CCIE Routing and Switching v5.0
Volume 1
Fifth Edition

NARBIK KOCHARIANS, CCIE® No. 12410
PETER PALÚCH, CCIE® No. 23527
CCIE Routing and Switching v5.0 Official Cert Guide, Volume 1
Fifth Edition

Narbik Kocharians, CCIE No. 12410
Peter Palúch, CCIE No. 23527
CCIE Routing and Switching v5.0 Official Cert Guide, Volume 1, Fifth Edition

Narbik Kocharians, CCIE No. 12410
Peter Palúch, CCIE No. 23527

Copyright © 2015 Pearson Education, Inc.

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

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

Printed in the United States of America

Second Printing February 2015

Library of Congress Control Number: 2014944345

Warning and Disclaimer

This book is designed to provide information about Cisco CCIE Routing and Switching Written Exam, No. 400-101. 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 authors and are not necessarily those of Cisco Systems, Inc.
About the Authors

Narbik Kocharians, CCIE No. 12410 (Routing and Switching, Security, SP), is a Triple CCIE with more than 32 years of experience in the IT industry. He has designed, implemented, and supported numerous enterprise networks. Narbik is the president of Micronics Training Inc. (www.micronicstraining.com), where he teaches CCIE R&S and SP boot camps.

Peter Palúch, CCIE No. 23527 (Routing and Switching), is an assistant professor, Cisco Networking Academy instructor, and instructor trainer at the Faculty of Management Science and Informatics, University of Zilina, Slovakia. Peter has cooperated in various educational activities in Slovakia and abroad, focusing on networking and Linux-based network server systems. He is also active at the Cisco Support Community, holding the Cisco Designated VIP award in LAN & WAN Routing and Switching areas since the award program inception in 2011. Upon invitation by Cisco in 2012, Peter joined two Job Task Analysis groups that assisted defining the upcoming CCIE R&S and CCNP R&S certification exam topics. Peter holds an M.Sc. degree in Applied Informatics and a doctoral degree in the area of VoIP quality degradation factors. Together with his students, Peter has started the project of implementing the EIGRP routing protocol into the Quagga open-source routing software suite, and has been driving the effort since its inception in 2013.
About the Technical Reviewers

Paul Negron, CCIE No. 14856, CCSI No. 22752, has been affiliated with networking technologies for 17 years and has been involved with the design of core network services for a number of service providers, such as Comcast, Qwest, British Telecom, and Savvis to name a few. He currently instructs all the CCNP Service Provider–level courses, including Advanced BGP, MPLS, and the QoS course. Paul has six years of experience with satellite communications as well as ten years of experience with Cisco platforms.

Sean Wilkins is an accomplished networking consultant for SR-W Consulting (www.sr-wconsulting.com) and has been in the field of IT since the mid 1990s, working with companies such as Cisco, Lucent, Verizon, and AT&T as well as several other private companies. Sean currently holds certifications with Cisco (CCNP/CCDP), Microsoft (MCSE), and CompTIA (A+ and Network+). He also has a Master of Science in information technology with a focus in network architecture and design, a Master of Science in organizational management, a Master’s Certificate in network security, a Bachelor of Science in computer networking, and Associates of Applied Science in computer information systems. In addition to working as a consultant, Sean spends most of his time as a technical writer and editor for various companies; check out this work at his author website: www.infodispersion.com.
Dedications

From Narbik Kocharians:
I would like to dedicate this book to my wife, Janet, for her love, encouragement, and continuous support, and to my dad for his words of wisdom.

From Peter Palúch:
To my family, students, colleagues, and friends.
Acknowledgments

From Narbik Kocharians:

First, I would like to thank God for giving me the opportunity and ability to write, teach, and do what I truly enjoy doing. Also, I would like to thank my family, especially my wife of 29 years, Janet, for her constant encouragement and help. She does such an amazing job of interacting with students and handling all the logistics of organizing classes as I focus on teaching. I also would like to thank my children, Chris, Patrick, Alexandra, and my little one, Daniel, for their patience.

A special thanks goes to Mr. Brett Bartow for his patience and our constant changing of the deadlines. It goes without saying that the technical editors and reviewers did a phenomenal job; thank you very much. Finally, I would like to thank all my students who inspire me every day, and you, for reading this book.

From Peter Palúch:

The opportunity to cooperate on the new edition of this book has been an honor and privilege beyond words for me. Wendell Odom, who has so gracefully and generously passed the torch to us, was the key person in introducing me to the Cisco Press representatives as a possible author, and I will be forever indebted to him for all the trust he has blessed us with. I have strived very much to live up to the unparalleled high level of content all previous authors have maintained throughout all editions of this book, and I would like to sincerely thank all of them for authoring such a great book that has significantly helped me achieve my certification in the first place.

My next immense thank you goes to Brett Bartow, the executive editor for this book. Brett's inviting and forthcoming attitude throughout the time of editing the book, compounded with his patience and understanding for my ever-moving (and constantly missed) deadlines, is second to none. He has done all in his power to help us, the authors, without compromising the quality of the work.

I would not have been able to complete my work on this volume without the endless support of my family. They have encouraged me, supported me, and gone out of their way to accommodate my needs. Words are not enough to express my gratitude.

Psalm 127, whose musical setting in works of Monteverdi, Handel, or Vivaldi I have come to admire, begins with words “Unless the Lord build the house, they labor in vain who build.” Indeed, if it was not first and foremost the Lord's blessing and help throughout, this work would not have been finished successfully. To my Lord and Savior, Jesus Christ—thank you!
Contents at a Glance

Introduction xxiv

Part I LAN Switching
Chapter 1 Ethernet Basics 3
Chapter 2 Virtual LANs and VLAN Trunking 47
Chapter 3 Spanning Tree Protocol 103

Part II IP Networking
Chapter 4 IP Addressing 183
Chapter 5 IP Services 227

Part III IP IGP Routing
Chapter 6 IP Forwarding (Routing) 267
Chapter 7 RIPv2 and RIPng 313
Chapter 8 EIGRP 347
Chapter 9 OSPF 453
Chapter 10 IS-IS 563
Chapter 11 IGP Route Redistribution, Route Summarization, Default Routing, and Troubleshooting 633

Part IV Final Preparation
Chapter 12 Final Preparation 701

Part V Appendixes
Appendix A Answers to the “Do I Know This Already?” Quizzes 707
Appendix B CCIE Exam Updates 713

CD-Only
Appendix C Decimal to Binary Conversion Table
Appendix D IP Addressing Practice
Appendix E Key Tables for CCIE Study
Appendix F Solutions for Key Tables for CCIE Study
Appendix G Study Planner

Glossary
Contents

Introduction xxiv

Part I LAN Switching

Chapter 1 Ethernet Basics 3

“Do I Know This Already?” Quiz 3

Foundation Topics 8

Ethernet Layer 1: Wiring, Speed, and Duplex 8

RJ-45 Pinouts and Category 5 Wiring 8

Autonegotiation, Speed, and Duplex 9

CSMA/CD 10

Collision Domains and Switch Buffering 10

Basic Switch Port Configuration 11

Ethernet Layer 2: Framing and Addressing 14

Types of Ethernet Addresses 16

Ethernet Address Formats 17

Protocol Types and the 802.3 Length Field 18

Switching and Bridging Logic 19

SPAN, RSPAN, and ERSPAN 22

Core Concepts of SPAN, RSPAN, and ERSPAN 23

Restrictions and Conditions 24

Basic SPAN Configuration 26

Complex SPAN Configuration 26

RSPAN Configuration 26

ERSPAN Configuration 27

Virtual Switch System 28

Virtual Switching System 29

VSS Active and VSS Standby Switch 30

Virtual Switch Link 30

Multichassis EtherChannel (MEC) 31

Basic VSS Configuration 31

VSS Verification Procedures 35

IOS-XE 38

Foundation Summary 41
Chapter 3 Spanning Tree Protocol 103

“Do I Know This Already?” Quiz 103

Foundation Topics 107

802.1D Spanning Tree Protocol and Improvements 107

Choosing Which Ports Forward: Choosing Root Ports and Designated Ports 109

Electing a Root Switch 110

Determining the Root Port 111

Determining the Designated Port 113

Converging to a New STP Topology 115

Topology Change Notification and Updating the CAM 117

Transitioning from Blocking to Forwarding 119

Per-VLAN Spanning Tree and STP over Trunks 119

STP Configuration and Analysis 124

Rapid Spanning Tree Protocol 128

New Port Roles, States and Types, and New Link Types 128

Changes to BPDU Format and Handling 132

Proposal/Agreement Process in RSTP 133

Topology Change Handling in RSTP 136

Rapid Per-VLAN Spanning Tree Plus (RPVST+) 137

Multiple Spanning Trees: IEEE 802.1s 137

MST Principles of Operation 138

Interoperability Between MST and Other STP Versions 141

MST Configuration 144

Protecting and Optimizing STP 148

PortFast Ports 148

Root Guard, BPDU Guard, and BPDU Filter: Protecting Access Ports 149

Protecting Against Unidirectional Link Issues 151

Configuring and Troubleshooting EtherChannels 154

Load Balancing Across Port-Channels 154

Port-Channel Discovery and Configuration 157

Troubleshooting Complex Layer 2 Issues 161

Layer 2 Troubleshooting Process 162

Layer 2 Protocol Troubleshooting and Commands 163

Troubleshooting Using Cisco Discovery Protocol 163

Troubleshooting Using Link Layer Discovery Protocol 165

Troubleshooting Using Basic Interface Statistics 167
Troubleshooting Spanning Tree Protocol 170
Troubleshooting Trunking 171
Troubleshooting VTP 172
Troubleshooting EtherChannels 174
Approaches to Resolving Layer 2 Issues 175
Foundation Summary 177
Memory Builders 179
Fill in Key Tables from Memory 179
Definitions 179
Further Reading 179

Part II  IP Networking

Chapter 4 IP Addressing 183
“Do I Know This Already?” Quiz 183
Foundation Topics 187
IP Operation 187
TCP Operation 187
UDP Operation 188
IP Addressing and Subnetting 188
IP Addressing and Subnetting Review 188
Subnetting a Classful Network Number 189
Comments on Classless Addressing 191
Subnetting Math 192
Dissecting the Component Parts of an IP Address 192
Finding Subnet Numbers and Valid Range of IP Addresses—
  Binary 193
Decimal Shortcuts to Find the Subnet Number and Valid Range of IP
  Addresses 194
Determining All Subnets of a Network—Binary 196
Determining All Subnets of a Network—Decimal 198
VLSM Subnet Allocation 200
Route Summarization Concepts 201
Finding Inclusive Summary Routes—Binary 202
Finding Inclusive Summary Routes—Decimal 203
Finding Exclusive Summary Routes—Binary 204
CIDR, Private Addresses, and NAT 205
  Classless Interdomain Routing 206
  Private Addressing 207
Network Address Translation 207
Static NAT 209
Dynamic NAT Without PAT 210
Overloading NAT with Port Address Translation 211
Dynamic NAT and PAT Configuration 212
IPv6 214
IPv6 Address Format 215
Network Prefix 215
IPv6 Address Types 216
Address Management and Assignment 216
Static Configuration 217
Stateless Address Autoconfiguration 217
Stateful DHCPv6 217
Stateless DHCP 218
IPv6 Transition Technologies 218
Dual Stack 218
Tunneling 219
Translation 220
Foundation Summary 221
Memory Builders 225
Fill in Key Tables from Memory 225
Definitions 225
Further Reading 225

Chapter 5  IP Services 227
“Do I Know This Already?” Quiz 227
Foundation Topics 232
ARP, Proxy ARP, Reverse ARP, BOOTP, and DHCP 232
ARP and Proxy ARP 232
RARP, BOOTP, and DHCP 233
DHCP 234
HSRP, VRRP, and GLBP 236
Network Time Protocol 240
SNMP 241
SNMP Protocol Messages 243
SNMP MIBs 244
SNMP Security 245
Syslog 245
Web Cache Communication Protocol 246
   Implementing the Cisco IOS IP Service Level Agreement (IP SLA) Feature 249
   Implementing NetFlow 250
   Implementing Router IP Traffic Export 252
   Implementing Cisco IOS Embedded Event Manager 253
   Implementing Remote Monitoring 254
   Implementing and Using FTP on a Router 255
   Implementing a TFTP Server on a Router 256
   Implementing Secure Copy Protocol 257
   Implementing HTTP and HTTPS Access 257
   Implementing Telnet Access 258
   Implementing SSH Access 258
Foundation Summary 259
Memory Builders 264
   Fill In Key Tables from Memory 264
   Definitions 264
   Further Reading 264

Part III  IP IGP Routing

Chapter 6  IP Forwarding (Routing) 267
   “Do I Know This Already?” Quiz 267
   Foundation Topics 271
   IP Forwarding 271
      Process Switching, Fast Switching, and Cisco Express Forwarding 272
      Load Sharing with CEF and Related Issues 282
   Multilayer Switching 286
      MLS Logic 286
      Using Routed Ports and Port-channels with MLS 287
      MLS Configuration 291
   Policy Routing 296
   Routing Protocol Changes and Migration 299
      Planning the Migration Strategy 300
      Activating New IGP While Keeping the Current IGP Intact 300
      Verifying New IGP Adjacencies and Working Database Contents 301
      Deactivating Current IGP 301
      Removing New IGP’s Temporary Settings 303
      Specifics of Distance-Vector Protocols in IGP Migration 303
Chapter 7  RIPv2 and RIPng  313
“Do I Know This Already?” Quiz  313
Foundation Topics  316
Introduction to Dynamic Routing  316
RIPv2 Basics  318
RIPv2 Convergence and Loop Prevention  320
  Converged Steady-State Operation  327
  Triggered (Flash) Updates and Poisoned Routes  328
  RIPv2 Convergence When Routing Updates Cease  331
  Convergence Extras  334
RIPv2 Configuration  334
  Enabling RIPv2 and the Effects of Autosummarization  335
  RIPv2 Authentication  337
  RIPv2 Next-Hop Feature and Split Horizon  338
  RIPv2 Offset Lists  338
  Route Filtering with Distribute Lists and Prefix Lists  338
RIPng for IPv6  339
Foundation Summary  342
Memory Builders  345
  Definitions  345
  Further Reading  345

Chapter 8  EIGRP  347
“Do I Know This Already?” Quiz  347
Foundation Topics  356
EIGRP Basics and Evolution  356
  EIGRP Roots: Interior Gateway Routing Protocol  357
  Moving from IGRP to Enhanced IGRP  358
EIGRP Metrics, Packets, and Adjacencies  360
  EIGRP Classic Metrics  360
  Bandwidth Metric Component  361
  Delay Metric Component  361
Chapter 9  **OSPF**  453

“Do I Know This Already?” Quiz  453

Foundation Topics  460

OSPF Database Exchange  460
  OSPF Router IDs  460
  Becoming Neighbors, Exchanging Databases, and Becoming Adjacent  461
  **OSPF Neighbor States**  462
  **Becoming Neighbors: The Hello Process**  464
  Transmitting LSA Headers to Neighbors  466
  **Database Description Exchange: Master/Slave Relationship**  466
  Requesting, Getting, and Acknowledging LSAs  468
  Designated Routers on LANs  469
  **Designated Router Optimization on LANs**  470
  **DR Election on LANs**  471
  Designated Routers on WANs and OSPF Network Types  472
  **Caveats Regarding OSPF Network Types over NBMA Networks**  474
  Example of OSPF Network Types and NBMA  474
  SPF Calculation  479
  Steady-State Operation  480

OSPF Design and LSAs  480
  OSPF Design Terms  480
  OSPF Path Selection Process  482
  LSA Types  482
  **LSA Types 1 and 2**  484
  **LSA Type 3 and Inter-Area Costs**  488
Chapter 10  IS-IS  563

“Do I Know This Already?” Quiz  563
Foundation Topics  571
OSI Network Layer and Addressing  572
Levels of Routing in OSI Networks  576
IS-IS Metrics, Levels, and Adjacencies  577
IS-IS Packet Types  579
  Hello Packets  579
  Link State PDUs  580
  Complete and Partial Sequence Numbers PDUs  585
IS-IS Operation over Different Network Types  586
  IS-IS Operation over Point-to-Point Links  587
  IS-IS Operation over Broadcast Links  592
Areas in IS-IS  598
Authentication in IS-IS  608
IPv6 Support in IS-IS  610
Configuring IS-IS  613
Foundation Summary  625
Memory Builders  629
  Fill In Key Tables from Memory  630
  Definitions  630
  Further Reading  630

Chapter 11  IGP Route Redistribution, Route Summarization, Default Routing, and Troubleshooting  633

“Do I Know This Already?” Quiz  633
Foundation Topics  638
Route Maps, Prefix Lists, and Administrative Distance  638
  Configuring Route Maps with the route-map Command  638
  Route Map match Commands for Route Redistribution  640
  Route Map set Commands for Route Redistribution  641
IP Prefix Lists  641
Administrative Distance  644
Icons Used in This Book

Communication Server
PC
PC with Software
Sun Workstation
Macintosh
Branch Office
Headquarters
Terminal
File Server
Web Server
Cisco Works Workstation
House, Regular
Printer
Laptop
IBM Mainframe
Label Switch Router
Cluster Controller
Gateway
Router
Bridge
Hub
ATM router
Cisco MDS 9500
Catalyst Switch
Multilayer Switch
ATM Switch
Route/Switch Processor
LAN2LAN Switch
Cisco MDS 9500
Optical Services Router
Enterprise Fibre Channel disk
Fibre Channel JBOD
ONS 15540
Network Cloud
Line: Ethernet
Line: Serial
Line: Switched Serial
Command Syntax Conventions

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

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

The Cisco Certified Internetwork Expert (CCIE) certification might be the most challenging and prestigious of all networking certifications. It has received numerous awards and certainly has built a reputation as one of the most difficult certifications to earn in all of the technology world. Having a CCIE certification opens doors professionally and typically results in higher pay and looks great on a resume.

Cisco currently offers several CCIE certifications. This book covers the version 5.0 exam blueprint topics of the written exam for the CCIE Routing and Switching certification. The following list details the currently available CCIE certifications at the time of this book’s publication; check www.cisco.com/go/ccie for the latest information. The certifications are listed in the order in which they appear on the web page:

- CCDE
- CCIE Collaboration
- CCIE Data Center
- CCIE Routing & Switching
- CCIE Security
- CCIE Service Provider
- CCIE Service Provider Operations
- CCIE Wireless

Each of the CCDE and CCIE certifications requires the candidate to pass both a written exam and a one-day, hands-on lab exam. The written exam is intended to test your knowledge of theory, protocols, and configuration concepts that follow good design practices. The lab exam proves that you can configure and troubleshoot actual gear.

Why Should I Take the CCIE Routing and Switching Written Exam?

The first and most obvious reason to take the CCIE Routing and Switching written exam is that it is the first step toward obtaining the CCIE Routing and Switching certification. Also, you cannot schedule a CCIE lab exam until you pass the corresponding written exam. In short, if you want all the professional benefits of a CCIE Routing and Switching certification, you start by passing the written exam.

The benefits of getting a CCIE certification are varied and include the following:

- Better pay
- Career-advancement opportunities
Applies to certain minimum requirements for Cisco Silver and Gold Channel Partners, as well as those seeking Master Specialization, making you more valuable to Channel Partners

- Better movement through the problem-resolution process when calling the Cisco TAC
- Prestige
- Credibility for consultants and customer engineers, including the use of the Cisco CCIE logo

The other big reason to take the CCIE Routing and Switching written exam is that it recertifies an individual’s associate-, professional-, and expert-level Cisco certifications, regardless of his or her technology track. Recertification requirements do change, so please verify the requirements at www.cisco.com/go/certifications.

CCIE Routing and Switching Written Exam 400-101

The CCIE Routing and Switching written exam, at the time of this writing, consists of a two-hour exam administered at a proctored exam facility affiliated with Pearson VUE (www.vue.com/cisco). The exam typically includes approximately 100 multiple-choice questions. No simulation questions are currently part of the written exam.

As with most exams, everyone wants to know what is on the exam. Cisco provides general guidance as to topics on the exam in the CCIE Routing and Switching written exam blueprint, the most recent copy of which can be accessed from www.cisco.com/go/ccie.

Cisco changes both the CCIE written and lab blueprints over time, but Cisco seldom, if ever, changes the exam numbers. However, exactly this change occurred when the CCIE Routing and Switching blueprint was refreshed for v5.0. The previous written exam for v4.0 was numbered 350-001; the v5.0 written exam is identified by 400-101.

Table I-1 lists the CCIE Routing and Switching written exam blueprint 5.0 at press time. Table I-1 also lists the chapters that cover each topic.

