing a Path Through the Internet

The Looking Glass route servers located at http://www.nanog.org/lookingglass.html can also be used to trace a path through the Internet from a route server back to your PC:

1. This time, let’s use the CERFnet route server.

2. HyperTerminal will open or a command box will appear. No username or password is required.

3. Enter the show ip int brief command. This will display all the interfaces on a router. The only interface configured with an IP address is the Ethernet 1/0 interface with the 12.129.193.235 IP address (see Figure 1-4).

4. On your PC, open the command box using the Start, Run and enter cmd.

5. When the command box opens, enter tracert 12.129.193.235.

6. This will trace the path from your PC, through your network, through the Internet to the route server whose IP address you entered.
7. This will display the name of the domain and IP addresses of each router you pass through. Depending on where you are in the world will determine how many routers you pass through and the names of the domains in between (see Figure 1-5).

Tracert might not always work because the computers you are using might be behind a firewall that blocks Internet Control Message Protocol (ICMP) traffic. However, if you enter the command `traceroute www.cisco.com` on the CERNET router you just connected to by Telnet, you see the same results.
WAN Technology Concepts

WANs typically function on Layers 1 and 2 of the OSI model. Layer 1 describes the interface between the DTE and DCE and uses various protocols based on connection speeds. The protocols determine the parameters that devices use to communicate. Layer 2 is concerned with how data is encapsulated before it crosses the WAN. HDLC, PPP, Frame Relay, and ATM are some of the more common data link layer protocols. It is important to remember that a router strips the LAN header from a frame and inserts a WAN header in its place before forwarding the packet across the WAN.

WANs also use several fundamental devices that differ from LANs. These devices are identified based on their location either on the customer or carrier side of the connection. customer premises equipment (CPE) and the data terminal equipment (DTE) are located on the customer side. The data communication equipment (DCE) is located on the carrier’s side of the network. The local loop or subscriber line connects the customer at the demarc to the carrier’s network. A router, CSU/DSU, modem, WAN switch, and access server are typical WAN devices.

Circuit switching such as ISDN is a dedicated circuit that requires call setup and termination. ISDN uses time-division multiplexing (TDM), which allows voice, video, and data to share the available bandwidth, allocating fixed timeslots for each. Packet switching does not require call setup and termination and generally uses leased lines that are always on. Frame Relay and X.25 are examples of packet-switched technologies. An ISP uses virtual circuits to connect multiple locations. These circuits are brought up on demand using Layer 2 identifiers called data link connection identifiers (DLCI).

Review Question

When a packet goes from a LAN to a WAN, the router strips the Layer 2 LAN header from the packet and replaces it with a Layer 2 WAN header. Explain the reason for doing this and how a WAN header differs from a LAN header.

When a packet is sent and destined for a network outside of the LAN, its LAN header has to be stripped and replaced with a WAN header. WAN headers are added in place of LAN headers for various reasons. WAN headers carry WAN encapsulation information for protocols such as HDLC and PPP. They are also used when devices issue a proxy ARP.

WAN Connection Options

A network administrator has many connection options and speeds to choose from when connecting to an ISP. These options include analog dialup, ISDN, cable, DSL, Frame Relay, ATM, and leased lines such as a T1. Speeds can range from a 56-kbps dialup connection to an OC-768 fiber line of up to 39.81312 Gbps. Of course you realize the more bandwidth there is, the more money it will cost. A point-to-point leased line is an option instead of using a shared connection such as Frame Relay. Dedicated leased lines are more expensive, but dedicated output and limiting latency and delay far outweigh the cost. Analog dialup connections still exist; they are located where high-speed connectivity isn’t yet available. Now throw in the cost factor, and analog connections are still a viable option for businesses to transmit small files.

ISDN BRI is twice the speed of dialup (128 kbps) and uses existing phone lines to transmit digital signals. It provides faster call setup and transfer of data than traditional analog dialup. ISDN uses two B channels for data transfer and a separate channel (D channel) for call setup and termination. ISDN PRI uses 23 B channels and provides 1.544 Mbps of throughput (the same as a T1).
Packet-switched connection options include X.25, Frame Relay, and ATM. X.25 operates on Layer 3 and uses switched virtual circuits (SVC) with low-speed connections and extensive error checking. Frame Relay is similar to X.25, but has several differences. It operates at Layer 2 only and uses permanent virtual circuits (PVC), which are identified using DLCIs.

