Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact international@pearsoned.com.

Feedback Information

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

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

We greatly appreciate your assistance.

Publisher: Paul Boger
Associate Publisher: Dave Dusthimer
Business Operation Manager, Cisco Press: Jan Cornelssen
Executive Editor: Brett Bartow
Managing Editor: Sandra Schroeder
Senior Development Editor: Christopher Cleveland
Senior Project Editor: Tonya Simpson
Copy Editor: John Edwards
Technical Editor(s): Dave Burns, Sean Wilkins
Editorial Assistant: Vanessa Evans
Cover Designer: Mark Shirar
Composition: Tricia Bronkella
Indexer: Tim Wright
Proofreader: Chuck Hutchinson
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.

Terry Vinson, CCIE No. 35347 (Routing and Switching, Data Center), is a seasoned instructor with nearly 25 years of experience teaching and writing technical courses and training materials. Terry has taught and developed training content, as well as provided technical consulting for high-end firms in the north Virginia/Washington, D.C. area. His technical expertise lies in the Cisco arena with a focus on all routing and switching technologies as well as the latest data center technologies, including Nexus switching, unified computing, and storage-area networking (SAN) technologies. Terry currently teaches for CCIE R&S and Data Center Bootcamps for Micronics Training, Inc. and enjoys sailing and game design in his “free time.”
About the Technical Reviewers

David Burns has in-depth knowledge of routing and switching technologies, network security, and mobility. He is currently a senior systems engineering manager for Cisco, leading the engineering team covering cable/MSO and content service providers in the United States. In July 2008, Dave joined Cisco as a lead systems engineer in several areas, including Femtocell, Datacenter, MTSO, and security architectures, working for a U.S.-based SP Mobility account. He came to Cisco from a large U.S.-based cable company, where he was a senior network and security design engineer. Dave held various roles before joining Cisco during his ten-plus years in the industry, working in SP operations, SP engineering, SP architecture, enterprise IT, and U.S. military intelligence communications engineering. He holds various sales and industry/Cisco technical certifications, including the CISSP, CCSP, CCDP, and two associate-level certifications. Dave recently passed the CCIE Security Written exam and is currently preparing for the CCIE Security Lab. Dave is a big advocate of knowledge transfer and sharing and has a passion for network technologies, especially as they relate to network security. Dave has been a speaker at Cisco Live on topics such as Femtocell (IP mobility) and IPS (security). Dave earned his Bachelor of Science degree in telecommunications engineering technology from Southern Polytechnic State University, Georgia, where he currently serves as a member of the Industry Advisory Board for the Computer & Electrical Engineering Technology School. Dave also earned a Master of Business Administration (MBA) degree from the University of Phoenix.

Sean Wilkins is an accomplished networking consultant for SR-W Consulting 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 degree 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 an Associate 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 his 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 Terry Vinson:
I would like to dedicate this book to my father, who has taught me many things in life and include the one thing I’ve tried to live by: “Never give up on your dreams. Hard work and diligence will see you through so long as you never give up.” So it is with all my love, respect, and admiration that I dedicate this to you.
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 to Mr. Brett Bartow for his patience with our constantly changing 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 Terry Vinson:

The opportunity to cooperate on the new edition of this book has been an honor and privilege beyond words for me. I have to thank Narbik for approaching me with the opportunity and for all his support and mentoring over the years. If it were not for him, I would not be where I am today. Additionally, I would like to thank all the fine people at Cisco Press for being so cool and understanding over the last few months. Among those people, I want to specifically thank Brett Bartow, whose patience has been almost infinite (yet I managed to tax it), David Burns, and Sean Wilkins for their incredible suggestions and devotion to making sure that I stayed on track. Last but not least among the Cisco Press crew there is Christopher Cleveland, who diligently nudged, kicked, and all-out shoved when necessary to see that things got done.

Personally, I need to thank my wife, Sheila. She has been the difference I was looking for in my life, the impetus to try to do more and to get up each day and try to make myself a better person, a better engineer, and a better instructor. Without her, I would not have the life I have come to love so much.

Finally, I want to thank my students and Micronics Training for giving me the opportunity to do what I enjoy every day. Thanks for all your questions, patience, and unbridled eagerness to learn. You guys are absolutely stellar examples of why this industry is like no other on the planet.
# Contents at a Glance

<table>
<thead>
<tr>
<th>Part</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part I</td>
<td>IP BGP Routing</td>
<td></td>
</tr>
<tr>
<td>Chapter 1</td>
<td>Fundamentals of BGP Operations</td>
<td>3</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>BGP Routing Policies</td>
<td>69</td>
</tr>
<tr>
<td>Part II</td>
<td>QoS</td>
<td></td>
</tr>
<tr>
<td>Chapter 3</td>
<td>Classification and Marking</td>
<td>135</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>Congestion Management and Avoidance</td>
<td>171</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>Shaping, Policing, and Link Fragmentation</td>
<td>207</td>
</tr>
<tr>
<td>Part III</td>
<td>Wide-Area Networks</td>
<td></td>
</tr>
<tr>
<td>Chapter 6</td>
<td>Wide-Area Networks</td>
<td>245</td>
</tr>
<tr>
<td>Part IV</td>
<td>IP Multicast</td>
<td></td>
</tr>
<tr>
<td>Chapter 7</td>
<td>Introduction to IP Multicasting</td>
<td>267</td>
</tr>
<tr>
<td>Chapter 8</td>
<td>IP Multicast Routing</td>
<td>317</td>
</tr>
<tr>
<td>Part V</td>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>Chapter 9</td>
<td>Device and Network Security</td>
<td>399</td>
</tr>
<tr>
<td>Chapter 10</td>
<td>Tunneling Technologies</td>
<td>483</td>
</tr>
<tr>
<td>Part VI</td>
<td>Multiprotocol Label Switching (MPLS)</td>
<td></td>
</tr>
<tr>
<td>Chapter 11</td>
<td>Multiprotocol Label Switching</td>
<td>515</td>
</tr>
<tr>
<td>Part VII</td>
<td>Final Preparation</td>
<td></td>
</tr>
<tr>
<td>Chapter 12</td>
<td>Final Preparation</td>
<td>573</td>
</tr>
</tbody>
</table>
Part VIII Appendixes

Appendix A Answers to the “Do I Know This Already?” Quizzes 579
Appendix B CCIE Exam Updates 583

Index 585

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

Glossary
Contents

Introduction xxvii

Part I IP BGP Routing

Chapter 1 Fundamentals of BGP Operations 3

“Do I Know This Already?” Quiz 3

Foundation Topics 8

Building BGP Neighbor Relationships 9

- Internal BGP Neighbors 10
- External BGP Neighbors 13

Checks Before Becoming BGP Neighbors 14

BGP Messages and Neighbor States 15

BGP Message Types 16

Purposefully Resetting BGP Peer Connections 16

Building the BGP Table 18

- Injecting Routes/Prefixes into the BGP Table 18
- BGP network Command 18

Redistributing from an IGP, Static, or Connected Route 21

Impact of Auto-Summary on Redistributed Routes and the network Command 23

Manual Summaries and the AS_PATH Path Attribute 25

Adding Default Routes to BGP 29

ORIGIN Path Attribute 30

Advertising BGP Routes to Neighbors 31

BGP Update Message 31

Determining the Contents of Updates 32

Example: Impact of the Decision Process and NEXT_HOP on BGP Updates 34

Summary of Rules for Routes Advertised in BGP Updates 40

Building the IP Routing Table 40

- Adding eBGP Routes to the IP Routing Table 40
- Backdoor Routes 41
- Adding iBGP Routes to the IP Routing Table 42

Using Sync and Redistributing Routes 44

Disabling Sync and Using BGP on All Routers in an AS 46

Confederations 47
Chapter 2  BGP Routing Policies  69

“Do I Know This Already?” Quiz  69

Foundation Topics  75

Route Filtering and Route Summarization  75
  Filtering BGP Updates Based on NLRI  76
  Route Map Rules for NLRI Filtering  79
  Soft Reconfiguration  79

Comparing BGP Prefix Lists, Distribute Lists, and Route Maps  80

Filtering Subnets of a Summary Using the aggregate-address Command  81

Filtering BGP Updates by Matching the AS_PATH PA  82

The BGP AS_PATH and AS_PATH Segment Types  82

Using Regular Expressions to Match AS_PATH  84

Example: Matching AS_PATHs Using AS_PATH Filters  87

Matching AS_SET and AS_CONFD_SEQ  91

BGP Path Attributes and the BGP Decision Process  93

Generic Terms and Characteristics of BGP PAs  93

The BGP Decision Process  95

Clarifications of the BGP Decision Process  96

Three Final Tiebreaker Steps in the BGP Decision Process  96

Adding Multiple BGP Routes to the IP Routing Table  97

Mnemonics for Memorizing the Decision Process  98

Configuring BGP Policies  99

Background: BGP PAs and Features Used by Routing Policies  99

Step 1: NEXT_HOP Reachable  101

Step 2: Administrative Weight  101

Step 3: Highest Local Preference (LOCAL_PREF)  104
Step 4: Choose Between Locally Injected Routes Based on ORIGIN PA 107
Step 5: Shortest AS_PATH 107
*Removing Private ASNs* 108
*AS_PATH Prepending and Route Aggregation* 109
Step 6: Best ORIGIN PA 112
Step 7: Smallest Multi-Exit Discriminator 112
*Configuring MED: Single Adjacent AS* 114
*Configuring MED: Multiple Adjacent Autonomous Systems* 115
*The Scope of MED* 115
Step 8: Prefer Neighbor Type eBGP over iBGP 116
Step 9: Smallest IGP Metric to the NEXT_HOP 116
The maximum-paths Command and BGP Decision Process
  *Tiebreakers* 116
Step 10: Lowest BGP Router ID of Advertising Router (with One Exception) 117
Step 11: Lowest Neighbor ID 117
*The BGP maximum-paths Command* 118
BGP Communities 119
  *Matching COMMUNITY with Community Lists* 123
  *Removing COMMUNITY Values* 124
  *Filtering NLRIs Using Special COMMUNITY Values* 125
Fast Convergence Enhancements 126
  *Fast External Neighbor Loss Detection* 127
  *Internal Neighbor Loss Detection* 127
  *EBGP Fast Session Deactivation* 128
Foundation Summary 129
Memory Builders 132
  *Fill In Key Tables from Memory* 133
  *Definitions* 133
  *Further Reading* 133

**Part II**  QoS

**Chapter 3**  Classification and Marking 135
*“Do I Know This Already?” Quiz* 135
Foundation Topics 139
Fields That Can Be Marked for QoS Purposes 139
  *IP Precedence and DSCP Compared* 139
Chapter 4  Congestion Management and Avoidance  171

“Do I Know This Already?” Quiz  171
Foundation Topics  175
Cisco Router Queuing Concepts  175
  Software Queues and Hardware Queues  175
  Queuing on Interfaces Versus Subinterfaces and Virtual Circuits  176
  Comparing Queuing Tools  176
Queuing Tools: CBWFQ and LLQ  177
  CBWFQ Basic Features and Configuration  178
  Defining and Limiting CBWFQ Bandwidth  180
  Low-Latency Queuing  182
  Defining and Limiting LLQ Bandwidth  184
  LLQ with More Than One Priority Queue  185
  Miscellaneous CBWFQ/LLQ Topics  186
Queuing Summary  186
Weighted Random Early Detection  187
  How WRED Weights Packets  188
  WRED Configuration  189
Modified Deficit Round-Robin  190
LAN Switch Congestion Management and Avoidance  193
  Cisco Switch Ingress Queuing  193
Creating a Priority Queue  193
Cisco 3560 Congestion Avoidance  195
Cisco 3560 Switch Egress Queuing  197
Resource Reservation Protocol (RSVP)  199
  RSVP Process Overview  200
  Configuring RSVP  201
  Using RSVP for Voice Calls  203
Foundation Summary  205
Memory Builders  205
  Fill In Key Tables from Memory  205
  Definitions  205
  Further Reading  205

Chapter 5  Shaping, Policing, and Link Fragmentation  207

“Do I Know This Already?” Quiz  207
Foundation Topics  211
Traffic-Shaping Concepts  211
Shaping Terminology 211
Shaping with an Excess Burst 213
Underlying Mechanics of Shaping 213
Generic Traffic Shaping 214
Class-Based Shaping 216
  Tuning Shaping for Voice Using LLQ and a Small Tc 218
  Configuring Shaping by Bandwidth Percent 221
  CB Shaping to a Peak Rate 222
  Adaptive Shaping 222
Policing Concepts and Configuration 222
  CB Policing Concepts 222
  Single-Rate, Two-Color Policing (One Bucket) 223
  Single-Rate, Three-Color Policer (Two Buckets) 224
  Two-Rate, Three-Color Policer (Two Buckets) 225
  Class-Based Policing Configuration 227
  Single-Rate, Three-Color Policing of All Traffic 227
Policing a Subset of the Traffic 228
CB Policing Defaults for Be and Be 229
Configuring Dual-Rate Policing 229
Multi-Action Policing 229
Policing by Percentage 230
Committed Access Rate 231
Hierarchical Queuing Framework (HQF) 233
  Flow-Based Fair-Queuing Support in Class-Default 235
  Default Queuing Implementation for Class-Default 236
  Class-Default and Bandwidth 236
  Default Queuing Implementation for Shape Class 236
  Policy Map and Interface Bandwidth 236
  Per-Flow Queue Limit in Fair Queue 236
  Oversubscription Support for Multiple Policies on Logical Interfaces 236
  Shaping on a GRE Tunnel 237
  Nested Policy and Reference Bandwidth for Child-Policy 237
  Handling Traffic Congestion on an Interface Configured with Policy Map 237
QoS Troubleshooting and Commands 237
  Troubleshooting Slow Application Response 238
  Troubleshooting Voice and Video Problems 239
Other QoS Troubleshooting Tips 240
Approaches to Resolving QoS Issues 240
Foundation Summary 242
Memory Builders 243
Fill In Key Tables from Memory 243
Definitions 243
Further Reading 243

Part III Wide-Area Networks

Chapter 6 Wide-Area Networks 245
“Do I Know This Already?” Quiz 245
Foundation Topics 247
Layer 2 Protocols 247
HDLC 247
Point-to-Point Protocol 249
PPP Link Control Protocol 250
Basic LCP/PPP Configuration 251
Multilink PPP 252
MLP Link Fragmentation and Interleaving 254
PPP Compression 255
PPP Layer 2 Payload Compression 256
Header Compression 256
PPPoE 257
Server Configuration 258
Client Configuration 259
Authentication 260
Ethernet WAN 262
VPLS 262
Metro-Ethernet 263
Foundation Summary 264
Memory Builders 265
Fill In Key Tables from Memory 265
Definitions 265
Further Reading 265
Part IV  IP Multicast

Chapter 7  Introduction to IP Multicasting  267

“Do I Know This Already?” Quiz  267

Foundation Topics  270

Why Do You Need Multicasting?  270

Problems with Unicast and Broadcast Methods  270

How Multicasting Provides a Scalable and Manageable Solution  273

Multicast IP Addresses  276

Multicast Address Range and Structure  276

Well-Known Multicast Addresses  276

Multicast Addresses for Permanent Groups  277

Multicast Addresses for Source-Specific Multicast Applications and Protocols  278

Multicast Addresses for GLOP Addressing  278

Multicast Addresses for Private Multicast Domains  278

Multicast Addresses for Transient Groups  278

Summary of Multicast Address Ranges  279

Mapping IP Multicast Addresses to MAC Addresses  280

Managing Distribution of Multicast Traffic with IGMP  281

Joining a Group  282

Internet Group Management Protocol  282

IGMP Version 2  283

IGMPv2 Host Membership Query Functions  285

IGMPv2 Host Membership Report Functions  286

IGMPv2 Solicited Host Membership Report  286

IGMPv2 Unsolicited Host Membership Report  288

IGMPv2 Leave Group and Group-Specific Query Messages  289

IGMPv2 Querier  291

IGMPv2 Timers  292

IGMP Version 3  292

IGMPv1 and IGMPv2 Interoperability  294

IGMPv2 Host and IGMPv1 Routers  294

IGMPv1 Host and IGMPv2 Routers  294

Comparison of IGMPv1, IGMPv2, and IGMPv3  295

LAN Multicast Optimizations  296

Cisco Group Management Protocol  296

IGMP Snooping  303
Chapter 8 IP Multicast Routing  317
“Do I Know This Already?” Quiz  317
Foundation Topics  321
Multicast Routing Basics  321
Overview of Multicast Routing Protocols  322
Multicast Forwarding Using Dense Mode  322
Reverse Path Forwarding Check  323
Multicast Forwarding Using Sparse Mode  325
Multicast Scoping  327
TTL Scoping  327
Administrative Scoping  328
Dense-Mode Routing Protocols  329
Operation of Protocol Independent Multicast Dense Mode  329
Forming PIM Adjacencies Using PIM Hello Messages  329
Source-Based Distribution Trees  330
Prune Message  331
PIM-DM: Reacting to a Failed Link  333
Rules for Pruning  335
Steady-State Operation and the State Refresh Message  337
Graft Message  339
LAN-Specific Issues with PIM-DM and PIM-SM  340
Prune Override  340
Assert Message  341
Designated Router  343
Summary of PIM-DM Messages  343
Distance Vector Multicast Routing Protocol  344
Multicast Open Shortest Path First  344
Sparse-Mode Routing Protocols 345
  Operation of Protocol Independent Multicast Sparse Mode 345
Similarities Between PIM-DM and PIM-SM 346
Sources Sending Packets to the Rendezvous Point 346
Joining the Shared Tree 348
Completion of the Source Registration Process 350
Shared Distribution Tree 352
Steady-State Operation by Continuing to Send Joins 353
Examining the RP’s Multicast Routing Table 354
Shortest-Path Tree Switchover 355
Pruning from the Shared Tree 357
Dynamically Finding RPs and Using Redundant RPs 358
Dynamically Finding the RP Using Auto-RP 359
Dynamically Finding the RP Using BSR 363
Anycast RP with MSDP 365
Interdomain Multicast Routing with MSDP 367
Summary: Finding the RP 369
Bidirectional PIM 370
  Comparison of PIM-DM and PIM-SM 371
Source-Specific Multicast 372
Implementing IPv6 Multicast PIM 373
  Designated Priority Manipulation 376
PIM6 Hello Interval 377
IPv6 Sparse-Mode Multicast 379
IPv6 Static RP 379
IPv6 BSR 381
Multicast Listener Discovery (MLD) 385
Embedded RP 389
Foundation Summary 393
Memory Builders 397
  Fill In Key Tables from Memory 397
Definitions 397
Further Reading 397
Part V  Security

