Official Cert Guide

Learn, prepare, and practice for exam success

CCNA ICND2 640-816
Third Edition

Wendell Odom, CCIE® No. 1624

ciscopress.com
Warning and Disclaimer
This book is designed to provide information about the Cisco ICND2 (640-816) and CCNA (640-802) exams. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it. The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc. Trademark Acknowledgments
All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

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

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

For sales outside the United States please contact:
International Sales
international@pearsoned.com
Feedback Information

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

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

We greatly appreciate your assistance.

Publisher: Paul Boger
Associate Publisher: Dave Dusthimer
Executive Editor: Brett Bartow
Managing Editor: Sandra Schroeder
Project Editor: Mandie Frank
Book and Cover Designer: Gary Adair
Composition: Mark Shirar
Proofreader: Chrissy White

Manager Global Certification: Erik Ullanderson
Business Operation Manager, Cisco Press: Anand Sundaram
Technical Editors: Elan Beer, Teri Cook, Steve Kalman
Development Editor: Andrew Cupp
Copy Editor: Sheri Cain
Editorial Assistant: Vanessa Evans
Indexer: Larry Sweazy
About the Author

Wendell Odom, CCIE No. 1624, has been in the networking industry since 1981. He has worked as a network engineer, consultant, systems engineer, instructor, and course developer; he currently works writing and creating certification tools. He is author of all the previous editions of the Cisco Press CCNA Official Certification Guide series, as well as the CCNP ROUTE 642-902 Official Certification Guide, the CCIE Routing and Switching Official Certification Guide, Computer Networking First Step, the CCNA Video Mentor, IP Networking (a college textbook), and he is the primary networking consultant for the CCNA 640-802 Network Simulator from Pearson. He maintains study tools, links to his blogs, and other resources at www.certskills.com.
About the Technical Reviewers

Elan Beer is a senior consultant and Cisco instructor specializing in multi-protocol network design, network configuration, troubleshooting, and network maintenance. For the past 20 years, Elan has trained thousands of industry experts in routing, switching, and data center architectures. Elan has been instrumental in large scale professional service efforts designing and troubleshooting internetworks, performing network audits, and assisting clients with their short and long term design objectives. Elan has a global perspective of network architectures via his international clientele. Elan has used his expertise to design and troubleshoot networks in Malaysia, North America, Europe, Australia, Africa, China and the Middle East. Most recently Elan has been focused on data center design, configuration, and troubleshooting as well as service provider technologies.

In 1993, Elan was amongst the first to obtain Cisco’s Certified System Instructor (CCSI) certification and in 1996, Elan was amongst the first to attain Cisco System’s highest technical certification the Cisco Certified Internetworking Expert (CCIE). Since then Elan has been involved in numerous large-scale telecommunications networking projects worldwide. Elan is known internationally as a leader in network architecture and training and has worked on many high profile projects assisting companies with their goal of implementing leading edge technologies in their corporate infrastructure.

Teri Cook (CCSI, CCDP, CCNP, CCDA, CCNA, MCT, and MCSE 2000/2003: Security) has more than 10 years of experience in the IT industry. She has worked with different types of organizations within the private business and DoD sectors, providing senior-level network and security technical skills in the design and implementation of complex computing environments. Since obtaining her certifications, Teri has been committed to bringing quality IT training to IT professionals as an instructor. She is an outstanding instructor that utilizes real-world experience to present complex networking technologies. As an IT instructor, Teri has been teaching Cisco classes for more than five years.

Stephen Kalman is a data security trainer and the author or tech editor of more than 20 books, courses, and CBT titles. His most recent book is Web Security Field Guide, published by Cisco Press. In addition to those responsibilities he runs a consulting company, Esquire Micro Consultants, which specializes in network security assessments and forensics. Mr. Kalman holds SSCP, CISSP, ISSMP, CEH, CHFI, CCNA, CCSA (Checkpoint), A+, Network+, and Security+ certifications and is a member of the New York State Bar.
Dedication

For Hannah Odom, from your earthly Dad. I love you, my girl!
Acknowledgments

You know, after writing books for 13 years now, I would think that there would be something normal, something repetitive, and that each book would pretty much follow the same process as others. It now seems that normal is actually abnormal, and that requires everyone to think outside the box.

More so than probably any other editions of these books, these books really are the result of a team effort. The biggest news relates to all the extras Cisco Press added to the package. Thanks to Dave, Brett, Kourtnaye, Sandra, and all the folks at Cisco Press for going several extra miles to make this “extra” edition happen, and with so many extra valuable pieces. I think the readers will appreciate the added value. Now, on to the specifics.

First, my hat’s off to Drew Cupp. Wow. Between this book, the matching ICND2 Official Cert Guide, and another title, Drew and I went from having no books to working on three together all at once. And they all fell into the same 5-month stretch from start to finish. It makes my head hurt thinking about it. Besides taking on extra work to get it done, Drew’s clarity of thought about how to get from here to there through the process, with so many different print, DVD, and online elements, wow, no way this book gets done without Drew. Thanks, Drew: You da man!

Brian, Teri, and Steve all did a great job technical editing the book. Besides helping find mistakes and keeping the book accurate, each tech editor brought a different perspective to the process. I hope we can work together on future editions. And a special thanks to Elan Beer, the best tech editor in the business, for working on the new materials for this edition.