ATM forwards data in fixed-length cells of 53 bytes. It requires 20 percent more bandwidth than Frame Relay and can support connection speeds of up to 622 Mbps (OC-12) and up.

DSL, cable, and wireless are broadband connection options. DSL is an always-on connection that uses existing phone lines to transport data. It provides customers with a dedicated line to the carrier’s switch. Cable connections use coaxial cable from a carrier that provides cable television service. Most cable subscribers can now get their television, Internet, and phone service from their carrier through the same coaxial cable. Each signal is sent through the line using a different frequency.

Wireless technology is becoming more and more common, especially in home networks. Municipal WiFi and WiMax are some of the newer developments in broadband wireless. They are designed to travel longer distances and provide greater bandwidth speeds. Virtual private networks (VPN) enable businesses to create secured tunnels through an unsecure network called the Internet. Benefits of using VPN technology include scalability, cost savings, compatibility with broadband services, and of course, security. Metro Ethernet is a maturing technology that uses multilayer switches. These switches operate at Layers 2 and 3 and have routing capabilities. The connection type is Ethernet or fiber, but the use of a router is not necessary with this type of connection. It can provide faster connection speeds at lower costs through a switch that can route packets much faster than a router.

**Review Questions**

Take a survey of the network of the educational institution that you are currently enrolled in as a student. Ask the instructor or network administrator whether a tour of the school’s main distribution facility (MDF) is possible. If the answer is no, ask whether you could ask the following questions without seeing it:

1. Which devices are used for WAN connectivity?
   
   A CSU/DSU and/or router. In some cases, a modem can be found if DSL or cable is used to connect to the Internet.

2. What type of connection do they use (T1–T3 Frame Relay, and so forth)?
   
   Typical WAN connections can be a T1, T3, ISDN, cable, DSL, and possibly a dialup connection.

3. Do they have offsite campuses, and if yes, how do they connect to them and at what speeds?
   
   Some colleges and high schools have offsite campuses that can be connected by DSL, cable, T1s, and possibly dialup connections. The link speeds can range from 56 kbps up to 10 Mbps.

4. Do they monitor their WAN the same way they monitor their LAN?
   
   Some administrators monitor WAN connection throughput speeds and traffic congestion. This will help the administrator to determine whether more bandwidth is needed.
Chapter Review Vocabulary Exercise: Matching

Match the definition on the right with the correct term on the left.

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Hierarchical Network Model</td>
<td><em>i</em>. Subscriber devices and inside wiring</td>
</tr>
<tr>
<td>b. WAN</td>
<td><em>m</em>. Secure remote connection through the Internet</td>
</tr>
<tr>
<td>c. Distribution layer</td>
<td>____ g. Customer devices that pass the data from a customer network for transmission over the WAN</td>
</tr>
<tr>
<td>d. Leased line</td>
<td>____ p. Permanent, shared, medium-bandwidth connectivity that carries voice and data traffic</td>
</tr>
<tr>
<td>e. Cable modem</td>
<td><em>s</em>. Always-on connection that uses existing phone lines</td>
</tr>
<tr>
<td>f. Demarcation point</td>
<td><em>r</em>. A dedicated circuit between nodes</td>
</tr>
<tr>
<td>g. Data terminal equipment</td>
<td>____ h. Allows the transmission of data across immense geographic remoteness</td>
</tr>
<tr>
<td>h. Campus</td>
<td>____ f. The location in a building that separates the customer’s equipment with the service provider’s equipment</td>
</tr>
<tr>
<td>i. Customer premises equipment</td>
<td>____ d. Preestablished WAN connection</td>
</tr>
<tr>
<td>j. ISDN</td>
<td><em>e</em>. Provides an always-on connection that uses coaxial cable</td>
</tr>
<tr>
<td>k. CSU/DSU</td>
<td>____ a. High-level tool for designing a reliable network infrastructure</td>
</tr>
<tr>
<td>l. Central office</td>
<td>____ k. Terminates the digital signal and ensures connection integrity</td>
</tr>
<tr>
<td>m. Virtual private network (VPN)</td>
<td>____ q. A device that sits between the data terminal equipment and transmission circuit</td>
</tr>
<tr>
<td>n. Multiplexing</td>
<td>____ h. A network that consists of multiple LANs or subnetworks each devoted to a separate department</td>
</tr>
<tr>
<td>o. DLCI</td>
<td>____ c. Aggregates WAN connections at the edge of the campus</td>
</tr>
<tr>
<td>p. Frame Relay</td>
<td>____ t. Routes packets over a shared network</td>
</tr>
<tr>
<td>q. Data communications equipment</td>
<td>____ l. Facility or building where local telephone cables link communication lines through a system of switches and other equipment</td>
</tr>
<tr>
<td>r. Circuit switching</td>
<td>____ o. Identifies a predetermined route for a packet j.</td>
</tr>
<tr>
<td>s. DSL</td>
<td><em>n</em>. A method for sending multiple signals along a single communication path</td>
</tr>
<tr>
<td>t. Packet switching</td>
<td>____ n. A method for sending multiple signals along a single communication path</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction to WANs