<table>
<thead>
<tr>
<th>Topics</th>
<th>Book Volume</th>
<th>Book Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Network Principles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1 Network theory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1a Describe basic software architecture differences between IOS and IOS XE</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1.1a (i) Control plane and Forwarding plane</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1.1a (ii) Impact on troubleshooting and performance</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1.1a (iii) Excluding a specific platform’s architecture</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Topics | Book Volume | Book Chapter
--- | --- | ---
1.1.b Identify Cisco Express Forwarding concepts
1.1.b (i) RIB, FIB, LFIB, Adjacency table | 1 | 6
1.1.b (ii) Load-balancing hash | 1 | 6
1.1.b (iii) Polarization concept and avoidance | 1 | 6
1.1.c Explain general network challenges
1.1.c (i) Unicast flooding | 1 | 4
1.1.c (ii) Out-of-order packets | 1 | 4
1.1.c (iii) Asymmetric routing | 1 | 4
1.1.c (iv) Impact of micro burst | 1 | 4
1.1.d Explain IP operations
1.1.d (i) ICMP unreachable, redirect | 1 | 4
1.1.d (ii) IPv4 options, IPv6 extension headers | 1 | 4
1.1.d (iii) IPv4 and IPv6 fragmentation | 1 | 4
1.1.d (iv) TTL | 1 | 4
1.1.d (v) IP MTU | 1 | 4
1.1.e Explain TCP operations
1.1.e (i) IPv4 and IPv6 PMTU | 1 | 4
1.1.e (ii) MSS | 1 | 4
1.1.e (iii) Latency | 1 | 4
1.1.e (iv) Windowing | 1 | 4
1.1.e (v) Bandwidth delay product | 1 | 4
1.1.e (vi) Global synchronization | 1 | 4
1.1.e (vii) Options | 1 | 4
1.1.f Explain UDP operations
1.1.f (i) Starvation | 1 | 4
1.1.f (ii) Latency | 1 | 4
1.1.f (iii) RTP/RTCP concepts | 1 | 4
1.2 Network implementation and operation
1.2.a Evaluate proposed changes to a network
1.2.a (i) Changes to routing protocol parameters | 1 | 7–10
1.2.a (ii) Migrate parts of a network to IPv6 | 1 | 4
<table>
<thead>
<tr>
<th>Topics</th>
<th>Book Volume</th>
<th>Book Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.a (iii) Routing protocol migration</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>1.2.a (iv) Adding multicast support</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>1.2.a (v) Migrate Spanning Tree Protocol</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>1.2.a (vi) Evaluate impact of new traffic on existing QoS design</td>
<td>2</td>
<td>3, 4, 5</td>
</tr>
<tr>
<td><strong>1.3 Network troubleshooting</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3.a Use IOS troubleshooting tools</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3.a (i) debug, conditional debug</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.3.a (ii) ping, traceroute with extended options</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.3.a (iii) Embedded packet capture</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>1.3.a (iv) Performance monitor</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>1.3.b Apply troubleshooting methodologies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3.b (i) Diagnose the root cause of networking issues (analyze symptoms, identify and describe root cause)</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>1.3.b (ii) Design and implement valid solutions according to constraints</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>1.3.b (iii) Verify and monitor resolution</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>1.3.c Interpret packet capture</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3.c (i) Using Wireshark trace analyzer</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>1.3.c (ii) Using IOS embedded packet capture</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td><strong>2.0 Layer 2 Technologies</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1 LAN switching technologies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.a Implement and troubleshoot switch administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.a (i) Managing the MAC address table</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2.1.a (ii) erdisable recovery</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2.1.a (iii) L2 MTU</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2.1.b Implement and troubleshoot Layer 2 protocols</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.b (i) CDP, LLDP</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2.1.b (ii) UDLD</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2.1.c Implement and troubleshoot VLAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.c (i) Access ports</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2.1.c (ii) VLAN database</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2.1.c (iii) Normal, extended VLAN, voice VLAN</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Topics</td>
<td>Book Volume</td>
<td>Book Chapter</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>2.1.d Implement and troubleshoot trunking</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.d (i) VTPv1, VTPv2, VTPv3, VTP pruning</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2.1.d (ii) dot1Q</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2.1.d (iii) Native VLAN</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2.1.d (iv) Manual pruning</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2.1.e Implement and troubleshoot EtherChannel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.e (i) LACP, PAgP, manual</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2.1.e (ii) Layer 2, Layer 3</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2.1.e (iii) Load balancing</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2.1.e (iv) EtherChannel misconfiguration guard</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2.1.f Implement and troubleshoot spanning tree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.f (i) PVST+/RPVST+/MST</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2.1.f (ii) Switch priority, port priority, path cost, STP timers</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2.1.f (iii) PortFast, BPDU Guard, BPDU Filter</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2.1.f (iv) Loop Guard, Root Guard</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2.1.g Implement and troubleshoot other LAN switching technologies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.g (i) SPAN, RSPAN, ERSpan</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2.1.h Describe chassis virtualization and aggregation technologies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.h (i) Multichassis</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2.1.h (ii) VSS concepts</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2.1.h (iii) Alternatives to STP</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2.1.h (iv) Stackwise</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2.1.h (v) Excluding specific platform implementation</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2.1.i Describe spanning-tree concepts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.i (i) Compatibility between MST and RSTP</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2.1.i (ii) STP dispute, STP Bridge Assurance</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2.2 Layer 2 multicast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.a Implement and troubleshoot IGMP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.a (i) IGMPv1, IGMPv2, IGMPv3</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>2.2.a (ii) IGMP snooping</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>2.2.a (iii) IGMP querier</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Topics</td>
<td>Book Volume</td>
<td>Book Chapter</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>2.2.a (iv) IGMP filter</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>2.2.a (v) IGMP proxy</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>2.2.b Explain MLD</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>2.2.c Explain PIM snooping</td>
<td>2</td>
<td>8</td>
</tr>
</tbody>
</table>

### 2.3 Layer 2 WAN circuit technologies

<table>
<thead>
<tr>
<th>Topics</th>
<th>Book Volume</th>
<th>Book Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3.a Implement and troubleshoot HDLC</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>2.3.b Implement and troubleshoot PPP</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>2.3.b (i) Authentication (PAP, CHAP)</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>2.3.b (ii) PPPoE</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>2.3.b (iii) MLPPP</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>2.3.c Describe WAN rate-based Ethernet circuits</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>2.3.c (i) Metro and WAN Ethernet topologies</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>2.3.c (ii) Use of rate-limited WAN Ethernet services</td>
<td>2</td>
<td>6</td>
</tr>
</tbody>
</table>

### 3.0 Layer 3 Technologies

#### 3.1 Addressing technologies

<table>
<thead>
<tr>
<th>Topics</th>
<th>Book Volume</th>
<th>Book Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.a Identify, implement, and troubleshoot IPv4 addressing and subnetting</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>3.1.a (i) Address types, VLSM</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>3.1.a (ii) ARP</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>3.1.b Identify, implement, and troubleshoot IPv6 addressing and subnetting</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>3.1.b (i) Unicast, multicast</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>3.1.b (ii) EUI-64</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>3.1.b (iii) ND, RS/RA</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>3.1.b (iv) Autoconfig/SLAAC, temporary addresses (RFC 4941)</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>3.1.b (v) Global prefix configuration feature</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>3.1.b (vi) DHCP protocol operations</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>3.1.b (vii) SLAAC/DHCPv6 interaction</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>3.1.b (viii) Stateful, stateless DHCPv6</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>3.1.b (ix) DHCPv6 prefix delegation</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

#### 3.2 Layer 3 multicast

<table>
<thead>
<tr>
<th>Topics</th>
<th>Book Volume</th>
<th>Book Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.a Troubleshoot reverse path forwarding</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>Topics</td>
<td>Book Volume</td>
<td>Book Chapter</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>3.2.a (i) RPF failure</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3.2.a (ii) RPF failure with tunnel interface</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3.2.b Implement and troubleshoot IPv4 protocol independent multicast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2.b (i) PIM dense mode, sparse mode, sparse-dense mode</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3.2.b (ii) Static RP, auto-RP, BSR</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3.2.b (iii) Bidirectional PIM</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3.2.b (iv) Source-specific multicast</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3.2.b (v) Group-to-RP mapping</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3.2.b (vi) Multicast boundary</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3.2.c Implement and troubleshoot multicast source discovery protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2.c (i) Intra-domain MSDP (anycast RP)</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3.2.c (ii) SA filter</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3.2.d Describe IPv6 multicast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2.d (i) IPv6 multicast addresses</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>3.2.d (ii) PIMv6</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>3.3 Fundamental routing concepts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3.a Implement and troubleshoot static routing</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>3.3.b Implement and troubleshoot default routing</td>
<td>1</td>
<td>7–11</td>
</tr>
<tr>
<td>3.3.c Compare routing protocol types</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3.c (i) Distance vector</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>3.3.c (ii) Link state</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>3.3.c (iii) Path vector</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>3.3.d Implement, optimize, and troubleshoot administrative distance</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>3.3.e Implement and troubleshoot passive interface</td>
<td>1</td>
<td>7–10</td>
</tr>
<tr>
<td>3.3.f Implement and troubleshoot VRF lite</td>
<td>2</td>
<td>11</td>
</tr>
<tr>
<td>3.3.g Implement, optimize, and troubleshoot filtering with any routing protocol</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>3.3.h Implement, optimize, and troubleshoot redistribution between any routing protocols</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>3.3.i Implement, optimize, and troubleshoot manual and auto summarization with any routing protocol</td>
<td>1</td>
<td>7–10</td>
</tr>
<tr>
<td>Topics</td>
<td>Book Volume</td>
<td>Book Chapter</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>3.3.j Implement, optimize, and troubleshoot policy-based routing</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>3.3.k Identify and troubleshoot suboptimal routing</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>3.3.l Implement and troubleshoot bidirectional forwarding detection</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>3.3.m Implement and troubleshoot loop prevention mechanisms</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3.m (i) Route tagging, filtering</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>3.3.m (ii) Split horizon</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>3.3.m (iii) Route poisoning</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>3.3.n Implement and troubleshoot routing protocol authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3.n (i) MD5</td>
<td>1</td>
<td>7–10</td>
</tr>
<tr>
<td>3.3.n (ii) Key-chain</td>
<td></td>
<td>7–10</td>
</tr>
<tr>
<td>3.3.n (iii) EIGRP HMAC SHA2-256bit</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.3.n (iv) OSPFv2 SHA1-192bit</td>
<td></td>
<td>9</td>
</tr>
<tr>
<td>3.3.n (v) OSPFv3 IPsec authentication</td>
<td></td>
<td>9</td>
</tr>
<tr>
<td>3.4 RIP (v2 and v6)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.4.a Implement and troubleshoot RIPv2</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>3.4.b Describe RIPv6 (RIPng)</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>3.5 EIGRP (for IPv4 and IPv6)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5.a Describe packet types</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5.a (i) Packet types (hello, query, update, and so on)</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.a (ii) Route types (internal, external)</td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>3.5.b Implement and troubleshoot neighbor relationship</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5.b (i) Multicast, unicast EIGRP peering</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.b (ii) OTP point-to-point peering</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.b (iii) OTP route-reflector peering</td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>3.5.b (iv) OTP multiple service providers scenario</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.c Implement and troubleshoot loop-free path selection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5.c (i) RD, FD, FC, successor, feasible successor</td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>3.5.c (ii) Classic metric</td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>3.5.c (iii) Wide metric</td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>3.5.d Implement and troubleshoot operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5.d (i) General operations</td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>Topics</td>
<td>Book Volume</td>
<td>Book Chapter</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>3.5.d (ii) Topology table, update, query, active, passive</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.d (iii) Stuck in active</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.d (iv) Graceful shutdown</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.e Implement and troubleshoot EIGRP stub</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5.e (i) Stub</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.e (ii) Leak-map</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.f Implement and troubleshoot load balancing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5.f (i) equal-cost</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.f (ii) unequal-cost</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.f (iii) add-path</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.g Implement EIGRP (multiaddress) named mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5.g (i) Types of families</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.g (ii) IPv4 address-family</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.g (iii) IPv6 address-family</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.h Implement, troubleshoot, and optimize EIGRP convergence and scalability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5.h (i) Describe fast convergence requirements</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.h (ii) Control query boundaries</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.h (iii) IP FRR/fast reroute (single hop)</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.h (iv) Summary leak-map</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.h (v) Summary metric</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.6 OSPF (v2 and v3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.6.a Describe packet types</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.6.a (i) LSA types (1, 2, 3, 4, 5, 7, 9)</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.a (ii) Route types (N1, N2, E1, E2)</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.b Implement and troubleshoot neighbor relationship</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.c Implement and troubleshoot OSPFv3 address-family support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.6.c (i) IPv4 address-family</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.c (ii) IPv6 address-family</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.d Implement and troubleshoot network types, area types, and router types</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.6.d (i) Point-to-point, multipoint, broadcast, nonbroadcast</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>Topics</td>
<td>Book Volume</td>
<td>Book Chapter</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>3.6.d (ii) LSA types, area type: backbone, normal, transit, stub, NSSA, totally stub</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.d (iii) Internal router, ABR, ASBR</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.d (iv) Virtual link</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.e Implement and troubleshoot path preference</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.f Implement and troubleshoot operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.6.f (i) General operations</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.f (ii) Graceful shutdown</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.f (iii) GTSM (Generic TTL Security Mechanism)</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.g Implement, troubleshoot, and optimize OSPF convergence and scalability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.6.g (i) Metrics</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.g (ii) LSA throttling, SPF tuning, fast hello</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.g (iii) LSA propagation control (area types, ISPF)</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.g (iv) IP FRR/fast reroute (single hop)</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.g (v) LFA/loop-free alternative (multihop)</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.6.g (vi) OSPFv3 prefix suppression</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.7 BGP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.7.a Describe, implement, and troubleshoot peer relationships</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.7.a (i) Peer-group, template</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3.7.a (ii) Active, passive</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3.7.a (iii) States, timers</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3.7.a (iv) Dynamic neighbors</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3.7.b Implement and troubleshoot IBGP and EBGP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.7.b (i) EBGP, IBGP</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3.7.b (ii) 4-byte AS number</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3.7.b (iii) Private AS</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3.7.c Explain attributes and best-path selection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.7.d Implement, optimize, and troubleshoot routing policies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.7.d (i) Attribute manipulation</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.d (ii) Conditional advertisement</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.d (iii) Outbound route filtering</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Topics</td>
<td>Book Volume</td>
<td>Book Chapter</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>3.7.d (iv) Communities, extended communities</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.d (v) Multihoming</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.e Implement and troubleshoot scalability</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.e (i) Route-reflector, cluster</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.e (ii) Confederations</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.e (iii) Aggregation, AS set</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.f Implement and troubleshoot multiprotocol BGP</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7f (i) IPv4, IPv6, VPN address-family</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.g Implement and troubleshoot AS path manipulations</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.g (i) Local AS, allow AS in, remove private AS</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.g (ii) Prepend</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.g (iii) Regexp</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.h Implement and troubleshoot other features</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.h (i) Multipath</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.h (ii) BGP synchronization</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.h (iii) Soft reconfiguration, route refresh</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.i Describe BGP fast convergence features</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.i (i) Prefix independent convergence</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.i (ii) Add-path</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7.i (iii) Next-hop address tracking</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.8 IS-IS (for IPv4 and IPv6)</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>3.8.a Describe basic IS-IS network</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>3.8.a (i) Single area, single topology</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>3.8.b Describe neighbor relationship</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>3.8.c Describe network types, levels, and router types</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>3.8.c (i) NSAP addressing</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>3.8.c (ii) Point-to-point, broadcast</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>3.8.d Describe operations</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>3.8.e Describe optimization features</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>3.8.e (i) Metrics, wide metric</td>
<td>1</td>
<td>10</td>
</tr>
</tbody>
</table>

4.0 VPN Technologies
<table>
<thead>
<tr>
<th>Topics</th>
<th>Book Volume</th>
<th>Book Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 Tunneling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.a Implement and troubleshoot MPLS operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.a (i) Label stack, LSR, LSP</td>
<td>2</td>
<td>11</td>
</tr>
<tr>
<td>4.1.a (ii) LDP</td>
<td>2</td>
<td>11</td>
</tr>
<tr>
<td>4.1.a (iii) MPLS ping, MPLS traceroute</td>
<td>2</td>
<td>11</td>
</tr>
<tr>
<td>4.1.b Implement and troubleshoot basic MPLS L3VPN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.b (i) L3VPN, CE, PE, P</td>
<td>2</td>
<td>11</td>
</tr>
<tr>
<td>4.1.b (ii) Extranet (route leaking)</td>
<td>2</td>
<td>11</td>
</tr>
<tr>
<td>4.1.c Implement and troubleshoot encapsulation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.c (i) GRE</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>4.1.c (ii) Dynamic GRE</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>4.1.c (iii) LISP encapsulation principles supporting EIGRP OTP</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>4.1.d Implement and troubleshoot DMVPN (single hub)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.d (i) NHRP</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>4.1.d (ii) DMVPN with IPsec using preshared key</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>4.1.d (iii) QoS profile</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>4.1.d (iv) Pre-classify</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>4.1.e Describe IPv6 tunneling techniques</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.e (i) 6in4, 6to4</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>4.1.e (ii) ISATAP</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>4.1.e (iii) 6RD</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>4.1.e (iv) 6PE/6VPE</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>4.1.g Describe basic Layer 2 VPN—wireline</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.g (i) L2TPv3 general principles</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>4.1.g (ii) ATOM general principles</td>
<td>2</td>
<td>11</td>
</tr>
<tr>
<td>4.1.h Describe basic L2VPN—LAN services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1.h (i) MPLS-VPLS general principles</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>4.1.h (ii) OTV general principles</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>4.2 Encryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.2.a Implement and troubleshoot IPsec with preshared key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.2.a (i) IPv4 site to IPv4 site</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>Topics</td>
<td>Book Volume</td>
<td>Book Chapter</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>4.2.a (ii) IPv6 in IPv4 tunnels</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>4.2.a (iii) Virtual tunneling Interface (VTI)</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>4.2.b Describe GET VPN</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td><strong>5.0 Infrastructure Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>5.1 Device security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1.a Implement and troubleshoot IOS AAA using local database</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.1.b Implement and troubleshoot device access control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1.b (i) Lines (VTY, AUX, console)</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>5.1.b (ii) SNMP</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>5.1.b (iii) Management plane protection</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.1.b (iv) Password encryption</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>5.1.c Implement and troubleshoot control plane policing</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.1.d Describe device security using IOS AAA with TACACS+ and RADIUS</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.1.d (i) AAA with TACACS+ and RADIUS</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.1.d (ii) Local privilege authorization fallback</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td><strong>5.2 Network security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.2.a Implement and troubleshoot switch security features</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.a (i) VACL, PACL</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.a (ii) Stormcontrol</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.a (iii) DHCP snooping</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.a (iv) IP source-guard</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.a (v) Dynamic ARP inspection</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.a (vi) port-security</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.a (vii) Private VLAN</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>5.2.b Implement and troubleshoot router security features</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.b (i) IPv4 access control lists (standard, extended, time-based)</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.b (ii) IPv6 traffic filter</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.b (iii) Unicast reverse path forwarding</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.c Implement and troubleshoot IPv6 first-hop security</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.c (i) RA guard</td>
<td>2</td>
<td>9</td>
</tr>
</tbody>
</table>
### Topics

<table>
<thead>
<tr>
<th>Topics</th>
<th>Book Volume</th>
<th>Book Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.c (ii) DHCP guard</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.c (iii) Binding table</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.c (iv) Device tracking</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.c (v) ND inspection/snooping</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.c (vii) Source guard</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.c (viii) PACL</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.d Describe 802.1x</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.d (i) 802.1x, EAP, RADIUS</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>5.2.d (ii) MAC authentication bypass</td>
<td>2</td>
<td>9</td>
</tr>
</tbody>
</table>

### 6.0 Infrastructure Services

#### 6.1 System management

<table>
<thead>
<tr>
<th>Topics</th>
<th>Book Volume</th>
<th>Book Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1.a Implement and troubleshoot device management</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.1.a (i) Console and VTY</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.1.a (ii) Telnet, HTTP, HTTPS, SSH, SCP</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.1.a (iii) (T)FTP</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.1.b Implement and troubleshoot SNMP</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.1.b (i) v2c, v3</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.1.c Implement and troubleshoot logging</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.1.c (i) Local logging, syslog, debug, conditional debug</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.1.c (ii) Timestamp</td>
<td>2</td>
<td>6</td>
</tr>
</tbody>
</table>

#### 6.2 Quality of service

<table>
<thead>
<tr>
<th>Topics</th>
<th>Book Volume</th>
<th>Book Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.a Implement and troubleshoot end-to-end QoS</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>6.2.a (i) CoS and DSCP mapping</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>6.2.b Implement, optimize, and troubleshoot QoS using MQC</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>6.2.b (i) Classification</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>6.2.b (ii) Network-based application recognition (NBAR)</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>6.2.b (iii) Marking using IP precedence, DSCP, CoS, ECN</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>6.2.b (iv) Policing, shaping</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>6.2.b (v) Congestion management (queuing)</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>6.2.b (vi) HQoS, subrate Ethernet link</td>
<td>2</td>
<td>3, 4, 5</td>
</tr>
<tr>
<td>6.2.b (vii) Congestion avoidance (WRED)</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Topics</td>
<td>Book Volume</td>
<td>Book Chapter</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>6.2.c Describe Layer 2 QoS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2.c (i) Queuing, scheduling</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>6.2.c (ii) Classification, marking</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>6.3 Network services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.3.a Implement and troubleshoot first-hop redundancy protocols</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.3.a (i) HSRP, GLBP, VRRP</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.3.a (ii) Redundancy using IPv6 RS/RA</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.3.b Implement and troubleshoot Network Time Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.3.b (i) NTP master, client, version 3, version 4</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.3.b (ii) NTP Authentication</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.3.c Implement and troubleshoot IPv4 and IPv6 DHCP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.3.c (i) DHCP client, IOS DHCP server, DHCP relay</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.3.c (ii) DHCP options</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.3.c (iii) DHCP protocol operations</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.3.c (iv) SLAAC/DHCPv6 interaction</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>6.3.c (v) Stateful, stateless DHCPv6</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>6.3.c (vi) DHCPv6 prefix delegation</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>6.3.d Implement and troubleshoot IPv4 Network Address Translation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.3.d (i) Static NAT, dynamic NAT, policy-based NAT, PAT</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.3.d (ii) NAT ALG</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>6.3.e Describe IPv6 Network Address Translation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.3.e (i) NAT64</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>6.3.e (ii) NPTv6</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>6.4 Network optimization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.4.a Implement and troubleshoot IP SLA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.4.a (i) ICMP, UDP, jitter, VoIP</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.4.b Implement and troubleshoot tracking object</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.4.b (i) Tracking object, tracking list</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.4.b (ii) Tracking different entities (for example, interfaces, routes, IPSLA, and so on)</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.4.c Implement and troubleshoot NetFlow</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To give you practice on these topics, and pull the topics together, Edition 5 of the *CCIE Routing and Switching v5.0 Official Cert Guide, Volume 1* includes a large set of CD questions that mirror the types of questions expected for the Version 5.0 blueprint. By their very nature, these topics require the application of the knowledge listed throughout the book. This special section of questions provides a means to learn and practice these skills with a proportionally larger set of questions added specifically for this purpose.

These questions will be available to you in the practice test engine database, whether you take full exams or choose questions by category.

**About the CCIE Routing and Switching v5.0 Official Cert Guide, Volume 1, Fifth Edition**

This section provides a brief insight into the contents of the book, the major goals, and some of the book features that you will encounter when using this book.

**Book Organization**

This volume contains four major parts. Beyond the chapters in these parts of the book, you will find several useful appendixes gathered in Part V.

Following is a description of each part’s coverage:

- **Part I, “LAN Switching” (Chapters 1–3)**
  
  This part focuses on LAN Layer 2 features, specifically Ethernet (Chapter 1), VLANs and trunking (Chapter 2), and Spanning Tree Protocol (Chapter 3).

- **Part II, “IP Networking” (Chapters 4–5)**
  
  This part covers details across the spectrum of the TCP/IP protocol stack. It includes Layer 3 basics (Chapter 4) and IP services such as DHCP and ARP (Chapter 5).
Part III, “IP IGP Routing” (Chapters 6–11)

This part covers some of the more important topics on the exam and is easily the largest part of this volume. It covers Layer 3 forwarding concepts (Chapter 6), followed by three routing protocol chapters, one each about RIPv2, EIGRP, OSPF, and IS-IS (Chapters 7 through 10, respectively), and concludes with a discussion of IGP redistribution and routing information optimization (Chapter 11).

Part IV, “Final Preparation”

Chapter 12, “Final Preparation,” contains instructions about using the testing software on the CD to verify your knowledge, presents suggestions on approaching your studies, and includes hints about further expanding your knowledge by participating in the Cisco Learning Network.

Part V, “Appendixes”

- Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes”—This appendix lists answers and explanations for the questions at the beginning of each chapter.
- Appendix B, “Exam Updates”—As of the first printing of the book, this appendix contains only a few words that reference the web page for this book, at www.ciscopress.com/title/9781587143960. As the blueprint evolves over time, the authors will post new materials at the website. Any future printings of the book will include the latest newly added materials in printed form in Appendix B. If Cisco releases a major exam update, changes to the book will be available only in a new edition of the book and not on this site.

Note: Appendixes C, D, E, F, and G and the Glossary are in printable, PDF format on the CD.

- Appendix C, “Decimal to Binary Conversion Table” (CD-only)—This appendix lists the decimal values 0 through 255, with their binary equivalents.
- Appendix D, “IP Addressing Practice” (CD-only)—This appendix lists several practice problems for IP subnetting and finding summary routes. The explanations to the answers use the shortcuts described in the book.
- Appendix E, “Key Tables for CCIE Study” (CD-only)—This appendix lists the most important tables from the core chapters of the book. The tables have much of the content removed so that you can use them as an exercise. You can print the PDF file and then fill in the table from memory, checking your answers against the completed tables in Appendix F.
- Appendix G, “Study Planner” (CD-only)—This appendix is a spreadsheet with major study milestones, where you can track your progress through your study.
- Glossary (CD-only)—The Glossary contains the key terms listed in the book.
Book Features

The core chapters of this book have several features that help you make the best use of your time:

- **“Do I Know This Already?” Quizzes:** Each chapter begins with a quiz that helps you to determine the amount of time you need to spend studying that chapter. If you score yourself strictly, and you miss only one question, you might want to skip the core of the chapter and move on to the “Foundation Summary” section at the end of the chapter, which lets you review facts and spend time on other topics. If you miss more than one, you might want to spend some time reading the chapter or at least reading sections that cover topics about which you know you are weaker.

- **Foundation Topics:** These are the core sections of each chapter. They explain the protocols, concepts, and configuration for the topics in that chapter.

- **Foundation Summary:** The “Foundation Summary” section of this book departs from the typical features of the “Foundation Summary” section of other Cisco Press Exam Certification Guides. This section does not repeat any details from the “Foundation Topics” section; instead, it simply summarizes and lists facts related to the chapter but for which a longer or more detailed explanation is not warranted.

- **Key topics:** Throughout the “Foundation Topics” section, a Key Topic icon has been placed beside the most important areas for review. After reading a chapter, when doing your final preparation for the exam, take the time to flip through the chapters, looking for the Key Topic icons, and review those paragraphs, tables, figures, and lists.