You know, it’s great when the person you rely on most at work is consistently helpful and always comes through, whether working on an opportunity or an issue. But, when that person actually works for a partner company, it’s all the more impressive. I am fortunate enough to have such an ally in Brett Bartow—thank you so much for walking this journey with me.

Mandie Frank gets the “hot potato” award for working as the project editor with this book and with ICND1. The nature of this project plus the ICND1 book at practically the same time can create some challenges. Mandie handled them all with grace and aplomb, and she seamlessly managed the entire process with the rest of the production team. Thanks, Mandie, and the whole group! And thanks especially for the extra attention to the pages review.

Thanks to Richard Bennett, who slaved on a short schedule on some figure improvements that I really wanted to include in this book and for his work on the question database. Dude, Robin Williams would be proud!
A special thank you goes to you readers, who write in with suggestions, possible errors, and especially those of you who post online at the Cisco Learning Network (CLN). Without a doubt, the comments I receive directly and overhear by participating at CLN made this edition a better book.

Finally, thanks to my wife Kris for all her support with my writing efforts, her prayers, and understanding when the deadline didn’t quite match with our vacation plans this summer. (Yes, that’s twice in a row that when this book reved, we cancelled vacation—you’re a doll!) And thanks to Jesus Christ—all this effort is just striving after the wind without Him.
# Contents at a Glance

## Introduction  xxv

### Part I: LAN Switching  3

- Chapter 1  Virtual LANs  5
- Chapter 2  Spanning Tree Protocol  57
- Chapter 3  Troubleshooting LAN Switching  109

### Part II: IP Routing  157

- Chapter 4  IP Routing: Static and Connected Routes  159
- Chapter 5  Variable Length Subnet Masks  199
- Chapter 6  Route Summarization  227
- Chapter 7  Basic IP Access Control Lists  251
- Chapter 8  Advanced IP Access Control Lists  275
- Chapter 9  Troubleshooting IP Routing  305

### Part III: Routing Protocols  339

- Chapter 10  Routing Protocol Theory  341
- Chapter 11  OSPF  379
- Chapter 12  EIGRP  413
- Chapter 13  Troubleshooting Routing Protocols  443

### Part IV: Wide-Area Networks  467

- Chapter 14  Point-to-Point WANs  469
- Chapter 15  Frame Relay Concepts  493
- Chapter 16  Frame Relay Configuration  523
- Chapter 17  Virtual Private Networks  565

### Part V: Scaling the IP Address Space  583

- Chapter 18  Network Address Translation  585
- Chapter 19  IP Version 6  617

### Part VI: Final Preparation  657

- Chapter 20  Final Preparation  659

### Part VII: Appendices  669

- Appendix A  Answers to the “Do I Know This Already?” Quizzes  671
- Appendix B  Numeric Reference Tables  684
- Appendix C  ICND2 Exam Updates: Version 1.0  692
- Glossary  696
- Index  674
Part VIII: DVD-Only

Appendix D  Practice for Chapter 5: Variable Length Subnet Masks
Appendix E  Practice for Chapter 6: Route Summarization
Appendix F  Practice for Chapter 7: Basic IP Access Control Lists
Appendix G  Additional Scenarios
Appendix H  Video Scenario Reference
Appendix I  ICND1 Chapter 23: WAN Configuration
Appendix J  Memory Tables
Appendix K  Memory Tables Answer Key
Appendix L  ICND2 Open-Ended Questions
Contents

Introduction  xxv

Part I:  LAN Switching  3

Chapter 1  Virtual LANs  5

“Do I Know This Already?” Quiz  5

Foundation Topics  9

Virtual LAN Concepts  10

Trunking with ISL and 802.1Q  11

ISL  13

IEEE 802.1Q  13

ISL and 802.1Q Compared  14

IP Subnets and VLANs  15

VLAN Trunking Protocol (VTP)  16

Normal VTP Operation Using VTP Server and Client Modes  17

Three Requirements for VTP to Work Between Two Switches  19

Avoiding VTP by Using VTP Transparent Mode  20

Storing VLAN Configuration  20

VTP Versions  21

VTP Pruning  22

Summary of VTP Features  23

VLAN and VLAN Trunking Configuration and Verification  23

Creating VLANs and Assigning Access VLANs to an Interface  24

VLAN Configuration Example 1: Full VLAN Configuration  25

VLAN Configuration Example 2: Shorter VLAN Configuration  28

VLAN Trunking Configuration  29

Controlling Which VLANs Can Be Supported on a Trunk  33

Trunking to Cisco IP Phones  36

Securing VLANs and Trunking  37

VTP Configuration and Verification  38

Using VTP: Configuring Servers and Clients  38

Caveats When Moving Away from Default VTP Configuration  42

Avoiding VTP: Configuring Transparent Mode  43

Troubleshooting VTP  44

Determining Why VTP Is Not Currently Working  44

Problems When Connecting New Switches and Bringing Up Trunks  50

Avoiding VTP Problems Through Best Practices  51

Exam Preparation Tasks  53

Review All the Key Topics  53

Complete the Tables and Lists from Memory  54

Definitions of Key Terms  54

Command Reference to Check Your Memory  54
Chapter 2  Spanning Tree Protocol  57

“Do I Know This Already?” Quiz  57

Foundation Topics 61

Spanning Tree Protocol (IEEE 802.1d) 61

The Need for Spanning Tree 61
What IEEE 802.1d Spanning Tree Does 63
How Spanning Tree Works 65