Chapter 9  Device and Network Security  399

“Do I Know This Already?” Quiz  399

Foundation Topics  403

Router and Switch Device Security  403

Simple Password Protection for the CLI  403
Better Protection of Enable and Username Passwords  405
Using Secure Shell Protocol  405
User Mode and Privileged Mode AAA Authentication  406
Using a Default Set of Authentication Methods  407
Using Multiple Authentication Methods  408
Groups of AAA Servers  410
Overriding the Defaults for Login Security  410

PPP Security  411

Layer 2 Security  412

Switch Security Best Practices for Unused and User Ports  413
Port Security  413
Dynamic ARP Inspection  417
DHCP Snooping  420
IP Source Guard  422
802.1X Authentication Using EAP  423
Storm Control  426

General Layer 2 Security Recommendations  427

Layer 3 Security  429

IP Access Control List Review  430
ACL Rule Summary  431
Wildcard Masks  433

General Layer 3 Security Considerations  433
Smurf Attacks, Directed Broadcasts, and RPF Checks  433
Inappropriate IP Addresses  435
TCP SYN Flood, the Established Bit, and TCP Intercept  436

Classic Cisco IOS Firewall  438
TCP Versus UDP with CBAC  439
Cisco IOS Firewall Protocol Support  439
Cisco IOS Firewall Caveats  440
Cisco IOS Firewall Configuration Steps  440
Cisco IOS Zone-Based Firewall  441
Control-Plane Policing 446
Preparring for CoPP Implementation 447
Implementing CoPP 448
Dynamic Multipoint VPN 451
Step 1: Basic Configuration of IP Addresses 452
Step 2: GRE Multipoint Tunnel Configuration on All Routers (for Spoke-to-Spoke Connectivity) 453
Step 3: Configure IPsec to Encrypt mGRE Tunnels 457
Step 4: DMVPN Routing Configuration 459
IPv6 First Hop Security 461
First Hop Security for IPv6 461
Link Operations 463
End Node Security Enforcement 463
First Hop Switch Security Enforcement 464
Last Router Security Enforcement 464
ICMPv6 and Neighbor Discovery Protocol 464
Secure Neighbor Discovery (SeND) 465
Securing at the First Hop 466
RA Guard 467
DHCPv6 Guard 468
DHCPv6 Guard and the Binding Database 469
IPv6 Device Tracking 471
IPv6 Neighbor Discovery Inspection 472
IPv6 Source Guard 473
Port Access Control Lists (PACL) 475
Foundation Summary 476
Memory Builders 480
Fill In Key Tables from Memory 480
Definitions 480
Further Reading 480

Chapter 10 Tunneling Technologies 483
“Do I Know This Already?” Quiz 483
Foundation Topics 486
GRE Tunnels 486
Dynamic Multipoint VPN Tunnels 487
DMVPN Operation 488
DMVPN Components 488
DMVPN Operation 489
IPv6 Tunneling and Related Techniques 495

Tunneling Overview 496

Manually Configured Tunnels 497

Automatic IPv4-Compatible Tunnels 499

IPv6-over-IPv4 GRE Tunnels 499

Automatic 6to4 Tunnels 499

ISATAP Tunnels 501

SLAAC and DHCPv6 502

NAT-PT 502

NAT ALG 502

NAT64 502

Layer 2 VPNs 503

Tagged Mode 503

Raw Mode 503

Layer 2 Tunneling Protocol (L2TPv3) 504

AToM (Any Transport over MPLS) 504

Virtual Private LAN Services (VPLS) 505

Overlay Transport Virtualization (OTV) 506

GET VPN 506

Foundation Summary 512

Memory Builders 512

Definitions 512

Part VI Multiprotocol Label Switching (MPLS)

Chapter 11 Multiprotocol Label Switching 515

“Do I Know This Already?” Quiz 515

Foundation Topics 519

MPLS Unicast IP Forwarding 519

MPLS IP Forwarding: Data Plane 520

CEF Review 520

Overview of MPLS Unicast IP Forwarding 521

MPLS Forwarding Using the FIB and LFIB 522

The MPLS Header and Label 524

The MPLS TTL Field and MPLS TTL Propagation 524

MPLS IP Forwarding: Control Plane 526

MPLS LDP Basics 527

The MPLS Label Information Base Feeding the FIB and LFIB 529
Examples of FIB and LFIB Entries 532
Label Distribution Protocol Reference 534

MPLS VPNs 535
The Problem: Duplicate Customer Address Ranges 535
The Solution: MPLS VPNs 537
MPLS VPN Control Plane 539
Virtual Routing and Forwarding Tables 540
MP-BGP and Route Distinguishers 541
Route Targets 543
Overlapping VPNs 545
MPLS VPN Configuration 546
Configuring the VRF and Associated Interfaces 548
Configuring the IGP Between PE and CE 550
Configuring Redistribution Between PE-CE IGP and MP-BGP 553
Configuring MP-BGP Between PEs 555
MPLS VPN Data Plane 558
Building the (Inner) VPN Label 559
Creating LFIB Entries to Forward Packets to the Egress PE 560
Creating VRF FIB Entries for the Ingress PE 562
Penultimate Hop Popping 564

Other MPLS Applications 565
Implement Multi-VRF Customer Edge (VRF Lite) 566
VRF Lite, Without MPLS 566
VRF Lite with MPLS 569

Foundation Summary 570
Memory Builders 570
Fill In Key Tables from Memory 570
Definitions 570
Further Reading 570

Part VII Final Preparation

Chapter 12 Final Preparation 573
Tools for Final Preparation 573
Pearson Cert Practice Test Engine and Questions on the CD 573
Install the Software from the CD 574
Activate and Download the Practice Exam 574
Activating Other Exams 575
Premium Edition 575
The Cisco Learning Network 575
Memory Tables 575
Chapter-Ending Review Tools 576
Suggested Plan for Final Review/Study 576
Using the Exam Engine 576
Summary 577

Part VIII  Appendixes
Appendix A  Answers to the “Do I Know This Already?” Quizzes 579
Appendix B  CCIE Exam Updates 583
            Index 584

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
            Glossary
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, typically results in higher pay, and looks great on a résumé.

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, among which are 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 as 350-001; the v5.0 written exam is identified by 400-101.

The CCIE Routing and Switching written exam blueprint 5.0, as of the time of publication, is listed in Table I-1. 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>1.1.a Describe basic software architecture differences between IOS and IOS XE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.a (i) Control plane and Forwarding plane</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1.1.a (ii) Impact to troubleshooting and performances</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1.1.a (iii) Excluding specific platform's architecture</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1.1.b Identify Cisco Express Forwarding concepts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.b (i) RIB, FIB, LFIB, adjacency table</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>1.1.b (ii) Load-balancing hash</td>
<td>1</td>
<td>6</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>1.1.b (iii) Polarization concept and avoidance</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>1.1.c Explain general network challenges</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.c (i) Unicast flooding</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.c (ii) Out-of-order packets</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.c (iii) Asymmetric routing</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.c (iv) Impact of micro-burst</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.d Explain IP operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.d (i) ICMP unreachable, redirect</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.d (ii) IPv4 options, IPv6 extension headers</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.d (iii) IPv4 and IPv6 fragmentation</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.d (iv) TTL</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.d (v) IP MTU</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.e Explain TCP operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.e (i) IPv4 and IPv6 PMTU</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.e (ii) MSS</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.e (iii) Latency</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.e (iv) Windowing</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.e (v) Bandwidth delay product</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.e (vi) Global synchronization</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.e (vii) Options</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.f Explain UDP operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.f (i) Starvation</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.f (ii) Latency</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1.1.f (iii) RTP/RTCP concepts</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

1.2 Network implementation and operation

<table>
<thead>
<tr>
<th>Topics</th>
<th>Book Volume</th>
<th>Book Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.a Evaluate proposed changes to a network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2.a (i) Changes to routing protocol parameters</td>
<td>1</td>
<td>7–10</td>
</tr>
<tr>
<td>1.2.a (ii) Migrate parts of a network to IPv6</td>
<td>1</td>
<td>4</td>
</tr>
<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>
</tbody>
</table>
### Topics

<table>
<thead>
<tr>
<th>Topics</th>
<th>Book Volume</th>
<th>Book Chapter</th>
</tr>
</thead>
<tbody>
<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><strong>1.3.b Apply troubleshooting methodologies</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3.b (i) Diagnose the root cause of networking issue</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>(analyze symptoms, identify and describe root cause)</td>
<td></td>
<td></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><strong>1.3.c Interpret packet capture</strong></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><strong>2.1 LAN switching technologies</strong></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 MAC address table</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2.1.a (ii) errdisable 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) Alternative 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>Topics</td>
<td>Book Volume</td>
<td>Book Chapter</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>2.2.a (iii) IGMP querier</td>
<td>2</td>
<td>7</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*

| 2.3.a Implement and troubleshoot HDLC | 2 | 6 |
| 2.3.b Implement and troubleshoot PPP |  |  |
| 2.3.b (i) Authentication (PAP, CHAP) | 2 | 6 |
| 2.3.b (ii) PPPoE | 2 | 6 |
| 2.3.b (iii) MLPPP | 2 | 6 |

2.3.c Describe WAN rate-based Ethernet circuits

| 2.3.c (i) Metro and WAN Ethernet topologies | 2 | 6 |
| 2.3.c (ii) Use of rate-limited WAN Ethernet services | 2 | 6 |

3.0 *Layer 3 Technologies*

3.1 *Addressing technologies*

| 3.1.a Identify, implement, and troubleshoot IPv4 addressing and subnetting |  |  |
| 3.1.a (i) Address types, VLSM | 1 | 4 |
| 3.1.a (ii) ARP | 1 | 4 |

| 3.1.b Identify, implement, and troubleshoot IPv6 addressing and subnetting |  |  |
| 3.1.b (i) Unicast, multicast | 1 | 4 |
| 3.1.b (ii) EUI-64 | 1 | 4 |
| 3.1.b (iii) ND, RS/RA | 1 | 4 |
| 3.1.b (iv) Autoconfig/SLAAC, temporary addresses (RFC 4941) | 1 | 4 |
| 3.1.b (v) Global prefix configuration feature | 1 | 4 |
| 3.1.b (vi) DHCP operations | 1 | 4 |
| 3.1.b (vii) SLAAC/DHCPv6 interaction | 2 | 10 |
| 3.1.b (viii) Stateful, stateless DHCPv6 | 1 | 4 |
| 3.1.b (ix) DHCPv6 prefix delegation | 1 | 4 |
### 3.2 Layer 3 multicast

<table>
<thead>
<tr>
<th>Topic</th>
<th>Book Volume</th>
<th>Book Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.a Troubleshoot reverse path forwarding</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>
</tbody>
</table>

### 3.3 Fundamental routing concepts

<table>
<thead>
<tr>
<th>Topic</th>
<th>Book Volume</th>
<th>Book Chapter</th>
</tr>
</thead>
<tbody>
<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>Topics</td>
<td>Book Volume</td>
<td>Book Chapter</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>3.3.h Implement, optimize, and troubleshoot redistribution between any routing protocol</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>3.3.i Implement, optimize, and troubleshoot manual and autosummarization with any routing protocol</td>
<td>1</td>
<td>7–10</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>1</td>
<td>7</td>
</tr>
<tr>
<td>3.3.m (iii) Route Poisoning</td>
<td>1</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>1</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 SHA1-196bit</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>3.3.n (v) OSPFv3 IPsec authentication</td>
<td>1</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>1</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>1</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>Topics</td>
<td>Book Volume</td>
<td>Book Chapter</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>3.5.b (iii) OTP route-reflector peering</td>
<td>1</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>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.c (ii) Classic metric</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>3.5.c (iii) Wide metric</td>
<td>1</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>1</td>
<td>8</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 (multi-address) 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>
</tbody>
</table>

3.6 OSPF (v2 and v3)
<table>
<thead>
<tr>
<th>Topics</th>
<th>Book Volume</th>
<th>Book Chapter</th>
</tr>
</thead>
<tbody>
<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>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>Topics</td>
<td>Book Volume</td>
<td>Book Chapter</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>3.7a (ii) Active, passive</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3.7a (iii) States, timers</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3.7a (iv) Dynamic neighbors</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td><strong>3.7.b Implement and troubleshoot iBGP and iBGP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.7b (i) eBGP, iBGP</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3.7b (ii) 4-byte AS number</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3.7b (iii) Private AS</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td><strong>3.7c Explain attributes and best-path selection</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3.7.d Implement, optimize, and troubleshoot routing policies</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.7d (i) Attribute manipulation</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7d (ii) Conditional advertisement</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7d (iii) Outbound route filtering</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7d (iv) Communities, extended communities</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7d (v) Multihoming</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td><strong>3.7.e Implement and troubleshoot scalability</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.7e (i) Route-reflector, cluster</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7e (ii) Confederations</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7e (iii) Aggregation, AS set</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td><strong>3.7.f Implement and troubleshoot multiprotocol BGP</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.7f (i) IPv4, IPv6, VPN address-family</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td><strong>3.7.g Implement and troubleshoot AS path manipulations</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.7g (i) Local AS, allow AS in, remove private AS</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7g (ii) Prepend</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7g (iii) Regexp</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td><strong>3.7.h Implement and troubleshoot other features</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.7h (i) Multipath</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7h (ii) BGP synchronization</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3.7h (iii) Soft reconfiguration, route refresh</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.i Describe BGP fast convergence features</td>
<td></td>
<td></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></td>
<td></td>
</tr>
<tr>
<td>3.8.a Describe basic IS-IS network</td>
<td></td>
<td></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></td>
<td></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></td>
<td></td>
</tr>
<tr>
<td>3.8.e (i) Metrics, wide metric</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>4.0 VPN Technologies</td>
<td></td>
<td></td>
</tr>
<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>Topics</td>
<td>Book Volume</td>
<td>Book Chapter</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>--------------</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>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>5.0 Infrastructure Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 Device security</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>
</tbody>
</table>
5.1.d Describe device security using IOS AAA with TACACS+ and RADIUS

5.1.d (i) AAA with TACACS+ and RADIUS
5.1.d (ii) Local privilege authorization fallback

5.2 Network security

5.2.a Implement and troubleshoot switch security features

5.2.a (i) VACL, PAACL
5.2.a (ii) Storm control
5.2.a (iii) DHCP snooping
5.2.a (iv) IP source-guard
5.2.a (v) Dynamic ARP inspection
5.2.a (vi) port-security
5.2.a (vii) Private VLAN

5.2.b Implement and troubleshoot router security features

5.2.b (i) IPv4 access control lists (standard, extended, time-based)
5.2.b (ii) IPv6 traffic filter
5.2.b (iii) Unicast reverse path forwarding

5.2.c Implement and troubleshoot IPv6 first-hop security

5.2.c (i) RA Guard
5.2.c (ii) DHCP Guard
5.2.c (iii) Binding table
5.2.c (iv) Device tracking
5.2.c (v) ND inspection/snooping
5.2.c (vi) Source Guard
5.2.c (viii) PAACL

5.2.d Describe 802.1x

5.2.d (i) 802.1x, EAP, RADIUS
5.2.d (ii) MAC authentication bypass

6.0 Infrastructure Services
<table>
<thead>
<tr>
<th>Topics</th>
<th>Book Volume</th>
<th>Book Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6.1 System management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.a Implement and troubleshoot device management</td>
<td></td>
<td></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) TFTP</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.1.b Implement and troubleshoot SNMP</td>
<td></td>
<td></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></td>
<td></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>
<tr>
<td><strong>6.2 Quality of service</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2.a Implement and troubleshoot end-to-end QoS</td>
<td></td>
<td></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></td>
<td></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>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><strong>6.3 Network services</strong></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>Topics</td>
<td>Book Volume</td>
<td>Book Chapter</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------</td>
<td>--------------</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,</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>routes, IP SLA, and so on)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.4.c Implement and troubleshoot NetFlow</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.4.c (i) NetFlow v5, v9</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.4.c (ii) Local retrieval</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.4.c (iii) Export (configuration only)</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6.4.d Implement and troubleshoot embedded event manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.4.d (i) EEM policy using applet</td>
<td>1</td>
<td>5</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 2* 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 Exam Guide, Volume 2, 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 six major parts. Beyond the chapters in these parts of the book, you will find several useful appendixes gathered in Part VIII.

Following is a description of each part's coverage:

- **Part I, “IP BGP Routing” (Chapters 1 and 2):** This part focuses on the details of BGP (Chapter 1), with Chapter 2 looking at BGP path attributes and how to influence BGP’s choice of best path.

- **Part II, “QoS” (Chapters 3–5):** This part covers the more popular QoS tools, including some MQC-based tools, as well as several older tools, particularly FRTS. The chapters include coverage of classification and marking (Chapter 3), queuing and congestion avoidance (Chapter 4), plus shaping, policing, and link efficiency (Chapter 5).

- **Part III, “Wide-Area Networks” (Chapter 6):** The WAN coverage has been shrinking over the last few revisions to the CCIE R&S written exam. Chapter 6 includes some brief coverage of PPP and Frame Relay. Note that the previous version (V4.0) and current version (V5.0) of the blueprint include another WAN topic, MPLS, which is covered in Part VI, Chapter 11.
Part IV, “IP Multicast” (Chapters 7 and 8): Chapter 7 covers multicast on LANs, including IGMP and how hosts join multicast groups. Chapter 8 covers multicast WAN topics.