- **Fill In Key Tables from Memory:** The more important tables from the chapters have been copied to PDF files available on the CD as Appendix E. The tables have most of the information removed. After printing these mostly empty tables, you can use them to improve your memory of the facts in the table by trying to fill them out. This tool should be useful for memorizing key facts. That same CD-only appendix contains the completed tables so that you can check your work.

- **CD-based practice exam:** The companion CD contains multiple-choice questions and a testing engine. The CD includes 200 questions unique to the CD. As part of your final preparation, you should practice with these questions to help you get used to the exam-taking process, as well as to help refine and prove your knowledge of the exam topics.

- **Key terms and Glossary:** The more important terms mentioned in each chapter are listed at the end of each chapter under the heading “Definitions.” The Glossary, found on the CD that comes with this book, lists all the terms from the chapters. When studying each chapter, you should review the key terms, and for those terms about which you are unsure of the definition, you can review the short definitions from the Glossary.

- **Further Reading:** Most chapters include a suggested set of books and websites for additional study on the same topics covered in that chapter. Often, these references will be useful tools for preparation for the CCIE Routing and Switching lab exam.
This page intentionally left blank
Blueprint topics covered in this chapter:

This chapter covers the following subtopics from the Cisco CCIE Routing and Switching written exam blueprint. Refer to the full blueprint in Table I-1 in the Introduction for more details on the topics covered in each chapter and their context within the blueprint.

- Cisco Express Forwarding Concepts
- Routing Protocol Migration
- Policy-Based Routing
This chapter begins with coverage of the details of the forwarding plane—the actual forwarding of IP packets. This process of forwarding IP packets is often called IP routing, or simply routing. Also, many people also refer to IP routing as the data plane, meaning the plane (topic) related to the end-user data.

Chapters 7 through 11 cover the details of the IP control plane. In contrast to the term data plane, the control plane relates to the communication of control information—in short, routing protocols like OSPF and BGP. These chapters cover the routing protocols on the exam, plus an additional chapter on redistribution and route summarization.

“Do I Know This Already?” Quiz

Table 6-1 outlines the major headings in this chapter and the corresponding “Do I Know This Already?” quiz questions.

<table>
<thead>
<tr>
<th>Foundation Topics Section</th>
<th>Questions Covered in This Section</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Forwarding</td>
<td>1–6</td>
<td></td>
</tr>
<tr>
<td>Multilayer Switching</td>
<td>7–9</td>
<td></td>
</tr>
<tr>
<td>Policy Routing</td>
<td>10–11</td>
<td></td>
</tr>
<tr>
<td>Total Score</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To best use this pre-chapter assessment, remember to score yourself strictly. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes.”

1. What command is used to enable CEF globally for IPv4 packets?
   a. enable cef
   b. ip enable cef
   c. ip cef
   d. cef enable
   e. cef enable ip
   f. cef ip
2. What command is used to enable CEF globally for IPv6 packets?
   a. `enable cef6`
   b. `ipv6 enable cef`
   c. `ipv6 cef`
   d. `ip cef` (the command automatically enables CEF for IPv4 and IPv6)

3. Can CEF for IPv6 be enabled independently of CEF for IPv4?
   a. Yes
   b. No

4. Which of the following triggers an update to a CEF FIB?
   a. Receipt of an ICMPv6 Neighbor Advertisement message with previously unknown information
   b. Receipt of a LAN ARP reply message with previously unknown information
   c. Addition of a new route to the IP routing table by EIGRP
   d. Addition of a new route to the IP routing table by adding an `ip route` command
   e. The removal of a route from the IP routing table by EIGRP

5. Which of the following triggers an update to a CEF adjacency table?
   a. Receipt of a CDP multicast on the PVC connected to Router1
   b. Receipt of an ARP response with previously unknown information
   c. Receipt of a packet that needs to be routed to another router over a point-to-point interface
   d. Receipt of an ICMPv6 Neighbor Advertisement with previously unknown information

6. Which of the following packet-switching paths is considered to be the slowest?
   a. Process Switching
   b. Fast Switching
   c. Route Cache
   d. Cisco Express Forwarding

7. Which of the following commands is used on a Cisco IOS Layer 3 switch to use the interface as a `routed interface` instead of a `switched interface`?
   a. `ip routing` or `ipv6 unicast-routing` global command
   b. `ip routing` or `ipv6 unicast-routing` interface subcommand
   c. `ip address` interface subcommand
   d. `switchport mode routed` interface subcommand
   e. `no switchport` interface subcommand
8. On a Cisco Catalyst 3560 switch, the first line of the output of a `show interface vlan 55` command lists the state as “Vlan 55 is down, line protocol is down.” Which of the following might be causing that state to occur?

   a. VLAN interface has not been `no shut` yet.
   b. The `ip routing` global command is missing from the configuration.
   c. On at least one interface in the VLAN, a cable that was previously plugged in has been unplugged.
   d. VTP mode is set to transparent.
   e. The VLAN has not yet been created on this switch, or is not in the active state.

9. On a Cisco Catalyst 3560 switch, the first line of the output of a `show interface vlan 55` command lists the state as “Vlan 55 is up, line protocol is down.” Which of the following might be causing that state to occur?

   a. VLAN interface has not been `no shut` yet.
   b. The `ip routing` global command is missing from the configuration.
   c. There is no switch port on the switch with this VLAN allowed and in the STP forwarding state.
   d. STP has been administratively deactivated for this VLAN.
   e. The VLAN has not yet been created on this switch, or is not in the active state.

10. Imagine a route map used for policy routing, in which the route map has a `set default interface serial0/0` command. Serial0/0 is a point-to-point link to another router. A packet arrives at this router, and the packet matches the policy routing `route-map` clause whose only `set` command is the one just mentioned. Which of the following general characterizations is true?

   a. The packet will be routed out interface s0/0; if s0/0 is down, it will be routed using the default route from the routing table.
   b. The packet will be routed using the default route in the routing table; if there is no default, the packet will be routed out s0/0.
   c. The packet will be routed using the best match of the destination address with the routing table; if no match is found, the packet will be routed out s0/0.
   d. The packet will be routed out interface s0/0; if s0/0 is down, the packet will be discarded.
Router1 has an fa0/0 interface and two point-to-point WAN links back to the core of the network (s0/0 and s0/1, respectively). Router1 accepts routing information only over s0/0, which Router1 uses as its primary link. When s0/0 fails, Router1 uses policy routing to forward the traffic out the relatively slower s0/1 link. Which of the following set commands in Router1's policy routing route map could have been used to achieve this function?

a. set ip default next-hop
b. set ip next-hop
c. set default interface
d. set interface
Foundation Topics

IP Forwarding

*IP forwarding*, or *IP routing*, is the process of receiving an IP packet, making a decision of where to send the packet next, and then forwarding the packet. The forwarding process needs to be relatively simple, or at least streamlined, for a router to forward large volumes of packets. Ignoring the details of several Cisco optimizations to the forwarding process for a moment, the internal forwarding logic in a router works basically as shown in Figure 6-1.

**Figure 6-1**  *Forwarding Process at Router3, Destination Telnet Server*

The following list summarizes the key steps shown in Figure 6-1:

1. A router receives the frame and checks the received frame check sequence (FCS); if errors occurred, the frame is discarded. The router makes no attempt to recover the lost packet.
2. If no errors occurred, the router checks the Ethernet Type field for the packet type and extracts the packet. The Data Link header and trailer can now be discarded.
3. Assuming an IPv4 packet, its header checksum is first verified. In case of mismatch, the packet is discarded. With IPv6 packets, this check is skipped, as IPv6 headers do not contain a checksum.
4. If the header checksum passed, the router checks whether the destination IP address is one of the addresses configured on the router itself. If it does, the packet has just arrived at its destination. The router analyzes the Protocol field in the IP header, identifying the upper-layer protocol, and hands the packet’s payload over to the appropriate upper-protocol driver.

5. If the destination IP address does not match any of the router’s configured addresses, the packet must be routed. The router first verifies whether the TTL of the packet is greater than 1. If not, the packet is dropped and an ICMP Time Exceeded message is sent to the packet’s sender.

6. The router checks its IP routing table for the most specific prefix match of the packet’s destination IP address.

7. The matched routing table entry includes the outgoing interface and next-hop router. This information is used by the router to look up the next-hop router’s Layer 2 address in the appropriate mapping table, such as ARP, IP/DLCI, IP/VPI-VCI, dialer maps, and so on. This lookup is needed to build a new Data Link frame and optionally dial the proper number.

8. Before creating a new frame, the router updates the IP header TTL or Hop Count field, requiring a recomputation of the IPv4 header checksum.

9. The router encapsulates the IP packet in a new Data Link header (including the destination address) and trailer (including a new FCS) to create a new frame.

The preceding list is a generic view of the process. Next, a few words on how Cisco routers can optimize the routing process by using Cisco Express Forwarding (CEF).

Process Switching, Fast Switching, and Cisco Express Forwarding

Steps 6 and 7 from the generic routing logic shown in the preceding section are the most computation-intensive tasks in the routing process. A router must find the best route to use for every packet, requiring some form of table lookup of routing information. Also, a new Data Link header and trailer must be created, and the information to put in the header (like the destination Data Link address) must be found in another table.

Cisco has created several different methods to optimize the forwarding processing inside routers, termed switching paths. This section examines the two most likely methods to exist in Cisco router networks today: fast switching and CEF.

With fast switching, the first packet to a specific destination IP address is process switched, meaning that it follows the same general algorithm as shown in Figure 6-1. With the first packet, the router adds the results of this daunting lookup to the fast-switching cache, sometimes called the route cache, organized for fast lookups. The cache contains the destination IP address, the next-hop information, and the data-link header information that needs to be added to the packet before forwarding (as in Step 6 in Figure 6-1). Future packets to the same destination address match the cache entry, so it takes the router less time to process and forward the packet, as all results are already stored in the cache. This approach is also sometimes termed route once, forward many times.
Although it is much better than process switching, fast switching has significant drawbacks. The first packet must be process switched, because an entry can be added to the cache only when a packet is routed and the results of its routing (next hop, egress interface, Layer 2 rewrite information) are computed. A huge inflow of packets to destinations that are not yet recorded in the route cache can have a detrimental effect on the CPU and the router's performance, as they all need to be process switched. The cache entries are timed out relatively quickly, because otherwise the cache could get overly large as it has an entry per each destination address, not per destination subnet/prefix. If the routing table or Layer 3-to-Layer 2 tables change, parts of the route cache must be invalidated rather than updated, causing packets for affected destinations to become process switched again. Also, load balancing can only occur per destination with fast switching. Overall, fast switching was a great improvement at the time it was invented, but since that time, better switching mechanisms have been developed. One of them, Cisco Express Forwarding (CEF), has become the major packet-forwarding mechanism in all current Cisco IP routing implementations, with fast switching becoming practically unused. The support for unicast fast switching has therefore been discontinued and removed from IOS Releases 12.2(25)S and 12.4(20)T onward.

To learn the basic idea behind CEF as an efficient mechanism to perform routing decisions, it is important to understand that the crucial part of routing a packet through a router is finding out how to construct the Layer 2 frame header to allow the packet to be properly encapsulated toward its next hop, and forward the packet out the correct interface. Often, this operation is called a Layer 2 frame rewrite because that is what it resembles: A packet arrives at a router, and the router rewrites the Layer 2 frame, encapsulating the packet appropriately, and sends the packet toward the next hop. The packet's header does not change significantly—in IPv4, only the TTL and checksum are modified; with IPv6, only the Hop Count is decremented. An efficient routing mechanism should therefore focus on speeding up the construction of Layer 2 rewrite information and egress interface lookup. The process switching is highly inefficient in this aspect: The routing table lookup is relatively slow and might need recursive iterations until the directly attached next hop and egress interface are identified. The next-hop information must then be translated in ARP or other Layer 3-to-Layer 2 mapping tables to the appropriate Layer 2 address and the frame header must be constructed, and only then the packet can be encapsulated and forwarded. With each subsequent packet, this process repeats from the beginning.

One important observation is that while the routing table can hold tens of thousands of destination networks (prefixes), a router typically has only a handful of neighbors—the next hops toward all the known destinations. All destinations reachable through a particular next hop are using the same Layer 2 rewrite information. To reach any of the networks behind a particular adjacent next hop, the packets will be encapsulated into frames having the same Layer 2 header addresses and sent out the same egress interface. It makes sense, then, to trade memory for speed: Preconstruct the Layer 2 frame headers and egress interface information for each neighbor, and keep them ready in an adjacency table stored in the router's memory. This adjacency table can be constructed immediately as the routing table is populated, using IP addresses of next hops in the routing table and utilizing ARP or other Layer 3-to-Layer 2 mapping tables to translate next-hop...
IP addresses into their corresponding Layer 2 addresses. A packet that is to be routed through a particular next hop will then simply use the preconstructed Layer 2 frame header for that next hop, without needing to visit the ARP or similar tables over and over again. The process of routing a packet will then transform itself to the process of deciding which entry from the adjacency table should be used to encapsulate and forward the packet. After the proper entry is selected, encapsulating the packet and forwarding it out the egress interface can be done in an extremely rapid way, as all necessary data is readily available.

Another important observation is that the routing table itself is not truly optimized for rapid lookups. It contains lots of information crucial to its construction but not that important for routing lookups, such as origin and administrative distances of routes, their metrics, age, and so on. Entries in the routing table can require recursive lookups: After matching a destination network entry, the next-hop information might contain only the IP address of the next hop but not the egress interface, so the next hop's IP address has to be looked up in the routing table in the next iteration—and the depth of this recursion is theoretically unlimited. Even after matching the ultimate entry in the routing table that finally identifies the egress interface, it does not really say anything about the Layer 2 rewrite that is necessary to forward the packet. The last found next-hop IP address during this lookup process has to be further matched in the ARP or similar mapping tables for the egress interface to find out how to construct the Layer 2 frame header. All these shortcomings can be improved, though: The destination prefixes alone from the routing table can be stored in a separate data structure called the Forwarding Information Base, or FIB, optimized for rapid lookups (usually, tree-based data structures meet this requirement). Instead of carrying the plain next hop's IP address from the routing table over into the FIB, each entry in the FIB that represents a destination prefix can instead contain a pointer toward the particular entry in the adjacency table that stores the appropriate rewrite information: Layer 2 frame header and egress interface indication. Any necessary recursion in the routing table is resolved while creating the FIB entries and setting up the pointers toward appropriate adjacency table entries. No other information needs to be carried over from the routing table into the FIB. In effect, the FIB stores only destination prefixes alone. The forwarding information itself is stored as Layer 2 rewrite information in the adjacency table, and entries in the FIB point toward appropriate entries in the adjacency table. All FIB entries that describe networks reachable through a particular next hop point to the same adjacency table entry that contains prepared Layer 2 header and egress information toward that next hop.

After the FIB and adjacency table are created, the routing table is not used anymore to route packets for which all forwarding information is found in the FIB/adjacency table. With FIB-based routers, the routing table can be used for packets that require more complex processing not available through straightforward Layer 2 rewrite; however, for plain packet routing, only the FIB and the adjacency table are used. The routing table therefore becomes more of a source of routing data to build the FIB and adjacency table contents but is not necessarily used to route packets anymore. Therefore, such a routing table is
called the **Routing Information Base (RIB)**—it is the master copy of routing information from which the FIB and other structures are populated, but it is not necessarily used to route packets itself. Note that many routing protocols including Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) construct their own internal routing tables that are also called RIBs. These per-protocol RIBs are usually separate from the router's routing table and shall not be confused with the RIB discussed in this chapter.

Advantages of this approach should be immediately obvious. The FIB contains only the essential information to match a packet's destination address to a known prefix. A single lookup in the FIB immediately produces a pointer toward complete Layer 2 rewrite information for the packet to be forwarded. If the next hop for a destination changes, only the pointer in the respective FIB entry needs to be updated to point toward the new adjacency table entry; the FIB entry itself that represents the destination prefix is unchanged. Both FIB and adjacency tables can be readily constructed from the routing table and the available Layer 3–to–Layer 2 mapping tables, without requiring any packet flows as was the case in fast switching. To those readers familiar with database systems, the FIB can be seen as an index over the adjacency table, with IP prefixes being the lookup keys and the indexed data being the Layer 2 rewrite entries in the adjacency table.

These ideas are at the core of Cisco Express Forwarding, or CEF. Conceptually, CEF consists of two parts—the **Forwarding Information Base** and the **adjacency table**. The FIB contains all known destination prefixes from the routing table, plus additional specific entries, organized as a so-called **mtrie** or a **multiway prefix tree**. The adjacency table contains a Layer 2 frame header prepared for each known next hop or directly attached destination.

The CEF as just described can be implemented in a relatively straightforward way in software, and this is exactly what all software-based Cisco routers do: They implement CEF purely in software, as part of the operating system they run. Both FIB and adjacency tables are maintained in router's memory, and lookups in these structures are done by the CPU as part of interrupt handler executed when a packet is received. Figure 6-2, reused from the Cisco document “How to Choose the Best Router Switching Path for Your Network,” Document ID 13706 available on the Cisco website, illustrates the concept.

Multilayer switches and high-end Cisco router platforms go even further, and instead of software-based FIB, they use specialized circuits (specifically, Ternary Content Addressable Memory [TCAM]) to store the FIB contents and perform even faster lookups. Using a TCAM, an address lookup is performed in an extremely short time that does not depend on the number of FIB entries, as the TCAM performs the matching on its entire contents in parallel. On these platforms, the CEF structures are distributed to individual linecards if present, and stored in TCAMs and forwarding ASICs.
To illustrate the CEF in action, consider the network in Figure 6-3 and related Example 6-1.

In this network, Router R1 is connected to two other routers and one multilayer switch. The Data Link Layer technologies interconnecting the devices are diverse: Between R1 and R2, HDLC is used; R1 and R3 are connected over a PPP link; R1 and MLS4 are using Ethernet interconnection in two VLANs—native VLAN and VLAN 2. OSPF is the routing protocol in use. R2 advertises networks 10.2.0.0/24 through 10.2.3.0/24 and FD00:2::/64 through FD00:2:3::/64. In a similar fashion, R3 advertises networks 10.3.4.0/24 through 10.3.7.0/24 and FD00:3:4::/64 through FD00:3:7::/64. MLS4 advertises networks 10.4.8.0/24 and 10.4.9.0/24, and FD00:4:8::/64 and FD00:4:9::/64, over both VLANs. Multiple interface encapsulations and multiple networks reachable over a single next hop are used in this example to show how potentially numerous destination prefixes map to a single adjacent next hop and how the Layer 2 rewrite information is built depending on the Data Link Layer technology. CEF is activated for both IPv4 and IPv6 using the `ip cef` and `ipv6 cef` global configuration commands on R1.
Example 6-1 CEF FIB and Adjacency Table

! On R1, `show ip route ospf` shows a portion of the RIB

\[\text{R1#} \text{ show ip route ospf} \]

```
10.0.0.0/8 is variably subnetted, 12 subnets, 2 masks
O  10.2.0.0/24 [110/782] via 192.168.12.2, 00:07:06, Serial0/0/0
O  10.2.1.0/24 [110/782] via 192.168.12.2, 00:07:06, Serial0/0/0
O  10.2.2.0/24 [110/782] via 192.168.12.2, 00:07:06, Serial0/0/0
O  10.2.3.0/24 [110/782] via 192.168.12.2, 00:07:06, Serial0/0/0
O  10.3.0.0/24 [110/782] via 192.168.13.3, 00:07:06, Serial0/0/1
O  10.3.1.0/24 [110/782] via 192.168.13.3, 00:07:06, Serial0/0/1
O  10.3.2.0/24 [110/782] via 192.168.13.3, 00:07:06, Serial0/0/1
O  10.3.3.0/24 [110/782] via 192.168.13.3, 00:07:06, Serial0/0/1
O  10.3.4.0/24 [110/782] via 192.168.13.3, 00:07:06, Serial0/0/1
O  10.3.5.0/24 [110/782] via 192.168.13.3, 00:07:06, Serial0/0/1
O  10.3.6.0/24 [110/782] via 192.168.13.3, 00:07:06, Serial0/0/1
O  10.3.7.0/24 [110/782] via 192.168.13.3, 00:07:06, Serial0/0/1
O  10.3.8.0/24 [110/782] via 192.168.13.3, 00:07:06, Serial0/0/1
O  10.3.9.0/24 [110/782] via 192.168.13.3, 00:07:06, Serial0/0/1
```

! Another crucial part of information is the ARP table that resolves
! next hop IP addresses of hosts connected via Ethernet to MAC addresses
! Serial interface technologies in this example are point-to-point and
! hence require no Layer 3-to-Layer 2 mapping tables. This information will
! be used in construction of adjacency table entries

\[\text{R1#} \text{ show ip arp} \]

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Address</th>
<th>Age (min)</th>
<th>Hardware Addr</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>192.168.14.4</td>
<td>41</td>
<td>0017.9446.b340</td>
<td>ARPA</td>
<td>FastEthernet0/0</td>
</tr>
</tbody>
</table>
show ip cef shows the FIB contents. In the following output, only routes learned via OSPF are shown for brevity reasons. Note how a set of prefixes resolves through a particular adjacency (next hop IP and egress interface).

```
R1# show ip cef 10.0.0.0 255.0.0.0 longer-prefixes
Prefix              Next Hop             Interface
10.2.0.0/24         192.168.12.2         Serial0/0/0
10.2.1.0/24         192.168.12.2         Serial0/0/0
10.2.2.0/24         192.168.12.2         Serial0/0/0
10.2.3.0/24         192.168.12.2         Serial0/0/0
10.3.4.0/32         192.168.13.3         Serial0/0/1
10.3.5.0/24         192.168.13.3         Serial0/0/1
10.3.6.0/24         192.168.13.3         Serial0/0/1
10.3.7.0/24         192.168.13.3         Serial0/0/1
10.4.8.0/24         192.168.24.4         FastEthernet0/0.2
192.168.14.4         FastEthernet0/0
10.4.9.0/24         192.168.24.4         FastEthernet0/0.2
192.168.14.4         FastEthernet0/0
```

Similarly, for IPv6, the relevant outputs are:

```
R1# show ipv6 route ospf
O   FD00:2::/64 [110/782]   via FE80::2, Serial0/0/0
O   FD00:2:1::/64 [110/782] via FE80::2, Serial0/0/0
O   FD00:2:2::/64 [110/782] via FE80::2, Serial0/0/0
O   FD00:2:3::/64 [110/782] via FE80::2, Serial0/0/0
O   FD00:3:4::/64 [110/782] via FE80::3, Serial0/0/1
O   FD00:3:5::/64 [110/782] via FE80::3, Serial0/0/1
O   FD00:3:6::/64 [110/782] via FE80::3, Serial0/0/1
O   FD00:3:7::/64 [110/782] via FE80::3, Serial0/0/1
O   FD00:4:8::/64 [110/782] via FE80::4, FastEthernet0/0.2
```

```
R1# show ipv6 neighbors
IPv6 Address                              Age Link-layer Addr State Interface
FD00:14::4                                  1 0017.9446.b340  STALE Fa0/0
FD00:24::4                                  1 0017.9446.b341  STALE Fa0/0.2
FE80::3                                     - -               REACH Se0/0/1
FE80:14::4                                  2 0017.9446.b340  STALE Fa0/0
```
R1# show ipv6 cef

! Output shortened and reformatted for brevity
FD00:2::/64 nexthop FE80::2 Serial0/0/0
FD00:2:1::/64 nexthop FE80::2 Serial0/0/0
FD00:2:2::/64 nexthop FE80::2 Serial0/0/0
FD00:2:3::/64 nexthop FE80::2 Serial0/0/0
FD00:2:4::/64 nexthop FE80::2 Serial0/0/0
FD00:2:5::/64 nexthop FE80::2 Serial0/0/0
FD00:2:6::/64 nexthop FE80::2 Serial0/0/0
FD00:2:7::/64 nexthop FE80::2 Serial0/0/0
FD00:2:8::/64 nexthop FE80:24::4 FastEthernet0/0.2
FD00:2:9::/64 nexthop FE80:24::4 FastEthernet0/0.2
FD00:3::/64 nexthop FE80::3 Serial0/0/1
FD00:3:1::/64 nexthop FE80::3 Serial0/0/1
FD00:3:2::/64 nexthop FE80::3 Serial0/0/1
FD00:3:3::/64 nexthop FE80::3 Serial0/0/1
FD00:3:4::/64 nexthop FE80::3 Serial0/0/1
FD00:3:5::/64 nexthop FE80::3 Serial0/0/1
FD00:3:6::/64 nexthop FE80::3 Serial0/0/1
FD00:3:7::/64 nexthop FE80::3 Serial0/0/1
FD00:3:8::/64 nexthop FE80:24::4 FastEthernet0/0.2
FD00:3:9::/64 nexthop FE80:24::4 FastEthernet0/0.2
FD00:4::/64 nexthop FE80:24::4 FastEthernet0/0.2
FD00:4:1::/64 nexthop FE80:24::4 FastEthernet0/0.2
FD00:4:2::/64 nexthop FE80:24::4 FastEthernet0/0.2
FD00:4:3::/64 nexthop FE80:24::4 FastEthernet0/0.2
FD00:4:4::/64 nexthop FE80:24::4 FastEthernet0/0.2
FD00:4:5::/64 nexthop FE80:24::4 FastEthernet0/0.2

! The show adjacency shows an abbreviated list of adjacency table entries
! Note that separate entries are created for IPv4 and IPv6 adjacencies,
! as the Protocol or EtherType field value in pre-constructed frame headers
! is different for IPv4 and IPv6

R1# show adjacency

Protocol Interface Address
IPV6 Serial0/0/0 point2point(12)
IP Serial0/0/0 point2point(13)
IPV6 Serial0/0/1 point2point(10)
IP Serial0/0/1 point2point(15)
IPV6 FastEthernet0/0.2 FE80:24:4(12)
IP FastEthernet0/0 192.168.14.4(23)
IPV6 FastEthernet0/0 FE80:14:4(12)
IP FastEthernet0/0.2 192.168.24.4(23)
IPV6 Serial0/0/1 point2point(4)
IPV6 FastEthernet0/0.2 FD00:24:4(5)
IPV6 FastEthernet0/0 FD00:14:4(7)

! Now focus on the adjacency table details. There are adjacencies via multiple
! interfaces. Serial0/0/0 is running HDLC. Note in the show adjacency detail
! command output the prepared HDLC header for all IPv6 prefixes (0F0086DD)
! and IP prefixes (0F008800) resolving through this adjacency.