The STP Bridge ID and Hello BPDU 66
E lecting the Root Switch 67
Choosing Each Switch’s Root Port 69
Choosing the Designated Port on Each LAN Segment 70
Reacting to Changes in the Network 72

Optional STP Features 75
EtherChannel 76
PortFast 77
STP Security 77

Rapid STP (IEEE 802.1w) 78

RSTP Link and Edge Types 79
RSTP Port States 80
RSTP Port Roles 81
RSTP Convergence 82

Edge-Type Behavior and PortFast 83
Link-Type Shared 83
Link-Type Point-to-Point 83
An Example of Speedy RSTP Convergence 83

STP Configuration and Verification 86

Multiple Instances of STP 87
Configuration Options That Influence the Spanning Tree Topology 88

The Bridge ID and System ID Extension 89
Per-VLAN Port Costs 89

STP Configuration Option Summary 90
Verifying Default STP Operation 90
Configuring STP Port Costs and Switch Priority 92
Configuring PortFast and BPDU Guard 95
Configuring EtherChannel 95
Configuring RSTP 97

STP Troubleshooting 98

Determining the Root Switch 99
Determining the Root Port on Nonroot Switches 100
Determining the Designated Port on Each LAN Segment 102
STP Convergence 104

Exam Preparation Tasks  105

Review All the Key Topics  105
Complete the Tables and Lists from Memory  106
Definitions of Key Terms  106
Command Reference to Check Your Memory  106
Chapter 3  Troubleshooting LAN Switching  109

“Do I Know This Already?” Quiz  109

Foundation Topics  110

Generalized Troubleshooting Methodologies  110

Analyzing and Predicting Normal Network Operation  111
  Data Plane Analysis  111
  Control Plane Analysis  113

Predicting Normal Operations: Summary of the Process  114

Problem Isolation  114

Root Cause Analysis  115

Real World Versus the Exams  116

Troubleshooting the LAN Switching Data Plane  117

An Overview of the Normal LAN Switch Forwarding Process  117

Step 1: Confirm the Network Diagrams Using CDP  119

Step 2: Isolate Interface Problems  121
  Interface Status Codes and Reasons for Nonworking States  122
  The notconnect State and Cabling Pinouts  123

Interface Speed and Duplex Issues  124

Step 3: Isolate Filtering and Port Security Problems  127

Step 4: Isolate VLAN and Trunking Problems  132

Ensuring That the Right Access Interfaces Are in the Right VLANs  132

Access VLANs Not Being Defined or Being Active  133

Identify Trunks and VLANs Forwarded on Those Trunks  134

Example: Troubleshooting the Data Plane  136

Step 1: Verify the Accuracy of the Diagram Using CDP  138

Step 2: Check for Interface Problems  139

Step 3: Check for Port Security Problems  141

Step 4: Check for VLAN and VLAN Trunk Problems  143

Predicting Normal Operation of the LAN Switching Data Plane  147

PCI Broadcast in VLAN 1  147

Forwarding Path: Unicast from R1 to PC1  151

Exam Preparation Tasks  155

Review All the Key Topics  155

Complete the Tables and Lists from Memory  155

Part II:  IP Routing  157

Chapter 4  IP Routing: Static and Connected Routes  159

“Do I Know This Already?” Quiz  159

Foundation Topics  162

IP Routing and Addressing  162

IP Routing  162

IP Addressing and Subnetting  166

IP Forwarding by Matching the Most Specific Route  169

DNS, DHCP, ARP, and ICMP  171

Fragmentation and MTU  173
Routes to Directly Connected Subnets 175
  Secondary IP Addressing 175
  Supporting Connected Routes to Subnet Zero 177
  ISL and 802.1Q Configuration on Routers 178
Static Routes 180
  Configuring Static Routes 182
  The Extended ping Command 183
  Static Default Routes 186
    Default Routes Using the ip route Command 186
    Default Routes Using the ip default-network Command 188
  Default Route Summary 190
Classful and Classless Routing 190
  Summary of the Use of the Terms Classless and Classful 190
  Classless and Classful Routing Compared 191

Exam Preparation Tasks 194
  Review All the Key Topics 194
  Complete the Tables and Lists from Memory 194
  Definitions of Key Terms 195
  Command Reference to Check Your Memory 195

Chapter 5 Variable Length Subnet Masks 199
  “Do I Know This Already?” Quiz 199

Foundation Topics 202
  VLSM Concepts and Configuration 202
    Classless and Classful Routing Protocols 203
    VLSM Configuration and Verification 204
  Finding VLSM Overlaps 205
    An Example of Finding a VLSM Overlap 206
    Practice Finding VLSM Overlaps 208
  Adding a New Subnet to an Existing VLSM Design 208
    An Example of Adding a New VLSM Subnet 209
    Practice Adding New VLSM Subnets 211
  Designing a Subnetting Plan Using VLSM 211
    Choosing VLSM Masks 212
    Assigning the Largest Subnet IDs First 213
    An Example of VLSM Subnet Design 215
    Summary of the Formal VLSM Subnet Design Process 217
    Practice Designing VLSM Subnets 218