Part V, “Security” (Chapters 9 and 10): Given the CCIE tracks for both Security and Voice, Cisco has a small dilemma regarding whether to cover those topics on CCIE Routing and Switching, and if so, in how much detail. This part covers a variety of security topics appropriate for CCIE Routing and Switching. This chapter focuses on switch and router security.

Part VI, “Multiprotocol Label Switching (MPLS)” (Chapter 11): As mentioned in the WAN section, the CCIE R&S exam’s coverage of MPLS has been growing over the last two versions of the blueprint. This chapter focuses on enterprise-related topics such as core MPLS concepts and MPLS VPNs, including basic configuration.

Part VII, “Final Preparation” (Chapter 12): This part provides a set of tools and a study plan to help you complete your preparation for the exams.

Part VIII, “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, “CCIE 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/9781587144912. 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 inside 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 through F and the Glossary are in printable, PDF format on the CD.

(CD-only) Appendix C, “Decimal-to-Binary Conversion Table”: This appendix lists the decimal values 0 through 255, with their binary equivalents.

(CD-only) Appendix D, “IP Addressing Practice”: This appendix lists several practice problems for IP subetting and finding summary routes. The explanations to the answers use the shortcuts described in the book.

(CD-only) Appendix E, “Key Tables for CCIE Study”: 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 and then fill in the table from memory, checking your answers against the completed tables in Appendix F.

(CD-only) Appendix F, “Solutions for Key Tables for CCIE Study”

(CD-only) Glossary: 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 configurations 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. The CD-only Appendix F 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.

- **Special question section for the “Implement Proposed Changes to a Network” section of the Blueprint:** To provide practice and perspectives on these exam topics, a special section of questions has been developed to help you prepare for these new types of questions.
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.

- Modular QoS CLI (MQC)
- Network-Based Application Recognition (NBAR)
- QoS Classification
- QoS Marking
- Cisco AutoQoS
Classification and Marking

The goal of classification and marking tools is to simplify the classification process of other quality of service (QoS) tools by performing complicated classification steps as few times as possible. For example, a classification and marking tool might examine the source IP address of packets, incoming Class of Service (CoS) settings, and possibly TCP or UDP port numbers. Packets matching all those fields might have their IP Precedence (IPP) or DiffServ Code Points (DSCP) field marked with a particular value. Later, other QoS tools—on the same router/switch or a different one—can simply look for the marked field when making a QoS decision, rather than having to perform the detailed classification again before taking the desired QoS action.

“Do I Know This Already?” Quiz

Table 3-1 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>Fields That Can Be Marked for QoS Purposes</td>
<td>1–4</td>
<td></td>
</tr>
<tr>
<td>Cisco Modular QoS CLI</td>
<td>5–7</td>
<td></td>
</tr>
<tr>
<td>Classification and Marking Tools</td>
<td>8–10</td>
<td></td>
</tr>
<tr>
<td>AutoQoS</td>
<td>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. According to the DiffServ RFCs, which PHB defines a set of three DSCPs in each service class, with different drop characteristics for each of the three DSCP values?
   a. Expedited Forwarding
   b. Class Selector
   c. Assured Forwarding
   d. Multi-class-multi-drop
2. Which of the following are true about the location of DSCP in the IP header?
   a. High-order 6 bits of ToS byte/DS field.
   b. Low-order 6 bits of ToS byte.
   c. Middle 6 bits of ToS byte.
   d. Its first 3 bits overlap with IP Precedence.
   e. Its last 3 bits overlap with IP Precedence

3. Imagine that a packet is marked with DSCP CS3. Later, a QoS tool classifies the packet. Which of the following classification criteria would match the packet, assuming that the marking had not been changed from the original CS3 marking?
   a. Match on DSCP CS3
   b. Match on precedence 3
   c. Match on DSCP AF32
   d. Match on DSCP AF31
   e. Match on DSCP decimal 24

4. Imagine that a packet is marked with AF31. Later, a QoS tool classifies the packet. Which of the following classification criteria would match the packet, assuming that the marking had not been changed from the original AF31 marking?
   a. Match on DSCP CS3
   b. Match on precedence 3
   c. Match on DSCP 24
   d. Match on DSCP 26
   e. Match on DSCP 28

5. Examine the following output from a router that shows a user adding configuration to a router. Which of the following statements is true about the configuration?

   ```
   Router(config)# class-map fred
   Router(config-cmap)# match dscp EF
   Router(config-cmap)# match access-group 101
   ```
   a. Packets that match both DSCP EF and ACL 101 will match the class.
   b. Packets that match either DSCP EF or ACL 101 will match the class.
   c. Packets that match ACL 101 will match the class, because the second match command replaces the first.
   d. Packets will only match DSCP EF because the first match exits the class map.
6. Router R1 is configured with the following three class maps. Which class map(s) would match an incoming frame whose CoS field is set to 3, IP Precedence is set to 2, and DSCP is set to AF21?

```
class-map match-all c1
  match cos 3 4
class-map match-any c2
  match cos 2 3
  match cos 1
class-map match-all c3
  match cos 3 4
  match cos 2
```

a. c1  
b. c2  
c. c3  
d. All of these answers are correct.

7. Examine the following example of commands typed in configuration mode to create a class map. Assuming that the `class fred` command was used inside a policy map, and the policy map was enabled on an interface, which of the following would be true with regard to packets classified by the class map?

```
Router(config)# class-map fred
Router(config-cmap)# match ip dscp ef
Router(config-cmap)# match ip dscp af31
```

a. Match packets with both DSCP EF and AF31  
b. Match packets with either DSCP EF or AF31  
c. Match all packets that are neither EF nor AF31  
d. Match no packets  
e. Match packets with precedence values of 3 and 5

8. The `service-policy output fred` command is found in Router R1's configuration under Frame Relay subinterface s0/0.1. Which of the following could be true about this CB Marking policy map?

a. The policy map can classify packets using class maps that match based on the DE bit.  
b. The policy map can refer to class maps that match based on DSCP.  
c. The policy map can set CoS.  
d. The policy map can set CLP.  
e. The policy map can set DE.
9. Which of the following is true regarding the listed configuration steps?

```plaintext
Router(config)# class-map barney
Router(config-cmap)# match protocol http url "this-here.jpg"
Router(config-cmap)# policy-map fred
Router(config-pmap)# class barney
Router(config-pmap-c)# set dscp af21
Router(config-pmap-c)# interface fa0/0
Router(config-if)# service-policy output fred
```

a. If not already configured, the `ip cef` global command is required.

b. The configuration does not use NBAR because the `match nbar` command was not used.

c. The `service-policy` command would be rejected because `match protocol` is not allowed as an output function.

d. None of these answers are correct.

10. In which mode(s) can the `qos pre-classify` command be issued on a router?

a. In crypto map configuration mode

b. In GRE tunnel configuration mode

c. In point-to-point subinterface configuration mode

d. Only in physical interface configuration mode

e. In class map configuration mode

f. In global configuration mode

11. Which of the following statements about Cisco AutoQoS are true?

a. It can be used only on switches, not routers.

b. It makes QoS configuration quicker, easier, and cheaper.

c. AutoQoS can be used to configure quality of service for voice, video, and other types of data.

d. AutoQoS commands are applied at the interface.

e. AutoQoS must be disabled before its settings can be modified.
Chapter 3: Classification and Marking

Foundation Topics

This chapter has three major sections. The chapter begins by examining the fields that can be marked by the classification and marking (C&M) tools. Next, the chapter covers the mechanics of the Cisco IOS Modular QoS CLI (MQC), which is used by all the IOS QoS tools that begin with the words “Class-Based.” Finally, the C&M tools are covered, with most of the content focused on the most important C&M tool, Class-Based Marking (CB Marking).

Fields That Can Be Marked for QoS Purposes

The IP header, LAN trunking headers, Frame Relay header, and ATM cell header all have at least one field that can be used to perform some form of QoS marking. This section lists and defines those fields, with the most significant coverage focused on the IP header IP Precedence (IPP) and Differentiated Services Code Point (DSCP) fields.

IP Precedence and DSCP Compared

The IP header is defined in RFC 791, including a 1-byte field called the Type of Service (ToS) byte. The ToS byte was intended to be used as a field to mark a packet for treatment with QoS tools. The ToS byte itself was further subdivided, with the high-order 3 bits defined as the IP Precedence (IPP) field. The complete list of values from the ToS byte’s original IPP 3-bit field, and the corresponding names, is provided in Table 3-2.

<table>
<thead>
<tr>
<th>Name</th>
<th>Decimal Value</th>
<th>Binary Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routine</td>
<td>Precedence 0</td>
<td>000</td>
</tr>
<tr>
<td>Priority</td>
<td>Precedence 1</td>
<td>001</td>
</tr>
<tr>
<td>Immediate</td>
<td>Precedence 2</td>
<td>010</td>
</tr>
<tr>
<td>Flash</td>
<td>Precedence 3</td>
<td>011</td>
</tr>
<tr>
<td>Flash Override</td>
<td>Precedence 4</td>
<td>100</td>
</tr>
<tr>
<td>Critic/Critical</td>
<td>Precedence 5</td>
<td>101</td>
</tr>
<tr>
<td>Internetwork Control</td>
<td>Precedence 6</td>
<td>110</td>
</tr>
<tr>
<td>Network Control</td>
<td>Precedence 7</td>
<td>111</td>
</tr>
</tbody>
</table>

Bits 3 through 6 of the ToS byte included flag fields that were toggled on or off to imply a particular QoS service. The final bit (bit 7) was not defined in RFC 791. The flags were not used very often, so in effect, the ToS byte’s main purpose was to hold the 3-bit IPP field.
A series of RFCs collectively called *Differentiated Services (DiffServ)* came along later. DiffServ needed more than 3 bits to mark packets, so DiffServ standardized a redefinition of the ToS byte. The ToS byte itself was renamed the *Differentiated Services (DS)* field, and IPP was replaced with a 6-bit field (high-order bits 0–5) called the *Differentiated Services Code Point (DSCP)* field. Later, RFC 3168 defined the low-order 2 bits of the DS field for use with the QoS *Explicit Congestion Notification (ECN)* feature. Figure 3-1 shows the ToS byte’s format with the pre-DiffServ and post-DiffServ definition of the field.

![Figure 3-1 IP ToS Byte and DS Field Compared](image)

C&M tools often mark DSCP or IPP because the IP packet remains intact as it is forwarded throughout an IP network. The other possible marking fields reside inside Layer 2 headers, which means that the headers are discarded when forwarded by a Layer 3 process. Thus, the latter cannot be used to carry QoS markings beyond the current hop.

**DSCP Settings and Terminology**

Several DiffServ RFCs suggest a set of values to use in the DSCP field and an implied meaning for those settings. For example, RFC 3246 defines a DSCP of decimal 46, with a name *Expedited Forwarding (EF)*. According to that RFC, packets marked as EF should be given queuing preference so that they experience minimal latency, but the packets should be policed to prevent them from taking over a link and preventing any other types of traffic from exiting an interface during periods when this high-priority traffic reaches or exceeds the interface bandwidth. These suggested settings, and the associated QoS behavior recommended when using each setting, are called *Per-Hop Behaviors (PHB)* by DiffServ. (The particular example listed in this paragraph is called the Expedited Forwarding PHB.)

**Class Selector PHB and DSCP Values**

IPP overlaps with the first 3 bits of the DSCP field because the DS field is simply a redefinition of the original ToS byte in the IP header. Because of this overlap, RFC 2475
defines a set of DSCP values and PHBs, called Class Selector (CS) PHBs that provide backward compatibility with IPP. A C&M feature can set a CS DSCP value, and if another router or switch just looks at the IPP field, the value will make sense from an IPP perspective. Table 3-3 lists the CS DSCP names and values, and the corresponding IPP values and names.

<table>
<thead>
<tr>
<th>DSCP Class Selector Names</th>
<th>Binary DSCP Values</th>
<th>IPP Binary Values</th>
<th>IPP Names</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default/CS0*</td>
<td>000000</td>
<td>000</td>
<td>Routine</td>
</tr>
<tr>
<td>CS1</td>
<td>001000</td>
<td>001</td>
<td>Priority</td>
</tr>
<tr>
<td>CS2</td>
<td>010000</td>
<td>010</td>
<td>Immediate</td>
</tr>
<tr>
<td>CS3</td>
<td>011000</td>
<td>011</td>
<td>Flash</td>
</tr>
<tr>
<td>CS4</td>
<td>100000</td>
<td>100</td>
<td>Flash Override</td>
</tr>
<tr>
<td>CS5</td>
<td>101000</td>
<td>101</td>
<td>Critical</td>
</tr>
<tr>
<td>CS6</td>
<td>110000</td>
<td>110</td>
<td>Internetwork Control</td>
</tr>
<tr>
<td>CS7</td>
<td>111000</td>
<td>111</td>
<td>Network Control</td>
</tr>
</tbody>
</table>

*The terms “CS0” and “Default” both refer to a binary DSCP of 000000, but most Cisco IOS commands allow only the keyword “default” to represent this value.

Besides defining eight DSCP values and their text names, the CS PHB also suggests a simple set of QoS actions that should be taken based on the CS values. The CS PHB simply states that packets with larger CS DSCPs should be given better queuing preference than packets with lower CS DSCPs.

**Assured Forwarding PHB and DSCP Values**

The Assured Forwarding (AF) PHB (RFC 2597) defines four classes for queuing purposes, along with three levels of drop probability inside each queue. To mark packets and distinguish into which of four queues a packet should be placed, along with one of three drop priorities inside each queue, the AF PHB defines 12 DSCP values and their meanings. The names of the AF DSCPs conform to the following format:

AFxy

where x implies one of four queues (values 1 through 4) and y implies one of three drop priorities (values 1 through 3).

The AF PHB suggests that the higher the value of x in the DSCP name AFxy, the better the queuing treatment a packet should get. For example, packets with AF11 DSCPs should get worse queuing treatment than packets with AF23 DSCP values. Additionally, the AF PHB suggests that the higher the value of y in the DSCP name AFxy, the worse the drop treatment for those packets. (Treating a packet worse for drop purposes means that the packet has a higher probability of being dropped.) For example, packets with
AF11 DSCPs should get better drop treatment than packets with AF23 DSCP values. Table 3-4 lists the names of the DSCP values, the queuing classes, and the implied drop likelihood.

<table>
<thead>
<tr>
<th>Queue Class</th>
<th>Low Drop Probability</th>
<th>Medium Drop Probability</th>
<th>High Drop Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name/Decimal/Binary</td>
<td>Name/Decimal/Binary</td>
<td>Name/Decimal/Binary</td>
</tr>
<tr>
<td>1</td>
<td>AF11/10/001010</td>
<td>AF12/12/001100</td>
<td>AF13/14/001110</td>
</tr>
<tr>
<td>2</td>
<td>AF21/18/010010</td>
<td>AF22/20/010100</td>
<td>AF23/22/010110</td>
</tr>
<tr>
<td>3</td>
<td>AF31/26/011010</td>
<td>AF32/28/011100</td>
<td>AF33/30/011110</td>
</tr>
<tr>
<td>4</td>
<td>AF41/34/100010</td>
<td>AF42/36/100100</td>
<td>AF43/38/100110</td>
</tr>
</tbody>
</table>

The text AF PHB names do not follow the “bigger-is-better” logic in all cases. For example, the name AF11 represents a decimal value of 10, and the name AF13 represents a decimal DSCP of 14. However, AF11 is “better” than AF13, because AF11 and AF13 are in the same queuing class, but AF11 has a lower probability of being dropped than AF13.

The binary version of the AF DSCP values shows the patterns of the values. The first 3 bits of the binary DSCP values designate the queuing class (bits 0 through 2 counting left to right), and the next 2 bits (bits 3 and 4) designate the drop preference. As a result, queuing tools that operate only on IPP can still react to the AF DSCP values, essentially making the AF DSCPs backward compatible with non-DiffServ nodes for queuing purposes.

**Note** To convert from the AF name to the decimal equivalent, you can use a simple formula. If you think of the AF values as AF<sub>x,y</sub>, the formula is

\[8x + 2y = \text{decimal value}\]

For example, AF41 gives you a formula of \((8 \times 4) + (2 \times 1) = 34\).

### Expedited Forwarding PHB and DSCP Values

RFC 2598 defines the *Expedited Forwarding (EF)* PHB, which was described briefly in the introduction to this section. This RFC defines a very simple pair of PHB actions:

- Queue EF packets so that they get scheduled quickly, to give them low latency.
- Police the EF packets so that they do not consume all bandwidth on the link or starve other queues.

The DSCP value defined for EF is named EF, with decimal value 46, binary value 101110.
Non-IP Header Marking Fields

As IP packets pass through an internetwork, the packet is encapsulated in a variety of other headers. In several cases, these other headers have QoS fields that can be used for classification and marking.

Ethernet LAN Class of Service

Ethernet supports a 3-bit QoS marking field, but the field only exists when the Ethernet header includes either an 802.1Q or ISL trunking header. IEEE 802.1Q defines its QoS field as the 3 most-significant bits of the 2-byte Tag Control field, calling the field the user-priority bits. ISL defines the 3 least-significant bits from the 1-byte User field, calling this field the Class of Service (CoS). Generally speaking, most people (and most IOS commands) refer to these fields as CoS, regardless of the type of trunking. Figure 3-2 shows the general location of the CoS field inside ISL and 802.1P headers.

WAN Marking Fields

Frame Relay and ATM support a single bit that can be set for QoS purposes, but these single bits are intended for a very strict use related to drop probability. Frames or cells with these bits set to 1 are considered to be better candidates to be dropped than frames or cells without the bit set to 1. Named the Frame Relay Discard Eligibility (DE) bit and the ATM Cell Loss Priority (CLP) bit, these bits can be set by a router, or by an ATM or Frame Relay switch. Router and switch drop features can then be configured to more aggressively drop frames and cells that have the DE or CLP bit set, respectively.

MPLS defines a 3-bit field called the MPLS Experimental (EXP) bit that is intended for general QoS marking. Often, C&M tools are used on the edge of MPLS networks to
remap DSCP or IPP values to MPLS Experimental bit values to provide QoS inside the MPLS network.