Chapter Review Multiple-Choice Questions

Choose the best answer for each of the questions that follow.

1. Which packet-switched connection uses low-capacity speeds but offers error correction?
   - A. Frame Relay
   - B. X.25
   - C. ISDN
   - D. ATM
   - E. PSTN

2. Which of the following are characteristics of the core layer of a hierarchical design? (Choose all that apply.)
   - A. Rapid convergence
   - B. Aggregates WAN connections at the edge of the campus
   - C. High availability
   - D. Connects users
   - E. Connects remote sites
   - F. Fast packet switching

3. Which packet-switched technology use cells that are always a fixed length of 53 bytes?
   - A. Frame Relay
   - B. x.25
   - C. ISDN
   - D. ATM

4. Which of the following describes virtual private networks?
   - A. An encrypted connection between public networks over the Internet
   - B. An encrypted connection between private networks over a public network
   - C. An encrypted connection between public networks over a private network
   - D. An encrypted network between a private network using the Internet

5. Which of the following best describes an SVC?
   - A. Permanently established circuit
   - B. Configured by the service provider
   - C. Decreases bandwidth and increases costs
   - D. Releases the circuit when done which results in reduced costs

6. Which three are WAN physical layer standards?
   - A. EIA/TIA 449
   - B. X.21 male
   - C. X.25 female
   - D. V.35
   - E. IEEE 802.11G
7. What are devices that put data on the local loop called? (Choose all that apply.)
   A. Data circuit-terminating equipment
   B. Data communications equipment
   C. Data connection equipment
   D. Data terminal equipment

8. Which of the following best describes WAN physical layer protocols?
   A. Defines how data is encapsulated
   B. Converts packets into frames
   C. Provides flow control
   D. Provides functional connections to the ISP

9. Which of the following are examples of packet-switched communication links? (Choose all that apply.)
   A. ATM
   B. ISDN
   C. PSTN
   D. X.25
   E. Frame Relay
   F. POTS

10. Which of the following uses two bearer channels and one delta channel for sending data over existing phone lines?
    A. BRI
    B. PRI
    C. PSTN
    D. POTS

11. Which of the following devices converts analog signals to digital signals and vice versa?
    A. Modem
    B. CSU/DSU
    C. Access server
    D. WAN switch
    E. CPE

12. Which of the following authorities define WAN access standards? (Choose all that apply.)
    A. International Organization for Standardization
    B. Internetwork Operating Systems
    C. American Registry for Internet Numbers
    D. Telecommunication Industry Association
    E. Electronic Industries Alliance
    F. Electrical Industries Association
13. Which of the following are benefits of using VPNs? (Choose all that apply)
   A. Eliminates the need for expensive dedicated WAN links
   B. Uses advanced encryption and authentication protocols
   C. Supports DSL and cable
   D. Cost savings using ISDN and PSTN connections
   E. Easy to add new users
   F. Cost savings using PVCs

14. Which of the following are the three major characteristics of WANS?
   A. Use serial connections
   B. Require the services of telephone companies
   C. Connect remote devices that are on the same LAN
   D. Connect devices on remote LANs
   E. Use the Internet rather than a carrier

15. What is another name for the local loop? (Choose two.)
   A. Subscriber line
   B. Demarc
   C. Last mile
   D. Telecommunications carrier signal line

16. The unlicensed radio spectrum is available to anyone who has which two things?
   A. License
   B. Wireless router
   C. Wireless device
   D. Security access code
   E. Permission to access the spectrum

17. Which two things best describe a router’s role in a WAN?
   A. A multiport internetworking device used in carrier networks
   B. Can support multiple telecommunications interfaces
   C. Concentrates dial-in and dial-out user communications
   D. Converts carrier-line frames into frames that the LAN can interpret
   E. Needs a CSU/DSU or modem to connect to the POP