Exam Preparation Tasks 219
  Review All the Key Topics 219
  Complete the Tables and Lists from Memory 219
  Definitions of Key Terms 219
  Read Appendix G Scenarios 220
  Appendix D Practice Problems 220
Answers to Earlier Practice Problems 220
Answers to Practice Finding VLSM Overlaps 220
Answers to Practice Adding VLSM Subnets 221
  Problem 1 222
  Problem 2 222
  Problem 3 222
  Problem 4 223
  Problem 5 224
Answers to Practice Designing VLSM Subnets 224
  Answers for VLSM Subnet Design, Problem 1 224
  Answers for VLSM Subnet Design, Problem 2 225

Chapter 6  Route Summarization 227
“Do I Know This Already?” Quiz 228

Foundation Topics 230

Manual Route Summarization 230
  Understanding Route Summarization Concepts 230
  Verifying Manually Summarized Routes 232
  Configuring Manually Summarized Routes 233

Choosing the Best Summary Routes 235
  The Process to Find the Best Summary Route 235
  Sample “Best” Summary on Router R3 236
  Sample “Best” Summary on Router R2 237

Practice Choosing the Best Summary Routes 238

Autosummarization and Discontiguous Classful Networks 239
  An Example of Autosummarization 240
  Discontiguous Classful Networks 241
  Autosummarization Support and Configuration 243

Review All the Key Topics 245

Complete the Tables and Lists from Memory 245
Definitions of Key Terms 245
Read Appendix G Scenarios 245
Command Reference to Check Your Memory 246
Answers to Practice Problems 246
  Problem 1 246
  Problem 2 247
  Problem 3 247
  Problem 4 248

Chapter 7  Basic IP Access Control Lists 251
“Do I Know This Already?” Quiz 251

Foundation Topics 254

IP Access Control List Basics 254
  ACL Locations 254
  Matching Packets 255
  Taking Action When a Match Occurs 256
  Types of IP ACLs 256
Standard Numbered IPv4 ACLs  257
  List Logic with IP ACLs  258
  Matching Logic and Command Syntax  260
    Matching the Exact IP Address  260
    Matching a Subset of the Address with Wildcards  260
    Binary Wildcard Masks  262
    Finding the Right Wildcard Mask to Match a Subnet  263
    Matching Any/All Addresses  263
  Implementing Standard IP ACLs  264
    Standard Numbered ACL Example 1  264
    Standard Numbered ACL Example 2  266
Practice Applying Standard IP ACLs  268
  Practice Building access-list Commands  268
  Reverse Engineering from ACL to Address Range  269

Exam Preparation Tasks  271
  Review All the Key Topics  271
  Read the Appendix G Scenarios  271
  Definitions of Key Terms  271
  Appendix F Practice Problems  272
  Command Reference to Check Your Memory  272
  Answers to Earlier Practice Problems  273

Chapter 8 Advanced IP Access Control Lists  275
  “Do I Know This Already?” Quiz  276

Foundation Topics  278
  Extended Numbered IP Access Control Lists  278
    Matching the Protocol, Source IP, and Destination IP  278
    Matching TCP and UDP Port Numbers  280
    Extended IP ACL Configuration  283
    Extended IP Access Lists: Example 1  284
    Extended IP Access Lists: Example 2  286
  Practice Building access-list Commands  288
  Named ACLs and ACL Editing  288
    Named IP Access Lists  288
    Editing ACLs Using Sequence Numbers  291
  Miscellaneous ACL Topics  294
    Controlling Telnet and SSH Access with ACLs  295
    ACL Implementation Considerations  295
    Reflexive Access Lists  297
    Dynamic ACLs  299
    Time-Based ACLs  300

Exam Preparation Tasks  301
  Review All the Key Topics  301
  Read the Appendix G Scenarios  301
  Definitions of Key Terms  302
Chapter 9  Troubleshooting IP Routing  305