Locations for Marking and Matching

Figure 3-3 shows a sample network, with notes about the locations of the QoS fields.

Figure 3-3  Sample Network Showing Non-IP Markable QoS Fields

In such a network, the IPP and DSCP inside the IP packet remain intact from end to end. However, some devices might not be able to look at the IPP or DSCP fields, and some might find it more convenient to look at some other header field. For example, an MPLS Label Switch Router (LSR) inside the MPLS cloud can be configured to make QoS decisions based on the 3-bit MPLS EXP field in the MPLS label, but unable to look at the encapsulated IP header and DSCP field. In such cases, QoS tools might need to be configured on edge devices to look at the DSCP and then mark a different field.

The non-IP header markable fields exist in only parts of the network. As a result, those fields can be used for classification or marking only on the appropriate interfaces. The rules for where these fields (CoS, DE, CLP, EXP) can be used are as follows:

- **For classification**: On ingress only, and only if the interface supports that particular header field
- **For marking**: On egress only, and only if the interface supports that particular header field

For example, if CB Marking were to be configured on R1's fa0/0.1 802.1Q subinterface, it could classify incoming frames based on their CoS values, and mark outgoing frames with a CoS value. However, on ingress, it could not mark CoS, and on egress, it could not classify based on CoS. Similarly, on that same fa0/0.1 subinterface, CB Marking could neither classify nor mark based on a DE bit, CLP bit, or MPLS EXP bits, because these headers never exist on Ethernet interfaces.

Table 3-5 summarizes the QoS marking fields.
Cisco Modular QoS CLI

For many years and over many IOS releases, Cisco added QoS features and functions, each of which used its own separate set of configuration and exec commands. Eventually, the number of different QoS tools and different QoS commands got so large that QoS configuration became a big chore. Cisco created the Modular QoS CLI (MQC) to help resolve these problems, by defining a common set of configuration commands to configure many QoS features in a router or switch.

MQC is not a totally new CLI, different from IOS configuration mode, for configuring QoS. Rather, it is a method of categorizing IOS classification, marking, and related actions into logical groupings to unify the command-line interface. MQC defines a new set of configuration commands—commands that are typed in using the same IOS CLI, in configuration mode. However, after you understand MQC, you typically need to learn only one new command to know how to configure any additional MQC-based QoS tools. You can identify MQC-based tools by the name of the tool; they all begin with the phrase “Class-Based” (abbreviated CB for this discussion). These tools include CB Marking, CB Weighted Fair Queuing (CBWFQ), CB Policing, CB Shaping, and CB Header Compression.

Mechanics of MQC

MQC separates the classification function of a QoS tool from the action (PHB) that the QoS tool wants to perform. To do so, there are three major commands with MQC, with several subordinate commands:

- The **class-map** command defines the matching parameters for classifying packets into service classes.
- The PHB actions (marking, queuing, and so on) are configured under a **policy-map** command.
- The policy map is enabled on an interface by using a **service-policy** command.

<table>
<thead>
<tr>
<th>Field</th>
<th>Location</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Precedence (IPP)</td>
<td>IP header</td>
<td>3 bits</td>
</tr>
<tr>
<td>IP DSCP</td>
<td>IP header</td>
<td>6 bits</td>
</tr>
<tr>
<td>DS field</td>
<td>IP header</td>
<td>1 byte</td>
</tr>
<tr>
<td>ToS byte</td>
<td>IP header</td>
<td>1 byte</td>
</tr>
<tr>
<td>CoS</td>
<td>ISL and 802.1Q header</td>
<td>3 bits</td>
</tr>
<tr>
<td>Discard Eligible (DE)</td>
<td>Frame Relay header</td>
<td>1 bit</td>
</tr>
<tr>
<td>Cell Loss Priority (CLP)</td>
<td>ATM cell header</td>
<td>1 bit</td>
</tr>
<tr>
<td>MPLS Experimental</td>
<td>MPLS header</td>
<td>3 bits</td>
</tr>
</tbody>
</table>
Figure 3-4 shows the general flow of commands.

```
class-map myclass1
    (matching parameters follow …)
class-map myclass2
    (matching parameters follow …)

policy-map mypolicy
    class myclass1
        (Actions/PHB’s FOR THIS CLASS follow: marking, queuing, etc.)
    class myclass2
        (Actions/PHB’s FOR THIS CLASS follow: marking, queuing, etc.)

Interface S 0/0
    service-policy output mypolicy
```

**Figure 3-4**  
MQC Commands and Their Correlation

In Figure 3-4, the network’s QoS policy calls for treating packets in one of two categories, called QoS service classes. (The actual types of packets that are placed into each class are not shown, to keep the focus on the general flow of how the main commands work together.) Classifying packets into two classes calls for the use of two class-map commands. Each class-map command would be followed by a match subcommand, which defines the actual parameters that are compared to the frame/packet header contents to match packets for classification.

For each class, some QoS action (PHB) needs to be performed; this action is configured using the policy-map command. Under a single policy map, multiple classes can be referenced; in Figure 3-4, the two classes are myclass1 and myclass2. Inside the single policy called mypolicy, under each of the two classes myclass1 and myclass2, you can configure separate QoS actions. For example, you could apply different markings to packets in myclass1 and myclass2 at this point. Finally, when the service-policy command is applied to an interface, the QoS features are enabled either inbound or outbound on that interface.

The next section takes a much closer look at packet classification using class maps. Most of the discussion of policy maps will be included when specifically covering CB Marking configuration later in the chapter.

**Classification Using Class Maps**

MQC-based tools classify packets using the match subcommand inside an MQC class map. The following list details the rules surrounding how class maps work for matching and classifying packets:

- The match command has many options for matching packets, including QoS fields, ACLs, and MAC addresses.
- Class-map names are case sensitive.
The match protocol command means that IOS uses Network-Based Application Recognition (NBAR) to perform that match.

The match any command matches any packet—in other words, any and all packets.

Example 3-1 shows a simple CB Marking configuration, with comments focused on the classification configuration. Note that the names and logic match Figure 3-4.

Example 3-1  Basic CB Marking Example

```
! CEF is required for CB Marking. Without it, the class map and policy map configuration would be allowed, but the service-policy command would be rejected.
ip cef
! The first class map matches all UDP/RTP packets with UDP ports between 16384 and 32767 (the 2nd number is added to the first to get the end of the range.) The second class map matches any and all packets.
class-map match-all myclass1
  match ip rtp 16384 16383
class-map match-all myclass2
  match any
! The policy map calls each of the two class maps for matching. The set command implies that the PHB is marking, meaning that this is a CB Marking config.
policy-map mypolicy
  class myclass1
    set dscp EF
  class myclass2
    set dscp default
! The policy map processes packets leaving interface fa0/0.
interface Fastethernet0/0
service-policy output mypolicy
```

With Example 3-1, each packet leaving interface fa0/0 will match one of the two classes. Because the policy map uses a set dscp command in each class, and all packets happen to match either myclass1 or myclass2, each packet will leave the interface marked either with DSCP EF (decimal 46) or default (decimal 0). (If the matching logic was different and some packets match neither myclass1 nor myclass2, those packets would not be marked, and would retain their existing DSCP values.)

Using Multiple match Commands

In some cases, a class map might need to examine multiple items in a packet to decide whether the packet should be part of that class. Class maps can use multiple match commands, and even nest class maps inside other class maps, to achieve the desired combination of logic. The following list summarizes the key points regarding these more complex matching options:

- Up to four (CoS and IPP) or eight (DSCP) values can be listed on a single match cos, match precedence, or match dscp command, respectively. If any of the values are found in the packet, the statement is matched.
If a class map has multiple `match` commands in it, the `match-any` or `match-all` (default) parameter on the `class-map` command defines whether a logical OR or a logical AND (default) is used between the `match` commands, respectively.

The `match` class name command refers to another class map by name, nesting the named class map’s matching logic; the `match` class name command is considered to match if the referenced class map also results in a match.

Example 3-2 shows several examples of this more complicated matching logic, with notations inside the example of what must be true for a class map to match a packet.

**Example 3-2 Complex Matching with Class Maps**

```
! class-map example1 uses match-all logic (default), so this class map matches packets that are permitted by ACL 102, and that also have an IP precedence of 5.
class-map match-all example1
  match access-group 102
  match precedence 5
!
! class-map example2 uses match-any logic, so this class map matches packets that are permitted by ACL 102, or have DSCP AF21, or both.
class-map match-any example2
  match access-group 102
  match dscp AF21
!
! class-map example3 matches no packets, due to a common mistake—the two `match` commands use a logical AND between them due to the default `match-all` argument, meaning that a single packet must have DSCP 0 and DSCP 1, which is impossible.
! class-map example4 shows how to correctly match either DSCP 0 or 1.
class-map match-all example3
  match dscp 0
  match dscp 1
!
class-map match-any example4
  match dscp 0 1
!
! class-map i-am-nesting refers to class-map i-am-nested through the `match class` i-am-nested command. The logic is explained after the example.
class-map match-all i-am-nested
  match access-group 102
  match precedence 5
!
class-map match-any i-am-nesting
  match class i-am-nested
  match cos 5
```

The trickiest part of Example 3-2 is how the class maps can be nested, as shown at the end. `class-map i-am-nesting` uses OR logic between its two `match` commands, meaning “I will match if the CoS is 5, or if `class-map i-am-nested` matches the packet, or both.”
When combined with the match-all logic of the `i-am-nested` class map, the logic matches the following packets/frames:

Packets that are permitted by ACL 102, AND marked with precedence 5
or
frames with CoS 5

**Classification Using NBAR**

NBAR classifies packets that are normally difficult to classify. For example, some applications use dynamic port numbers, so a statically configured `match` command, matching a particular UDP or TCP port number, simply could not classify the traffic. NBAR can look past the UDP and TCP header, and refer to the host name, URL, or MIME type in HTTP requests. (This deeper examination of the packet contents is sometimes called *deep packet inspection*.) NBAR can also look past the TCP and UDP headers to recognize application-specific information. For example, NBAR allows recognition of different Citrix application types, and allows searching for a portion of a URL string.

NBAR itself can be used for a couple of different purposes. Independent of QoS features, NBAR can be configured to keep counters of traffic types and traffic volume for each type. For QoS, NBAR can be used by CB Marking to match difficult-to-match packets. Whenever the MQC `match protocol` command is used, IOS is using NBAR to match the packets. Table 3-6 lists some of the more popular uses of the `match protocol` command and NBAR.

**Table 3-6  Popular Fields Matchable by CB Marking Using NBAR**

<table>
<thead>
<tr>
<th>Field</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP audio versus video</td>
<td>RTP uses even-numbered UDP ports from 16,384 to 32,768. The odd-numbered port numbers are used by RTCP for call control traffic. NBAR allows matching the even-numbered ports only, for classification of voice payload into a different service class from that used for voice signaling.</td>
</tr>
<tr>
<td>Citrix applications</td>
<td>NBAR can recognize different types of published Citrix applications.</td>
</tr>
<tr>
<td>Host name, URL string, MIME type</td>
<td>NBAR can also match URL strings, including the host name and the MIME type, using regular expressions for matching logic.</td>
</tr>
<tr>
<td>Peer-to-peer applications</td>
<td>NBAR can find file-sharing applications like KaZaa, Morpheus, Grokster, and Gnutella.</td>
</tr>
</tbody>
</table>

**Classification and Marking Tools**

The final major section of this chapter covers CB Marking, with a brief mention of a few other, less popular marking tools.
Class-Based Marking (CB Marking) Configuration

As with the other QoS tools whose names begin with the phrase “Class-Based,” you will use MQC commands to configure CB Marking. The following list highlights the key points regarding CB Marking configuration and logic:

- CB Marking requires CEF (enabled using the `ip cef` global command).
- Packets are classified based on the logic in MQC class maps.
- An MQC policy map refers to one or more class maps using the `class class-map-name` command; packets classified into that class are then marked.
- CB Marking is enabled for packets either entering or exiting an interface using the MQC `service-policy in | out policy-map-name interface` subcommand.
- A CB Marking policy map is processed sequentially; after a packet has matched a class, it is marked based on the `set` command(s) defined for that class.
- You can configure multiple `set` commands in one class to set multiple fields, for example, to set both DSCP and CoS.
- Packets that do not explicitly match a defined class are considered to have matched a special class called `class-default`.
- For any class inside the policy map for which there is no `set` command, packets in that class are not marked.

Table 3-7 lists the syntax of the CB Marking `set` command, showing the familiar fields that can be set by CB Marking. Table 3-8 lists the key `show` commands available for CB Marking.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>set [ip] precedence ip-precedence-value</code></td>
<td>Marks the value for IP Precedence for IPv4 and IPv6 packets if the <code>ip</code> parameter is omitted; sets only IPv4 packets if the <code>ip</code> parameter is included</td>
</tr>
<tr>
<td><code>set [ip] dscp ip-dscp-value</code></td>
<td>Marks the value for IP DSCP for IPv4 and IPv6 packets if the <code>ip</code> parameter is omitted; sets only IPv4 packets if the <code>ip</code> parameter is included</td>
</tr>
<tr>
<td><code>set cos cos-value</code></td>
<td>Marks the value for CoS</td>
</tr>
<tr>
<td><code>set qos-group group-id</code></td>
<td>Marks the group identifier for the QoS group</td>
</tr>
<tr>
<td><code>set atm-clp</code></td>
<td>Sets the ATM CLP bit</td>
</tr>
<tr>
<td><code>set fr-de</code></td>
<td>Sets the Frame Relay DE bit</td>
</tr>
</tbody>
</table>
Table 3-8  EXEC Command Reference for CB Marking

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>show policy-map policy-map-name</td>
<td>Lists configuration information about a policy map</td>
</tr>
<tr>
<td>show policy-map interface-spec [input</td>
<td>Lists statistical information about the behavior of a policy map when enabled on an interface</td>
</tr>
<tr>
<td>output] [class class-name]</td>
<td></td>
</tr>
</tbody>
</table>

CB Marking Example

The first CB Marking example uses the network shown in Figure 3-5. Traffic was generated in the network to make the show commands more meaningful. Two G.711 voice calls were completed between R4 and R1 using Foreign Exchange Station (FXS) cards on these two routers, with Voice Activity Detection (VAD) disabled. Client1 performed an FTP get of a large file from Server1, and downloaded two large HTTP objects, named important.jpg and not-so.jpg. Finally, Client1 and Server1 held a Microsoft NetMeeting conference, using G.723 for the audio and H.263 for the video.

Figure 3-5  Sample Network for CB Marking Examples

The following criteria define the requirements for marking the various types of traffic for Example 3-3:

- VoIP payload is marked with DSCP EF.
- NetMeeting video traffic is marked with DSCP AF41.
■ Any HTTP traffic whose URL contains the string “important” anywhere in the URL is marked with AF21.

■ Any HTTP traffic whose URL contains the string “not-so” anywhere in the URL is marked with AF23.

■ All other traffic is marked with DSCP Default (0).

Example 3-3 lists the annotated configuration, including the appropriate show commands.

**Example 3-3  CB Marking Example 1, with show Command Output**

```plaintext
ip cef
! Class map voip-rtp uses NBAR to match all RTP audio payload, but not the video
! or the signaling.
class-map voip-rtp
  match protocol rtp audio
! Class map http-impo matches all packets related to downloading objects whose
! name contains the string "important," with any text around it. Similar logic
! is used for class-map http-not.
class-map http-impo
  match protocol http url "*important*"

! Class map http-not
  match protocol http url "*not-so*"
! Class map NetMeet matches two RTP subtypes—one for G.723 audio (type 4) and
! one for H.263 video (type 34). Note the match-any logic so that if either is
! true, a match occurs for this class map.
class-map match-any NetMeet
  match protocol rtp payload-type 4
  match protocol rtp payload-type 34
! policy-map laundry-list calls each of the class maps. Note that the order
! listed here is the order in which the class commands were added to the policy
! map.
policy-map laundry-list
  class voip-rtp
    set ip dscp EF
  class NetMeet
    set ip dscp AF41
  class http-impo
    set ip dscp AF21
  class http-not
    set ip dscp AF23
  class class-default
    set ip DSCP default
! Above, the command class class-default is only required if some nondefault action
! needs to be taken for packets that are not explicitly matched by another class.
```
In this case, packets not matched by any other class fall into the **class-default** class, and are marked with DSCP Default (decimal 0). Without these two commands, packets in this class would remain unchanged.

Below, the policy map is enabled for input packets on fa0/0.

```bash
interface Fastethernet 0/0
service-policy input laundry-list
```

! The command `show policy-map laundry-list` simply restates the configuration.

```bash
R3# show policy-map laundry-list
Policy Map laundry-list
  Class voip-rtp
    set ip dscp 46
  Class NetMeet
    set ip dscp 34
  Class http-impo
    set ip dscp 18
  Class http-not
    set ip dscp 22
  Class class-default
    set ip dscp 0
```

! The command `show policy-map interface` lists statistics related to MQC features.
! Several stanzas of output were omitted for brevity.

```bash
R3# show policy-map interface fastethernet 0/0 input
Fastethernet0/0

Service-policy input: laundry-list

  Class-map: voip-rtp (match-all)
    35268 packets, 2609832 bytes
    5 minute offered rate 59000 bps, drop rate 0 bps
    Match: protocol rtp audio
    QoS Set
      ip dscp 46
      Packets marked 35268

  Class-map: NetMeet (match-any)
    817 packets, 328768 bytes
    5 minute offered rate 19000 bps, drop rate 0 bps
    Match: protocol rtp payload-type 4
    protocol rtp payload-type 34
    QoS Set
      ip dscp 34
      Packets marked 817
```

! omitting stanza of output for class `http-impo`
Example 3-3 includes several different classification options using the `match` command, including the matching of Microsoft NetMeeting traffic. NetMeeting uses RTP for the video flows, and by default uses G.723 for audio and H.323 for video. To match both the audio and video for NetMeeting, a class map that matches either of the two RTP payload subtypes for G.723 and H.263 is needed. So, class map `NetMeet` uses match-any logic, and matches on RTP payload types 4 (G.723) and 34 (H.263). (For more background information on RTP payload types, refer to www.cisco.com/en/US/products/ps6616/products_white_paper09186a0080110040.shtml.)