R1# show adjacency s0/0/0 detail

Protocol Interface Address
IPV6 Serial0/0/0 point2point(12)
0 packets, 0 bytes
0F0086DD
Similar output can be achieved for Serial0/0/1 that runs PPP. In the following output, note the prepared PPP headers for IPv6 (FF030057) and IPv4 (FF030021) prefixes resolving through these adjacencies. There are two IPv6 adjacencies present as IPV6CP specifically installs an adjacency towards the neighbor's link local address.

```
R1# show adjacency s0/0/1 detail
Protocol Interface     Address
IPV6     Serial0/0/1   point2point(10)
          0 packets, 0 bytes
          FF030057
          IPv6 CEF  never
          Epoch: 2
IP       Serial0/0/1   point2point(15)
          0 packets, 0 bytes
          FF030021
          CEF  expires: 00:02:30
              refresh: 00:00:30
          Epoch: 2
IPV6     Serial0/0/1   point2point(4)
          0 packets, 0 bytes
          FF030057
          IPv6 ND  never
          IPv6 ND  never
          Epoch: 2
```

Adjacencies on Fa0/0 show preconstructed Ethernet headers for the neighbors 192.168.14.4, FE80:14::4 and FD00:14::4 - destination MAC, source MAC, EtherType. Compare the MAC addresses with contents of ARP and IPv6 ND tables above.

```
R1# show adjacency fa0/0 detail
Protocol Interface     Address
IP       FastEthernet0/0 192.168.14.4(23)
          0 packets, 0 bytes
          0017946B3400019E87F38E40800
          ARP  02:29:07
          Epoch: 2
```
Finally, adjacencies on Fa0/0.2 show preconstructed Ethernet headers for neighbors 192.168.24.4, FE80:24::4 and FD00:24::4 - destination MAC, source MAC, 802.1Q VLAN tag, EtherType. Compare the MAC addresses with contents of ARP and IPv6 ND tables.

Table 6-2 summarizes a few key points about the three main options for router switching paths.
<table>
<thead>
<tr>
<th>Switching Path</th>
<th>Structures That Hold the Forwarding Information</th>
<th>Load-Balancing Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process switching</td>
<td>Routing table</td>
<td>Per packet</td>
</tr>
<tr>
<td>Fast switching</td>
<td>Fast-switching cache (per flow route cache)</td>
<td>Per destination IP address</td>
</tr>
<tr>
<td>CEF</td>
<td>FIB tree and adjacency table</td>
<td>Per a hash of the packet source and destination, or per packet</td>
</tr>
</tbody>
</table>

The `ip cef` global configuration command enables CEF for all interfaces on a Cisco router. For IPv6, the `ipv6 cef` command is used to activate CEF support. Note that it is possible to run IPv4 CEF without IPv6 CEF, but the converse is not true: To run IPv6 CEF, IPv4 CEF must be active. The `no ip route-cache cef` interface subcommand can then be used to selectively disable CEF on an interface.

### Load Sharing with CEF and Related Issues

One of major advantages of CEF is its native support for different load-sharing mechanisms, allowing the use of multiple paths toward a destination network if present in the FIB. CEF supports two modes of load sharing: per-packet and per-destination. With per-packet load sharing, packets destined to a destination network are distributed across multiple paths in a packet-by-packet fashion. With the per-destination mode, the CEF actually takes the source and destination IP address and optionally other data to produce a hash value that identifies the particular path to carry the packet. In effect, for a particular source and destination pair, all packets flow through a single path. Other particular source/destination address combinations toward the same destination network can produce a different hash and thus be forwarded over a different path. In fact, the per-destination load-sharing mode in CEF would be better called per-flow load sharing.

The per-destination load-sharing mode is the default (hardware-based CEF implementations might not support the per-packet load sharing mode), and in general, it is preferred because it avoids packet reordering within a single conversation.

Per-destination load sharing in CEF is technically achieved by placing a so-called loadshare table between the FIB and the adjacency table. This loadshare table contains up to 16 pointers to entries in the adjacency table, and the individual loadshare entries are populated so that the counts of loadshare pointers to particular adjacency entries are proportional to the costs of parallel routes toward the same destination. (That is, if there are two equal-cost paths to the same destination, eight loadshare entries will point to one next-hop adjacency entry while another eight loadshare entries will point to another next-hop adjacency entry. If there are three equal cost paths, only 15 loadshare entries will be populated, with each five loadshare entries pointing to one of the three next-hop adjacency entries.) When a packet arrives, the router performs a hashing operation over the packet’s source and destination address fields, and uses the hash result value as an index.
into the loadshare table to select one of the possible paths toward the destination. This concept is illustrated in Figure 6-4, also taken from the Cisco document “How to Choose the Best Router Switching Path for Your Network,” Document ID 13706.

Figure 6-4  CEF Load Balancing

The particular method of per-packet or per-destination load sharing can be activated on egress interfaces of a router using the \texttt{ip load-share \{ per-destination | per-packet \}} interface-level command. The availability of this command might be limited depending on the hardware capabilities of the device. Often, multilayer switches performing hardware-accelerated switching do not support this command while software-based ISR routers do.

With the hashing performed over fixed packet and/or segment address fields, a single hash function produces the same result for all packets in a flow. While this is desirable on a single router to always select a single path for a flow, it leads to unpleasant consequences in a network where multiple routers down a path to a destination have multiple routes toward it.
Consider the network shown in the Figure 6-5.

Router R1 has two neighbors, R2 and R3, toward the destination network 10.0.0.0/24. Let's assume that it is receiving 64 different flows destined to stations inside the network 10.0.0.0/24. Under ideal conditions, 32 flows will be forwarded from R1 through R2 and 32 other flows will be forwarded through R3. On R2, we now expect that it again balances the 32 received flows across its neighbors, forwarding 16 flows through R4 and another 16 flows through R5. However, if R2 is using the same hashing function as R1, this is no longer the case. All 32 flows received by R2 have produced the same hashing value on R1—that is why R2 is receiving all of them in the first place. Running the same hashing function over these 32 flows will again produce the same value for all of them, and as a result, R2 will no longer load-share them; rather, all 32 flows will be forwarded from R2 through a single path to the destination. Thus, no load sharing will occur farther down the path below R1. Quite the same fate will meet the remaining 32 flows on R3. This phenomenon is called CEF polarization, and will cause the advantage of load sharing to be lost quickly.

To avoid this, the basic CEF load-sharing mechanism has been enhanced. Each router chooses a random 4B-long number called a Universal ID (details of its selection are not public). This Universal ID is used as a seed in the hashing function used by CEF. Because with high probability, different routers will have unique Universal IDs, they will also produce different hashing results for a particular packet flow. As a result, a set of flows producing a single hashing value on one router might produce a set of different hashing values on another router, enabling the set of flows to be load-balanced again across multiple paths.
In recent IOSs, there are multiple variations of the CEF load-sharing algorithm:

- **Original algorithm**: As the name suggests, this is the original unseeded implementation prone to CEF polarization.
- **Universal algorithm**: An improved algorithm using the Universal ID to avoid the CEF polarization.
- **Tunnel algorithm**: A further improvement on the Universal algorithm especially suitable to environments where tunnels are extensively deployed, possibly resulting in a relatively small number of outer source/destination pairs. Avoids the CEF polarization. Might not be available for IPv6 CEF.
- **L4 port algorithm**: Based on the Universal algorithm while also taking the L4 source and/or destination ports into account. Avoids the CEF polarization.

Except from the Original algorithm, all other algorithms listed here avoid the CEF polarization issue by seeding the hash function using the Universal ID. This ID can be specified for these algorithms in the `ip cef load-sharing algorithm` and `ipv6 cef load-sharing algorithm` global configuration commands manually if necessary. This command is also used to select the particular load-sharing algorithm as described in the preceding list. To verify the current load-sharing mechanism and Universal ID value, the output of `show cef state`, `show ip cef summary`, or `show ip cef detail`, especially the heading, shall be examined (the output of these commands differs on different platforms).

The Catalyst 6500 platform (and some others that are directly derived from it, such as selected 7600 Series supervisors and linecards), enjoying a long history of existence during the time the details of CEF were fleshed out and perfected in software-based IOSs, has its own set of workarounds about the CEF polarization problem. On this platform, instead of the `ip cef load-sharing algorithm` command, the `mls ip cef load-sharing` command is used to select the load-sharing algorithm. The individual options are as follows:

- **Default (default mls ip cef load-sharing)**: Uses source and destination IP, plus the Universal ID if supported by the hardware. Avoids CEF polarization.
- **Full (mls ip cef load-sharing full)**: Uses source IP, destination IP, source L4 port, and destination L4 port. Does not use Universal ID. Prone to CEF polarization. However, to alleviate its impact, this load-balancing algorithm causes the traffic to split equally among multiple paths only if the number of paths is odd. With an even number of parallel paths, the ratio of traffic split will not be uniform.
- **Simple (mls ip cef load-sharing simple)**: Uses source and destination IP only. Does not use Universal ID. Prone to CEF polarization.
- **Full Simple (mls ip cef load-sharing full simple)**: Uses source IP, destination IP, source L4 port, and destination L4 port. Does not use Universal ID. Prone to CEF polarization. The difference from Full mode is that all parallel paths receive an equal weight, and fewer adjacency entries in hardware are used. This mode avoids unequal traffic split seen with Full mode.
Multilayer Switching

Multilayer Switching (MLS) refers to the process by which a LAN switch, which operates at least at Layer 2, also uses logic and protocols from layers other than Layer 2 to forward data. The term Layer 3 switching refers specifically to the use of the Layer 3 destination address, compared to the routing table (or equivalent), to make the forwarding decision. (The latest switch hardware and software from Cisco uses CEF switching to optimize the forwarding of packets at Layer 3.)

MLS Logic

Layer 3 switching configuration works similarly to router configuration—IP addresses are assigned to interfaces, and routing protocols are defined. The routing protocol configuration works just like a router. However, the interface configuration on MLS switches differs slightly from routers, using VLAN interfaces, routed interfaces, and Port-channel Layer 3 interfaces.

VLAN interfaces give a Layer 3 switch a Layer 3 interface attached to a VLAN. Cisco often refers to these interfaces as switched virtual interfaces (SVI). To route between VLANs, a switch simply needs a virtual interface attached to each VLAN, and each VLAN interface needs an IP address in the respective subnets used on those VLANs.

Note Although it is not a requirement, the devices in a VLAN are typically configured in the same single IP subnet. However, you can use secondary IP addresses on VLAN interfaces to configure multiple subnets in one VLAN, just like on other router interfaces.

The operational state of SVI interfaces deserves a word on its own. For an MLS, an SVI is the Layer 3 interface that interconnects the internal “router” inside the MLS with the particular VLAN, much like an interface on a real router connects it to a particular network. An MLS can directly send packets to or through a particular VLAN by forwarding them over the corresponding SVI. These SVIs will be present in an MLS’s routing table as egress interfaces for packets delivered into or through particular VLANs. The operational state of an SVI should therefore reflect the true ability of the MLS to directly forward packets into the corresponding VLAN. The SVI—despite being a virtual interface—must not be in the “up, line protocol up” state if the MLS is not truly capable of forwarding packets into the corresponding VLAN. In other words, the state of SVIs must mimic the behavior of ordinary routers. If an interface is not in the “up, line protocol up” state, the configured directly connected network on that interface and all routes formerly reachable over it must be removed from the routing table, and can be put back only if the interface becomes fully operational again.

There are two primary reasons why an MLS might be unable to forward packets into a particular VLAN: Either that VLAN is not created and active on the MLS, or the VLAN exists and is active but there is no physical Layer 2 interface on the switch allowing it to forward frames into that VLAN. Consequently, the state of an SVI can be one of the following:
■ **Administratively down, line protocol down**: The SVI interface is shut down.

■ **Down, line protocol down**: The corresponding VLAN does not exist, or is not in an active state (the `state suspend` or `shutdown` commands were issued in the VLAN’s configuration).

■ **Up, line protocol down**: The corresponding VLAN exists, but it is not allowed and in an STP forwarding state on any Layer 2 switch port (access or trunk).

■ **Up, line protocol up**: The VLAN is created and the MLS is capable of forwarding frames (and hence packets) into that VLAN.

To avoid the “up, line protocol down,” at least one of the following conditions must be true:

■ At least one physical trunk that is itself in the “up, line protocol up” state must have this VLAN allowed, not VTP pruned, and in the STP forwarding state. This can be verified, for example, using the `show interfaces trunk` command (check the bottom-most section labeled with “Vlans in spanning tree forwarding state and not pruned”).

■ At least one physical switch port that is itself in the “up, line protocol up” state must have this VLAN configured as an access or voice VLAN and in the STP forwarding state. This can be verified, for example, using `show vlan` and `show spanning-tree` commands.

When using VLAN interfaces, the switch must take one noticeable but simple additional step when routing a packet. Like typical routers, MLS makes a routing decision to forward a packet. As with routers, the routes in an MLS routing table entry list an outgoing interface (a VLAN interface in this case), as well as a next-hop Layer 3 address. The adjacency information (for example, the IP ARP table or the CEF adjacency table) lists the VLAN number and the next-hop device’s MAC address to which the packet should be forwarded—again, typical of normal router operation.

At this point, a true router would know everything it needs to know to forward the packet. An MLS switch, however, then also needs to use Layer 2 logic to decide which physical interface to physically forward the packet already encapsulated in a Layer 2 frame. The switch will simply find the next-hop device’s MAC address in the CAM and forward the frame to that address based on the CAM.

### Using Routed Ports and Port-channels with MLS

In some point-to-point topologies, VLAN interfaces are not required. For example, when an MLS switch connects to a router using a cable from a switch interface to a router’s LAN interface, and the only two devices in that subnet are the router and that one physical interface on the MLS switch, the MLS switch can be configured to treat that one interface as a **routed port**. (Another typical topology for using routed ports is when two MLS switches connect for the purpose of routing between the switches, again creating a case with only two devices in the VLAN/subnet.)
A routed port on an MLS switch has the following characteristics:

- The interface is not placed into any user-defined VLAN (internally in an MLS switch, an internal usage VLAN is created for each individual routed port).
- On most Catalyst platforms, a routed port cannot be configured with subinterfaces.
- The switch does not keep any Layer 2 switching table information for the interface.
- Layer 3 settings, such as the IP address, are configured under the physical interface, just like a router.
- The adjacency table lists the outgoing physical interface or Port-channel, which means that Layer 2 switching logic is not required in these cases.

The internal usage VLAN created on behalf of a routed port deserves a special mention. For a VLAN-aware MLS, all operations are performed within the context of a VLAN in which the frame or packet is processed. The most natural way for these switches to implement a routed port is in fact to create a hidden, standalone, and dedicated VLAN for each separate routed port, and deactivate the typical Layer 2 control plane protocols on it. These dedicated VLANs are called internal usage VLANs. On Catalyst switches supporting an extended VLAN range, these internal usage VLANs are allocated from the extended range, depending on the setting of the vlan internal allocation policy { ascending | descending } global configuration command. If the ascending option is used, internal usage VLANs are allocated from VLAN ID 1006 upward. Conversely, if the descending option is used, internal usage VLANs are allocated from VLAN ID 4094 downward. On lower-end Catalyst platforms, this command is present in the configuration with the ascending option but cannot be modified.

The current allocation of internal usage VLANs can be displayed only using the show vlan internal usage command; they do not appear in common show vlan output. As an example, observe the output in the Example 6-2.

**Example 6-2  Internal Usage VLANs Created for Routed Ports**

```
| On this 3560G switch, ports GigabitEthernet0/12 and GigabitEthernet0/13 will |
| be configured as routed ports, and the internal usage VLANs will be observed. |
| The switch is configured with vlan internal allocation policy ascending |

Switch(config)# do show vlan internal usage

VLAN Usage
---- ---------------------

Switch(config)# interface gi0/12
Switch(config-if)# no switchport
Switch (config-if)# do show vlan internal usage
```
Internal usage VLANs are internal to the switch, and regardless of the VTP mode, they are not stored in the VLAN database and are not advertised to any other switch in the VTP domain. The assignment of internal usage VLANs to routed ports is therefore only done at runtime and can differ between restarts of a switch, depending on the order that the routed ports are configured and on the unused extended VLAN IDs.

Because of the relatively discreet nature of internal usage VLANs (they are not visible in ordinary `show vlan` output), conflicts can ensue if an administrator tries to create an extended VLAN whose ID is—unknowingly to the administrator—already used by an internal usage VLAN, as shown in the Example 6-3.

**Example 6-3  Possible Internal Usage VLAN Conflict While Creating Extended VLANs**

```plaintext
! Building on the previous example, internal usage VLANs 1006 and 1007 exist ! on this switch. An administrator is not aware about their existence, though, ! and tries to create VLAN 1006 for its own use. Notice how the switch refuses ! to add the VLAN only after exiting the VLAN configuration.

Switch(config)# do show vlan internal usage

VLAN Usage
---- -------------------
1006 GigabitEthernet0/12
1007 GigabitEthernet0/13

Switch(config)# vlan 1006
Switch(config-vlan)# name SomeExtendedVLAN
Switch(config-vlan)# exit
% Failed to create VLANs 1006
VLAN(s) not available in Port Manager.
% Failed to commit extended VLAN(s) changes.
```
This problem can become especially unpleasant if VTPv3 is used that is capable of handling extended VLAN IDs. If the administrator creates an extended range VLAN on a VTP Primary Server switch, and the particular VLAN ID is already used by an internal usage VLAN on some other switch in the domain, VTP will fail to create this VLAN on that switch, resulting in connectivity issues. The conflict will be logged only on the switch experiencing the VLAN ID collision and so can elude the administrator’s attention.

It is therefore generally recommended that if extended VLANs are used, they should be allocated from the end of the extended VLAN range that is opposite to the current internal VLAN allocation policy, to minimize the risk of creating VLAN ID collisions.

Keeping all these facts in mind, a routed port is practically equivalent to a switch port placed into a dedicated VLAN, with the Layer 2 control plane protocols deactivated on that port. From this viewpoint, a routed port is a syntactical device in the configuration to make the configuration quick and convenient, while the switch continues to handle the port internally as a switch port with a slightly modified operation.

The following two configuration snippets in Example 6-4 are practically equivalent; just the routed port is simpler to configure.

Example 6-4  Routed Port and Its Internal Treatment by a Multilayer Switch

Following the previous example, assume the Gi0/12 is configured as follows:

```
Switch(config)# int gi0/12
Switch(config-if)# no switchport
Switch(config-if)# ip address 192.168.12.1 255.255.255.0
Switch(config-if)# do show vlan internal usage
```

> VLAN Usage
> ---- ------------------
> 1006 GigabitEthernet0/12

The above configuration is effectively equivalent to the following configuration:

```
Switch(config)# int gi0/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1006
Switch(config-if)# ip address 192.168.12.1 255.255.255.0
```

```
Switch(config)# vlan 1006
Switch(config-vlan)# exit
Switch(config)# no spanning-tree vlan 1006
Switch(config)# no mac address-table learning vlan 1006
Switch(config)# interface GigabitEthernet0/12
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1006
Switch(config-if)# switchport nonegotiate
Switch(config-if)# no vtp
Switch(config-if)# exit
Switch(config)# interface Vlan1006
Switch(config-if)# ip address 192.168.12.1 255.255.255.0
```
Ethernet Port-channels can be used as routed interfaces as well. To do so, physical interfaces must be configured with the `no switchport` command before adding them to a channel group. The automatically created Port-channel interface inherits the configuration of the first physical interface added to the channel group; if that interface is configured as a routed interface, the entire Port-channel will be working as a routed port. An existing Layer 2 Port-channel cannot be changed from Layer 2 to Layer 3 operation and vice versa. If such a modification is necessary, it is first required to completely delete the entire Port-channel, unbundle the physical ports, reconfigure them into the desired mode of operation, and then add them into a channel group again, re-creating the Port-channel interface in the process. Also, when using a Port-channel as a routed interface, Port-channel load balancing should be based on Layer 3 addresses because the Layer 2 addresses will mostly be the MAC addresses of the two MLS switches on either end of the Port-channel. Port-channels can also be used as Layer 2 interfaces when doing MLS. In that case, VLAN interfaces would be configured with an IP address, and the Port-channel would simply act as any other Layer 2 interface.

Table 6-3 lists some of the specifics about each type of Layer 3 interface.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Forwarding to Adjacent Device</th>
<th>Configuration Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN interface</td>
<td>Uses Layer 2 logic and Layer 2 MAC address table</td>
<td>Create VLAN interface; VLAN must also exist</td>
</tr>
<tr>
<td>Physical (routed) interface</td>
<td>Forwards out physical interface</td>
<td>Use the <code>no switchport</code> command to create a routed interface</td>
</tr>
<tr>
<td>Port-channel (switched) interface</td>
<td>Not applicable; just used as another Layer 2 forwarding path</td>
<td>No special configuration; useful with VLAN interfaces</td>
</tr>
<tr>
<td>Port-channel (routed) interface</td>
<td>Balances across links in Port-channel</td>
<td>Needs the <code>no switchport</code> command to be used as a routed interface; optionally change load-balancing method</td>
</tr>
</tbody>
</table>

**MLS Configuration**

The upcoming MLS configuration example is designed to show all the configuration options. The network design is shown in Figures 6-6 and 6-7. In Figure 6-6, the physical topology is shown, with routed ports, VLAN trunks, a routed Port-channel, and access links. Figure 6-7 shows the same network, with a Layer 3 view of the subnets used in the network.
A few design points bear discussion before jumping into the configuration. First, SW1 and SW2 need Layer 2 connectivity to support traffic in VLANs 11 and 12. In this particular example, a trunk is used between SW1 and SW2 as well as between SW1/SW2 and SW3/SW4. Focusing on the Layer 2 portions of the network, SW1 and SW2, both distribution MLS switches, connect to SW3 and SW4, which are access layer
switches. SW1 and SW2 are responsible for providing full connectivity in VLANs 11 and 12. Having full Layer 2 connectivity between switches in a topology is the traditional approach. In newer deployments, a new approach is favored in which SW1 and SW2 are interconnected through a routed port (Layer 3 link) only, and the connections toward access layer switches are Layer 2 or even Layer 3. This allows for shrinking the size of Layer 2 domain and the resulting scope of STP operation. If only a routed link was left between SW1 and SW2, the Layer 2 topology between SW1/SW2 and SW3/SW4 would be physically loop-free and there would be no ports blocked by STP, requiring little or no reaction of STP if a link is added or removed.