“Do I Know This Already?” Quiz  305

Foundation Topics  306

The ping and traceroute Commands  306

Internet Control Message Protocol (ICMP)  306

The ping Command and the ICMP Echo Request and Echo Reply  307

The Destination Unreachable ICMP Message  307

The Redirect ICMP Message  310

The ICMP Time Exceeded Message  310

The traceroute Command  312

Troubleshooting the Packet Forwarding Process  314

Isolating IP Routing Problems Related to Hosts  314

Isolating IP Routing Problems Related to Routers  316

Troubleshooting Scenario 1: Forward Route Problem  318

Troubleshooting Scenario 2: Reverse Route Problem  321

An Alternative Problem Isolation Process for Steps 3, 4, and 5  324

Troubleshooting Tools and Tips  324

Host Routing Tools and Perspectives  324

Host Troubleshooting Tips  324

LAN Switch IP Support  325

show ip route Reference  326

Interface Status  328

VLSM Issues  328

Recognizing When VLSM Is Used  328

Configuring Overlapping VLSM Subnets  329

Symptoms with Overlapping Subnets  331

VLSM Troubleshooting Summary  333

Discontiguous Networks and Autosummary  333

Access List Troubleshooting Tips  334

Exam Preparation Tasks  337

Review All the Key Topics  337

Complete the Tables and Lists from Memory  337

Definitions of Key Terms  337

Part III: Routing Protocols  339

Chapter 10  Routing Protocol Theory  341

“Do I Know This Already?” Quiz  341

Foundation Topics  345

Dynamic Routing Protocol Overview  345

Routing Protocol Functions  346

Interior and Exterior Routing Protocols  347
Comparing IGPs 349
   IGP Routing Protocol Algorithms 349
   Metrics 350
   IGP Comparisons: Summary 351
Administrative Distance 352
Distance Vector Routing Protocol Features 354
   The Concept of a Distance and a Vector 354
   Distance Vector Operation in a Stable Network 355
   Distance Vector Loop Prevention 356
   Route Poisoning 357
   Problem: Counting to Infinity over a Single Link 358
   Split Horizon 360
   Poison Reverse and Triggered Updates 362
   Problem: Counting to Infinity in a Redundant Network 363
   The Holdown Process and Holdown Timer 366
Distance Vector Summary 368
Link-State Routing Protocol Features 369
   Building the Same LSDB on Every Router 369
   Applying Dijkstra SPF Math to Find the Best Routes 371
   Convergence with Link-State Protocols 373
   Summary and Comparisons to Distance Vector Protocols 373
Exam Preparation Tasks 375
   Review All the Key Topics 375
   Complete the Tables and Lists from Memory 376
   Definitions of Key Terms 376
   Command Reference to Check Your Memory 376

Chapter 11 OSPF 379
   “Do I Know This Already?” Quiz 379
Foundation Topics 383
   OSPF Protocols and Operation 383
   OSPF Neighbors 383
      Identifying OSPF Routers with a Router ID 384
      Meeting Neighbors by Saying Hello 384
      Potential Problems in Becoming a Neighbor 385
      Neighbor States 386
   OSPF Topology Database Exchange 388
      Overview of the OSPF Database Exchange Process 388
      Choosing a Designated Router 388
      Database Exchange 390
      Maintaining the LSDB While Being Fully Adjacent 391
      Summary of Neighbor States 391
      Building the IP Routing Table 392
   Scaling OSPF Through Hierarchical Design 393
      OSPF Areas 394
      OSPF Area Design Advantages 396
Neighbor Relationships 454

   EIGRP Neighbor Requirements 455
   OSPF Neighbor Requirements 457
   OSPF Neighbor Example 1 459
   OSPF Neighbor Example 2 461
   The MTU Matching Requirement 463

Exam Preparation Tasks 464

   Review All the Key Topics 464
   Complete the Tables and Lists from Memory 464
   Command Reference to Check Your Memory 464

Part IV:  Wide-Area Networks 467

Chapter 14  Point-to-Point WANs 469
   “Do I Know This Already?” Quiz 469

Foundation Topics 472

   PPP Concepts 472
      The PPP Protocol Field 472
      PPP Link Control Protocol (LCP) 473
         Looped Link Detection 474
         Enhanced Error Detection 475
      PPP Multilink 475
      PPP Authentication 476

   PPP Configuration 478
      Basic PPP Configuration 478
      CHAP Configuration and Verification 479
      PAP Configuration 480

   Troubleshooting Serial Links 480
      Troubleshooting Layer 1 Problems 482
      Troubleshooting Layer 2 Problems 483
         Keepalive Failure 484
         PAP and CHAP Authentication Failure 485
      Troubleshooting Layer 3 Problems 486

Exam Preparation Tasks 489

   Review All the Key Topics 489
   Complete the Tables and Lists from Memory 489
   Definitions of Key Terms 489
   Command Reference to Check Your Memory 490

Chapter 15  Frame Relay Concepts 493
   “Do I Know This Already?” Quiz 493

Foundation Topics 497

   Frame Relay Overview 497
      Frame Relay Standards 500
      Virtual Circuits 500
      LMI and Encapsulation Types 503
Frame Relay Addressing  505
   Frame Relay Local Addressing  506
   Frame Forwarding with One DLCI Field  507
   Frame Relay Global Addressing (DLCIs)  509
Network Layer Concerns with Frame Relay  511
   Frame Relay Layer 3 Addressing: One Subnet Containing All Frame Relay
      DTEs  511
   Frame Relay Layer 3 Addressing: One Subnet Per VC  512
   Frame Relay Layer 3 Addressing: Hybrid Approach  514
   Layer 3 Broadcast Handling  515
Controlling Speed and Discards in the Frame Relay Cloud  516
   FECN and BECN  517
      The Discard Eligibility (DE) Bit  518
Exam Preparation Tasks  519
   Review All the Key Topics  519
   Complete the Tables and Lists from Memory  519
   Definitions of Key Terms  520

Chapter 16  Frame Relay Configuration  523
   “Do I Know This Already?” Quiz  523
Foundation Topics  527
   Frame Relay Configuration and Verification  527
      Planning a Frame Relay Configuration  527
      A Fully Meshed Network with One IP Subnet  529
      Configuring the Encapsulation and LMI  531
   Frame Relay Address Mapping  532
      Inverse ARP  535
      Static Frame Relay Mapping  536
   A Partially Meshed Network with One IP Subnet Per VC  537
      Assigning a DLCI to a Particular Subinterface  540
      Comments About Global and Local Addressing  540
      Frame Relay Verification  541
   A Partially Meshed Network with Some Fully Meshed Parts  543
Frame Relay Troubleshooting  547
   A Suggested Frame Relay Troubleshooting Process  547
      Layer 1 Issues on the Access Link (Step 1)  549
      Layer 2 Issues on the Access Link (Step 2)  549
      PVC Problems and Status (Step 3)  551
         Find the Connected Subnet and Outgoing Interface (Steps 3a and 3b)  552
         Find the PVCs Assigned to That Interface (Step 3c)  553
         Determine Which PVC Is Used to Reach a Particular Neighbor (Step 3d)  554
      PVC Status  555
         Subinterface Status  556
   Frame Relay Mapping Issues (Step 4)  558
      End-to-End Encapsulation (Step 5)  559
      Mismatched Subnet Numbers (Step 6)  559
Exam Preparation Tasks  560
Review All the Key Topics  560
Complete the Tables and Lists from Memory  560
Read the Appendix G Scenarios  560
Command Reference to Check Your Memory  561