The `show policy-map interface` command provides statistical information about the number of packets and bytes that have matched each class in the policy maps. The generic syntax is as follows:

```
show policy-map interface interface-name [vc [vpi/] vci] [dlci dlci] [input | output] [class class-name]
```

The end of Example 3-3 shows a sample of the command, which lists statistics for marking. If other MQC-based QoS features were configured, statistics for those features would also be displayed. As you can see from the generic command, the `show policy-map interface` command allows you to select just one interface, either input or output, and even select a single class inside a single policy map for display.

The `load-interval` interface subcommand can also be useful when looking at any QoS tool's statistics. The `load-interval` command defines the time interval over which IOS measures packet and bit rates on an interface. With a lower load interval, the statistics change more quickly; with a larger load interval, the statistics change more slowly. The default setting is 5 minutes, and it can be lowered to 30 seconds.

Example 3-3 also shows a common oversight with QoS configuration. Note that the first class in `policy-map laundry-list` is `class voip-rtp`. Because that class map matches all RTP audio, it matches the Microsoft NetMeeting audio stream as well, so the NetMeeting audio is not matched by class `NetMeet` that follows. If the first two classes (`voip-rtp` and `NetMeet`) called in the policy map had been reversed, the NetMeeting audio would have been correctly matched in the `NetMeet` class, and all other audio would have been marked as part of the `voip-rtp` class.

---

Example:

```plaintext
Class-map: class-default (match-all)
  33216 packets, 43649458 bytes
  5 minute offered rate  747000 bps, drop rate 0 bps
Match: any
QoS Set
  ip dscp 0
Packets marked 33301
```
CB Marking of CoS and DSCP

Example 3-4 shows how a router might be configured for CB Marking when an attached LAN switch is performing QoS based on CoS. In this case, R3 looks at frames coming in its fa0/0 interface, marking the DSCP values based on the incoming CoS settings. Additionally, R3 looks at the DSCP settings for packets exiting its fa0/0 interface toward the switch, setting the CoS values in the 802.1Q header. The actual values used on R3’s fa0/0 interface for classification and marking are as follows:

- Frames entering with CoS 5 will be marked with DSCP EF.
- Frames entering with CoS 1 will be marked with DSCP AF11.
- Frames entering with any other CoS will be marked DSCP 0.
- Packets exiting with DSCP EF will be marked with CoS 5.
- Packets exiting with DSCP AF11 will be marked with CoS 1.
- Packets exiting with any other DSCP will be marked with CoS 0.

Example 3-4  Marking DSCP Based on Incoming CoS, and Vice Versa

```plaintext
! The class maps each simply match a single CoS or DSCP value.
class-map cos1
  match cos 1
!
class-map cos5
  match cos 5
!
class-map AF11
  match dscp af11
!
class-map EF
  match dscp EF
! This policy map will map incoming CoS to a DSCP value
policy-map map-cos-to-dscp
  class cos1
    set DSCP af11
  class cos5
    set ip DSCP EF
  class class-default
    set ip dscp default
! This policy map will map incoming DSCP to outgoing CoS. Note that the DSCP ! value is not changed.
policy-map map-dscp-to-cos
  class AF11
    set cos 1
  class EF
    set cos 5
```
The QoS policy requires two policy maps in this example. Policy map `map-cos-to-dscp` matches CoS values for frames entering R3’s fa0/0.1 interface, and marks DSCP values, for packets flowing right to left in Figure 3-5. Therefore, the policy map is enabled on input of R3’s fa0/0.1 interface. Policy map `map-dscp-to-cos` matches DSCP values for packets exiting R3’s fa0/0.1 interface, and marks the corresponding CoS value. Therefore, the policy map was enabled on the output of R3’s fa0/0.1 interface. Neither policy map could be applied on the WAN interface, because only interfaces configured for 802.1Q accept `service-policy` commands that reference policy maps that either classify or mark based on CoS.

Note that you cannot enable a `policy-map` that refers to CoS on interface fa0/0.2 in this example. That subinterface is in the native VLAN, meaning that no 802.1Q header is used.

### Network-Based Application Recognition

CB Marking can make use of NBAR’s powerful classification capabilities through the `match protocol` subcommand. Example 3-5 shows a configuration for CB Marking and NBAR in which the following requirements are met:

- Any HTTP traffic whose URL contains the string “important” anywhere in the URL is marked with AF21.
- Any HTTP traffic whose URL contains the string “not-so” anywhere in the URL is marked with DSCP default.
- All other traffic is marked with AF11.

Example 3-5 shows the configuration, along with a few NBAR-related `show` commands.

**Example 3-5 CB Marking Based on URLs, Using NBAR for Classification**

```plaintext
ip cef
! The "*" in the url string is a wildcard meaning "0 or more characters."
class-map http-impo
    match protocol http url "*important*"
class-map http-not
    match protocol http url "*not-so*"
```
The policy map lists the three classes in order, setting the DSCP values.

```plaintext
policy-map http
  class http-import
    set dscp AF21
  !
  class http-not
    set dscp default
  !
  class class-default
    set DSCP AF11
```

The `ip nbar protocol discovery` command may or may not be required—see the notes following this example.

```plaintext
interface fastethernet 0/0
  ip nbar protocol-discovery
  service-policy input http
```

The `show ip nbar` command only displays statistics if the `ip nbar protocol-discovery` command is applied to an interface. These statistics are independent of those created by CB Marking. This example shows several of the large number of options on the command.

```plaintext
R3# show ip nbar protocol-discovery interface fastethernet 0/0 stats packet-count top-n 5

FastEthernet0/0

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Input Packet Count</th>
<th>Output Packet Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>http</td>
<td>721</td>
<td>428</td>
</tr>
<tr>
<td>eigrp</td>
<td>635</td>
<td>0</td>
</tr>
<tr>
<td>netbios</td>
<td>199</td>
<td>0</td>
</tr>
<tr>
<td>icmp</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>bgp</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>unknown</td>
<td>46058</td>
<td>63</td>
</tr>
<tr>
<td>Total</td>
<td>47614</td>
<td>492</td>
</tr>
</tbody>
</table>
```

**Key Topic**

Before the 12.2T/12.3 IOS releases, the `ip nbar protocol-discovery` command was required on an interface before using a `service-policy` command that used NBAR matching. With 12.2T/12.3 train releases, this command is no longer required. The use of the `match protocol` command implies that NBAR will be used to match the packet.

Unlike most other IOS features, NBAR can be upgraded without changing to a later IOS version. Cisco uses a feature called *Packet Description Language Modules (PDLM)* to define new protocols that NBAR should match. When Cisco decides to add one or more new protocols to the list of protocols that NBAR should recognize, it creates and compiles a PDLM. You can then download the PDLM from Cisco, copy it into Flash memory, and add the `ip nbar pdlm pdlm-name` command to the configuration, where `pdlm-name`
is the name of the PDLM file in Flash memory. NBAR can then classify based on the protocol information from the new PDLM.

**CB Marking Design Choices**

The intent of CB Marking is to simplify the work required of other QoS tools by marking packets of the same class with the same QoS marking. For other QoS tools to take advantage of those markings, packets should generally be marked as close to the ingress point of the packet as possible. However, the earliest possible point might not be a trusted device. For example, in Figure 3-5 (the figure upon which Examples 3-3 and 3-4 are based), Server1 could set its own DSCP and even CoS if its network interface card (NIC) supported trunking. However, trusting the server administrator might or might not be desirable. So, the following rule summarizes how to choose the best location to perform marking:

Mark as close to the ingress edge of the network as possible, but not so close to the edge that the marking is made by an untrusted device.

Cisco QoS design guide documents make recommendations not only as to where to perform marking, but also as to which CoS, IPP, and DSCP values to set for certain types of traffic. Table 3-9 summarizes those recommendations.

<table>
<thead>
<tr>
<th>Type of Traffic</th>
<th>CoS</th>
<th>IPP</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice payload</td>
<td>5</td>
<td>5</td>
<td>EF</td>
</tr>
<tr>
<td>Video payload</td>
<td>4</td>
<td>4</td>
<td>AF41</td>
</tr>
<tr>
<td>Voice/video signaling</td>
<td>3</td>
<td>3</td>
<td>CS3</td>
</tr>
<tr>
<td>Mission-critical data</td>
<td>3</td>
<td>3</td>
<td>AF31, AF32, AF33</td>
</tr>
<tr>
<td>Transactional data</td>
<td>2</td>
<td>2</td>
<td>AF21, AF22, AF23</td>
</tr>
<tr>
<td>Bulk data</td>
<td>1</td>
<td>1</td>
<td>AF11, AF12, AF13</td>
</tr>
<tr>
<td>Best effort</td>
<td>0</td>
<td>0</td>
<td>BE</td>
</tr>
<tr>
<td>Scavenger (less than best effort)</td>
<td>0</td>
<td>0</td>
<td>2, 4,6</td>
</tr>
</tbody>
</table>

Also note that Cisco recommends not to use more than four or five different service classes for data traffic. When you use more classes, the difference in behavior between the various classes tends to blur. For the same reason, do not give too many data service classes high-priority service.

**Marking Using Policers**

Traffic policers measure the traffic rate for data entering or exiting an interface, with the goal of determining whether a configured traffic contract has been exceeded. The contract has two components: a traffic rate, configured in bits/second, and a burst size, configured as a number of bytes. If the traffic is within the contract, all packets are
considered to have *conformed* to the contract. However, if the rate or burst exceeds the contract, some packets are considered to have *exceeded* the contract. QoS actions can be taken on both categories of traffic.

The simplest form of policing enforces the traffic contract strictly by forwarding conforming packets and discarding packets that exceed the contract. However, both IOS policers allow a compromise action in which the policer *marks down* packets instead of dropping them. To mark down the packet, the policer re-marks a QoS field, typically IPP or DSCP, with a value that makes the packet more likely to be discarded downstream. For example, a policer could re-mark AF11 packets that exceed a contract with a new DSCP value of AF13, but not discard the packet. By doing so, the packet still passes through the router, but if the packet experiences congestion later in its travels, it is more likely to be discarded than it would have otherwise been. (Remember, DiffServ suggests that AF13 is more likely to be discarded than AF11 traffic.)

When marking requirements can be performed by using CB Marking, CB Marking should be used instead of either policer. However, if a requirement exists to mark packets based on whether they conform to a traffic contract, marking with policers must be used. Chapter 5, “Shaping, Policing, and Link Fragmentation,” covers CB policing, with an example of the syntax it uses for marking packets.

**QoS Pre-Classification**

With unencrypted, unencapsulated traffic, routers can match and mark QoS values, and perform ingress and egress actions based on markings, by inspecting the IP headers. However, what happens if the traffic is encrypted? If we encapsulate traffic inside a VPN tunnel, the original headers and packet contents are unavailable for inspection. The only thing we have to work with is the ToS byte of the original packet, which is automatically copied to the tunnel header (in IPsec transport mode, in tunnel mode, and in GRE tunnels) when the packet is encapsulated. But features like NBAR are broken when we are dealing with encapsulated traffic.

The issue that arises from this inherent behavior of tunnel encapsulation is the inability of a router to take egress QoS actions based on encrypted traffic. To mitigate this limitation, Cisco IOS includes a feature called QoS pre-classification. This feature can be enabled on VPN endpoint routers to permit the router to make egress QoS decisions based on the original traffic, before encapsulation, rather than just the encapsulating tunnel header. QoS pre-classification works by keeping the original, unencrypted traffic in memory until the egress QoS actions are taken.

You can enable QoS pre-classification in tunnel interface configuration mode, virtual-template configuration mode, or crypto map configuration mode by issuing the `qos pre-classify` command. You can view the effects of pre-classification using several `show` commands, which include `show interface` and `show crypto-map`.

Table 3-10 lists the modes in which you apply the `qos pre-classify` command.
Table 3-10  Where to Use the qos pre-classify Command

<table>
<thead>
<tr>
<th>Configuration Command Under Which qos pre-classify Is Configured</th>
<th>VPN Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface tunnel</td>
<td>GRE and IPIP</td>
</tr>
<tr>
<td>interface virtual-template</td>
<td>L2F and L2TP</td>
</tr>
<tr>
<td>crypto map</td>
<td>IPSec</td>
</tr>
</tbody>
</table>

Policy Routing for Marking

Policy routing provides the capability to route a packet based on information in the packet besides the destination IP address. The policy routing configuration uses route maps to classify packets. The route-map clauses include set commands that define the route (based on setting a next-hop IP address or outgoing interface).

Policy routing can also mark the IPP field, or the entire ToS byte, using the set command in a route map. When you use policy routing for marking purposes, the following logic sequence is used:

1. Packets are examined as they enter an interface.
2. A route map is used to match subsets of the packets.
3. Mark either the IPP or entire ToS byte using the set command.
4. The traditional policy routing function of using the set command to define the route might also be configured, but it is not required.

Policy routing should be used to mark packets only in cases where CB Marking is not available, or when a router needs to both use policy routing and mark packets entering the same interface.

AutoQoS

AutoQoS is a macro that helps automate class-based quality of service (QoS) configuration. It creates and applies QoS configurations based on Cisco best-practice recommendations. Using AutoQoS provides the following benefits:

- Simpler QoS deployment.
- Less operator error, because most steps are automated.
- Cheaper QoS deployment because less staff time is involved in analyzing network traffic and determining QoS configuration.
- Faster QoS deployment because there are dramatically fewer commands to issue.
- Companies can implement QoS without needing an in-depth knowledge of QoS concepts.
There are two flavors—AutoQoS for VoIP and AutoQoS for the Enterprise—as discussed in the following sections.

**AutoQoS for VoIP**

AutoQoS for VoIP is supported on most Cisco switches and routers, and provides QoS configuration for voice and video applications. It is enabled on individual interfaces, but creates both global and interface configurations. When enabled on access ports, AutoQoS uses Cisco Discovery Protocol (CDP) to detect the presence or absence of a Cisco phone or softphone, and configures the interface QoS appropriately. When enabled on uplink or trunk ports, it trusts the COS or DSCP values received and sets up the interface QoS.

**AutoQoS VoIP on Switches**

AutoQoS assumes that switches will have two types of interfaces: user access and uplink. It also assumes that a user access interface might or might not have an IP phone connected to it. There is no need to enable QoS globally. After it is enabled for any interface, the command starts a macro that globally enables QoS, configures interface ingress and egress queues, configures class maps and policy maps, and applies the policy map to the interface.

AutoQoS is enabled for an access interface by the interface-level command `auto qos voip {cisco-phone | cisco-softphone}`. When you do this, the switch uses CDP to determine whether a Cisco phone or softphone is connected to the interface. If one is not found, the switch marks all traffic down to DSCP 0 and treats it as best effort. This is the default behavior for a normal trunk port. If a phone is found, the switch then trusts the QoS markings it receives. On the ingress interface, the following traffic is put into the priority, or expedite, queue:

- Voice and video control traffic
- Real-time video traffic
- Voice traffic
- Routing protocol traffic
- Spanning-tree BPDU traffic

All other traffic is placed in the normal ingress queue. On the egress side, voice is placed in the priority queue. The remaining traffic is distributed among the other queues, depending on the number and type of egress queues supported by that particular switch or switch module.

AutoQoS is enabled for an uplink port by the interface-level command `auto qos voip trust`. When this command is given, the switch trusts the COS values received on a Layer 2 port and the DSCP values received on a Layer 3 port.
The AutoQoS macro also creates quite a bit of global configuration in the switch. It generates too much to reproduce here, but the following list summarizes the configuration created:

- Globally enables QoS.
- Creates COS-to-DCSP mappings and DSCP-to-COS mappings. As the traffic enters the switch, the frame header containing the COS value is removed. The switch uses the COS value in the frame header to assign a DSCP value to the packet. If the packet exits a trunk port, the internal DSCP value is mapped back to a COS value.
- Enables priority or expedite ingress and egress queues.
- Creates mappings of COS values to ingress and egress queues and thresholds.
- Creates mappings of DSCP values to ingress and egress queues and thresholds.
- Creates class maps and policy maps to identify, prioritize, and police voice traffic. Applies those policy maps to the interface.

For best results, enable AutoQoS before configuring any other QoS on the switch. You can then go back and modify the default configuration if needed to fit your specific requirements.

### AutoQoS VoIP on Routers

The designers of AutoQoS assumed that routers would be connecting to downstream switches or the WAN, rather than user access ports. Therefore, the VoIP QoS configuration is simpler. The command to enable it is `auto qos voip [trust]`. Make sure that the interface bandwidth is configured before giving this command. If you change it later, the QoS configuration will not change. When you issue the `auto qos voip` command on an individual data circuit, the configuration it creates differs depending on the bandwidth of the circuit itself. Compression and fragmentation are enabled on links of 768 kbps bandwidth and lower. They are not enabled on links faster than 768 kbps. The router additionally configures traffic shaping and applies an AutoQoS service policy regardless of the bandwidth.

When you issue the command on a serial interface with a bandwidth of 768 kbps or less, the router changes the interface encapsulation to PPP. It creates a PPP Multilink interface and enables Link Fragmentation and Interleave (LFI) on the interface. Serial interfaces with a configured bandwidth greater than 768 kbps keep their configured encapsulation, and the router merely applies an AutoQoS service policy to the interface.

If you use the `trust` keyword in the command, the router creates class maps that group traffic based on its DSCP values. It associates those class maps with a created policy map and assigns it to the interface. You would use this keyword when QoS markings are assigned by a trusted device.
If you do not use the **trust** keyword, the router creates access lists that match voice and video data and call control ports. It associates those access lists with class maps with a created policy map that marks the traffic appropriately. Any traffic not matching those access lists is marked with DSCP 0. You would use this command if the traffic either arrives at the router unmarked or arrives marked by an untrusted device.