18. Which of the following describe the characteristics of a point-to-point link? (Choose all that apply.)
   A. Provides a preestablished LAN communications path to a remote site
   B. Provides a preestablished WAN communications path to a remote site
   C. Uses leased lines to provide a dedicated connection
   D. Uses leased lines to provide a temporary connection
19. Which layer of the OSI reference model does MPLS reside on?
   A. Layer 1 
   B. Layer 2 
   C. Layer 3 
   D. Between Layers 2 and 3

20. Which of the following fields can be found in LAN and WAN headers? (Choose all that apply.)
   A. Enter 
   B. FCS 
   C. Data 
   D. Flags 
   E. Protocol 
   F. Control
Labs and Activities

Lab 1-1: Challenge Review Lab (1.4.1)

Upon completion of this lab, you will be able to

- Cable a network according to the topology diagram in Figure 1-6.
- Erase the startup configuration and reload a router to the default state.
- Perform basic configuration tasks on a router.
- Configure and activate interfaces.
- Configure Spanning Tree Protocol.
- Configure trunk ports on all switches.
- Configure VTP servers and client.
- Configure VLANs on the switches.
- Configure RIP routing on all the routers.
- Configure OSPF routing on all the routers.
- Configure EIGRP routing on all the routers.

Figure 1-6 shows the network topology for this lab, and Table 1-1 provides the IP addresses, subnet masks, and default gateways (where applicable) for all devices in the topology.

Figure 1-6  Network Topology for Lab 1-1
Table 1-1  Lab 1-1 Addressing Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Default Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Fa0/1</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Fa0/1.10</td>
<td>192.168.10.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Fa0/1.12</td>
<td>10.12.12.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Fa0/1.13</td>
<td>10.13.13.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>S0/0/0</td>
<td>10.1.1.1</td>
<td>255.255.255.252</td>
<td>N/A</td>
</tr>
<tr>
<td>R2</td>
<td>Fa0/1</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Fa0/1.12</td>
<td>10.12.12.2</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Fa0/1.20</td>
<td>192.168.20.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>S0/0/0</td>
<td>10.1.1.2</td>
<td>255.255.255.252</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>S0/0/1</td>
<td>10.2.2.1</td>
<td>255.255.255.252</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Lo0</td>
<td>209.165.200.161</td>
<td>255.255.255.224</td>
<td>N/A</td>
</tr>
<tr>
<td>R3</td>
<td>Fa0/1</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Fa0/1.13</td>
<td>10.13.13.3</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Fa0/1.30</td>
<td>192.168.30.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>S0/0/1</td>
<td>10.2.2.2</td>
<td>255.255.255.252</td>
<td>N/A</td>
</tr>
<tr>
<td>S1</td>
<td>VLAN10</td>
<td>192.168.10.2</td>
<td>255.255.255.0</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>S2</td>
<td>VLAN20</td>
<td>192.168.20.2</td>
<td>255.255.255.0</td>
<td>192.168.20.1</td>
</tr>
<tr>
<td>S3</td>
<td>VLAN30</td>
<td>192.168.30.2</td>
<td>255.255.255.0</td>
<td>192.168.30.1</td>
</tr>
<tr>
<td>PC1</td>
<td>NIC</td>
<td>192.168.10.10</td>
<td>255.255.255.0</td>
<td>192.168.10.1</td>
</tr>
<tr>
<td>PC3</td>
<td>NIC</td>
<td>192.168.30.10</td>
<td>255.255.255.0</td>
<td>192.168.30.1</td>
</tr>
</tbody>
</table>

Scenario

In this lab, you review basic routing and switching concepts. Try to do as much on your own as possible. Refer back to previous material when you cannot proceed on your own.

Note: Configuring three separate routing protocols (RIP, OSPF, and EIGRP) to route the same network is emphatically not a best practice. It should be considered a worst practice and is not something that would be done in a production network. It is done here so that you can review the major routing protocols before proceeding, and so that you can see a dramatic illustration of the concept of administrative distance.

Task 1: Prepare the Network

Step 1.  Cable a network similar to the one in Figure 1-6.