Chapter 17  Virtual Private Networks  565
“Do I Know This Already?” Quiz  565

Foundation Topics  568
VPN Fundamentals  568
IPsec VPNs  571
  IPsec Encryption  572
  IPsec Key Exchange  573
  IPsec Authentication and Message Integrity  574
  The ESP and AH Security Protocols  576
  IPsec Implementation Considerations  577
SSL VPNs  578

Exam Preparation Tasks  580
Review All the Key Topics  580
Complete the Tables and Lists from Memory  580
Definitions of Key Terms  580

Part V:  Scaling the IP Address Space  583

Chapter 18  Network Address Translation  585
“Do I Know This Already?” Quiz  585

Foundation Topics  589
Perspectives on IPv4 Address Scalability  589
  CIDR  590
    Route Aggregation for Shorter Routing Tables  590
    IPv4 Address Conservation  591
  Private Addressing  592
Network Address Translation Concepts  593
  Static NAT  593
  Dynamic NAT  596
    Overloading NAT with Port Address Translation (PAT)  598
    Translating Overlapping Addresses  600
NAT Configuration and Troubleshooting  602
  Static NAT Configuration  602
  Dynamic NAT Configuration  604
  NAT Overload (PAT) Configuration  608
  NAT Troubleshooting  611

Exam Preparation Tasks  613
Review All the Key Topics  613
Complete the Tables and Lists from Memory  613
Definitions of Key Terms  614
Command Reference to Check Your Memory  614
Icons Used in This Book

- Printer
- Web Server
- Web Browser
- PC
- Laptop
- Server
- Phone
- IP Phone
- Router
- Multiservice Switch
- Switch
- ATM Switch
- Frame Relay Switch
- Cable Modem
- PBX
- Access Point
- ASA
- DSLAM
- WAN Switch
- CSU/DSU
- Hub
- PIX Firewall
- Bridge
- Wireless Connection
- Network Cloud
- Ethernet Connection
- Serial Line Connection
- Virtual Circuit

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

Congratulations! If you’re reading far enough to look at this book’s Introduction, then you’ve probably already decided to go for your Cisco certification. If you want to succeed as a technical person in the networking industry at all, you need to know Cisco. Cisco has a ridiculously high market share in the router and switch marketplace, with more than 80 percent market share in some markets. In many geographies and markets around the world, networking equals Cisco. If you want to be taken seriously as a network engineer, Cisco certification makes perfect sense.

Historically speaking, the first entry-level Cisco certification has been the Cisco Certified Network Associate (CCNA) certification, first offered in 1998. The first three versions of the CCNA certification required that you pass a single exam to become certified. However, over time, the exam kept growing, both in the amount of material covered, and the difficulty level of the questions. So, for the fourth major revision of the exams, announced in 2003, Cisco continued with a single certification (CCNA), but offered two options for the exams to get certified: a single exam option and a two-exam option. The two-exam option allowed people to study roughly half of the material, take and pass one exam, before they moved to the next one.

Structure of the Exams

For the current certifications, announced in June 2007, Cisco created the ICND1 (640-822) and ICND2 (640-816) exams, along with the CCNA (640-802) exam. (The exams just prior, from 2003 to 2007, followed the same structure, but were called INTRO, ICND, and CCNA.) To become CCNA certified, you can pass both the ICND1 and ICND2 exams, or just pass the CCNA exam. The CCNA exam simply covers all the topics on the ICND1 and ICND2 exams, which gives you two options for gaining your CCNA certification. The two-exam path gives those people with less experience a chance to study for a smaller set of topics at a time, whereas the one-exam option provides an option for those who want to prepare for all the topics at once.

Although the two-exam option will be useful for some certification candidates, Cisco designed the ICND1 exam with a much more important goal in mind. The CCNA certification had grown to the point that it tested knowledge and skills beyond what an entry-level network technician would need to have. Cisco needed a certification that was more reflective of the skills required for entry-level networking jobs. So, Cisco designed its Interconnecting Cisco Networking Devices 1 (ICND1) course, and the corresponding ICND1 exam, to include the knowledge and skills most needed by an entry-level technician in a small enterprise network. To show that you have the skills required for those entry-level jobs, Cisco created a new certification: CCENT.
Figure I-1 shows the basic organization of the certifications and the exams used for getting your CCENT and CCNA certifications. (Note that there is no separate certification for passing the ICND2 exam.)

**Figure I-1   Cisco Entry-Level Certifications and Exams**

As you can see, although you can obtain the CCENT certification by taking the ICND1 exam, you do not have to be CCENT certified before you get your CCNA certification. You can choose to take the CCNA exam and bypass the CCENT certification.