### Verifying AutoQoS VoIP

Displaying the running configuration shows all the mappings, class and policy maps, and interface configurations created by the AutoQoS VoIP macro. Use the following commands to get more specific information:

- **show auto qos**: Displays the interface AutoQoS commands
- **show mls qos**: Has several modifiers that display queuing and COS/DSCP mappings
- **show policy-map interface**: Verifies the actions of the policy map on each interface specified

### AutoQoS for the Enterprise

AutoQoS for the Enterprise is supported on Cisco routers. The main difference between it and AutoQoS VoIP is that it automates the QoS configuration for VoIP plus other network applications, and is meant to be used for WAN links. It can be used for Frame Relay and ATM subinterfaces only if they are point-to-point links. It detects the types and amounts of network traffic and then creates policies based on that. As with AutoQoS for VoIP, you can modify those policies if you desire. There are two steps to configuring Enterprise AutoQoS. The first step discovers the traffic, and the second step provides the recommended QoS configuration.

### Discovering Traffic for AutoQoS Enterprise

The command to enable traffic discovery is **auto discovery qos [trust]** and is issued at the interface, DLCI, or PVC configuration level. Make sure that Cisco Express Forwarding (CEF) is enabled, that the interface bandwidth is configured, and that no QoS configuration is on the interface before giving the command. Use the **trust** keyword if the traffic arrives at the router already marked, and if you trust those markings, because the AutoQoS policies will use those markings during the configuration stage.

Traffic discovery uses NBAR to learn the types and amounts of traffic on each interface where it is enabled. You should run it long enough for it to gather a representative sample of your traffic. The router will classify the traffic collected into one of ten classes. Table 3-11 shows the classes, the DSCP values that will be mapped to each if you use the **trust** option in the command, and sample types of traffic that NBAR will map to each. Note that the traffic type is not a complete list, but is meant to give you a good feel for each class.
Table 3-11  *AutoQoS for the Enterprise Classes and DSCP Values*

<table>
<thead>
<tr>
<th>Class</th>
<th>DSCP/PHB Value</th>
<th>Traffic Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing</td>
<td>CS6</td>
<td>EIGRP, OSPF</td>
</tr>
<tr>
<td>VoIP</td>
<td>EF (46)</td>
<td>RTP Voice Media</td>
</tr>
<tr>
<td>Interactive video</td>
<td>AF41</td>
<td>RTP Video Media</td>
</tr>
<tr>
<td>Streaming video</td>
<td>CS4</td>
<td>Real Audio, Netshow</td>
</tr>
<tr>
<td>Control</td>
<td>CS3</td>
<td>RTCP, H323, SIP</td>
</tr>
<tr>
<td>Transactional</td>
<td>AF21</td>
<td>SAP, Citrix, Telnet, SSH</td>
</tr>
<tr>
<td>Bulk</td>
<td>AF11</td>
<td>FTP, SMTP, POP3, Exchange</td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1</td>
<td>Peer-to-peer applications</td>
</tr>
<tr>
<td>Management</td>
<td>CS2</td>
<td>SNMP, Syslog, DHCP, DNS</td>
</tr>
<tr>
<td>Best effort</td>
<td>All others</td>
<td>All others</td>
</tr>
</tbody>
</table>

**Generating the AutoQoS Configuration**

When the traffic discovery has collected enough information, the next step is to issue the `auto qos` command on the interface. This runs a macro that creates templates based on the traffic collected, creates class maps to classify that traffic, and creates a policy map to allocate bandwidth and mark the traffic. The router then automatically applies the policy map to the interface. In the case of a Frame Relay DLCI, the router applies the policy map to a Frame Relay map class, and then applies that class to the DLCI. You can optionally turn off NBAR traffic collection with the `no auto discovery qos` command.

**Verifying AutoQoS for the Enterprise**

As with AutoQoS VoIP, displaying the running configuration will show all the mappings, class and policy maps, and interface configurations created by the AutoQoS macro. Use the following commands to get more specific information:

- `show auto discovery qos`: Lists the types and amounts of traffic collected by NBAR
- `show auto qos`: Displays the class maps, policy maps, and interface configuration generated by the AutoQoS macro
- `show policy-map interface`: Displays each policy map and the actual effect it had on the interface traffic
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 3-12 lists the various match commands that can be used for MQC tools like CB Marking.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>match [ip] precedence precedence-value [precedence-value precedence-value precedence-value]</td>
<td>Matches precedence in IPv4 packets when the ip parameter is included; matches IPv4 and IPv6 packets when the ip parameter is missing.</td>
</tr>
<tr>
<td>match access-group {access-group</td>
<td>Matches an ACL by number or name.</td>
</tr>
<tr>
<td>name access-group-name}</td>
<td></td>
</tr>
<tr>
<td>match any</td>
<td>Matches all packets.</td>
</tr>
<tr>
<td>match class-map class-map-name</td>
<td>Matches based on another class map.</td>
</tr>
<tr>
<td>match destination-address mac address</td>
<td>Matches a destination MAC address.</td>
</tr>
<tr>
<td>match fr-dlci dlci-number</td>
<td>Matches a particular Frame Relay DLCI.</td>
</tr>
<tr>
<td>match input-interface interface-name</td>
<td>Matches an ingress interface.</td>
</tr>
<tr>
<td>match ip dscp [ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value ip-dscp-value]</td>
<td>Matches DSCP in IPv4 packets when the ip parameter is included; matches IPv4 and IPv6 packets when the ip parameter is missing.</td>
</tr>
<tr>
<td>match ip rtp starting-port-number port-range</td>
<td>Matches the RTP's UDP port-number range, even values only.</td>
</tr>
<tr>
<td>match mpls experimental number</td>
<td>Matches an MPLS Experimental value.</td>
</tr>
<tr>
<td>match mpls experimental topmost value</td>
<td>When multiple labels are in use, matches the MPLS EXP field in the topmost label.</td>
</tr>
<tr>
<td>match not match-criteria</td>
<td>Reverses the matching logic. In other words, things matched by the matching criteria do not match the class map.</td>
</tr>
</tbody>
</table>
Table 3-13 lists AutoQoS and QoS verification commands.

### Table 3-13  AutoQoS and QoS Verification Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto qos voip [cisco-phone</td>
<td>Enables AutoQoS VoIP on a switch access</td>
</tr>
<tr>
<td>cisco-softphone]</td>
<td>interface</td>
</tr>
<tr>
<td>auto qos voip trust</td>
<td>Enables AutoQoS VoIP on a switch uplink interface</td>
</tr>
<tr>
<td>auto qos voip [trust]</td>
<td>Enables AutoQoS VoIP on a router interface</td>
</tr>
<tr>
<td>auto discovery qos [trust]</td>
<td>Enables NBAR traffic discovery for AutoQoS Enterprise</td>
</tr>
<tr>
<td>auto qos</td>
<td>Enables AutoQoS Enterprise on an interface</td>
</tr>
<tr>
<td>show auto qos</td>
<td>Displays the interface AutoQoS commands</td>
</tr>
<tr>
<td>show mls qos</td>
<td>Displays queueing and COS/DSCP mappings</td>
</tr>
<tr>
<td>show policy-map interface</td>
<td>Displays the interface queuing actions caused by the</td>
</tr>
<tr>
<td></td>
<td>policy map</td>
</tr>
<tr>
<td>show auto discovery qos</td>
<td>Displays the traffic collected by NBAR</td>
</tr>
<tr>
<td>show auto qos</td>
<td>Displays the configuration generated by the AutoQoS</td>
</tr>
<tr>
<td></td>
<td>macro</td>
</tr>
</tbody>
</table>
Table 3-14 lists the RFCs related to DiffServ.

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2474</td>
<td>Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers</td>
<td>Contains the details of the 6-bit DSCP field in an IP header</td>
</tr>
<tr>
<td>2475</td>
<td>An Architecture for Differentiated Service</td>
<td>The core DiffServ conceptual document</td>
</tr>
<tr>
<td>2597</td>
<td>Assured Forwarding PHB Group</td>
<td>Defines a set of 12 DSCP values and a convention for their use</td>
</tr>
<tr>
<td>3246</td>
<td>An Expedited Forwarding PHB</td>
<td>Defines a single DSCP value as a convention for use as a low-latency class</td>
</tr>
<tr>
<td>3260</td>
<td>New Terminology and Clarifications for DiffServ</td>
<td>Clarifies, but does not supersede, existing DiffServ RFCs</td>
</tr>
</tbody>
</table>

**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:

- IP Precedence, ToS byte, Differentiated Services, DS field, Per-Hop Behavior, Assured Forwarding, Expedited Forwarding, Class Selector, Class of Service, Differentiated Services Code Point, User Priority, Discard Eligible, Cell Loss Priority, MPLS Experimental bits, class map, policy map, service policy, Modular QoS CLI, Class-Based Marking, Network-Based Application Recognition, QoS preclassification, AutoQoS

Refer to the glossary to check your answers.
Further Reading

*Cisco QoS Exam Certification Guide*, by Wendell Odom and Michael Cavanaugh

*End-to-End QoS Network Design*, by Tim Szigeti and Christina Hattingh

Numerics

802.1X authentication, 423-426

A

AAA (authentication, authorization, and accounting), 406-410
   enabling, 407
   RADIUS server groups, configuring, 410
accessing CLI via Telnet, 405
ACE (access control entry) logic, 431-432
ACLs, 430-433
   ACE logic, 431-432
   command reference, 430
   PACLs, 475
   rules, 431-432
   VACLs, 475
   wildcard masks, 433
ACS (Cisco Access Control Server), 407
activating the practice exam, 574
active state (BGP), 16
adaptive shaping, 222
address families, 58
adjacencies (PIM-DM), forming, 329-330
administrative scoping, 328-329
administrative weight, BGP decision process, 101-104
advertising BGP routes, 31-40
   best route selection, 33-34
   rules, 40
AF (Assured Forwarding) PHB, 141-142
   converting values to decimal, 142
aggregate-address command, 25-29
   route filtering, 81-82
AGGREGATOR PA, 94
Anycast RP with MSDP, 365-367
AS (autonomous systems)
   BGP sync, disabling, 46-47
   confederations, 47-52
      configuring, 49-52
      routing loops, preventing, 47
   eBGP neighbors, configuring, 13-14
   iBGP neighbors, 9-12
      configuring, 11-12
   neighbor relationships, requirements for, 14-15
AS_CONFED_SEQ segment, 82
AS_PATH PA, 8, 94
   prepend feature, 109-112
   private ASNs, removing, 108-109
   route filtering, 82-93
      examples, 87-91
matching AS_SET and AS_CONFED_SEQ, 91-93
regular expressions, 84-85
segments, 26, 82-84
shortest AS_PATH as BGP decision point, 107-108
summary routes, injecting into BGP, 25-29
AS_SEQ segment, 26, 82
AS_SET segment, 82
ASNs (autonomous system numbers), 8
removing private ASNs, 108-109
Assert messages (PIM-DM), 341-342
ATM (Asynchronous Transfer Mode), QoS marking-eligible fields, 143-144
AToM (Any Transport over MPLS), 504-505
ATOMIC AGGREGATE PA, 27, 94
attacks
  gratuitous ARPs, 417-419
  inappropriate IP addresses, preventing, 435-436
  smurf attacks, mitigating, 433-435
  TCP SYN floods, mitigating, 436-437
attributes, MP-BGP, 57-58
authentication
  802.1X, 423-426
  BGP neighbors, 9
  overriding default login authentication methods, 410-412
  PPoE, 260-261
  RADIUS, 406-407
    server groups, configuring, 410
  TACACS+, 406-407
    using multiple authentication methods, 408-409
automatic 6to4 tunnels, 499-501
automatic IPv4-compatible tunnels, 499
AutoQoS, 160-164
  for the Enterprise, 163-164
  for VoIP
    on routers, 162-163
    on switches, 161-162
    verifying, 163
Auto-RP, 359-363
auto-summary command, 23-25
average queue depth, 187

B

backdoor routes, 41-42
bandwidth
  CB Shaping based on, 221
  reserving
    CBWFQ, 180-182
    LLQ, 184-185
RSVP, 199-204
  configuring, 201-202
  reservation process, 200-201
  for voice calls, 203-204
Bc (committed burst), 212
default values, 229
Be (excess burst), 212-213
best practices
  for Layer 2 security, 427-429
  for port security, 413
best route selection. See also decision process (BGP)
administrative weight, 101-104
BGP, 33-34
highest local preference as decision point, 104
maximum-paths command, 118
mnemonics for memorizing decision points, 98-99
PAs used for, 99-101
tiebreaker steps, 95-97, 116-117
BGP
AS_PATH attribute, 8
AS_PATH PA, route filtering, 82-93
best route selection, 33-34
tiebreaker steps, 95-97
CLUSTER_LIST PA, 54
communities, 119-126
confederations, 47-52
configuring, 49-52
routing loops, preventing, 47
convergence, 126-128
fast external neighbor loss detection, 127
fast session deactivation, 128
internal neighbor loss detection, 127
decision process
  administrative weight, 101-104
  best ORIGIN PA selection, 112
  highest local preference, 104-107
  maximum-paths command, 118
  mnemonics for memorizing, 98-99
  neighbor type selection, 116
  NEXT_HOP reachability, 101, 116
  PAs, 99-101
tiebreaker steps, 116-117
decision process (BGP)
locally injected route selection, 107
shortest AS_PATH as BGP decision point, 107-108
smallest MED PA, 112-113
hold time, 9
iBGP neighbors
  configuring, 11-12
IP routing table, building
  adding iBGP-learned routes to IP routing table, 42-44
  backdoor routes, 41-42
  eBGP routes, adding, 40-41
keepalive interval, 9
Keepalive messages, 16
MED PA, 21
messages, Notification messages, 16
MP-BGP, 57-62
  attributes, 57-58
  configuring, 58-62
neighbor relationships, building, 9-18
eBGP neighbors, 9, 13-14
iBGP neighbors, 9-12
internal BGP neighbors, 9
requirements for, 14-15
neighbor states, 15-16
network command, 18-21
NEXT_HOP PA, 23
Open messages, 9, 16
ORIGIN PA, 30-31
ORIGINATOR_ID PA, 54
PAs
  characteristics of, 93-95
  optional, 94
  well-known, 93
path vector logic, 8
RIB
  building, 18-40
  classful networks, injecting, 23-25
default routes, injecting, 29-30
route advertisement process, 31-40
  summary routes, injecting, 25-29
route filtering, 75-93
  NLRI-based, 76-79
route maps, 79
  using aggregate-address command, 81-82
route redistribution, 21-23
routing policies, 69
RRs, 52-57
soft reconfiguration, 79-80
synchronization, 44-47
  disabling, 46-47
Update messages, 9, 16
Bidirectional PIM, 370-371
binding table (IPv6), 469-471
black holes, 44-47
BSR (BootStrap Router), 363-365, 381-384

building
BGP neighbor relationships, 9-18
eBGP neighbors, 9, 13-14
  established state, 9
iBGP neighbors, 9-12
  internal BGP neighbors, 9
resetting peer connections, 16-18
IP routing table
  backdoor routes, 41-42
eBGP routes, adding, 40-41
iBGP routes, adding, 42-44
RIB, 18-40

C

C&M (classification and marking)
ATM fields, marking, 143-144
CB Marking, 146-147
  configuring, 150
  CoS field, 155-156
design choices, 158
  DSCP field, 155-156
dual-action policing, 229
examples of, 151-154
  NBAR, 156-158
CB Policing
  CAR, 231-233
dual-rate policing, 229
multi-action policing, 229-230
  per class policing, 228
  percentage-based policing, 230-231
  single rate, three-color policing, 224-225
  single rate, two-color policing, 223-224
two-rate, three-color policing, 225-226
EF PHB, 142
Ethernet CoS field, 143
Frame Relay fields, marking, 143-144
IP Precedence field
  marking, 140
locations for marking, 144
NBAR, 149
policers, 158-159
policy routing, 160
QoS pre-classification, 159

calculating Tc, 213
CAR (committed access rate), 231-233

CB Marking, 146-147
  configuring, 150
  CoS field, 155-156
design choices, 158
DSCP field, 155-156
examples of, 151-154
NBAR, 156-158

CB Policing
  Bc, default values, 229
  CAR, 231-233
  configuring, 227
dual-rate policing, 229
  multi-action policing, 229-230
per class policing, 228
  percentage-based policing, 230-231
  single rate, three-color policing,
    224-225, 227-228
  single rate, two-color policing, 223-224
two-rate, three-color policing, 225-226

CB Shaping, 216-222
  adaptive shaping, 222
based on bandwidth percent, 221
rules for, 218

  shaping to peak rate, 222
  voice traffic shaping with LLQ, 218

CBAC (Context-Based Access Control), 438-439
CBWFQ (class-based weighted fair queuing), 176-182
configuring, 179-180
features, 178
  limiting bandwidth, 180-182

CE (customer edge), 537
CEF (Cisco Express Forwarding), 520-521

CGA (Cryptographical Generated Addresses), 466

CGMP (Cisco Group Management Protocol), 296-302

CHAP (Challenge Handshake Authentication Protocol), 411
characteristics of PAs, 93-95
CIR (committed information rate), 211

Cisco 3650 switches
  egress queuing, 197-199
  ingress queuing, 193-197
    congestion avoidance, 195-196
    priority queues, creating, 193-195

Cisco 12000 Series routers, MDRR, 190-192

Cisco IOS Firewall, 438-450
  caveats, 440
  CBAC, 438-439
  configuring, 440-441
  protocol support, 439-440