Step 2.  Clear any existing configurations on the routers.
Task 2: Perform Basic Device Configurations

Configure the R1, R2, and R3 routers and the S1, S2, S3 switches according to the following guide-lines:

- Configure the hostname.
- Disable DNS lookup.
- Configure an EXEC mode password.
- Configure a message-of-the-day banner.
- Configure a password for console connections.
- Configure synchronous logging.
- Configure a password for vty connections.

```plaintext
enable
configure terminal
no ip domain-lookup
secret class
banner motd "Unauthorized access strictly prohibited and prosecuted to the full extent of the law"
!
!
line con 0
exec-timeout 0 0
logging synchronous
password cisco login
!
line vty 0 4
password cisco
login
end
```

Task 3: Configure and Activate Serial and Ethernet Addresses

Step 1. Configure interfaces on R1, R2, and R3.

```plaintext
R1
!
interface FastEthernet0/1
no ip address
no shutdown
!
interface FastEthernet0/1.10
encapsulation dot1Q 10
```
ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/1.12
encapsulation dot1Q 12
ip address 10.12.12.1 255.255.255.0
!
interface FastEthernet0/1.13
encapsulation dot1Q 13
ip address 10.13.13.1 255.255.255.0
!
interface Serial0/0/0
ip address 10.1.1.1 255.255.255.252
no shutdown clock
rate 64000
!
R2
!
interface FastEthernet0/1
ip address
no shutdown
!
interface FastEthernet0/1.12
encapsulation dot1Q 12
ip address 10.12.12.2 255.255.255.0
no snmp trap link-status
!
interface FastEthernet0/1.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
no snmp trap link-status
!
interface Serial0/0/0
ip address 10.1.1.2 255.255.255.252
no shutdown
!
interface Serial0/0/1
ip address 10.2.2.1 255.255.255.252
clock rate 64000 no
shutdown
!
interface Loopback 0
ip address 209.165.200.161 255.255.255.224
Step 2. Verify IP addressing and interfaces.

R1# show ip interface brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK? Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet0/0</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>FastEthernet0/1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>FastEthernet0/1.10</td>
<td>192.168.10.1</td>
<td>YES manual</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>FastEthernet0/1.12</td>
<td>10.12.12.1</td>
<td>YES manual</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>FastEthernet0/1.13</td>
<td>10.13.13.1</td>
<td>YES manual</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Serial0/0/0</td>
<td>10.1.1.2</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Serial0/0/1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Serial0/1/0</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Serial0/1/1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
</tbody>
</table>

R2# show ip interface brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK? Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet0/0</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>FastEthernet0/1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>FastEthernet0/1.12</td>
<td>10.12.12.2</td>
<td>YES manual</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>FastEthernet0/1.20</td>
<td>192.168.20.1</td>
<td>YES manual</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Serial0/0/0</td>
<td>10.1.1.2</td>
<td>YES manual</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Serial0/0/1</td>
<td>10.2.2.1</td>
<td>YES manual</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Loopback 0</td>
<td>209.165.200.161</td>
<td>YES manual</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>

R3# show ip interface brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK? Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet0/0</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>FastEthernet0/1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>
Step 3. Configure the Management VLAN interface on S1, S2, and S3.

S1(config)# interface vlan10
S1(config-if)# ip address 192.168.10.2 255.255.255.0

S2(config)# interface vlan20
S2(config-if)# ip address 192.168.20.2 255.255.255.0

S3(config)# interface vlan30
S3(config-if)# ip address 192.168.30.2 255.255.255.0

Step 4. Configure the PC1 and PC3 Ethernet interfaces.

Step 5. Test connectivity between each PC and their default gateway.

Task 4: Configure STP

Step 1. Configure S1 to always be root.

S1(config)# spanning-tree vlan 1-1000 root primary

Step 2. Verify that S1 is root.

S1# show spanning-tree summary
Switch is in pvst mode

Root bridge for: VLAN0001
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled Portfast
BPDU Filter Default is disabled Loopguard
Default is disabled
EtherChannel misconfig guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Configured Pathcost method used is short

<table>
<thead>
<tr>
<th>Name</th>
<th>Blocking</th>
<th>Listening</th>
<th>Learning</th>
<th>Forwarding</th>
<th>STP Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>1 vlans</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>

Task 5: Configure VTP

Step 1. Configure S1 as the VTP server and create a domain name and password.