The ICND1 and ICND2 exams cover different sets of topics, with a minor amount of overlap. For example, ICND1 covers IP addressing and subnetting, while ICND2 covers a more complicated use of subnetting called variable-length subnet masking (VLSM), so ICND2 must then cover subnetting to some degree. The CCNA exam covers all the topics covered on both the ICND1 and ICND2 exams.

Although CCENT has slowly gained popularity over time, the Cisco CCNA certification remains the most popular entry-level networking certification program in the IT world. A CCNA certification proves that you have a firm foundation in the most important components of the Cisco product line—namely, routers and switches. It also proves that you have a broad knowledge of protocols and networking technologies.

**New 2011 Editions, But Cisco Did Not Change the Exams**

Unlike any previous editions of this book, this edition (Edition 3, 2011) was published even though Cisco did not revise the exams in 2011 and has not changed the exam topics nor the exam numbers. The previous editions (Editions 2, 2007) work well and still include all the content related to the current 640-822, 640-816, and 640-802 exams. So why come out with a 2011 edition when the content of the exam remains unchanged, and the coverage of the topics in the 2007 editions still does a great job?
Two reasons. First, the publisher wanted to add value other than just what’s printed on the pages of the book. To that end, the publisher has added:

- A free copy of CCNA Simulator Lite. This product runs the same software as the full CCNA Network Simulator, but with some commands disabled compared to the full-price product. This is a wonderful addition, especially for those totally new to Cisco, because you can get some exposure to the user interface of Cisco gear before choosing from the many options of how to practice.

- A special offer to purchase the *CCENT/CCNA ICND2 640-816 Official Cert Guide Premium Edition* eBook and Practice Test at a 70 percent discount off the list price. This digital product provides you with two additional complete ICND2 exams and two additional full CCNA exams worth of practice questions in the powerful Pearson IT Certification Practice Test engine. It also includes two versions of the eBook version of this title: a PDF version to read on your computer and an EPUB version to read on your mobile device, tablet, or eReader. In addition to the eBook and extra practice questions, the Premium Edition eBook and Practice Test also has enhanced features in the Pearson IT Certification Practice Test, which provides you with direct links from every question to the specific section in the eBook, giving you in-depth insight into the concepts behind the questions. To take advantage of this special offer, simply refer to the instructions printed on the coupon card inserted into the DVD sleeve. This card contains a unique coupon code you can use when purchasing the Premium Edition eBook and Practice Test from one of Pearson IT Certification’s sites.

Those changes alone make the new book, and the new library (that holds this book and the *ICND1 Official Cert Guide*), a much better deal than the earlier books. However, the books do change as well—not for new content, but for how the content is presented. I (Wendell) had already rewritten and improved many topics, particularly subnetting, with an eye toward a consistent approach to exercises that help you overcome the big mental hurdles. And while we were updating the books, I also updated several small topics to improve figures, clarify a point, and make adjustments when a technology might have changed in the last four years.

So, if you compare the new and the old books side by side, you will see a completely reorganized subnetting section (seven shorter chapters rather than one long one), updated figures in some chapters, and a few other changes here and there (often because of your feedback!). What you won’t see are a bunch of new topics, because the exams did not change at the same time, and the existing books already covered all the exam topics.

So, how do you know that Cisco hasn’t changed the exams since the time this book came out? Well, first ignore online speculation that’s not from Cisco, because sometimes people like to guess. Second, look at Cisco’s website. In particular, use www.cisco.com/go/ccna,
Cisco’s main page for the CCNA certification. If you see exam numbers other than the ones listed in the earlier figure, the exams have changed. (And if they have changed, go to www.ciscopress.com to learn about how to find the yet again new edition of this book!)

**Format of the CCNA Exams**

The ICND1, ICND2, and CCNA exams all follow the same general format. When you get to the testing center and check in, the proctor gives you some general instructions and then take you into a quiet room with a PC. When you’re at the PC, you have a few things to do before the timer starts on your exam—for instance, you can take a sample quiz, just to get accustomed to the PC and the testing engine. Anyone who has user-level skills in getting around a PC should have no problems with the testing environment. Additionally, Chapter 20, “Final Preparation,” points to a Cisco website at which you can see a demo of Cisco’s actual test engine.

When you start the exam, you will be asked a series of questions. You answer the question and then move on to the next question. *The exam engine does not let you go back and change your answer.* Yes, that’s true—when you move on to the next question, that’s it for the earlier question.

The exam questions can be in one of the following formats:

- Multiple choice (MC)
- Testlet
- Drag-and-drop (DND)
- Simulated lab (Sim)
- Simlet

The first three types of questions are relatively common in many testing environments. The multiple choice format simply requires that you point and click a circle beside the correct answer(s). Cisco traditionally tells you how many answers you need to choose, and the testing software prevents you from choosing too many answers. Testlets are questions with one general scenario, with multiple MC questions about the overall scenario. Drag-and-drop questions require you to left-click and hold, move a button or icon to another area, and release the clicker to place the object somewhere else—typically into a list. So for some questions, to get the question correct, you might need to put a list of five things in the proper order.

The last two types both use a network simulator to ask questions. Interestingly, the two types actually allow Cisco to assess two very different skills. First, Sim questions generally
describe a problem, and your task is to configure one or more routers and switches to fix
the problem. The exam then grades the question based on the configuration you changed or
added. Interestingly, Sim questions are the only questions that Cisco (to date) has openly
confirmed that partial credit is given.