Cisco Learning Network, 575

Cisco SAFE Blueprint document, 412

class maps, 146-149
  configuring on ZFW, 444-445
  using multiple match commands, 147-149
classful networks, injecting into RIB, 23-25
classification
  using class maps, 146-149
  using NBAR, 149
clear ip bgp command, 17
CLI
  password protection, 403-412
    enable password command, 405
    overriding default login authentication methods, 403-412
  PPP security, 411-412
  simple password protection, 403-404
  SSH, 405-406
    using multiple authentication methods, 408-409
  Telnet access, 405
client configuration, PPoE, 259-260
clock rate, 211
CLUSTER_LIST PA, 54, 94
codes, ORIGIN PA, 30
commands
  aggregate-address command, 25-29, 81-82
  auto-summary command, 23-25
  clear ip bgp command, 17
  debug ip bgp command, 16-18
  enable password command, 405
  helpful QoS troubleshooting commands, 240
  IP ACL command reference, 430
  maximum-paths, 118
  neighbor default-originate command, 30
  network command, 18-21
  pre-classify command, 159
router bgp command, 11-14
service password-encryption command, 404
service-policy output command, 217
shape command, 218
shape percent command, 221
show ip bgp command, 22-23, 34-37
show policy-map interface command, 154
xconnect command, 504
communities, 119-126
community lists, 123-124
COMMUNITY PA, 119-126
  community lists, 123-124
  removing strings from, 124-125
comparing
  IGMP versions, 295
  PIM-DM and PIM-SM, 346, 371
  prefix lists, route maps, and distribute lists, 80
  queuing tools, 176
compression, PPP, 255
  header compression, 256-257
  Layer 2 payload compression, 256
confederations, 47-52
  configuring, 49-52
  routing loops, preventing, 47
configuring
  BGP
    confederations, 49-52
    eBGP neighbors, 13-14
    iBGP neighbors, 11-12
    MED PA, 114-115
  CB Marking, 150
  CB Policing, 227
    dual-rate policing, 229
CBWFQ, 179-180
Cisco IOS Firewall, 440-441
DMVPN, 452-461
HDLC, 247-249
MP-BGP, 58-62
MPLS VPNs, 546-558
port security, 415-417
PPP, 405-406
RADIUS server groups, 410
RSVP, 201-202
SSH, 406
TCP intercept, 437-438
WRED, 189-190
ZFW
   class maps, 444-445
   zones, 443
conforming packets with single rate,
two-color policing, 223-224
congestion avoidance, on Cisco 3650
switches, 195-196
connect state (BGP), 16
contents of Update messages, viewing,
34-37
control plane, 526-527, 539
convergence, BGP, 126-128
   fast external neighbor loss detection,
   127
   fast session deactivation, 128
   internal neighbor loss detection, 127
converting AF values to decimal, 142
CoPP (control-plane policing), 446-450
CoS (Class of Service), CB Marking,
   155-156
CQ (custom queuing), 176

D
DAI (Dynamic ARP Inspection),
   417-420
   gratuitous ARPs, preventing, 417-419
data plane, 520
debug ip bgp command, 16-18
decision process (BGP), 95-96
   administrative weight, 101-104
   best ORIGIN PA selection, 112
   highest local preference, 104-107
   locally injected routes, 107
   maximum-paths command, 118
   mnemonics for memorizing, 98-99
   neighbor type selection, 116
   NEXT_HOP reachability, 116
   PAs, 99-101
   smallest MED PA, 112-113
   tiebreakers, 116-117
Deering, Dr. Steve, 270
default routes, injecting into RIB, 29-30
default values for Bc, 229
deficit feature (MDRR), 192
dense-mode routing protocols, 322-323,
   329-345
DVMRP, 343
MOSPF, 343-345
PIM-DM, 329
   adjacencies, forming, 329-330
   Assert messages, 341-342
   DRs, 343
   Graft messages, 339-340
   Hello messages, 329-330
   LAN-specific issues, 340
   messages, 343
   Prune messages, 331-333
Prune Override, 340-341
pruning, 335-337
reacting to failed links, 333-335
source-based distribution trees, 330-331
State Refresh message, 337-338
design choices for CB marking, 158
designated priority manipulation, 376-377
device tracking, 471-472
DHCP snooping, 420-422
DHCPv6 Guard, 468-471
DiffServ, 140
directed broadcasts, 434
disabling BGP sync, 46-47
discard categories (WRED), 187
displaying Update message contents, 34-37
distribute lists, 76-79
  comparing with route maps and prefix lists, 80
DMVPN (Dynamic Multipoint VPN), 451-461
  benefits of, 451
  configuring, 452-461
tunneling, 487-495
"Do I Know This Already?" quizzes
   Chapter 1, 4-7
   Chapter 2, 70-74
   Chapter 3, 135-138
   Chapter 4, 172-174
   Chapter 5, 208-210
   Chapter 6, 245-246
   Chapter 7, 267-269
   Chapter 8, 318-320
   Chapter 9, 400-402
   Chapter 10, 483-485
   Chapter 11, 516-518
downloading practice exam, 574
DRs (designated routers), 343
DSCP (Differentiated Services Code Point) field
   AF PHB, 141-142
   CB Marking, 155-156
   EF PHB, 142
   Ethernet CoS field, marking, 143
   marking, 139-142
dual-rate policing, 229
DVMRP (Distance Vector Multicast Routing Protocol), 343

E

EAP (Extensible Authentication Protocol), 423-426
eBGP neighbors, 9
  adding eBGP-learned routes to IP routing table, 40-41
  configuring, 13-14
EF (Expedited Forwarding) PHB, 142
egress blocking, 211
egress queuing on Cisco 3650 switches, 197-199
embedded RP, 389-392
enable password command, 405
enabling AAA, 407
enforcing traffic contracts, 158-159
established state (BGP), 16
establishing BGP neighbors, requirements, 14-15
EWAN (Ethernet WAN), 262-263
  Metro-E, 263
  VPLS, 262-263
exam, preparing for, 573-576
  Cisco Learning Network, 575
  memory tables, 575-576
  Pearson Cert Practice Test engine, 573
  activating the practice exam, 574
  installing, 574
examples
  of AS_PATH PA matching, 87-91
  of CB Marking, 151-154
exceeding packets, single rate, two-color policing, 223-224
extended community attribute (MP-BGP), 60

F

failed links (PIM-DM), reacting to, 333-335
fast external neighbor loss detection, 127
fast session deactivation, 128
features
  of CBWFQ, 178
  of IGMP, 284-285
  of LOCAL_PREF PA, 104
  of network command, 19
FEC (Forwarding Equivalence Class), 565
FHS (first hop security), 461-475
  DHCPv6 Guard, 468-471
  ICMPv6, 464-465
  IPv6 Source Guard, 473-475
  link operations, 463-464
  ND inspection, 472-473
  NDP, 464-465
  PACLs (port access lists), 475
  RA Guard, 467-468
  SeND, 465-466
FIB (Forwarding Information Base), 522-523
fields
  of IGMP, 283-284
  of MPLS header, 524-526
  QoS marking-eligible fields
    DSCP, 139-142
    Ethernet CoS, 143
    IP Precedence, 139-140
  of Update messages, 32
FIFO (first in, first out) queuing, 175
filtering BGP routes, 75-93
  based on NLRI, 76-79
  matching AS_PATH PA, 82-93
    examples, 87-91
    regular expressions, 84-85
  route maps, 79
  using aggregate-address command, 81-82
  using COMMUNITY PA values, 125-126
finding RPs, 358-369
  with Auto-RP, 359-363
  with BSR, 363-365
  using Anycast RP with MSDP, 365-367
firewalls
  Cisco IOS Firewall, 438-450
    caveats, 440
    CBAC, 438-439
    configuring, 440-441
    protocol support, 439-440
  CoPP, 446-450
IGMP (Internet Group Management Protocol) 593

ZFW, 441-446
   class maps, configuring, 444-445
   zones, configuring, 443
Frame Relay, QoS marking-eligible fields, 143-144
full drop, 187

G

GDOI (Group Domain of Interpretation), 506
GET (Group Encrypted Transport) VPN, 506-511
KS, 506
Rekey phase, 507
GLOP addressing, 278
Graft messages (PIM-DM), 339-340
gratuitous ARPs, 417-419
GRE (Generic Routing Encapsulation) tunnels, 486-487
   IPv6-over-IPv4 tunnels, 499
Group-Specific Query messages, 289-291
GTS (Generic Traffic Shaping), 214-216

H

hardware queuing, 175-176
HDLC (High-Level Data Link Control), 247-249
header compression (PPP), 256-257
header fields, MPLS, 524-526
Hello messages (PIM-DM), 329-330
helpful QoS troubleshooting commands, 240
hierarchical policy maps, 221
highest local preference as BGP decision point, 104-107
hold time (BGP), 9
Host Membership Protocol, 283
Host Membership Query messages, 285-286
Host Membership Report messages, 286
HQF (Hierarchical Queuing Framework), 233-237

I

IANA (Internet Assigned Numbers Authority), 276
iBGP neighbors, 9-12
   adding iBGP-learned routes to IP routing table, 42-44
   configuring, 11-12
ICMPv6 (Internet Control Message Protocol version 6), 464-465
idle state (BGP), 16
IGMP (Internet Group Management Protocol), 281-283, 295
   features, 284-285
   fields, 283-284
   Group-Specific Query messages, 289-291
   Host Membership Query messages, 285-286
   Host Membership Report messages, 286
   interoperability with version 2, 294-295
   joining a group, 282
   Leave Group messages, 289-291
   querier election process, 291
   Report Suppression process (IGMP), 286-287
Solicited Host Membership Report process, 286-287

timers, 292
traffic filters, 309-310

Unsolicited Host Membership Report messages, 288

IGMP proxy, 310-313

IGMP snooping, 303-307

IGMPv3, 292-293

IGPs (Interior Gateway Protocols), 8

inappropriate IP addresses, preventing, 435-436

incomplete ORIGIN code, 30

ingress queuing on Cisco 3650 switches, 193-197

congestion avoidance, 195-196

priority queues, creating, 193-195

injecting
classful networks into BGP, 23-25
default routes into RIB, 29-30
summary routes into BGP, 25-29

installing Pearson Cert Practice Test engine, 574

interdomain multicast routing with MSDP, 367-369

interfaces, queuing, 176

internal BGP neighbors, 9

internal neighbor loss detection, 127

IP ACLs, 430-433

command reference, 430
rules, 431-432
wildcard masks, 433

IP header

DSCP field

CB Marking, 155-156

PHBs, 140-142

IP Precedence field, QoS marking, 139-140

IP multicast, 273-275

addresses, 276-281

address ranges, 279
GLOP addresses, 278
mapping to MAC addresses, 280-281

for permanent groups, 277

for private multicast domains, 278

for source-specific applications and protocols, 278

well-known multicast addresses, 276

administrative scoping, 328-329

CGMP, 296-302
dense-mode routing protocols, 322-323, 329-345

DVMRP, 343

MOSPF, 343-345

PIM-DM, 329-343

IGMP, 281-283

features, 284-285
fields, 283-284

Group-Specific Query messages, 289-291

Host Membership Query messages, 285-286

Host Membership Report messages, 286

interoperability with version 2, 294-295

joining a group, 282

Leave Group messages, 289-291

querier election process, 291

Report Suppression process, 286-287
Solicited Host Membership Report process, 286-287
timers, 292
traffic filters, 309-310
Unsolicited Host Membership Report messages, 288
IGMP proxy, 310-313
IGMP snooping, 303-307
IPv6 multicast
  BSR, 381-384
designated priority manipulation, 376-377
embedded RP, 389-392
hello interval, 377-378
MLD, 385-389
static RP, 379-381
need for, 270-272
requirements for supporting, 273
RGMP, 307-309
RPF check, 323-325
sparse-mode routing protocols, 325-327, 345-373
  Bidirectional PIM, 370-371
SSM, 372-373
TTL scoping, 327-328
IP Precedence field, QoS marking, 139-140
IP routing table (BGP), building, 40-57
  backdoor routes, 41-42
eBGP routes, adding, 40-41
IP Source Guard, 422-423
IPsec, VTIs, 486
IPv6
  binding table, 469-471
device tracking, 471-472
FHS, 461-475
  DHCPv6 Guard, 468-471
  ICMPv6, 464-465
  link operations, 463-464
  NDP, 464-465
  RA Guard, 467-468
multicast, 373-392
  BSR, 381-384
designated priority manipulation, 376-377
  embedded RP, 389-392
  hello interval, 377-378
  MLD, 385-389
  static RP, 379-381
ND inspection, 472-473
tunneling, 495-496
  AToM, 504-505
  automatic 6to4 tunnels, 499-501
  automatic IPv4-compatible tunnels, 499
ISATAP tunnels, 501
L2TPv3, 504
Layer 2 VPNs, 503
  manually configured tunnels, 497-498
NAT ALG, 502
NAT64, 502-503
NAT-PT, 502
SLAAC, 502
IPv6-over-IPv4 tunnels, 499
ISATAP (Intra-Site Automatic Tunneling Protocol), 501
ISM (Internet Standard Multicast), 371
Join messages (PIM-SM), 353-354
joining
   IGMP groups, 282
   shared tree (PIM-SM), 348-350

keepalive interval (BGP), 9
Keepalive messages (BGP), 16
KEK (Key Encryption Key), 506
KS (Key Server), 506

L2TPv3 (Layer 2 Tunneling Protocol), 504
Layer 2 protocols. See also Layer 2 security; Layer 2 VPNs
HDLC, 247-249
PPoE, 257-261
   authentication, 260-261
   client configuration, 259-260
   server configuration, 258-259
PPP, 249-250
   compression, 255
   configuring, 405-406
Layer 2 payload compression, 256
LCP, 250-252
LFI, 254-255
MLP, 252-255
Layer 2 security
   802.1X, 423-426
   best practices, 427-429
   DAI, 417-420
   gratuitous ARPs, 417-419
   DHCP snooping, 420-422
EAP, 423-426
   IP Source Guard, 422-423
   port security, 413-417
      configuring, 415-417
      unused ports, securing, 412-413
      user ports, securing, 412-413
   storm control, 426-427
Layer 2 VPNs, 503
Layer 3 security, 429-461
   inappropriate IP addresses, preventing, 435-436
   IP ACLs, 430-433
   RPF checks, 434-435
   smurf attacks, mitigating, 433-435
   TCP intercept, 437-438
   TCP SYN floods, mitigating, 436-437
LCP (Link Control Protocol), 250-252
LDP (Label Distribution Protocol), 263, 527-535
Leave Group messages (IGMP), 289-291
LFI (Link Fragmentation and Interleaving), 254-255
LFIB (Label Forwarding Information Base), 522-523
link operations, FHS, 463-464
LLQ (Low Latency Queuing), 182-186
   limiting bandwidth, 184-185
   priority queues, 185-186
   shaping voice traffic, 218-221
LOCAL_PREF PA, highest local preference as BGP decision point, 104-107
locally injected routes, selection process, 107
locations for marking, 144
loose RPF, 435
LSRs (label-switch routers), 522
manually configured tunnels, 497-498
mapping multicast addresses to MAC addresses, 280-281
marking
  ATM fields, 143-144
  CB Marking
    configuring, 150
    CoS field, 155-156
    design choices, 158
    DSCP field, 155-156
    examples of, 151-154
    NBAR, 156-158
  DSCP field, 139-142
  EF PHB, 142
  Ethernet CoS field, 143
  Frame Relay fields, 143-144
  IP Precedence field, 139-140
  locations for, 144
  policers, 158-159
  policy routing, 160
match commands for class maps, 147-149
matching AS_PATH PA, 82-93
  examples, 87-91
  regular expressions, 84-85
maximum-paths command, 118
MDRR (Modified Deficit Round Robin), 190-192
  deficit feature, 192
  QV, 191
mechanics of MQC, 145-146
MED (Multi-Exit Discriminator) PA, 21
  configuring, 114-115
  scope of, 115-116
smallest MED PA as BGP decision point, 112-113
memorizing BGP decision process, 98-99
messages
  ARP messages, 417-418
  BGP
    Keepalive messages, 16
    Notification messages, 16
    Open messages, 9, 16
    Update messages, 9, 16
  CGMP, 302
  PIM-DM, 343
metrics (BGP), AS_PATH attribute, 8
Metro-E, 263
Meyer, David, 278
mitigating attacks
  smurf attacks, 433-435
  TCP SYN floods, 436-437
MLD (Multicast Listener Discovery), 385-389
MLP (multilink PPP), 252-255
mnemonics for memorizing BGP decision process, 98-99
MOSPF (Multicast Open Shortest Path First), 343-345
MP-BGP (Multiprotocol BGP), 57-62
  address families, 58
  attributes, 57-58
  configuring, 58-62
  extended community attribute, 60
  standard community attribute, 60
  VRF, 59
MP_REACH_NLRI attribute, 57-58
MPD (mark probability denominator), 188
MPLS (Multiprotocol Label Switching), 519-569
FEC, 565
header fields, 524-526
LDP, 527-535
LSRs, 522
unicast IP forwarding, 519-535
CEF, 520-521
c Control plane, 526-527
data plane, 520
FIB, 522-523
LFIB, 522-523
VPNs, 535-564
CE, 537
configuring, 546-558
c Control plane, 539
data plane, 558-559
LFIB entries, creating, 560-562
overlapping VPNS, 545-546
PE, 537
PHP, 564
route distinguishers, 541-543
route targets, 543-545
VPN label, building, 559-560
VRF, 537, 540-541
VRF FIB entries, creating, 562-564
VRF Lite, 566-569
MQC (Modular QoS CLI), 145-149
See also HQF (Hierarchical Queuing Framework)
CB Marking, 146-147
class maps, 146-149
using multiple match commands, 147-149
mechanics, 145-146
NBAR, 149