Additionally, this design uses SW1 and SW2 as Layer 3 switches, so the hosts in VLANs 11 and 12 will use SW1 or SW2 as their default gateway. For better availability, the two switches should use HSRP, VRRP, or GLBP. Regardless of which protocol is used, both SW1 and SW2 need to be in VLANs 11 and 12, with connectivity in those VLANs, to be effective as default gateways.

In addition to a Layer 2 trunk between SW1 and SW2, to provide effective routing, it makes sense for SW1 and SW2 to have a routed path between each other as well. Certainly, SW1 needs to be able to route packets to Router R1, and SW2 needs to be able to route packets to Router R2. However, routing between SW1 and SW2 allows for easy convergence if R1 or R2 fails.

Figure 6-6 shows two alternatives for routed connectivity between SW1 and SW2, and one option for Layer 2 connectivity. For Layer 2 connectivity, a VLAN trunk needs to be used between the two switches. Figure 6-6 shows a pair of trunks between SW1 and SW2 (labeled with a circled T) as a Layer 2 Port-channel. The Port-channel would support the VLAN 11 and 12 traffic.

To support routed traffic, the figure shows two alternatives: Simply route over the Layer 2 Port-channel using VLAN interfaces or use a separate routed Port-channel. First, to use the Layer 2 Port-channel, SW1 and SW2 could simply configure VLAN interfaces in VLANs 11 and 12. The alternative configuration uses a second Port-channel that will be used as a routed Port-channel. However, the routed Port-channel does not function as a Layer 2 path between the switches, so the original Layer 2 Port-channel must still be used for Layer 2 connectivity. Upcoming Example 6-5 shows both configurations.

Finally, a quick comment about Port-channels is needed. This design uses Port-channels between the switches, but they are not required. Most links between switches today use at least two links in a Port-channel, for the typical reasons—better availability, better convergence, and less STP overhead. This design includes the Port-channel to point out a small difference between the routed interface configuration and the routed Port-channel configuration.

Example 6-5 shows the configuration for SW1, with some details on SW2.
Example 6-5  MLS-Related Configuration on Switch1

Below, note that the switch is in VTP transparent mode, and VLANs 11 and 12 are configured, as required. Also note the `ip routing` global command, without which the switch will not perform Layer 3 switching of IP packets.

```
vlan 11

vlan 12
```

The `ip routing` global command is required before the MLS will perform Layer 3 forwarding. Similarly, `ipv6 unicast-routing` is required for IPv6 routing to be enabled. On selected Catalyst platforms, the use of the `distributed` keyword is required, as the CEF operates in distributed mode on these switches - over multiple ASICs or line cards.

```
ip routing
ipv6 unicast-routing distributed

vtp domain CCIE-domain
vtp mode transparent
```

Next, the configuration shows basic Port-channel creation commands, with the `no switchport` command being required before bundling physical ports into a Port-channel. Note the Port-channel interface will be created automatically.

```
interface GigabitEthernet0/1
  no switchport
  no ip address
  channel-group 1 mode desirable

interface GigabitEthernet0/2
  no switchport
  no ip address
  channel-group 1 mode desirable
```

```
Next, the Port-channel interface is assigned an IP address.

interface Port-channel1
  ip address 172.31.23.201 255.255.255.0
```

Below, similar configuration on the interface connected to Router1.
interface FastEthernet0/1
  no switchport
  ip address 172.31.21.201 255.255.255.0

! Next, interface Vlan 11 gives Switch1 an IP presence in VLAN 11. Devices in VLAN 11 can use 172.31.11.201 as their default gateway. However, using HSRP is better, so Switch1 has been configured to be HSRP primary in VLAN11, and Switch2 to be primary in VLAN12, with tracking so that if Switch1 loses its connection to Router1, HSRP will fail over to Switch2.

interface Vlan11
  ip address 172.31.11.201 255.255.255.0
  standby 11 ip 172.31.11.254
  standby 11 priority 90
  standby 11 preempt
  standby 11 track FastEthernet0/1

! Below, VLAN12 has similar configuration settings, but with a higher (better) HSRP priority than Switch2’s VLAN 12 interface.

interface Vlan12
  ip address 172.31.12.201 255.255.255.0
  standby 12 ip 172.31.12.254
  standby 12 priority 110
  standby 12 preempt
  standby 12 track FastEthernet0/1

Note  For MLS switches to route using VLAN interfaces, the ip routing global command must be configured. MLS switches will not perform Layer 3 routing without the ip routing command, which is not enabled by default. Similar comments apply to IPv6 routing that needs to be enabled by ipv6 unicast-routing.

As stated earlier, the routed Port-channel is not required in this topology. It was included to show an example of the configuration, and to provide a backdrop from which to discuss the differences. However, as configured, SW1 and SW2 are Layer 3 adjacent over the routed Port-channel as well as through their VLAN 11 and 12 interfaces. So, they could exchange interior gateway protocol (IGP) routing updates over three separate subnets. In such a design, the routed Port-channel was probably added so that it would be the normal Layer 3 path between SW1 and SW2. Care should be taken to tune the IGP implementation so that this route is chosen instead of the routes over the VLAN interfaces.
Policy Routing

All the options for IP forwarding (routing) in this chapter had one thing in common: The destination IP address in the packet header was the only thing in the packet that was used to determine how the packet was forwarded. Policy routing (or Policy-Based Routing [PBR]) allows a router to make routing decisions based on information besides the destination IP address.

Policy routing’s logic begins, depending on IPv4 or IPv6 in use, with the `ip policy` or `ipv6 policy` command on an interface. This command tells the IOS to process incoming packets on that interface with different logic before the normal forwarding logic takes place. (To be specific, policy routing intercepts the packet after Step 4, but before Step 5, in the routing process shown in Figure 6-1.) The IOS compares the received packets using the `route-map` referenced in the `ip policy` or `ipv6 policy` command. Figure 6-8 shows the basic logic.

![Figure 6-8 Basic Policy Routing Logic](image)

Specifying the matching criteria for policy routing is relatively simple compared to defining the routing instructions using the `set` command. The route maps used by policy routing must match either based on referring to an ACL (numbered or named IPv4/IPv6 ACL, using the `match ip address` or `match ipv6 address` command) or based on packet length (using the `match length` command). To specify the routing instructions—in other words, where to forward the packet next—use the `set` command. Table 6-4 lists the `set` commands and provides some insight into their differences.
### Table 6-4  Policy Routing Instructions (set Commands)

<table>
<thead>
<tr>
<th>Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>set ip next-hop ip-address [ ... ip-address]</td>
<td>Next-hop addresses must be in a connected subnet; forwards to the first address in the list for which the associated interface is up. Supported for both IPv4 and IPv6.</td>
</tr>
<tr>
<td>set ipv6 next-hop ipv6-address [ ... ipv6-address ]</td>
<td>Same logic as previous command, except policy routing first attempts to route based on the routing table, and only if no match is found in the routing table, the packet will be handled by PBR. Default route in the routing table is ignored; that is, if the packet's destination is matched only by the default route, the packet will be handled by PBR. Supported for both IPv4 and IPv6.</td>
</tr>
<tr>
<td>set ip default next-hop ip-address[... ip-address]</td>
<td>Same logic as previous command, except policy routing first attempts to route based on the routing table, and only if no match is found in the routing table, the packet will be handled by PBR. Default route in the routing table is ignored; that is, if the packet's destination is matched only by the default route, the packet will be handled by PBR. Supported for both IPv4 and IPv6.</td>
</tr>
<tr>
<td>set ipv6 default next-hop ipv6-address [ ... ipv6-address ]</td>
<td>Same logic as previous command, except policy routing first attempts to route based on the routing table, and only if no match is found in the routing table, the packet will be handled by PBR. Recommended only for point-to-point interfaces; strongly discouraged for multiaccess interfaces. Supported for both IPv4 and IPv6.</td>
</tr>
<tr>
<td>set interface interface-type interface-number [ ... interface-type interface-number]</td>
<td>Forwards packets using the first interface in the list that is up. Recommended only for point-to-point interfaces; strongly discouraged for multiaccess interfaces. Supported for both IPv4 and IPv6.</td>
</tr>
<tr>
<td>set default interface interface-type interface-number [ ... interface-type interface-number]</td>
<td>Same logic as previous command, except policy routing first attempts to route based on the routing table, and only if no match is found in the routing table, the packet will be handled by PBR. Recommended only for point-to-point interfaces; strongly discouraged for multiaccess interfaces. Supported for both IPv4 and IPv6.</td>
</tr>
<tr>
<td>set ip df number</td>
<td>Sets the IP DF bit; can be either 0 or 1. Supported only for IPv4.</td>
</tr>
<tr>
<td>set ip precedence number</td>
<td>Sets IP precedence bits; can be a decimal value in the range 0–7 or a textual name (IPv4 only). Supported for both IPv4 and IPv6.</td>
</tr>
<tr>
<td>set ipv6 precedence number</td>
<td>Sets the ToS bits (delay, throughput, reliability, monetary cost); can be decimal value or ASCII name. Supported for IPv4 only.</td>
</tr>
<tr>
<td>set ip tos number</td>
<td>Sets the ToS bits (delay, throughput, reliability, monetary cost); can be decimal value or ASCII name. Supported for IPv4 only.</td>
</tr>
</tbody>
</table>

The first four set commands in Table 6-4 are the most important ones to consider. Essentially, you set either the next-hop IP address or the outgoing interface. Use the outgoing interface option only when it is of point-to-point technology type—for example, do not refer to a LAN interface or multipoint Frame Relay subinterface. This will almost
certainly cause the policy-based routing to fail or act unexpectedly; details will be discussed later. Most importantly, note the behavior of the default keyword in the set commands. Use of the default keyword essentially means that policy routing tries the default (destination-based) routing first, and resorts to using the set command details only when the router finds no matching route in the routing table. Note that a default route is not considered a matching route by the default keyword. If a packet's destination is matched only by the default route, PBR treats this as if no match occurred, and the packet is eligible to be forwarded according to the set commands using the default keyword.

The remaining set commands set the bits inside the ToS byte of the packet; refer to Chapter 5, “Classification and Marking,” in Volume II for more information about the ToS byte and QoS settings. Note that you can have multiple set commands in the same route-map clause. For example, you might want to define the next-hop IP address and mark the packet's ToS at the same time. A single route map entry can even contain multiple set statements specifying where the packet shall be forwarded. In such cases, the set statements are evaluated in the following order:

1. set ip next-hop / set ipv6 next-hop
2. set interface
3. set ip default next-hop / set ipv6 default next-hop
4. set default interface

The use of set interface and set default interface is strongly recommended only with point-to-point interfaces. Using multiaccess interfaces in these commands will lead to PBR failing in most cases. IPv6 PBR using set [ default ] interface with a multiaccess interface fails outright; differences in very selected cases have been observed under different IOS versions. IPv4 PBR under the same circumstances might appear to work but the background processes are unintuitive: The router first performs a normal routing table lookup for the packet's destination IP address to look for the connected next-hop address, and then tries to translate this next-hop address into the appropriate Layer 2 address on the multiaccess interface specified in the set [ default ] interface command. This can fail for obvious reasons: The routing table might provide no match for the packet's destination and thus the set [ default ] interface is skipped, or the next hop itself might be connected to a different interface. Even Proxy ARP, if applicable, is not going to help much—Cisco routers perform a validity check on received ARP responses similar to a unicast reverse path forwarding check. A router verifies using its routing table whether the sender IPv4 address in the ARP response's body (the address whose MAC address is being asked for) is reachable through the interface the ARP response came in. If this check fails, the router will drop the ARP response, claiming that it arrived over the “wrong cable” in the debug arp output. Once again, the use of set [ default ] interface is appropriate only with point-to-point interfaces. IOS Releases 15.x display an explicit warning if the command is used with multiaccess interface types.

The IPv6 PBR with set interface in particular has one more peculiarity: In some IOS versions, the router checks whether there is a matching route (ignoring the default route) for the packet's destination even if the packet is to be handled by PBR. If there is no matching route in the routing table, the set interface command is ignored. It is also noteworthy
to mention that on some platforms, this behavior also depends on the state IPv6 CEF. The particular behavior of the IOS in question should therefore be verified using `debug ipv6` policy.

If PBR is required on a multilayer switch, many lower-end switches, such as Catalyst 3550, 3560, or 3750, require that the TCAM in the switch is repartitioned in a different way, providing TCAM space for PBR entries while taking away space from entries of other types. On these platforms, the size of TCAM regions for individual applications cannot be configured individually; instead, a set of templates is prepared for typical switch deployments. A switch should be configured with an appropriate TCAM partitioning template that allocates the most space to the types of entries most required in the particular switch's mode of deployment. A template that provides space for PBR entries must be active before the PBR can be configured. These templates are called Switch Database Management templates, or SDM templates for short. Current SDM templates can be shown using the `show sdm prefer` command, also displaying an approximate space for different TCAM entry types. This command can be also used to view the TCAM allocation policy for different templates if the `show sdm prefer template-name` form is used. To allow for PBR usage on the switch models mentioned previously, either the `routing`, `access`, or `dual-ipv4-and-ipv6 routing` (if supported) SDM template needs to be used. On Catalyst 3650 and 3850 Series, the `advanced` SDM template is required. To activate a particular template, the `sdm prefer template-name` global configuration level command is used. After you issue this command, the switch must be reloaded. It is strongly recommended to consult the appropriate switch model documentation for the list of supported SDM templates and the individual features they activate.

Apart from PBR, changing the SDM template on an MLS might also be required if routing or IPv6 support are to be activated. One of indications that an inappropriate SDM template is currently active is very visible: The IOS CLI appears to lack the commands necessary to configure routing, PBR, or IPv6, even though the IOS should support these features and the appropriate licenses are in place.

**Routing Protocol Changes and Migration**

The proper selection of a routing protocol for a network is always a sensitive (and understandably difficult) task. Many factors need to be taken into consideration, ranging from the protocol's scalability and speed of convergence through advanced features, ending with compatibility issues especially in multivendor environments; all of these are related to the network's design and requirements. As the network evolves, it might become necessary to reevaluate the choice of a particular routing protocol, and if it is found to be inappropriate, it might need to be replaced.

Migrating from one routing protocol to another is always a disruptive change to the network. It requires careful planning to minimize the outages, and even then, they are inevitable, although their duration can be kept very low. Therefore, a routing protocol migration always requires a maintenance window.
Routing protocol migration is usually accomplished with the following steps:

**Step 1.** Plan the migration strategy.

**Step 2.** Activate the new routing protocol on all routers in the topology, raising its administrative distance (AD) above the ADs of the current IGP. If the new IGP is Routing Information Protocol (RIP) or Enhanced Interior Gateway Routing Protocol (EIGRP), redistribution from the current into the new IGP has to be configured on each router as well. The current IGP is left intact.

**Step 3.** Verify the new IGP’s adjacencies and optionally the working database contents.

**Step 4.** Deactivate the current IGP in a gradual fashion.

**Step 5.** Remove the temporary settings from the new IGP.

We describe each of these steps in closer detail.

**Planning the Migration Strategy**

The deployment of a new routing protocol should be preplanned for the entire network, including the division of network into separate areas if and when a link-state IGP is to be used. Additionally, protocol features such as prefix summarization/filtration, stub features, and external information redistribution can further isolate areas of the network from one another. This planning should also involve the order in which routers will be migrated over from the current IGP to the new one. Ideally, routers should be migrated so that they form a contiguous, ever-growing part of the network running the new IGP, gradually shrinking the contiguous remainder of the network in which both the current and new IGP are run. If the current IGP is a link-state protocol, it is advisable to perform the migration in a per-area fashion. The backbone routers should be the last ones to migrate.

**Activating New IGP While Keeping the Current IGP Intact**

According to the planning in the previous step, the new IGP should be activated on the routers in the network, first setting its administrative distance (AD) to a higher value than the current IGP’s AD, and only then adding interfaces and networks to the new IGP and activating selected features. The current IGP is left running and its configuration is unchanged throughout this entire step. If the current IGP uses various ADs for different network types (for example, EIGRP uses 90 and 170 for internal and external routes, respectively), the new IGP’s AD should be reconfigured to be higher than the highest AD used by the existing IGP. As an example, if the current IGP is OSPF and the new IGP should be EIGRP, the ADs of EIGRP should, for the duration of the migration, be reconfigured to, say, 210 and 220 for internal and external EIGRP routes, respectively. This way, the new IGP can be deployed across the network, creating adjacencies between routers as usual but not influencing the routing tables and routing just yet. If the current IGP configuration includes redistribution from other sources (static routes, directly connected networks, and so on), the new IGP shall be configured similarly.
If the new IGP is a distance-vector routing protocol (RIP or EIGRP), each router must also be configured with redistribution from the current IGP into the new IGP. Reasons for this are explained later in the chapter.

Verifying New IGP Adjacencies and Working Database Contents

After the new IGP has been configured across the entire network, it should have created adjacencies in the usual fashion though the routing tables are not populated by its routes yet. These adjacencies should be verified to make sure that they are complete. After the current IGP is deactivated, these adjacencies are the only routing protocol adjacencies left between migrated routers, and so must be working as expected before the current IGP starts being removed.

It is often recommended to verify the contents of the working databases in the new IGP to check whether all expected networks are present, even though not placed into routing tables because of higher ADs. This step might be difficult to accomplish, though, because of two reasons. First, the amount and format of the data can be overwhelming to a human, requiring some kind of automated processing. The second reason is relevant only if the new IGP is a distance-vector protocol, that is, either RIP or EIGRP. These protocols advertise a learned route only if it is also installed in the routing table by the same protocol. This additional advertisement logic in distance-vector routing protocols is based on the fact that a router should not advertise a route it is not using itself. Because the AD of the new IGP has been configured to be higher than the current IGP’s AD, routes learned by the new IGP will not be placed into the router’s routing table as long as the current IGP is still running on the router, and hence will not be advertised further. As a result, if the new IGP is RIP or EIGRP, its working databases will contain only partial contents until the migration starts, making the verification before migration impossible. This behavior of distance-vector IGPs will be discussed in closer detail later in the chapter. Note that this additional advertisement logic does not apply to link-state IGPs such as OSPF and IS-IS, as the nature of routing information they generate and the flooding mechanism are strongly different from distance-vector IGPs and do not allow for such additional checks.

Deactivating Current IGP

The next step in the routing protocol migration involves the actual removal of the current IGP from a contiguous set of routers, one router at a time, allowing the new routing protocol to populate the routing table instead, and then proceeding to the next router. Alternatively, instead of plainly deleting the current IGP configuration from the router, it can be configured using the `passive-interface default` command that will effectively shut it down. In recent IOS versions, selected routing protocols even support the `protocol shutdown` or `shutdown` command. The obvious advantage of this approach is that the configuration of the current IGP is preserved, should it ever be necessary to activate it again quickly.

The removal or deactivation of the current IGP should be done in such a way that the network always consists of at most two regions. In one, both routing protocols are run...
(the unmigrated part of network), and in the other, only the new protocol is running (the migrated part of the network) and both regions are contiguous.

During a properly executed migration, the network consists of a contiguous region that runs both IGPs and of a contiguous region that runs the new IGP only. Traffic crossing the network enters either an unmigrated or a migrated router, and is destined to a network that is directly connected to a router that is again either migrated or unmigrated yet. These options have an impact on which IGPs carry the information about the destination and thus what source of routing information is used by routers along the way.

If traffic enters an unmigrated router and is destined to a network connected to an unmigrated router, the destination network is advertised in both IGPs but the new IGP has been configured with a higher AD, so it has no impact on the routing table contents. Consequently, the traffic completely follows the path provided by the current IGP, as if no migration was taking place.

If traffic enters a migrated router and is destined to a network connected to a migrated router, the destination network is advertised only in the new IGP, as the current IGP has been removed from the destination router. The current IGP does not advertise this network anymore and does not compete about this particular network with the new IGP (recall that it would otherwise be resolved in favor of the current IGP thanks to its lower AD). Consequently, all routers, both migrated and unmigrated, know about this destination only through the new IGP, and follow the path provided by the new IGP.

If traffic enters an unmigrated router and is destined to a network connected to a migrated router, the situation is very similar. As the current IGP has been removed from the destination router, the destination network is advertised only in the new IGP. All routers therefore know about this network through the new IGP only and follow the path provided by the new IGP.

Finally, if traffic enters a migrated router and is destined to a network connected to an unmigrated router, the situation is slightly more complex. The destination router advertises the network through both IGPs. Other unmigrated routers know the destination network through both IGPs and prefer the current IGP, while migrated routers, including the ingress router, know the network through the new IGP only. In the migrated path of the network, the traffic will be routed according to the new IGP until it is forwarded to the first unmigrated router. Starting with this router, all other routers on the path toward the destination still prefer the path provided by the current IGP. Therefore, beginning with this router, the traffic will be routed according to the current IGP.

This analysis shows that during a properly executed migration, the network remains fully connected and destinations should remain fully reachable. Transient outages can occur at the moment when the current IGP is removed from a router, as the routes provided by the current IGP will need to be flushed from the routing table and replaced by routes learned through the new IGP.
Removing New IGP’s Temporary Settings

After the network has been completely migrated to the new IGP and the previous IGP has been completely removed from all routers, the new IGP still contains temporary settings that were necessary for a seamless migration, especially the modified AD values, leftovers from redistribution of the previous IGP into the new IGP, and so on. These settings should be removed as the last step of the migration procedure. In link-state routing protocols, removing the temporary settings should not cause any additional interruptions in network service. However, in EIGRP, modifying the AD values causes the router to drop and reestablish its EIGRP adjacencies with neighboring routers, causing a transient disruption in network connectivity. These changes must therefore be also performed during a maintenance window.

Specifics of Distance-Vector Protocols in IGP Migration

Ideally, migrating to a different routing protocol should not involve any route redistribution between the current and the new IGP, as the redistribution involves additional complexity to the migration process. However, if the new IGP is a distance-vector protocol (such as RIP or EIGRP), a temporary redistribution is inevitable. The reason lies in the advertisement logic of these routing protocols: A learned route will be advertised further only if the router has placed that very learned route into the routing table as well. In other words, a learned route is advertised through the same routing protocol only if the router is using that route itself. As the migration process involves temporarily configuring the new IGP’s administrative distance (AD) to be higher than the AD of the current IGP, none of the learned routes through the new IGP are going to be placed into the routing table if the current IGP is still running. If the new IGP happens to be RIP or EIGRP, any route learned through that protocol won’t make it into the router’s routing table and will not be advertised further as a result. To illustrate this concept, consider the network in Figure 6-9 (split horizon rules in EIGRP have been omitted for simplicity).
OSPF is the current routing protocol in this network, and the network is planned to be migrated to EIGRP. All four routers are therefore configured with EIGRP as well, the EIGRP AD is set to 210 for internal and 220 for external routes, and all interfaces are added to EIGRP on all routers. OSPF’s operation is not influenced in any way, and because its AD remains at 110, routers still keep OSPF-learned routes in their routing table. If we focus on R1's operation and on the 10.1.0.0/24 network in particular, R1 advertises its directly connected networks, including 10.1.0.0/24 to R2 through EIGRP. R2 will have this route in its EIGRP topology table but will be unable to install it into the routing table because of EIGRP’s modified AD of 210. As a result, R2 will not propagate the EIGRP-learned route 10.1.0.0/24 through EIGRP to R3, so neither R3 nor R4 will learn about this network through EIGRP. This limited propagation of networks in EIGRP will take place on each router in this topology: Each router will advertise its directly connected networks in EIGRP to its immediate neighbors, but these neighbors are prevented from advertising them further, as shown in Figure 6-9. Looking into EIGRP topology tables of all routers confirms this, as shown in Example 6-6.