S1(config)# vtp mode server
Setting device to VTP SERVER mode
Chapter 1: Introduction to WANs

S1(config)# vtp domain cisco
Changing VTP domain name from NULL to cisco
S1(config)# vtp password cisco
Setting device VLAN database password to cisco

**Step 2.** Configure S2 and S3 as VTP clients as assign domain names and passwords.

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

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

**Step 3.** Verify the configuration.

S1# show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255 Number of existing VLANs : 10
VTP Operating Mode : Server
VTP Domain Name : cisco
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x97 0xB7 0xCF 0xD2 0xDD 0x77 0x88 0x34
Configuration last modified by 0.0.0.0 at 3-1-93 00:25:29
Local updater ID is 192.168.10.2 on interface Vl10 (lowest numbered VLAN interface found)
S2# show vtp stat
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255 Number of existing VLANs : 10
VTP Operating Mode : Client
VTP Domain Name : cisco
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xE7 0xD7 0x24 0xC0 0x33 0xD0 0x77 0x88 0x34
Task 6: Configure VLANs

Step 1. Configure S1 with VLANs.

   S1(config)# vlan 10, 12, 13, 20, 30

Step 2. Verify that S2 and S3 received VLAN configurations from S1.

   S1# show vlan brief

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 default</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gi0/1, Gi0/2</td>
</tr>
<tr>
<td>10 VLAN0010</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>12 VLAN0012</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>13 VLAN0013</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>20 VLAN0020</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>30 VLAN0030</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1002 fddi-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1003 token-ring-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1004 fddinet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1005 trnet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
</tbody>
</table>

   S2# show vlan brief
### Table: VLANs and Ports

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 default</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/17, Fa0/18, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gi0/1, Gi0/2</td>
</tr>
<tr>
<td>10 VLAN0010</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>12 VLAN0012</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>13 VLAN0013</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>20 VLAN0020</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>30 VLAN0030</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1002 fddi-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1003 token-ring-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1004 fddinet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1005 trnet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
</tbody>
</table>

S3# show vlan brief

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 default</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/17, Fa0/18, Fa0/21, Fa0/22, Fa0/23, Fa0/24, Gi0/1, Gi0/2</td>
</tr>
<tr>
<td>10 VLAN0010</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>12 VLAN0012</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>13 VLAN0013</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>20 VLAN0020</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>30 VLAN0030</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1002 fddi-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1003 token-ring-default</td>
<td>act/unsup</td>
<td></td>
</tr>
<tr>
<td>1004 fddinet-default</td>
<td>act/unsup</td>
<td></td>
</tr>
</tbody>
</table>
Fa0/13, Fa0/14, Fa0/17, Fa0/18.

Fa0/21, Fa0/22, Fa0/23.

Gi0/1, Gi0/2
**Step 3.** Assign ports to the appropriate VLANs.

**S1:**

```
interface FastEthernet0/1
  switchport trunk allowed vlan 10,12,13
  switchport mode trunk
!
interface FastEthernet0/2
  switchport access vlan 10
  switchport mode access
!
interface GigabitEthernet0/1
  switchport trunk allowed vlan 1,12,20
  switchport mode trunk
!
interface GigabitEthernet0/2
  switchport trunk allowed vlan 1,13,30
  switchport mode trunk
!
```

**S2:**

```
interface FastEthernet0/1
  switchport trunk allowed vlan 12,20
  switchport mode trunk
!
!
interface GigabitEthernet0/1
  switchport trunk allowed vlan 12
  switchport mode trunk
!
```

**S3:**

```
interface FastEthernet0/1
  switchport trunk allowed vlan 13,30
  switchport mode trunk
!
interface FastEthernet0/2
  switchport access vlan 30
  switchport mode access
!
interface GigabitEthernet0/1
  switchport trunk allowed vlan 13
  switchport mode trunk
!
```
Task 7: Configure RIP Routing

Step 1. Configure RIP routing on R1, R2, and R3.

R1
!
router rip
    version 2
    no auto-summary
    network 10.0.0.0
    network 192.168.10.0
!
R2
!
router rip
    version 2
    no auto-summary
    network 10.0.0.0
    network 192.168.20.0
!
R3
!
router rip
    version 2
    no auto-summary
    network 10.0.0.0
    network 192.168.30.0

Step 2. Test connectivity with ping.

R1:
R1# ping 10.1.1.2
Enter escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1# ping 10.2.2.1
Enter escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1# ping 10.2.2.2
Enter escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1# ping 10.12.12.2
Enter escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.12.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1# ping 10.13.13.3
Enter escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.13.13.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1# ping 192.168.10.2
Enter escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1# ping 192.168.10.10
Enter escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1# ping 192.168.20.1
Enter escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1# ping 192.168.20.2
Enter escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1# ping 192.168.30.1
Enter escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5). round-trip min/avg/max = 28/28/28 ms