MSDP (Multicast Source Discovery Protocol), 365
interdomain multicast routing, 367-369
multi-action policing, 229-230
multicast, 273-275, 321-322
addresses, 276-281
address ranges, 279
GLOP addresses, 278
mapping to MAC addresses, 280-281
for permanent groups, 277
for private multicast domains, 278
for source-specific applications and protocols, 278
well-known multicast addresses, 276
administrative scoping, 328-329
CGMP, 296-302
dense-mode routing protocols, 322-323, 329-345
DVMRP, 343
MOSPF, 343-345
PIM-DM, 329-343
IGMP, 281-283
features, 284-285
fields, 283-284
Group-Specific Query messages, 289-291
Host Membership Query messages, 285-286
Host Membership Report messages, 286
interoperability with version 2, 294-295
joining a group, 282
Leave Group messages, 289-291
querier election process, 291
Report Suppression process, 286-287
Solicited Host Membership Report process, 286-287
timers, 292
traffic filters, 309-310
Unsolicited Host Membership Report messages, 288
IGMP proxy, 310-313
IGMP snooping, 303-307
IPv6 multicast, 373-392
BSR, 381-384
designated priority manipulation, 376-377
embedded RP, 389-392
hello interval, 377-378
MLD, 385-389
need for, 270-272
requirements for supporting, 273
RGMP, 307-309
RPF check, 323-325
sparse-mode routing protocols, 325-327, 345-373
Bidirectional PIM, 370-371
SSM, 372-373
TTL scoping, 327-328
ND inspection, 472-473
NDP (Neighbor Discovery Protocol), 464-465
need for IP multicast, 270-272
neighbor default-originate command, 30
neighbor relationships, building, 9-18
eBGP neighbors, 9
  adding eBGP-learned routes to IP routing table, 40-41
iBGP neighbors, 9-12
  adding iBGP-learned routes to IP routing table, 42-44
internal BGP neighbors, 9
requirements for, 14-15
resetting peer connections, 16-18
neighbor states (BGP), 15-16
network command, 18-21
NEXT_HOP PA, 23, 94
  best route selection, 33-34
  BGP decision process, 101
  in BGP decision process, 116
NLRI (network layer reachability information), 18
  route filtering, 76-79
    with COMMUNITY PA values, 125-126
Notification messages (BGP), 16

NAT ALG (Network Address Translation Application Level Gateways), 502
NAT64, 502-503
NAT-PT (Network Address Translation-Protocol Translation), 502
NBAR (Network Based Application Recognition), 149, 156-158
open confirm state (BGP), 16
Open messages (BGP), 9, 16
open sent state (BGP), 16
optional PAs, 94
ORIGIN PA, 30-31, 94
  in BGP decision process, 112
ORIGINATOR_ID PA, 54, 94
OTV (Overlay Transport Virtualization), 506
overlapping VPNs, MPLS support for, 545-546
overriding default login authentication methods, 410-412

P

PACLs (port ACLs), 475
PAP (Password Authentication Protocol), 411
PAs (path attributes)
  AS PATH, 8
    summary routes, injecting into BGP, 25-29
  AS PATH PA
    prepend feature, 109-112
    route filtering, 82-93
    segments, 82-84
    shortest AS PATH as BGP decision point, 107-108
ATOMIC_AGGREGATE, 27
BGP decision process, 99-101
characteristics, 93-95
CLUSTER_LIST, 54
COMMUNITY, 119-126
  community lists, 123-124
  filtering NLRIs, 125-126
  removing strings from, 124-125
LOCAL_PREF PA, highest local preference as BGP decision point, 104-107
MED, 21
  configuring, 114-115
  scope of, 115-116
  smallest MED PA as BGP decision point, 112-113

NEXT_HOP, 23
  best route selection, 33-34
  BGP decision process, 101, 116
optional, 94
ORIGIN, 30-31
  best ORIGIN PA selection, 112
ORIGINATOR_ID, 54
  segments, 26
well-known, 93
password protection for CLI, 403-412
  enable password command, 405
PPP, 411-412
  simple password protection, 403-404
SSH, 405-406
  using multiple authentication methods, 408-409
Path Attributes field (Update messages), 32
path vector logic, BGP, 8
PE (provider edge), 537
Pearson Cert Practice Test engine, 573,
  576-577
  activating the practice exam, 574
  installing, 574
peer connections (BGP), resetting, 16-18
per class policing, 228
percentage-based policing, 230-231
PHBs (Per-Hop Behaviors), 140-142
  AF PHB, 141-142
PHP (penultimate hop popping), 564
PIM-DM (Protocol Independent Multicast Dense Mode), 329-343
  adjacencies, forming, 329-330
  Assert messages, 341-342
  DRS, 343
  Graft messages, 339-340
Hello messages, 329-330
LAN-specific issues, 340
messages, 343
Prune messages, 331-333
Prune Override, 340-341
pruning, 335-337
reacting to failed links, 333-335
source-based distribution trees, 330-331
State Refresh message, 337-338

PIM-SM (Protocol Independent Multicast Sparse Mode), 345-346
Join messages, 353-354
RPs, finding, 358-369
with Auto-RP, 359-363
with BSR, 363-365
using Anycast RP with MSDP, 365-367
sending packets to RP, 346-348
shared distribution trees, 352-353
shared trees
joining, 348-350
pruning, 357-358
source registration process, 350-352
SPT switchover, 355-357
steady state operation, 353-354

policing, 158-159
CB Policing, 222-233
CAR, 231-233
configuring, 227
dual-rate policing, 229
multi-action policing, 229-230
per class policing, 228
percentage-based policing, 230-231
single rate, three-color policing, 224-225, 227-228

single rate, two-color policing, 223-224
two-rate, three-color policing, 225-226

policy maps, hierarchical policy maps, policy routing, 160
populating RIB
with network command, 19
through redistribution, 21-23
port security, 413-417
configuring, 415-417
PPoE (PPP over Ethernet), 257-261
authentication, 260-261
client configuration, 259-260
server configuration, 258-259
PPP (Point-to-Point Protocol), 249-250
compression, 255
header compression, 256-257
Layer 2 payload compression, 256
configuring, 405-406
LCP, 250-252
LFI, 254-255
MLP, 252-255
security, 411-412

Practice Exam mode (Pearson Cert Practice Test engine), 577
pre-chapter assessment quizzes. See "Do I Know This Already?" quizzes
pre-classification, 159
pre-classify command, 159
Prefix field (Update messages), 32
Prefix Length field (Update messages), 32
prefix lists, 76-79
comparing with distribute lists and route maps, 80
comparing with route maps and distribute lists, 80
Premium Edition of this book, purchasing, 575
preparing for exam, 573-576
Cisco Learning Network, 575
memory tables, 575-576
Pearson Cert Practice Test engine, 573, 576-577
activating the practice exam, 574
installing, 574
prepend feature (AS_PATH), 109-112
preventing
inappropriate IP addresses, 435-436
routing loops within confederations, 47
priority queues, 185-186
creating, 193-195
private ASNs, removing, 108-109
Prune messages (PIM-DM), 331-333
Prune Override, 340-341
pruning
PIM-DM, 335-337
shared trees, 357-358
purchasing Premium Edition of this book, 575
PW (pseudowire), 503
raw mode, 503
tagged mode, 503

Q
QoS
ATM fields, marking, 143-144
AutoQoS, 160-164
for the Enterprise, 163-164
for VoIP, 161-163
Ethernet CoS field, marking, 143
IP Precedence field, marking, 139-140
MQC, 145-149
CB Marking, 146-147
class maps, 146-149
mechanics, 145-146
NBAR, 149
pre-classification, 159
RSVP, 199-204
SLAs, 238
troubleshooting, 237-240
helpful commands, 240
slow application response, 238-239
video over IP, 239-240
VoIP, 239-240
QoS marking-eligible fields, locations for marking, 144
querier election process, 291
queuing
AF PHB, 141-142
CBWFQ, 176-182
configuring, 179-180
features, 178
limiting bandwidth, 180-182
CQ, 176
egress queuing on Cisco 3650 switches, 197-199
hardware queuing, 175-176
HQF, 233-237
ingress queuing on Cisco 3650 switches, 193-197
on interfaces, 176
LLQ, 182-186
limiting bandwidth, 184-185
priority queues, 185-186
voice traffic shaping, 218
requirements for BGP neighbor establishment, 14-15
reserving bandwidth
for CBWFQ, 180-182
RSVP, 200-201
for voice calls, 203-204
resetting BGP peer connections, 16-18
RGMP (Router-Port Group Management Protocol), 307-309
RIB
best route selection (BGP), 33-34
building, 18-40
classful networks, injecting, 23-25
default routes injecting into RIB, 29-30
populating with network command, 19
route advertisement process, 31-40
summary routes, injecting, 25-29
route aggregation, 109-112
route distinguishers, 541-543
route filtering, 75-93
route maps, 79
using aggregate-address command, 81-82
using COMMUNITY PA values, 125-126
route maps, 76-79
route redistribution, BGP sync, 44-47
route summarization, injecting summary routes into BGP, 25-29
route targets, 543-545

MDRR, 190-192
deficit feature, 192
QV, 191
software queuing, 175
tail drop, 187
tools, comparing, 176
WFQ, 176
WRED, 187-190
average queue depth, 187
configuring, 189-190
discard categories, 187
full drop, 187
MPD, 188
traffic profiles, 188-189
QV (quantum value), 191

RA Guard, 467-468
RADIUS, 406-407
server groups, configuring, 410
raw mode (PW), 503
reachability, BGP decision process, 101
reacting to failed links (PIM-DM), 333-335
redistribution into BGP, 21-23
default routes, 29-30
regular expressions for matching AS_PATH PA, 84-85
Rekey phase (GET VPN), 507
removing
private ASNs, 108-109
strings from COMMUNITY PA, 124-125
Report Suppression process (IGMP), 286-287

as PATH PA matching, 82-93
examples, 87-91
matching AS_SET and AS_CONFED_SEQ, 91-93
regular expressions, 84-85
NLRI-based, 76-79
route maps, 79
using aggregate-address command, 81-82
using COMMUNITY PA values, 125-126
route maps, 76-79
route redistribution, BGP sync, 44-47
route summarization, injecting summary routes into BGP, 25-29
route targets, 543-545

Report Suppression process (IGMP), 286-287
router bgp command, 11-14
routers
   AutoQoS for VoiP, 162-163
   Cisco 12000 Series routers, MDDR, 190-192
routes
   advertising, 31-40
   best route selection, 33-34
   versus paths, 8
   RRs, 52-57
routing loops, preventing within confed-
erations, 47
routing policies (BGP), 69
   soft reconfiguration, 79-80
RP (Rendezvous Point), 346-348
   embedded RP, 389-392
   finding, 358-369
      with Auto-RP, 359-363
      with BSR, 363-365
      using Anycast RP with MSDP, 365-367
   static RP, 379-381
RPF checks, 323-325, 434-435
RPT (root-path tree), 349
RRs (route reflectors), 52-57
RSVP (Resource Reservation Protocol), 199-204
   configuring, 201-202
   reservation process, 200-201
   for voice calls, 203-204
RTP header compression, 256-257
rules
   for advertised routes in BGP Updates, 40
   for CB shaping, 218
   for IP ACLs, 431-432

S
scope of MED, 115-116
security
   ACLs, PACLS, 475
   authentication
      BGP neighbors, 9
      PPPoE, 260-261
      TACACS+, 406-407
      using multiple authentication methods, 408-409
   Cisco IOS Firewall, 438-450
      caveats, 440
      CBAC, 438-439
      configuring, 440-441
      protocol support, 439-440
   CLI password protection
      enable password command, 405
      overriding default login authenti-
cation methods, 410-412
      simple password protection, 403-404
      SSH, 405-406
   DMVPN, 451-461
      benefits of, 451
      configuring, 452-461
FHS
   DHCPv6 Guard, 468-471
   ICMPv6, 464-465
   IPv6 device tracking, 471-472
   IPv6 Source Guard, 473-475
   link operations, 463-464
   ND inspection, 472-473
   NDP, 464-465
   RA Guard, 467-468
   SeND, 465-466
firewalls
  CoPP, 446-450
Layer 2 security, 412-429
  802.1X, 423-426
  best practices, 427-429
DAI, 417-420
DHCP snooping, 420-422
EAP, 423-426
IP Source Guard, 422-423
port security, 413-417
storm control, 426-427
unused ports, securing, 412-413
user ports, securing, 412-413
Layer 3 security, 429-461
  inappropriate IP addresses, preventing, 435-436
RPF checks, 434-435
smurf attacks, mitigating, 433-435
TCP intercept, 437-438
TCP SYN floods, mitigating, 436-437
CB Shaping, 216-222
  adaptive shaping, 222
  based on bandwidth percent, 221
  rules for, 218
  shaping to peak rate, 222
  voice traffic shaping with LLQ, 218
CIR, 211
gress blocking, 211
GTS, 214-216
sending rate, 211
shaped rate, 212
Tc interval, 211
calculating, 213
token bucket model, 214
shared distribution trees, 352-353
shared trees
  joining, 348-350
  pruning, 357-358
shortest AS_PATH as BGP decision point, 107-108
show ip bgp command, 22-23, 34-37
show policy-map interface command, 154
simple password protection for CLI, 403-404
single rate, three-color policing, 224-225, 227-228
single rate, two-color policing, 223-224
SLAAC (Stateless Address Autoconfiguration), 502
SLAs (service-level agreements), 238
slow application response, troubleshooting, 238-239
smallest MED PA as BGP decision point, 112-113
smurf attacks, mitigating, 433-435
soft reconfiguration, 79-80
software queuing, 175
Solicited Host Membership Report process, 286-287
source registration process (PIM-SM), 350-352
source-based distribution trees, 330-331
sparse-mode routing protocols, 325-327, 345-373
Bidirectional PIM, 370-371
PIM-SM, 345-346
  Join messages, 353-354
  RPs, finding, 358-369
  sending packets to RP, 346-348
  shared distribution trees, 352-353
  shared tree, joining, 348-350
  source registration process, 350-352
  SPT switchover, 355-357
SPT (Shortest-Path Tree), 355-357
SRR (shared round-robin), 193
SSH (Secure Shell), 405-406
  configuring, 406
SSM (Source-Specific Multicast), 372-373
standard community attribute (MP-BGP), 60
State Refresh message (PIM-DM), 337-338
static RP, 379-381
steady state operation
  PIM-SM, 353-354
storm control, 426-427
strict RPF, 434
Study mode (Pearson Cert Practice Test engine), 576
sub-AS, confederations, 47-52
summary routes, injecting into RIB, 25-29
supplicants, 424
switches
  AutoQoS for VoiP, 161-162
Layer 2 security
  802.1X authentication, 423-426
  DAI, 417-420
  DHCP snooping, 420-422
  EAP, 423-426
  IP Source Guard, 422-423
  port security, 412-417
  storm control, 426-427
synchronization (BGP), 44-47
disabling, 46-47

T

TACACS+, 406-407
tagged mode (PW), 503
tail drop, 187
Tc interval, 211
  calculating, 213
TCP header compression, 256-257
TCP intercept, 437-438
TEK (Transport Encryption Key), 506
Telnet access to CLI, 405
tiebreaker steps for BGP decision process, 95-97, 116-117
timers, IGMP, 292
TLS (Transparent LAN Service), 262
token bucket model, 214
topology table (BGP)
  building, 18-40
ToS (Type of Service) field, 139
traffic policers, 158-159
traffic profiles (WRED), 188-189
traffic shaping, 211-222
  Bc, 212
  Be, 212-213
  CB Shaping, 216-222
    rules for, 218
    voice traffic shaping with LLQ, 218
  CIR, 211
  egress blocking, 211
  GTS, 214-216
  sending rate, 211
  shaped rate, 212
  Tc interval, 211
    calculating, 213
  token bucket model, 214
troubleshooting
  QoS, 237-240
    helpful commands, 240
    slow application response, 238-239
    video over IP, 239-240
    VoIP, 239-240
  TTL scoping, 327-328
tunneling, 496-497
  DMVPN tunnels, 487-495
  GET VPN, 506-511
    KS, 506
    Rekey phase, 507
  GRE tunnels, 486-487
  IPv6
    AToM, 504-505
    automatic 6to4 tunnels, 499-501
    automatic IPv4-compatible tunnels, 499
  IPv6-over-IPv4 tunnels, 499
  ISATAP tunnels, 501
  L2TPv3, 504
  Layer 2 VPNs, 503
  manually configured tunnels, 497-498
  NAT ALG, 502
  NAT64, 502-503
  NAT-PT, 502
  SLAAC, 502
  IPv6 tunneling, 495-496
  OTV, 506
  VPLS, 505
  VTIs, 486
two-rate, three-color policing, 225-226
  Tx queues, 175
U
  unicast IP forwarding, MPLS, 519-535
    CEF, 520-521
    control plane, 526-527
    data plane, 520
    FIB, 522-523
    LFIB, 522-523
  Unsolicited Host Membership Report messages, 288
  unused ports, securing, 412-413
  Update messages
    contents, viewing, 34-37
    fields, 32
    soft reconfiguration, 79-80
  Update messages (BGP), 9, 16
  uRPF (unicast RPF) checks, 434-435
  user ports, securing, 412-413
V

VACLs (VLAN access lists), 475
verifying
   AutoQoS for the Enterprise, 164
   AutoQoS for VoiP, 163
versions of IGMP, comparing, 295
video over IP, troubleshooting, 239-240
viewing Update message contents, 34-37
voice traffic, shaping with LLQ, 218
VoIP
   AutoQoS for VoiP
      on routers, 162-163
      on switches, 161-162
      verifying, 163
troubleshooting, 239-240
VPLS (Virtual Private LAN Service), 262-263, 505
VPNs (Virtual Private Networks)
   DMVPN, 451-461
      benefits of, 451
      configuring, 452-461
   GET VPN, 506-511
   KS, 506
Layer 2 VPNs, 503
MP-BGP
   address families, 58
   attributes, 57-58
   configuring, 58-62
MPLS, 535-564
   CE, 537
   configuring, 546-558
   control plane, 539
   LFIB entries, creating, 560-562
   overlapping VPNs, 545-546
   PE, 537
   PHP, 564
   route distinguishers, 541-543
   route targets, 543-545
   VRF, 537, 540-541
   VRF FIB entries, creating, 562-564
VRF (Virtual Routing and Forwarding), 59, 540-541
VRF Lite, 566-569
VTIs (virtual tunnel interfaces), 486

W

WANs, QoS marking, 143-144
websites, Cisco Learning Network, 575
well-known multicast addresses, 276
well-known PAs, 93
WFQ (weighted fair queuing), 176
wildcard masks, 433
Withdrawn Routes field (Update messages), 32
WRED (weighted random early detection), 187-190
   average queue depth, 187
   configuring, 189-190
   discard categories, 187
   full drop, 187
   MPD, 188
   traffic profiles, 188-189
WTD (weighted tail drop), 195-196
X-Y-Z

xconnect command, 504

ZFW (zone-based firewall), 441-446
  class maps, configuring, 444-445
  zones, configuring, 443
zone pairs (ZFW), 443
zones (ZFW), 442