**Example 6-6  Contents of EIGRP Topology Tables in Figure 6-9 Topology**

```plaintext
! On all routers in the topology from Figure 6-9, EIGRP is configured identically:

```

```plaintext
c
router eigrp 1
network 10.0.0.0
distance eigrp 210 220
no auto-summary
```

! It is assumed that OSPF is also running on all four routers.

! show ip eigrp topology on R1:

```
R1# show ip eigrp topology

IP-EIGRP Topology Table for AS(1)/ID(10.12.0.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 10.12.0.0/24, 1 successors, FD is 832000
   via Connected, Serial0/0/0
P 10.2.0.0/24, 0 successors, FD is Inaccessible
   via 10.12.0.2 (857600/281600), Serial0/0/0
P 10.1.0.0/24, 1 successors, FD is 281600
   via Connected, FastEthernet0/0
P 10.23.0.0/24, 0 successors, FD is Inaccessible
   via 10.12.0.2 (1344000/832000), Serial0/0/0

! show ip eigrp topology on R2:

```

```plaintext
R2# show ip eigrp topology
```
```
### IP-EIGRP Topology Table for AS(1)/ID(10.23.0.2)

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Successors</th>
<th>FD</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.12.0.0/24</td>
<td>1</td>
<td>832000</td>
<td>Connected, Serial0/0/1</td>
</tr>
<tr>
<td>10.2.0.0/24</td>
<td>1</td>
<td>281600</td>
<td>Connected, FastEthernet0/0</td>
</tr>
<tr>
<td>10.3.0.0/24</td>
<td>0</td>
<td>Inaccessible</td>
<td>10.23.0.3, Serial0/0/0 (857600/281600)</td>
</tr>
<tr>
<td>10.1.0.0/24</td>
<td>0</td>
<td>Inaccessible</td>
<td>10.12.0.1, Serial0/0/1 (857600/281600)</td>
</tr>
<tr>
<td>10.23.0.0/24</td>
<td>1</td>
<td>832000</td>
<td>Connected, Serial0/0/1</td>
</tr>
<tr>
<td>10.34.0.0/24</td>
<td>0</td>
<td>Inaccessible</td>
<td>10.23.0.3, Serial0/0/0 (1344000/832000)</td>
</tr>
</tbody>
</table>

```
! show ip eigrp topology on R3:
```

**R3# show ip eigrp topology**

### IP-EIGRP Topology Table for AS(1)/ID(10.34.0.3)

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Successors</th>
<th>FD</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.12.0.0/24</td>
<td>0</td>
<td>Inaccessible</td>
<td>10.23.0.2, Serial0/0/1 (1344000/832000)</td>
</tr>
<tr>
<td>10.2.0.0/24</td>
<td>0</td>
<td>Inaccessible</td>
<td>10.23.0.2, Serial0/0/1 (857600/281600)</td>
</tr>
<tr>
<td>10.3.0.0/24</td>
<td>1</td>
<td>281600</td>
<td>Connected, FastEthernet0/0</td>
</tr>
<tr>
<td>10.4.0.0/24</td>
<td>0</td>
<td>Inaccessible</td>
<td>10.34.0.4, Serial0/0/0 (857600/281600)</td>
</tr>
<tr>
<td>10.23.0.0/24</td>
<td>1</td>
<td>832000</td>
<td>Connected, Serial0/0/1</td>
</tr>
<tr>
<td>10.34.0.0/24</td>
<td>1</td>
<td>832000</td>
<td>Connected, Serial0/0/0</td>
</tr>
</tbody>
</table>

```
! show ip eigrp topology on R4:
```

**R4# show ip eigrp topology**

### IP-EIGRP Topology Table for AS(1)/ID(10.34.0.4)

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Successors</th>
<th>FD</th>
<th>Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.12.0.0/24</td>
<td>0</td>
<td>Inaccessible</td>
<td>10.23.0.2 (1344000/832000)</td>
</tr>
<tr>
<td>10.2.0.0/24</td>
<td>0</td>
<td>Inaccessible</td>
<td>10.34.0.4 (857600/281600)</td>
</tr>
<tr>
<td>10.3.0.0/24</td>
<td>1</td>
<td>281600</td>
<td>Connected, FastEthernet0/0</td>
</tr>
<tr>
<td>10.4.0.0/24</td>
<td>0</td>
<td>Inaccessible</td>
<td>10.34.0.4 (857600/281600)</td>
</tr>
<tr>
<td>10.23.0.0/24</td>
<td>1</td>
<td>832000</td>
<td>Connected, Serial0/0/1</td>
</tr>
<tr>
<td>10.34.0.0/24</td>
<td>1</td>
<td>832000</td>
<td>Connected, Serial0/0/0</td>
</tr>
</tbody>
</table>
Note that on each router, only directly connected networks of its immediate neighbors are learned through EIGRP, and all these networks are marked with a “0 successors, FD is Inaccessible” indication in their heading, preventing them from being advertised further.

After OSPF is removed from R4’s configuration as a step in the migration procedure, the OSPF-learned 10.1.0.0/24 will be removed from R4’s routing table without being replaced by an EIGRP-learned route, as R2 is still running OSPF and does not advertise this route through EIGRP. This will cause connectivity outages: R4 will learn only about directly connected networks from R3 through EIGRP, missing all other networks, and R3—still running OSPF—will be unable to forward EIGRP-learned routes from R4 back to R2. Clearly, full connectivity in this network will be restored only after OSPF is completely removed.

The solution to this problem is to configure route redistribution from the current IGP into the new IGP on each router in the topology. In the example network, the situation will be significantly different, then: Because each router knows about all networks through OSPF, redistributing them from OSPF into EIGRP allows each router to advertise them all to each directly connected neighbor. While the neighbor will not be allowed to advertise them further if still running OSPF, its EIGRP topology database will nonetheless be populated with the full set of networks from its own neighbors. When OSPF is deactivated on a router, EIGRP-learned routes will take over—they will get installed into the routing table, and the router will be able to forward them further.

If the new IGP is a link-state protocol, this redistribution is unnecessary and shall not be configured. Flooding of topological information in link-state protocols is not constrained by routing table contents. Routers will always flood the routing information in a link-state protocol, regardless of whether routes derived from that information are installed into routing tables or not.

To analyze how this approach works, assume that the migration of the network in Figure 6-9 continues by gradual deactivation of OSPF, starting on R4 and proceeding router by router toward R1. Table 6-5 summarizes how the individual networks are visible in the routing tables of individual routers. Only the first two octets of each prefix are listed for brevity. Prefixes in the O row are learned by OSPF; prefixes in the D row are learned by EIGRP. Directly connected networks are not listed, as they are not influenced by changes in routing protocols.
<table>
<thead>
<tr>
<th>OSPF Run On</th>
<th>R1</th>
<th>R2</th>
<th>R3</th>
<th>R4</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1 to R4</td>
<td>O</td>
<td>10.2/24</td>
<td>10.1/24</td>
<td>10.1/24</td>
</tr>
<tr>
<td></td>
<td>10.23/24</td>
<td>10.3/24</td>
<td>10.12/24</td>
<td>10.12/24</td>
</tr>
<tr>
<td></td>
<td>10.3/24</td>
<td>10.34/24</td>
<td>10.2/24</td>
<td>10.2/24</td>
</tr>
<tr>
<td></td>
<td>10.34/24</td>
<td>10.4/24</td>
<td>10.4/24</td>
<td>10.23/24</td>
</tr>
<tr>
<td></td>
<td>10.4/24</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>D</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>R1 to R3</td>
<td>O</td>
<td>10.2/24</td>
<td>10.1/24</td>
<td>10.1/24</td>
</tr>
<tr>
<td></td>
<td>10.23/24</td>
<td>10.3/24</td>
<td>10.12/24</td>
<td>10.12/24</td>
</tr>
<tr>
<td></td>
<td>10.3/24</td>
<td>10.34/24</td>
<td>10.2/24</td>
<td>10.2/24</td>
</tr>
<tr>
<td></td>
<td>10.34/24</td>
<td>10.4/24</td>
<td>10.4/24</td>
<td>10.23/24</td>
</tr>
<tr>
<td></td>
<td>D</td>
<td>10.4/24</td>
<td>10.4/24</td>
<td>10.4/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.12/24 (EX)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.2/24 (EX)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.23/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.3/24</td>
</tr>
<tr>
<td>R1 to R2</td>
<td>O</td>
<td>10.2/24</td>
<td>10.1/24</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>10.23/24</td>
<td>10.1/24</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>D</td>
<td>10.3/24</td>
<td>10.3/24</td>
<td>10.1/24 (EX)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.34/24</td>
<td>10.34/24</td>
<td>10.12/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.4/24</td>
<td>10.4/24</td>
<td>10.2/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.4/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>R1 only</td>
<td>O</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>D</td>
<td>10.2/24</td>
<td>10.1/24</td>
<td>10.1/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.23/24</td>
<td>10.3/24</td>
<td>10.12/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.3/24</td>
<td>10.34/24</td>
<td>10.2/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.34/24</td>
<td>10.4/24</td>
<td>10.4/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10.4/24</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>
Key observations about this table are as follows:

- Prefixes advertised from routers running both the original and new routing protocol are learned by the original routing protocol on all routers still running it.
- Prefixes advertised from routers running only the new routing protocol are learned by the new routing protocol across the entire network.
- At all times, all routers know about all prefixes.
- Traffic entering a router running both routing protocols and destined to a network on a router running both protocols is routed completely according to the original routing protocol without changes. This is because the network is advertised in both protocols and the new routing protocol's AD has been intentionally raised above the original protocol's AD.
- Traffic entering a router running the new routing protocol and destined to a network on a router running both protocols is routed completely according to the new routing protocol. This is because the network in question is not injected into the original routing protocol anymore, so the only source of the information is the new protocol.
- Traffic entering a router running both routing protocols and destined to a network on a router running the new routing protocol is routed completely according to the new routing protocol. The reason is the same as in the previous item.
- Traffic entering a router running the new routing protocol and destined to a network on a router running both routing protocols will be routed according to the new routing protocol until it hits the first router that still runs both routing protocols. Afterward, it will be routed according to the original routing protocol. This is because in the migrated part of the network, routers run only the new routing protocol, while in the remaining part of network running both protocols, the original routing protocol is preferred.

The last four items are valid if the migration is performed in such a way that the network always consists of at most two contiguous regions. In one, both routing protocols are run (the unmigrated part of network), and in the other, only the new protocol is running (the migrated part of the network). Also, if this rule is maintained throughout the migration process, the boundary between the new and original routing protocol as described in the last item is crossed only once.
Foundation Summary

This section lists additional details and facts to round out the coverage of the topics in this chapter. Unlike most of the Cisco Press Exam Certification Guides, this “Foundation Summary” does not repeat information presented in the “Foundation Topics” section of the chapter. Please take the time to read and study the details in the “Foundation Topics” section of the chapter, as well as review items noted with a Key Topic icon.

Table 6-6 lists the protocols mentioned in or pertinent to this chapter and their respective standards documents.

<table>
<thead>
<tr>
<th>Name</th>
<th>Standardized In</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Resolution Protocol (ARP)</td>
<td>RFC 826</td>
</tr>
<tr>
<td>IPv6 Neighbor Discovery</td>
<td>RFC 4861, RFC 5942</td>
</tr>
<tr>
<td>Differentiated Services Code Point (DSCP)</td>
<td>RFC 2474</td>
</tr>
</tbody>
</table>

Table 6-7 lists some of the key IOS commands related to the topics in this chapter. (The command syntax for switch commands was taken from the Catalyst 3560 Multilayer Switch Command Reference, 15.0(2)SE. Router-specific commands were taken from the IOS Release 15 mainline Command Reference.)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip arp</td>
<td>EXEC command that displays the contents of the IP ARP cache.</td>
</tr>
<tr>
<td>show ipv6 neighbors</td>
<td>EXEC command that displays the contents of the IPv6 neighbor cache.</td>
</tr>
<tr>
<td>[no] switchport</td>
<td>Switch interface subcommand that toggles an interface between a Layer 2 switched function (switchport) and a routed port (no switchport).</td>
</tr>
<tr>
<td>[no] ip route-cache cef</td>
<td>Interface subcommand that enables or disables CEF switching on an interface.</td>
</tr>
<tr>
<td>[no] ip cef</td>
<td>Global configuration command to enable (or disable) CEF on all interfaces.</td>
</tr>
<tr>
<td>[no] ipv6 cef</td>
<td>Global configuration command to enable (or disable) CEF for IPv6 on all interfaces. For IPv6 CEF to be activated, ip cef must also be present.</td>
</tr>
</tbody>
</table>
Command | Description
--- | ---
`[no] ip routing` | Enables IP routing; defaults to `no ip routing` and `no ipv6 unicast-routing` on a multilayer switch.
`[no] ipv6 unicast-routing` | 
`ip policy route-map map-tag` | Router interface subcommand that enables policy routing for the packets entering the interface.
`ipv6 policy route-map map-tag` |  

Refer to Table 6-4 for the list of set commands related to policy routing.

**Memory Builders**

The CCIE Routing and Switching written exam, like all Cisco CCIE written exams, covers a fairly broad set of topics. This section provides some basic tools to help you exercise your memory about some of the broader topics covered in this chapter.

**Fill In Key Tables from Memory**

Appendix E, “Key Tables for CCIE Study,” on the CD in the back of this book, contains empty sets of some of the key summary tables in each chapter. Print Appendix E, refer to this chapter’s tables in it, and fill in the tables from memory. Refer to Appendix F, “Solutions for Key Tables for CCIE Study,” on the CD to check your answers.

**Definitions**

Next, take a few moments to write down the definitions for the following terms:

- policy routing, process switching, CEF, polarization, MLS, ARP, Proxy ARP, routed interface, fast switching, TTL, RIB, FIB, adjacency table, control plane, switched interface, data plane, IP routing, IP forwarding

Refer to the glossary to check your answers.

**Further Reading**


Details on implementing and troubleshooting static routing can be found in numerous documents on the Cisco website. Recommended documents include "Specifying a Next Hop IP Address for Static Routes" (Document ID 27082), "Route Selection in Cisco Routers" (Document ID 8651), and "IOS Configuration Guide," in particular, the "IP Routing: Protocol-Independent Configuration Guide" section.
This page intentionally left blank
Index

Numerics

2-Way state, OSPF routers, 463
802.1d STP. See STP (Spanning Tree Protocol)
802.1Q trunking, 69-70
    configuring, 71-75
802.1Q-in-Q tunneling, 79-83
802.1s. See MST (Multiple Spanning Trees)
802.1w RSTP. See RSTP (Rapid STP)

A

ABRs (Area Border Routers), 480
    best path selection, 502-505
access ports, protecting
    BPDU Filter, 150-151
    BPDU Guard, 149-150
accessing Cisco IOS routers and switches
    HTTPS access, implementing, 257-258
    SSH access, implementing, 258
    Telnet access, implementing, 258
ACK packets (EIGRP), 372-373
Acknowledgment field, EIGRP packets, 369
Active state (EIGRP), 381
active switches (VSS), 30
active VLANs, 76
Add-Path support (EIGRP), 421-423
Address Family configuration mode, 414-415
address family support, OSPFv3, 548-551
addresses, Ethernet, 15-18
    format, 17-18
    most significant byte, 17
adjacencies, IS-IS, 578-579, 587
Adjacency State TLV, 589-591
adjusting
    administrative distance (EIGRP), 360
    EIGRP hop-count limitations, 359
administrative distance, 644
    EIGRP, adjusting, 360
    preventing suboptimal routes, 656-659
advertising default routes, 665-672
    using default-information originate command, 669
    using ip default-network command, 670-671
    using redistribute static command, 667-668
AFI (Authority and Format Identifier), 573-574
AFT (Address Family Translation), 220
agents (SNMP), 244
AH (Authentication Header), 546
alarms (RMON), 255
allowed VLANs, 76
Alternate Ports (RSTP), 130
anycast addresses, 216
architecture, CEF, 275-276
areas
ABRs, best path selection, 502-505
IS-IS
  inter-area routing, 598-600
  intra-area routing, 599
stubby areas, 496-501
  configuring, 498-501
  NSSA, 498-499
ARPs (Address Resolution Protocol), 232-233
ASBRs (Autonomous System Boundary Routers), 481
ATT flag (LSPs), 602-603
Attempt state, OSPF routers, 463
authentication
EIGRP, 356, 432-435
IS-IS, 608-610
key chains, 337
OSPF
  configuring, 517-520
  SHA-HMAC, configuring, 520-522
  on virtual links, configuring, 520
OSPFv3, 546-547
PFR, 674-675
RIPvng, 340
RIPv2, configuring, 337
SNMP, 245
automatic route summarization, 428
autonegotiation (Ethernet), 9
autosummarization, 335-337
AVG (Active Virtual Gateway), 239

B
bandwidth metric component, 361
basic configuration, SPAN, 26
BDRs (backup DRs), 469
best path selection, 317
  OSPF, 502-505
BGP (Border Gateway Protocol), 317
binary shortcuts
  exclusive summary routes, finding, 204-205
  finding all subnets of a network, 196-198
  inclusive summary routes, finding, 202-203
bitwise Boolean ANDs, 193
Blocking state (STP), 107
  transitioning to Forwarding state, 119
BOOTP (Bootstrap Protocol), 233-234
  comparing with DHCP and RARP, 236
border routers (PFR), 676-677
  configuring, 681-683
BPDU Filter, 150-151
BPDU Guard, 149-150
BPDUs (Bridge Protocol Data Units), 107-109
  Configuration BPDUs, 108
  Dispute mechanism, 154
  format, 107
  priorities, 108
  RBID, 109
  RSTP, 132-133
  Topology Change BPDUs, 108
BRAS (Broadband Remote Access Server), 96
Bridge Assurance, 154
  broadcast address, discovering, 195-196
  broadcast links, 587
  IS-IS over, 592-598
    DIS, election process, 592-593
    IS-IS router synchronization, 593-594
    pseudonodes, 594-598
  broadcast MAC addresses, 15
  broadcast networks, 473
  broadcast subnets, 192

Cabling
  Category 5, 8-9
  crossover, 8
  straight-through, 8
Calculating
  composite metric, 363-364
  OSPF cost, 508-509
CAM (Content Addressable Memory), updating, 117-119
Canonical bit order, 17
Category 5 wiring, 8-9
CD (Computed Distance), 386-387
CDP (Cisco Discovery Protocol), troubleshooting Layer 2 issues, 163-165
CEF (Cisco Express Forwarding), 273-285
  architecture, 275-276
  example of, 277-281
  FIB, 274
  load sharing, 282-285
    algorithms, 285
  lookup process, 274
  polarization, 284-285
  RIB, 274
  channel-group command, 33
  channel-protocol command, 161
  Checksum field, EIGRP packets, 369
  CIDR (classless interdomain routing), 206-207
  Cisco Catalyst switches, SPAN, 22-25
  Cisco Flexible NetFlow, 250-252
    configuring, 251-252
  Cisco IOS Embedded Event Manager, 253-254
  Cisco IOS IP SLA, 249-250
    configuring, 250
  Cisco Learning Network, 703
  Cisco switch ports, configuring, 11-14
  CIST (Common and Internal Spanning Tree), 140-141
  Class Metrics, 360-362
  classful addressing, 189-191
  classic mode (EIGRP), 410
  classic OSPF authentication, configuring, 517-520
  classless addressing, 191
  clear eigrp address-family command, 444
  clear ip ospf process command, 508-509
  clear ip route command, 444
Clearing
  IP routing table, 444
  OSPF process, 507-510
CLNP (ConnectionLess-mode Network Protocol), 572
Clusters, 247
configuring 717

collision domains, 10-11

command collisions, CSMA/CD, 10

commands

channel-group, 33
channel-protocol, 161
clear eigrp address-family, 444
clear ip ospf process, 508-509
clear ip route, 444
debug pppoe, 98
default-information originate, 669
distance, 658-659
distribute-list, 511-513
extended ping, 691-692
extended traceroute, 693-694
ip cef, 282
ip cef load-sharing algorithm, 285
ip default-network, 670-671
ip eigrp traffic, 371-372
ip ftp, 256
ip load-share, 283
is-is circuit-type, 618
network 0.0.0.0, 436
passive-interface, 431-432
pppoe session, 98
redistribute, 645
redistribute static command, 667-668
route-map, 638-640
router isis, 616
router process, 425-426
set commands (PBR), 296-299
show clns, 620-622
show interfaces, 167-169, 688-690
show ip ospf database, 488
show ip protocols, 426-427, 686-687
show ip route isis, 617
show ip route ospf, 516-517
show ip sla monitor statistics, 250
show isis database, 601-603
show isis hostname, 581-583
show rmon alarm, 255
show rmon event, 255
show running-config, 240-241
show sdm prefer, 299
switch convert mode virtual, 33-34
tftp-server, 257

communication rules for Private VLANs, 64-65

community VLANs, 61

community commands

configuring 717

complex configuration, SPAN, 26

complex configuration, SPAN, 26

component metrics, 360-361

bandwidth, 361
delay, 361-362
hop count, 363
influencing path selection with, 368
load, 362-363
MTU, 363
reliability, 362

component routes, 663

composite metric, calculating, 363-364

Conditional Receive, 375

Configuration BPDUs, 108-109

delay, 361-362

configuration files, copying with FTP, 256

delay, 361-362

configuring

802.1Q trunking, 71-75
Cisco Flexible NetFlow, 251-252
Cisco IOS Embedded Event Manager, 254
Cisco IOS IP SLA, 250
Cisco switch ports, 11-14
DHCP, 235-236
Dynamic NAT without PAT, 212-214

EIGRP
Add-Path feature, 422-423
authentication, 432-435
named mode, 410-417
OTP, 439-442
route summarization, 430-431
ERSPAN, 27-28
EtherChannel Port-channels, 157-161
HSRP, 237-238
IPv6
host addresses, 216-217
Stateless Address
Autoconfiguration, 217
IS-IS, 613-624
authentication, 608-610
ISL, 71-75
MLS, 291-295
MST, 144-148
NTP, 240-241
OSPF, 505-507
authentication, 517-520
incremental SPF, 527-528
LSA Throttling, 526-527
SPF Throttling, 524-525
stubby areas, 498-501
virtual links, 515-517
OSPFv3, 537-545
over Frame Relay, 537
PAT (Port Address Translation), 212-214
PFr (Performance Routing), 677
border routers, 681-683
MC, 677-681
PPPoE, 96-98
Private VLANs, 67-68
RIPv2, 334-339
authentication, 337
RMON, 255
route maps
match commands, 640-641
with route-map command, 638-640
ERSPAN, 26-27
SNMP, 245
SPAN
basic configuration, 26
complex configuration, 26
STP, 124-128
stub routing, 529-530
trunking
options, 76-77
on routers, 77-79
VLANs, 51-52
in configuration mode, 56-57
interfaces, 55-56
operational states, 57-69
VSS, 31-34
VTP, 89-95
extended-range VLANs, 94
global configuration options, 90-91
normal-range VLANs, 94
storing the configuration, 94-95
WCCP, 248-249
confirming Wide Metric support, 365-366
conflicts, 88
connection-mode operation (OSI), 572
connectionless-mode operation, OSI network layer, 572
content engines, WCCP, 246-249
contents of EIGRP topology table, 382-384
Control field (Ethernet), 15
control plane, 266
convergence
  RIPv2, 334
  steady-state operation, 327-328
timers for stalled routing update reception, 331-333
  triggered updates, 328-331
  STP, 115-117
copying
  configuration files with FTP, 256
  SCP, 257
costs
  OSPF, 507-510
  STP, 113
  Counting to Infinity, 322
  creating VLANs in VLAN database configuration mode, 52-55
crossover cabling, 8
CSMA/CD (Carrier Sense Multiple Access with Collision Detection), 10
CSNP (Complete Sequence Numbers PDU) packets, 585-586
CST (Common Spanning Tree), 120-124

D

data plane, 266
database exchange, OSPF
  DD packet exchange, 466-468
dead interval, 465
  DRs, 469
  Hello messages, 464-466
  LSAs
    requesting, 468-469
    sequence numbers, 468
  neighbor states, 462-464
  RIDs, 460-461
  transmitting LSA headers to neighbors, 466
  DBD (Database Description) messages, 461

  DD (Database Description) packet exchange, 466-468
dead interval (OSPF), 465
debug commands, troubleshooting Layer 3 issues, 694
debug pppoe command, 98
decimal shortcuts
  all subnets of a network, finding, 198-200
  broadcast address, finding, 195-196
  inclusive summary routes, finding, 203-204
  subnet number, finding, 194-196
default-information originate command, 669
default routing, 665-672
  EIGRP, 435-436
  using default-information originate command, 669
  using ip default-network command, 670-671
  using redistribute static command, 667-668
  using route summarization, 671-672
default settings for route redistribution, 646-649
delay metric component, 361-362
DES (Digital Encryption Standard), 245
designing OSPF networks, 496
  ABRs, 480
  ASBRs, 481
  path selection, 482
  Destination Service Access Point field (Ethernet), 15
DHCP (Dynamic Host Configuration Protocol), 233-236
configuring, 235-236
database agents, 235
DHCPv6, 217-218

diagnostic commands, IS-IS, 620-622
diffusing computation (EIGRP), 359, 392-396
Dijkstra SPF algorithm, 479
DIS (Designated IS), 579
election process, 592-593
discard routes, 429
Discarding state (RSTP), 129
displaying RID, 419-420
Dispute mechanism (BPDUs), 154
distance command, 658-659
distance-vector routing protocols, 316-317
best path selection, 317
Counting to Infinity, 322
EIGRP
ACK packets, 372-373
Add-Path support, 421-423
administrative distance, adjusting, 360
authentication, 432-435
bandwidth metric component, 361
clearing IP routing table, 444
composite metric, calculating, 363-364
default routing, 435-436
delay metric component, 361-362
diffusing computations, 359
DUAl, 359, 380-410
dynamic neighbor discovery, 376
event logging, 443
Feasibility Condition, 359
Graceful Shutdown, 432
Hello packets, 372
Hello protocol, 358
history of, 357
hop count metric component, 363
hop-count limitations, adjusting, 359
load metric component, 362-363
metrics, 360-361
neighbor table, 379
offset lists, 444
OTP, 437-442
packets, 368-374
passive interfaces, 431-432
Query packets, 374
reliability metric component, 362
Reply packets, 374
RID, 417-420
route filtering, 443-444
route summarization, 427-431, 664-665
router adjacencies, 376-379
RTP, 358, 374-376
Sequence number, 374
SIA-Query packets, 374
SIA-Reply packets, 374
Split Horizon, 436-437
stub routing, 423-427
topology table, 384-385
unequal-cost load balancing, 420-421
unreachable routes, 362
Update packets, 373
Wide Metrics, 364-368
migration strategy, 299-308
activating new IGP, 300-301
deactivating current IGPs, 301-303
verifying working database contents, 301
path-vector routing protocols, 317
RIPv2, 318-320
autosummarization, 335-337
configuring, 334-339
convergence, 334
distribute lists, 338-339
features, 318
Flushed after timer, 326
Holdown timer, 324-325
Invalid timer, 324-325
loop prevention, 320-326
messages, 319-320
metrics, 320
next-hop feature, 338
offset lists, 338
prefix lists, 338-339
Route Poisoning, 323
Split Horizon, 322, 338
steady-state convergence, 327-328
timers for stalled routing update reception, 331-333
triggered updates, 323, 328-331
distribute lists, 338-339
distribute-list command, 511-513
Down state, OSPF routers, 463
downloading practice exam, 702
DP (Designated Port), selecting, 113-115
draft-savage-eigrp, 356
DRs (designated routers)
on LANs, 469
election process, 471-472
optimizing, 470-471
on WANs, 472-474
DSCP (Differentiated Services Code Point), 251
DSP (Domain Specific Part), 573-574
DUAL (Diffusing Update Algorithm), 359, 380-410
FSM, 397-402
SIA states, 402-410
topology table, 380-384
dual stack, 218-219
duplex settings, 9
Dynamic NAT without PAT, 210-211
configuring, 212-214
dynamic neighbor discovery (EIGRP), 376
dynamic routing, 316-318

E

distribute lists, 338-339
distribute-list command, 511-513
Draft-savage-eigrp, 356
Dr (Designated Routers)
on LANs, 469
election process, 471-472
optimizing, 470-471
on WANs, 472-474
DSCP (Differentiated Services Code Point), 251
DSP (Domain Specific Part), 573-574
DUAL (Diffusing Update Algorithm), 359, 380-410
FSM, 397-402
SIA states, 402-410
topology table, 380-384
dual stack, 218-219
duplex settings, 9
Dynamic NAT without PAT, 210-211
configuring, 212-214
dynamic neighbor discovery (EIGRP), 376
dynamic routing, 316-318

edge routers, WCCP, 246-247
EIGRP (Enhanced Interior Gateway Routing Protocol)
Add-Path support, 421-423
administrative distance, adjusting, 360
authentication, 356, 432-435
Class Metrics, 362
default routing, 435-436
diffusing computations, 359
DUAL, 359, 380-410
SIA states, 402-410
topology table, 380-384
dynamic neighbor discovery, 376
event logging, 443
Feasibility Condition, 359
features, 356
Graceful Shutdown, 432
Hello protocol, 358
history of, 357
hop-count limitations, adjusting, 359
IP routing table, clearing, 444
LISP, 437-438
manual route summarization, 357
metrics, 360-361
bandwidth, 361
composite metric, calculating, 363-364
delay, 361-362
hop count, 363
influencing path selection with, 368
load, 362-363
MTU, 363
reliability, 362
Wide Metrics, 364-368
named mode, 410-417
Address Family configuration mode, 414-415
Per-AF Interface configuration mode, 415
Per-AF Topology configuration mode, 416-417
neighbor table, 379
offset lists, 444
open source implementation, 356
OTP, 437-442
configuring, 439-442
packets, 368-374
ACK packets, 372-373
format, 368-371
Hello packets, 372
Query packets, 374
Reply packets, 374
SIA-Query packets, 374
SIA-Reply packets, 374
TLVs, 369
Update packets, 373
passive interfaces, 431-432
RID, 417-420
displaying, 419-420
value selection, 419
route filtering, 443-444
route redistribution
into OSPF, 650
route summarization, 427-431, 664-665
automatic route summarization, 428
configuring, 430-431
discard routes, 429
manual route summarization, 428
route tags, 356
router adjacencies, 376-379
Hold time, 377
Pending state, 378
Q Cnt, 379
Up state, 378
RTP, 358, 374-376
Conditional Receive, 375
Sequence number, 374
Split Horizon, 436-437
stub routing, 423-427
Query handling, 424
topology table, 384-385
Active state, 381
CD, 386-387
contents of, 382-384
diffusing computation, 392-396
FD, 387-391
local computation, 392
Passive state, 381
RD, 386-387
show commands, 385-387
topology changes, 391-396
unequal-cost load balancing, 420-421
unreachable routes, 362
Wide Metrics
latency, 366
throughput, 366
election process
DISs, 592-593
DRs, 471-472
root switch, 110-111
Embedded Event Manager. See Cisco IOS Embedded Event Manager
enabling OSPFv3, 537-545
ERSPAN (Encapsulated Remote SPAN), 22-25
  configuring, 27-28
  restrictions, 24-25
  traffic supported, 25
ES (End System), 571
ESP (Encapsulating Security Payload), 546
EtherChannel, 154-161
  CSMA/CD, 10
  LACP, 159-161
  load balancing, 154-156
  MEC, 31
  PAgP, 159-161
  Port-channels, configuring, 157-161
  RJ-45 pinouts, 8-9
  switching loops, 159
  troubleshooting, 174-175
Ethernet, 3-2
  addresses, 15-18
    format, 17-18
    most significant byte, 17
  autonegotiation, 9
  Category 5 cabling, 8-9
  Cisco switch ports, configuring, 11-14
  collision domains, 10-11
  duplex settings, 9
  framing, 14-15
    Length field, 18
    Type field, 18
  header fields, 15
  hubs, 10
  PPPoE, configuring, 96-98
  SNAP headers, 14
  speed, 9
  switches, 11
    MAC address learning process, 19-22
  VSS, 28-38
    active and standby switches, 30
    configuring, 31-34
    MEC, 31
    verifying, 35-38
    VSL, 30
  event detectors, 253
  event logging
    Cisco IOS Embedded Event Manager, 253-254
    EIGRP, 443
    Syslog, 245-246
  events (RMON), 254
  examples
    of CEF operation, 277-281
    of OSPF over NBMA networks, 474-479
    of prefix lists, 643
    of RITE, 252
  exception dumps, sending with FTP, 256
  Exchange state, OSPF routers, 463
  exclusive summary routes, finding, 204-205
  ExStart state, OSPF routers, 463
  extended cryptographic OSPF authentication, configuring, 517-520
  Extended Local Circuit IDs, 587-589
  extended metrics (EIGRP), 366
  extended ping command, 691-692
  extended traceroute command, 693-694
  extended-range VLANs, configuring, 94
  external costs (MST), 140
  external interfaces, 674
  external routes (OSPF), 492-495
fast switching, 272-273
FD (Feasible Distance), 387-391
FDX (full duplex), 9
Feasibility Condition (EIGRP), 359
Feasible Successors
diffusing computation, 392-396
unequal-cost load balancing, 420-421
features
EIGRP, 356
of RIPv2, 318
of VTP, 84
FED (Forwarding Engine Driver), 40
FFM (Forwarding and Feature Manager), 40
FIB (Forwarding Information Base), 274
fields
of EIGRP packets, 368-371
of Ethernet headers, 15
filtering OSPF
route filtering, 510-513
Type 3 LSA filtering, 513-515
finding
all subnets of a network
binary shortcut, 196-198
decimal shortcut, 198-200
broadcast address, decimal shortcut, 195-196
exclusive summary routes, binary shortcut, 204-205
inclusive summary routes
binary shortcut, 202-203
decimal shortcut, 203-204
subnet number, decimal shortcut, 194-196
valid range of IP addresses, decimal shortcut, 194-196
Flags field, EIGRP packets, 369
flooding
double flooding, 469
LSAs, 469
LSPs, 591-592
flow exporters (NetFlow), 251
flow monitors (NetFlow), 251
flow samplers (NetFlow), 251
Flushed after timer, 326
format
of BPDUs, 107
of EIGRP packets, 368-371
of Ethernet addresses, 17-18
of IP addresses, 192
of IPv6 addresses, 215
of NSAP addresses, 574-575
Forwarding state (STP), 119
fragmentation, 214
LSPs, 581
Frame Relay, configuring OSPFv3 over, 537
framing, Ethernet, 14-15
Length field (Ethernet), 18
Type field, 18
FSM (DUAL Finite State Machine), 397-402
FTP (File Transfer Protocol), 255-256
Full state, OSPF routers, 464
G
Garcia-Luna-Aceves, Dr. J. J., 390
GLBP (Gateway Load Balancing Protocol), 239
global configuration options, VTP, 90-91
GR (Graceful Restart), 530-532
Graceful Shutdown, 432
OSPF, 532
OSPFv3, 552
**H**

HDX (half duplex), 9  
Hello messages (OSPF), 461, 464-466  
Hello packets  
  EIGRP, 372  
  IS-IS, 579-580  
  *authentication*, 608-610  
Hello protocol (EIGRP), 358  
history of EIGRP, 357  
HO-DSP (High-Order Domain Specific Part), 574  
Hold time, 377  
Holddown timer (RIPv2), 324-325  
hop count metric component, 363  
hop-count limitations (EIGRP), adjusting, 359  
host addresses (IPv6), configuring, 216-217  
HSRP (Hot Standby Router Protocol), 236-239  
  configuring, 237-238  
  MHSRP, 239  
HTTPS access, implementing, 257-258  
hub-and-spoke networks, stub routing, 425  
hubs (Ethernet), 10

**I**

IDI (Initial Domain Identifier), 573-574  
IDP (Initial Domain Part), 573  
IDSS (intrusion detection systems), RITE implementation, 252-253  
IETF Internet Drafts, draft-savage-eigrp, 356  
I/G (Individual/Group) bit, 17-18  
IGRP (Interior Gateway Routing Protocol), 357  
timers, 357-358  
Update packets, 357-358  
weaknesses of, 358  
IIH (IS-IS Hello) packets  
  Adjacency State TLV, 589-591  
  authentication, 608-610  
implementing  
  Cisco IOS IP SLA, 249-250  
  NetFlow, 250-252  
  RITE, 252-253  
  RMON, 254-255  
inclusive summary routes, finding  
  binary shortcut, 202-203  
  decimal shortcut, 203-204  
incremental SPF, 527-528  
inferior BPDUs, 108  
influencing route redistribution with metrics, 661-663  
Init state, OSPF routers, 463  
initiating FTP transfers, 256  
installing Pearson Cert Practice Test engine, 700-702  
Integrated IS-IS, 571  
inter-area routing (IS-IS), 598-600  
interface states (STP), 119  
interface subcommands, configuring OSPF, 518-520  
interfaces, creating on VLANs, 55-56  
internal interfaces, 674  
internal usage VLANs, 288-290  
internet networks, 191  
intra-area routing (IS-IS), 599  
Invalid timer (RIPv2), 324-325  
IOS-XE, 38-40  
IP addressing. *See also IPv6*  
  address format, 192  
  bitwise Boolean ANDs, 193  
  CIDR, 206-207
IP addressing

<table>
<thead>
<tr>
<th>Classful addressing</th>
<th>Classless addressing</th>
<th>Fragmentation</th>
<th>IP</th>
<th>NAT</th>
<th>Dynamic NAT without PAT</th>
<th>PAT</th>
<th>Static NAT</th>
<th>Private addressing</th>
<th>Route summarization</th>
<th>Subnetting</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dynamic NAT without PAT</td>
<td></td>
<td>Static NAT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>210-214</td>
<td></td>
<td>209-210</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PAT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Static NAT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>209-210</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Private addressing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>207</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Route summarization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>201-205</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Subnetting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>202-204</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TCP, 187-188
UDP, 188
VLSM, 200-201
ip cef command, 282
ip cef load-sharing algorithm command, 285
ip default-network command, 670-671
ip eigrp traffic command, 371-372
ip ftp command, 256
ip load-share command, 283
ip ospf process-id area area-id interface subcommand, 510

IP routing

CEF, 273-285
architecture, 275-276
example of, 277-281
FIB, 274
load sharing, 282-285
lookup process, 274
polarization, 284-285
RIB, 274
fast switching, 272-273
forwarding process, 271-272
MLS, 286-295
configuring, 291-295
Layer 3 interfaces, 291
logic, 286-287
Port-channels, 291
routed ports, 287-291
SVI, 286-287
PBR, 296-299
logic, 296
matching criteria, specifying, 296
SDM templates, 299
set commands, 296-299

IP routing table, clearing, 444
IP services
ARP, 232-233
BOOTT, 233-234
DHCP, 233-236
configuring, 235-236
database agents, 235
FTP, 255-256
GLBP, 239
HSRP, 236-239
HTTPS access, implementing, 257-258
MHSRP, 239
NTP, 240-241
Proxy ARP, 232-233
RARP, 233-234
SCP, 257
SNMP, 241-245
community, 242
configuring, 245
MIB, 242, 244
protocol messages, 243-244
RMON, 244
security, 245
Traps, 244
versions, 242
Syslog, 245-246
Telnet access, implementing, 258
VRPP, 239
WCCP, 246-249
IP SLA. See Cisco IOS IP SLA
IP Traffic Export. See RITE (Router IP Traffic Export)
IPCP (IP Configuration Protocol), 96
IPsec, OSPFv3 configuration, 546-547
IPv6, 214-220
  address format, 215
  address types, 216
  DHCPv6, 217-218
  fragmentation, 214
  host address, configuring, 216-217
  IS-IS support for, 610-613
  network prefix, 215-216
RIPng, 339-341
  authentication, 340
  messages, 339
Stateless Address Autoconfiguration, 217
stateless DHCPv6, 218
transition technologies, 218-220
IS-IS
  adjacencies, 578-579, 587
  areas, 598-608
    inter-area routing, 598-600
    intra-area routing, 599
  authentication, 608-610
  broadcast links, 587
  configuring, 613-624
diagnostic commands, 620-622
DIS, 579
IPv6 support, 610-613
link-state database in multiarea networks, 603-608
metrics, 577-578
NSAP addressing, 571
over broadcast links, 592-598
  DIS, election process, 592-593
  IS-IS router synchronization, 593-594
  pseudonodes, 594-598
over point-to-point links, 587-592
  Local Circuit IDs, 588
  three-way handshakes, 589-592
packets, 579-586
  CSNP packets, 585-586
  Hello packets, 579-580
  LSPs, 580-585
  PSNP packets, 585-586
System IDs, creating, 613
is-is circuit-type command, 618
ISL (Inter-Switch Link), 69-70
  configuring, 71-75
ISO OSI (International Standards Organization Open Systems Interconnection)
ES, 571
Extended Local Circuit IDs, 587-589
Level 0 routing, 576
Level 1 routing, 576
Level 2 routing, 576-577
Level 3 routing, 577
Local Circuit IDs, 587
network layer (OSI), modes of operation, 572
NSAP addressing, 573-576
  DSP, 574
  format, 574-575
  IDP, 573
NSEL, 574
SNPA, 576
Isolated PVLAN Trunks, 66-67
isolated VLANs, 61
IST (Internal Spanning Tree), 139-140
J-K

key chains, 337
K-values, 364

L

L4 port algorithm, 285
LACNIC (Latin American and Caribbean Internet Addresses Registry), 207
LACP (Link Aggregation Control Protocol), 159-161
LANs
DRs, 469
  election process, 471-472
  optimizing, 470-471
switch forwarding behavior, 19
Layer 2
frame rewrites, 273
troubleshooting, 161-169, 175-176
  with CDP, 163-165
  with LLDP, 165-167
  show interfaces command, 167-169
Layer 3
MLS interfaces, 291
troubleshooting, 695
debug commands, 694
extended ping command, 691-692
extended traceroute command, 693-694
show commands, 690-691
show interfaces command, 688-690
show ip interface command, 688-690
show ip protocols command, 686-687
Length field (Ethernet), 15, 18
Level 0 routing, 576
Level 1 routing, 576
Level 2 routing, 576-577
Level 3 routing, 577
Link Aggregation, 154-161
  load balancing, 154-156
link-state database (IS-IS) in multiarea networks, 603-608
link-state routing protocols, 317-318
IS-IS
  adjacencies, 578-579, 587
  broadcast links, 587
  DIS, 579
  IPv6 support, 610-613
  metrics, 577-578
  NSAP addressing, 571
  over broadcast links, 592-598
  over point-to-point links, 587-592
  packets, 579-586
  System IDs, creating, 613
migration strategy, 299-308
  activating new IGP, 300-301
  deactivating current IGPs, 301-303
  verifying working database contents, 301
OSPF, 464-466
  ABRs, 480
  ASBRs, 481
  best path selection, 502-505
  configuring, 505-507
  costs, 507-510
  DRs, 469
  external routes, 492-495
  GR, 530-532
  Graceful Shutdown, 532
  incremental SPF, 527-528
  LSA Throttling, 526-527
  messages, 461-462
  neighbor states, 462-464
  network types, 473
LSR (Link-State Request) messages  729

NSF, 530-532
over NBMA networks, 474-479
path selection, 482
prefix suppression (OSPF), 528-529
RIDs, 460-461
route summarization, 665
SPF calculation, 479
steady-state operation, 480
stub routers, configuring, 529-530
stubby areas, 496-501
transmitting LSA headers to neighbors, 466
TTL Security Check, 522-523
Type 1 LSAs, 484-488
Type 2 LSAs, 484-488
Type 3 LSAs, 488-492
Type 4 LSAs, 492-495
Type 5 LSAs, 492-495
LISP (Locator/Identifier Separation Protocol), 437-438
LLDP (Link Layer Discovery Protocol), troubleshooting Layer 2 issues, 165-167
load balancing
   EtherChannel, 154-156
   GLBP, 239
   methods for switching paths, 281
   PVST+, 119-124
   unequal-cost load balancing, 420-421
load metric component, 362-363
load sharing, CEF, 282-285
   algorithms, 285
Loading state, OSPF routers, 464
Local Circuit IDs, 587
local computation, 392
local interfaces, 674
logging
   EIGRP, 443
   Syslog, 245-246
logic
   MLS, 286-287
   PBR, 296
   of prefix lists, 642
   route maps, 638-640
lookup process, CEF, 274
Loop Guard, 259
loop prevention
   best path selection side effects on, 502-505
   RIPv2, 320-326
loopback networks, 473
LSA Throttling, 526-527
LSAck (Link-State Acknowledgment) messages, 461
LSAs
   comparing with LSPs, 584-585
   flooding, 469
   OSPFv3 types, 534-536
   pseudonodes, 485
   requesting, 468-469
   sequence numbers, 468
   transmitting headers to neighbors, 466
   Type 1 LSAs, 484-488
   Type 2 LSAs, 484-488
   Type 3 LSAs, 488-492
   Type 4 LSAs, 492-495
   Type 5 LSAs, 492-495
LSDBs (Link-State Databases), 481-482
LSPs (Link State Protocol Data Units), 580-585
   ATT flag, 602-603
   comparing with LSAs, 584-585
  flooding, 591-592
   fragmentation, 581
   O flag, 603
   Partition repair flag, 603
   Remaining Lifetime value, 581
   sequence numbers, 580-581
LSR (Link-State Request) messages, 461
M

MAC addresses, 15-18
  format, 17-18
  switch learning process, 19-22
managers (SNMP), 244
manual route summarization, 357, 428
master/slave relationship, DD packet exchange, 466-468
match commands for route maps, 640-641
matching criteria for PBR, specifying, 296
math used in subnetting, 192
MC (Master Controller), 675-676
  configuring, 677-681
measuring performance, Cisco IOS IP SLA, 249-250
MEC (Multichassis EtherChannel), 31
messages
  OSPF, 461-462
    Hello process, 464-466
  RIPng, 339
  RIPv2, 319-320
  SNMP protocol messages, 243-244
  VTP, 85-86
metrics
  EIGRP, 360-361
    bandwidth, 361
    composite metric, calculating, 363-364
    delay, 361-362
    extended metrics, 366
    hop count, 363
    influencing path selection with, 368
    load, 362-363
    MTU, 363
    reliability, 362
    Wide Metrics, 364-368
  IS-IS, 577-578
  RIPv2, 320
    route redistribution, influencing, 661-663
    setting for route redistribution, 649
    Wide Metrics, 365-368
      latency, 366
      support for, confirming, 365-366
MHSRP (Multiple HSRP), 239
MIB (Management Information Base), 242, 244
migration strategy for routing protocols, 299-308
  activating new IGP, 300-301
  deactivating current IGPs, 301-303
  distance-vector routing protocols, 303-308
  verifying working database contents, 301
MLS (Multilayer Switching), 286-295
  configuring, 291-295
  Layer 3 interfaces, 291
  logic, 286-287
  Port-channels, 291
  routed ports, 287-291
  SVI, 286-287
modifying VLAN operational states, 57-69
most significant byte, 17
MST (Multiple Spanning Trees), 137-148
  Bridge Assurance, 154
  CIST, 140-141
  configuring, 144-148
  external costs, 140
  interoperability with other STP versions, 141-144
  PortFast, 148-149
  principles of operation, 138-141
MTU metric component, 363
multiaccess links, IS-IS, 587
multicast
naïve reliable multicast, 375
reliable multicast, 374
multicast addresses, 216
multicast MAC addresses, 15
mutual redistribution at multiple routers, 654-656

N

naïve reliable multicast, 375
named mode (EIGRP), 410-417
Address Family configuration mode, 414-415
Per-AF Interface configuration mode, 415
Per-AF Topology configuration mode, 416-417
NAT (Network Address Translation), 207-208
Dynamic NAT without PAT, 210-211
PAT, 211-212
Static NAT, 209-210
NBMA networks, 473
OSPF over
  caveats, 474
  example, 474-479
OSPFv3 over, 536-537
neighbor states (OSPF), 462-464
neighbor table (EIGRP), 379
NetFlow
  configuring, 251-252
  implementing, 250-252
network 0.0.0.0 command, 436
network layer (OSI), modes of operation, 572
network prefix (IPv6), 215-216
network types, OSPF, 473
Next Multicast Sequence TLV, 375
next-hop feature (RIPv2), 338
Non-Edge Designated ports, 135
normal-range VLANs, configuring, 94
NSAP (Network Service Access Point)
  addressing, 571, 573-576
  DSP, 574
  format, 574-575
  IDP, 573
NSEL (NSAP Selector), 574
NSF (Non Stop Forwarding), 530-532
NSSAs (not-so-stubby areas), 498-499
NTP (Network Time Protocol), 240-241

O

O flag (LSPs), 603
offset lists, 338
offset lists (EIGRP), 444
Opcode field, EIGRP packets, 369
open source EIGRP implementation, 356
operating systems, IOS-XE, 38-40
operational roles, PfR, 675
operational states of VLANs, modifying, 57-69
optimizing
  DRs on LANs, 470-471
  STP with PortFast, 148-149
OSI (Open Systems Interconnection)
  ES, 571
  Extended Local Circuit IDs, 587-589
  IS-IS dependence on, 571
  Level 0 routing, 576
  Level 1 routing, 576
  Level 2 routing, 576-577
  Level 3 routing, 577
  Local Circuit IDs, 587
  network layer, modes of operation, 572
  NSAP addressing, 573-576
    DSP, 574
    format, 574-575
    IDP, 573
NSEL, 574
SNPA, 576
**OSPF. See also OSPFv3**
ABRs, 480
ASBRs, 481
authentication
  * classic OSPF authentication, configuring, 517-520
  * SHA-HMAC, configuring, 520-522
configuring, 505-507
costs, 507-510
database exchange
  * DD packet exchange, 466-468 LSAs, 468-469
  * transmitting LSA headers to neighbors, 466
dead interval, 465
dRs
  * on LANs, 469
  * optimizing, 470-471
  * on WANs, 472-474
dead routers, 492-495
filtering
  * route filtering, 510-513
  * Type 3 LSA filtering, 513-515
GR, 530-532
Graceful Shutdown, 532
incremental SPF, 527-528
LSAs
  * Type 1 LSAs, 484-488
  * Type 2 LSAs, 484-488
  * Type 3 LSAs, 488-492
  * Type 4 LSAs, 492-495
  * Type 5 LSAs, 492-495
messages, 461-462
  * Hello process, 464-466
neighbor states, 462-464
network types, 473
NSF, 530-532
versus OSPFv3, 533-534
over NBMA networks
  * caveats, 474
  * example of, 474-479
path selection
  * best path selection, 502-505
  * path choices not using cost, 502
performance tuning
  * LSA Throttling, 526-527
  * SPF Throttling, 524-525
prefix suppression, 528-529 RIDs, 460-461
route redistribution into EIGRP, 650
route summarization, 665
SPF calculation, 479
steady-state operation, 480
stub routers, configuring, 529-530
stubby areas, 496-501
TTL Security Check, 522-523
virtual links
  * authentication, configuring, 520
  * configuring, 515-517
**OSPFv3**
address family support, 548-551
authentication, 546-547
configuring, 537-545
Graceful Shutdown, 552
LSA types, 534-536
NBMA networks, 536-537
versus OSPFv2, 533-534
over Frame Relay, configuring, 537
SPI, 546
verifying configuration, 541-545
virtual links, 534
**OTP (Over the ToP), 437-442**
configuring, 439-442
LISP, 437-438
**OUI (Organizationally Unique Identifier)**
field, 15
P

packets. See also IP routing
EIGRP, 368-374. See also RTP (Reliable Transport Protocol)
   ACK packets, 372-373
   format, 368-371
   Hello packets, 372
   Query packets, 374
   Reply packets, 374
   SIA-Query packets, 374
   SIA-Reply packets, 374
   TLVs, 369
   Update packets, 373
forwarding process, 271-272
   fast switching, 272-273
IGRP, Update packets, 357-358
IS-IS, 579-586
   authentication, 608-610
   CSNP packets, 585-586
   Hello packets, 579-580
   LSPs, 580-585
   PSNP packets, 585-586
PAgP (Port Aggregation Protocol), 159-161
Partition repair flag (LSPs), 603
passive interfaces (EIGRP), 431-432
Passive state (EIGRP), 381
passive-interface command, 431-432
passwords, VTP, 87
PAT (Port Address Translation), 211-212
   configuring, 212-214
path selection
   influencing with interface metrics, 368
   OSPF, 482
      best path selection, 502-505
      path choices not using cost, 502
path-vector routing protocols, 317

PBR (Policy-Based Routing), 296-299
   logic, 296
   SDM templates, 299
   set commands, 296-299
   specifying matching criteria, 296
Pearson Cert Practice Test engine, 700-705
   installing, 700-702
   practice exam, downloading, 702
Pending state (EIGRP), 378
Per-AF Interface configuration mode (EIGRP), 415
Per-AF Topology configuration mode (EIGRP), 416-417
per-destination load sharing, 282-283
performance
   Cisco IOS IP SLA, 249-250
   OSPF
      LSA Throttling, 526-527
      SPF Throttling, 524-525
per-packet load sharing, 282
PfR (Performance Routing), 672-683
   authentication, 674-675
   configuring, 681-683
   configuring, 677
   operational roles, 675
   phases wheel, 673-674
   phases wheel (PfR), 673-674
PID (process ID), 465
pinouts, RJ-45, 8-9
point-to-multipoint networks, 473
point-to-multipoint nonbroadcast networks, 473
point-to-point links, IS-IS over, 587-592
  Local Circuit IDs, 588
  three-way handshakes, 589-592
point-to-point networks, 473
polarization, CEF, 284, 285
policy routing. See PBR (Policy-Based Routing)
Port-channels, 291
  configuring, 157-161
PortFast, 148-149
ports
  Cisco switch ports, configuring, 11-14
  promiscuous ports, 65
  routed ports, 287-291
RSTP, 128-131
  Alternate ports, 130
  Backup Ports, 130
  Non-Edge Designated ports, 135 roles, 129
  types, 131
VSL, configuring, 33
PPPoE (Point-to-Point Protocol over Ethernet), configuring, 96-98
pppoe session command, 98
practice exam, downloading, 702
Preamble field (Ethernet), 15
prefix lists, 338-339, 641-643
  examples, 643
  logic, 642
prefix suppression
  OSPF, 528-529
  OSPFv3, 552
prefixes, 191
Premium Edition of this book, 703
preparing for exam
  Cisco Learning Network, 703
  memory tables, 703
  Pearson Cert Practice Test engine, 700-705
preventing suboptimal routes
  setting administrative distance, 656-659
  using route tags, 659-661
primary servers, 88
principles of MST operation, 138-141
priorities, 108
private addressing, 207
Private VLANs, 60-68
  communication rules, 64-65
  configuring, 67-68
  Isolated PVLAN Trunks, 66-67
  secondary VLANs, 61-63
  tagging rules, 64
  on trunks, 65-67
  Promiscuous PVLAN Trunks, 66
promiscuous ports, 65
Promiscuous PVLAN Trunks, 66
Proposal/Agreement process (RSTP), 133-136
protocol messages (SNMP), 243-244
Proxy ARP, 232-233
pseudonodes, 485
  IS-IS, 594-598
PVST+ (Per VLAN Spanning Tree Plus), 119-124

Q

Q Cnt, 379
QoS (Quality of Service), evaluating
  with Cisco IOS IP SLA, 249-250
Quagga, 356
Query packets (EIGRP), 374
  handling by stub routers, 424
R

RARP (Reverse ARP), 233-234
comparing with BOOTP and DHCP, 236
RBID (Root Bridge ID), 109
RD (Reported Distance), 386-387
records (NetFlow), 251
redistribute command, 645
redistribute static command, 667-668
reliability metric component, 362
reliable multicast, 374
Remaining Lifetime value (LSPs), 581
Reply packets (EIGRP), 374
requesting LSAs, 468-469
resolving
Layer 2 issues, 175-176
Layer 3 issues, 695
restrictions of SPAN, 24-25
revision numbers, VTP, 86-87
RFC 1195, 571
RFC 6860, 528
RIB (Routing Information Base), 274, 368
RID (Router ID), 417-420
displaying, 419-420
OSPF, 460-461
value selection, 419
RIPng (RIP next generation), 339-341
authentication, 340
configuring, 340-341
messages, 339
RIPv1 (Routing Information Protocol version 1), 357
RIPv2 (Routing Information Protocol version 2), 318-320
authentication, configuring, 337
autosummarization, 335-337
configuring, 334-339
convergence, 334
steady-state operation, 327-328
timers for stalled routing update reception, 331-333
distribute lists, 338-339
features, 318
Flushed after timer, 326
Holddown timer, 324-325
Invalid timer, 324-325
loop prevention, 320-326
messages, 319-320
metrics, 320
next-hop feature, 338
offset lists, 338
prefix lists, 338-339
Route Poisoning, 323
Split Horizon, 322, 338
triggered updates, 323, 328-331
RITE (Router IP Traffic Export), 252-253
RMON (Remote Monitoring), 244, 254-255
alarms, 255
configuring, 255
events, 254
roles of RSTP ports, 129
Root Guard, 149
root switch, election process, 110-111
route filtering
EIGRP, 443-444
OSPF, 510-513
Type 3 LSA filtering, 513-515
route-map command, 638-640
route maps, 650-653
  configuring with route-map command, 638-640
  logic, 638-640
  match commands, 640-641
  set commands, 641
Route Poisoning, 323
route redistribution, 645-663
  EIGRP into OSPF, 650
  influencing with metrics, 661-663
  metrics, setting, 649
  mutual redistribution at multiple routers, 654-656
  OSPF into EIGRP, 650
  prefix lists, 641-643
  redistribute command, 645
  route maps, 638-640, 650-653
  set commands, 641
  suboptimal routes, 655-656
    preventing by setting administrative distance, 656-659
    preventing using route tags, 659-661
  using default settings, 646-649
route summarization, 201-205, 427-431, 663-665
  automatic route summarization, 428
  component routes, 663
  configuring, 430-431
  default routing, 671-672
  discard routes, 429
  EIGRP, 664-665
  exclusive summary routes, finding, 204-205
  manual route summarization, 428
  OSPF, 665
route tags, 356
  suboptimal routes, preventing, 659-661
routed ports, 287-291
router adjacencies (EIGRP), 376-379
  Hold time, 377
  Pending state, 378
  Q Cnt, 379
  Up state, 378
router isis command, 616
router process command, 425-426
routers
  configuring trunking on, 77-79
  implementing TFTP on, 256-257
routing loops (EIGRP), Feasibility Condition, 359
routing protocols, migration strategy, 299-308
  activating new IGP, 300-301
  deactivating current IGPs, 301-303
  distance-vector routing protocols, 303-308
  verifying working database contents, 301
“routing through a failure,” 531
RP (Root Port)
  selecting, 109, 111-113
RPC (Root Path Cost), 108
RPID (Receiver Port ID), 109
RPVST+ (Rapid Per-VLAN Spanning Tree Plus), 137
  Bridge Assurance, 154
RSPAN (Remote SPAN), 22-25
  configuring, 26-27
  restrictions, 24-25
  traffic supported, 25
RSTP (Rapid STP), 107, 128-137
  BPDUs, 132-133
  Discarding state, 129
  links, 131
  PortFast, 148-149
ports, 128-131

Alternate Ports, 130

Non-Edge Designated ports, 135

roles, 129
types, 131

proposal/agreement process, 133-136

RPVST+, 137
topology change handling, 136-137

RTO (retransmission timeout), 376

RTP (Reliable Transport Protocol), 358, 374-376

Conditional Receive, 375

RTR (Response Time Reporter). See Cisco IOS IP SLA

S

SAA (Service Assurance Agent). See Cisco IOS IP SLA

SBID (Sender Bridge ID), 108

SCP (Secure Copy Protocol), 257

SDM (Switch Database Management) templates, 299

secondary servers, 88

secondary VLANs, 61-63

security

authentication

EIGRP, 356, 432-435

IS-IS, 608-610

OSPF, 517-520

OSPFv3, 546-547

Pfr, 674-675

IDSs, RITE implementation, 252-253

as motivating factor in VLAN design, 60

SNMP, 245

VTP passwords, 87

selecting RPs, 109

sending exception dumps with FTP, 256

Sequence field, EIGRP packets, 369

sequence numbers, 374

LSAs, 468

LSPs, 580-581

Sequence TLV, 375

Set command (SNMP), 244

set commands

for PBR, 296-299

for route maps, 641

setting

administrative distance to prevent sub-optimal routes, 656-659

metrics for route redistribution, 649

SHA-HMAC (Secure Hash Algorithm Hash Message Authentication Code), OSPF configuration, 517-520

show clns command, 620-622

show interfaces command, 167-169, 688-690

show ip interface command, 167-169, 688-690

show ip ospf database command, 488

show ip protocols command, 426-427

troubleshooting Layer 3 issues, 686-687

show ip route isis command, 617

show ip route ospf command, 516-517

show ip sla monitor statistics command, 250

show isis database command, 601-603

show isis hostname command, 581-583

show rmon alarm command, 255

show rmon event command, 255

show running-config command, 240-241

show sdm prefer command, 299

SIA (Stuck-In-Active) states, 402-410

SIA-Query packets (EIGRP), 374

SIA-Reply packets (EIGRP), 374

slave/master relationship, DD packet exchange, 466-468

SLSM (static length subnet masking), 197, 200
SNAP (Sub-Network Access Protocol), 14
SNMP (Simple Network Management Protocol), 241-245
agents, 244
communities, 242
configuring, 245
managers, 244
MIBs, 242, 244
protocol messages, 243-244
RMON, 244
security, 245
Traps, 244
versions, 242
SNPA (Sub Network Point of Attachment), 576
Source Service Access Point field (Ethernet), 15
SPAN (Switch Port Analyzer), 22-25
configuring
   basic configuration, 26
   complex configuration, 26
restrictions, 24-25
traffic supported, 25
speed (Ethernet), 9
speed interface subcommand, 9
SPF Throttling, tuning OSPF performance with, 524-525
SPI (Security Parameter Index), 546
SPID (Sender Port ID), 109
Split Horizon, 322, 338, 436-437
Split Horizon with Poisoned Reverse, 321
spoke routers, stub routing, 423-427
SPs (service providers), Private VLANs, 60
SRTT (smooth round-trip time), 376
SSH (Secure Shell), 257-258
standby switches (VSS), 30
Start of Frame Delimiter field (Ethernet), 15
Stateless Address Autoconfiguration, 217
stateless DHCPv6, 218
Static NAT, 209-210
static routing, 316
steady-state convergence, RIPv2, 327-328
steady-state operation (OSPF), 480
storing VTP configuration, 94-95
STP (Spanning Tree Protocol)
   Blocking state, 107
   transitioning to Forwarding state, 119
BPDU Filter, 150-151
BPDU Guard, 149-150
BPDUs, 107-109
   RBID, 109
CAM, updating, 117-119
configuring, 124-128
converging to new topology, 115-117
costs, 113
CST, 120-124
DP, selecting, 113-115
interface states, 119
Loop Guard, 259
MST, 137-148
   CIST, 140-141
   configuring, 144-148
   external costs, 140
   interoperability with other STP versions, 141-144
   principles of operation, 138-141
PortFast, 148-149
PVST+, 119-124
root ports, selecting, 109
root switch, election process, 110-111
RP, selecting, 111-113
RSTP, 128-137
  BPDUs, 132-133
  Discarding state, 129
  links, 131
  ports, 128-131
Proposal/Agreement process, 133-136
RPVST+, 137
topology change handling, 136-137
System ID Extension, 111
TCN, 117-119
troubleshooting, 170
UDLD, 152-154
unidirectional links, 151-154
straight-through cabling, 8
stub routing, 423-427
  configuring, 529-530
  Query handling, 424
stubby areas, 496-501
  configuring, 498-501
subnet number, discovering, 194-196
subnetting, 188-205
  all subnets of a network, finding
    binary shortcut, 196-198
    decimal shortcut, 198-200
  bitwise Boolean ANDs, 193
  broadcast address, finding, 195-196
  broadcast subnets, 192
  classful addressing, 189-191
  classless addressing, 191
  math used in, 192
  subnet number, finding, 194-196
  valid range of IP addresses, finding, 194-196
  VLSM, 200-201
  zero subnets, 192
suboptimal routes, preventing
  setting administrative distance, 656-659
  using route tags, 659-661
summarization (EIGRP), 427-431
  automatic route summarization, 428
  configuring, 430-431
  discard routes, 429
  manual route summarization, 428
superior BPDUs, 108
SVI (switched virtual interfaces), 286-287
switch convert mode virtual command, 33-34
switches
  IOS-XE, 38-40
  MAC address learning process, 19-22
  SPAN, 22-25
  VLANs, 51
    Private VLANs, 60-68
  VSS, 28-38
switching loops (EtherChannel), 159
synchronization of IS-IS routers, 593-594
Syslog, 245-246
System ID Extension, 111
System IDs (IS-IS), creating, 613

T
tagging rules for Private VLANs, 64
TCN (Topology Change Notification), 117-119
TCP (Transport Control Protocol), 187-188
Telnet access, implementing, 258
TFTP (Trivial File Transfer Protocol) servers, implementing on routers, 256-257
tftp-server command, 257
three-way handshakes (IS-IS), 589-592
throughput metric, 366
timers
  Flushed after timer, 326
  Holdown timer, 324-325
  IGRP, 357-358
  Invalid timer, 324-325
TLVs (Type-Length-Values), 369-371
  Adjacency State TLV, 589-591
  Next Multicast Sequence TLV, 375
  Sequence TLV, 375
topologies
  changes in, RSTP handling of, 136-137
  STP convergence, 115-117
Topology Change BPDUs, 108-109
topology table, 384-385
  Active state, 381
  CD, 386-387
  contents of, 382-384
  diffusing computation, 392-396
DUAL
  FSM, 397-402
  SIA states, 402-410
FD, 387-391
Feasible Successors, unequal-cost load balancing, 420-421
local computation, 392
Passive state, 381
RD, 386-387
show commands, 385-387
topology changes, 391-396
transfers (FTP), initiating, 256
transition technologies for IPv6, 218-220
translation, IPv6, 220
Traps (SNMP), 244
triggered updates, 323, 328-331
troubleshooting
  EtherChannel, 174-175
  Layer 2 issues, 161-169
    with CDP, 163-165
    with LLDP, 165-167
    with show interfaces command, 167-169
  Layer 3 issues, 683-695
    debug commands, 694
    extended ping command, 691-692
    extended traceroute command, 693-694
    show commands, 690-691
    show interfaces command, 688-690
    show ip interface command, 688-690
    show ip protocols command, 686-687
  STP, 170
  trunking, 171-172
  VTP, 172-173
trunking
  802.1Q, 69-70
    configuring, 71-75
  802.1Q-in-Q tunneling, 79-83
  active VLANs, 76
  allowed VLANs, 76
  configuring
    options, 76-77
    on routers, 77-79
  ISL, 69-70
    configuring, 71-75
  Private VLANs, 65-67
    Isolated PVLAN Trunks, 66-67
    Promiscuous PVLAN Trunks, 66
troubleshooting, 171-172
  VTP, 83-95
    configuring, 89-95
    conflicts, 88
VLANs 741

V
valid range of IP addresses, finding, 194-196
value selection (RID), 419
vectors, 322
verifying
Cisco IOS IP SLA performance, 250
NetFlow configuration, 252
OSPFv3 configuration, 541-545
VSS, 35-38
Version field, EIGRP packets, 369
versions
of SNMP, 242
of VTP, 83-84
virtual links
OSPF
authentication, configuring, 520
configuring, 515-517
OSPFv3, 534
Virtual Router ID field, EIGRP packets, 369
VLAN database configuration mode
VLANs
creating, 52-55
interfaces, configuring, 55-56
VLANs, 51
configuring, 51-52
in configuration mode, 56-57
interfaces, configuring, 55-56
internal usage VLANs, 288-290
operational state, modifying, 57-69
Private VLANs, 60-68
configuring, 67-68
Isolated PVLAN Trunks, 66-67
Promiscuous PVLAN Trunks, 66
secondary VLANs, 61-63
tagging rules, 64
trunking, 65-67

U
UDLD (Unidirectional Link Detection), 152-154
UDP (User Datagram Protocol), 188
U/L (Universal/Local) bit, 17-18
unequal-cost load balancing, 420-421
unicast addresses, 216
unicast MAC addresses, 15
unidirectional links, 151-154
Universal ID, 284
universal load-sharing algorithm, 285
unreachable routes, 362
Up state (EIGRP), 378
Update packets (EIGRP), 373
Update packets (IGRP), 357-358
update process, VTP, 86-89
updates, EIGRP, 356
updating CAMs, 117-119

messages, 85-86
revision numbers, 86-87
storing the configuration, 94-95
update process, 86-87
versions of, 83-84
TTL Security Check, 522-523
tuning performance of OSPF
with LSA Throttling, 526-527
with SPF Throttling, 524-525
tunnel load-sharing algorithm, 285
tunneling
802.1Q-in-Q tunneling, 79-83
IPv6, 219-220
Txload, 363
Type field (Ethernet), 15, 18
types of LSAs, 482-496
trunking
  802.1Q, 69-75
  802.1Q-in-Q tunneling, 79-83
active VLANs, 76
allowed VLANs, 76
configuring, 76-79
ISL, 69-75
troubleshooting, 171-172
VTP
  configuring, 89-95
troubleshooting, 172-173
VLSM (variable-length subnet masking), 200-201
VPNs, OTP, 437-442
VRRP (Virtual Router Redundancy Protocol), 239
VSL (Virtual Switch Link), 30
VSS (Virtual Switch System), 28-38
  active switches, 30
  configuring, 31-34
  MEC, 31
  standby switches, 30
  verifying, 35-38
VSL, 30
  VTP (VLAN Trunking Protocol), 83-95
configuring, 89-95
  extended-range VLANs, 94
  global configuration options, 90-91
  normal-range VLANs, 94
  conflicts, 88
  passwords, 87
  revision numbers, 86-87
  storing the configuration, 94-95
  troubleshooting, 172-173
  versions of, 83-84
VTPv1
  messages, 85-86
  update process, 86-87
VTPv2
  messages, 85-86
  update process, 86-87
VTPv3, update process, 87-89

W

WANs, DRs, 472-474
WCCP (Web Cache Communication Protocol), 246-249
weaknesses of IGRP, 358
websites, Cisco Learning Network, 703
Wide Metrics, 360-361, 364-368
  latency, 366
  support for, confirming, 365-366
  throughput, 366
wiring, Category 5, 8-9

X-Y-Z

zero subnets, 192
Check out the NEW learning materials for v5.0 exam release!

Increase learning, comprehension, and certification readiness with these Cisco Press products!

Cisco CCIE Routing and Switching v5.0 Configuration Practice Labs
9780133786316

Cisco CCIE Routing and Switching v5.0 Troubleshooting Practice Labs
9780133786330

Cisco CCIE Routing and Switching v5.0 Configuration and Troubleshooting Practice Labs Bundle
9780133786323

Cisco CCIE Routing and Switching v5.0 Official Cert Guide, Volume 1
9781587143960

Cisco CCIE Routing and Switching v5.0 Official Cert Guide, Volume 2
9781587144912

Cisco CCIE Routing and Switching v5.0 Exam Roundup
9780789754035

SAVE ON ALL NEW CCIE R&S v5.0 Products
www.CiscoPress.com/CCIE