The Simlet questions may well be the most difficult style of question on the exams. Simlet
questions also use a network simulator, but instead of answering the question by changing
the configuration, the question includes 1 or more MC questions. The questions require that
you use the simulator to examine the current behavior of a network, interpreting the output
of any **show** commands that you can remember in order to answer the question. While Sim
questions require you to troubleshoot problems related to a configuration, Simlets require
you to both analyze both working and broken networks, correlating **show** command output
with your knowledge of networking theory and configuration commands.

**What’s on the CCNA Exam(s)?**

Ever since I was in grade school, whenever the teacher announced that we were having a
test soon, someone would always ask, “What’s on the test?” Even in college, people would
try to get more information about what would be on the exams. At heart, the goal is to know
what to study hard, what to study a little, and what to not study at all.

Cisco wants the public to know both the variety of topics, and an idea about the kinds of
knowledge and skills required for each topic, for every Cisco certification exam. To that
end, Cisco publishes a set of exam objectives for each exam. The objectives list the specific
topics, like IP addressing, RIP, and VLANs. The objectives also implies the kinds of skills
required that that topic. For example, one objective might start with “Describe…” and
another might begin with “Describe, configure, and troubleshoot….” The second objective
clearly states that you need a thorough and deep understanding of that topic. By listing the
topics and skill level, Cisco helps us all prepare for its exams.

Although the exam objectives are helpful, keep in mind that Cisco adds a disclaimer that
the posted exam topics for all of its certification exams are *guidelines*. Cisco makes the
effort to keep the exam questions within the confines of the stated exam objectives, and I
know from talking to those involved that every question is analyzed for whether it fits
within the stated exam topics.

**ICND1 Exam Topics**

Table I-1 lists the exam topics for the ICND1 exam, with the ICND2 exam topics following
in Table I-2. Although Cisco’s posted exam topics are not numbered, Cisco Press numbers
the exam topics for easier reference. Table I-1 also notes the book parts in which each exam
topic is covered. Because it is possible that the exam topics may change over time, it may
be worth the time to double-check the exam topics as listed on Cisco’s website (www.cisco.com/go/ccna). If Cisco does happen to add exam topics at a later date, note that Appendix C, “ICND2 Exam Updates: Version 1.0,” describes how to go to www.ciscopress.com and download additional information about those newly added topics.

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Book Parts (ICND1 Book)</th>
<th>Exam Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>I</td>
<td>Describe the operation of data networks</td>
</tr>
<tr>
<td>2</td>
<td>I</td>
<td>Describe the purpose and functions of various network devices</td>
</tr>
<tr>
<td>3</td>
<td>I, II, III, IV</td>
<td>Select the components required to meet a given network specification</td>
</tr>
<tr>
<td>4</td>
<td>I</td>
<td>Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network</td>
</tr>
<tr>
<td>5</td>
<td>I</td>
<td>Describe common networking applications including web applications</td>
</tr>
<tr>
<td>6</td>
<td>I</td>
<td>Describe the purpose and basic operation of the protocols in the OSI and TCP models</td>
</tr>
<tr>
<td>7</td>
<td>I–V</td>
<td>Describe the impact of applications (Voice over IP and Video over IP) on a network</td>
</tr>
<tr>
<td>8</td>
<td>I–V</td>
<td>Interpret network diagrams</td>
</tr>
<tr>
<td>9</td>
<td>I, III, IV, V</td>
<td>Determine the path between two hosts across a network</td>
</tr>
<tr>
<td>10</td>
<td>I–V</td>
<td>Describe the components required for network and Internet communications</td>
</tr>
<tr>
<td>11</td>
<td>I–V</td>
<td>Identify and correct common network problems at Layers 1, 2, 3 and 7 using a layered model approach</td>
</tr>
<tr>
<td>12</td>
<td>II</td>
<td>Differentiate between LAN/WAN operation and features</td>
</tr>
<tr>
<td>13</td>
<td>II</td>
<td>Implement a small switched network</td>
</tr>
<tr>
<td>14</td>
<td>II</td>
<td>Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts</td>
</tr>
<tr>
<td>15</td>
<td>II</td>
<td>Explain the technology and media access control method for Ethernet technologies</td>
</tr>
<tr>
<td>16</td>
<td>II</td>
<td>Explain network segmentation and basic traffic management concepts</td>
</tr>
<tr>
<td>17</td>
<td>II</td>
<td>Perform, save, and verify initial switch configuration tasks, including remote access management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Verify network status and switch operation using basic utilities (including ping, traceroute, telnet, SSH, arp, ipconfig), show and debug commands</td>
</tr>
<tr>
<td>Reference Number</td>
<td>Book Parts (ICND1 Book)</td>
<td>Exam Topic</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>18</td>
<td>II</td>
<td>Implement and verify basic security for a switch (port security, deactivate ports)</td>
</tr>
<tr>
<td>19</td>
<td>II</td>
<td>Identify, prescribe, and resolve common switched network media issues, configuration issues, autonegotiation, and switch hardware failures</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Implement an IP addressing scheme and IP services to meet network requirements for a small branch office</strong></td>
</tr>
<tr>
<td>20</td>
<td>I, III</td>
<td>Describe the need and role of addressing in a network</td>
</tr>
<tr>
<td>21</td>
<td>I, III</td>
<td>Create and apply an addressing scheme to a network</td>
</tr>
<tr>
<td>22</td>
<td>III, IV</td>
<td>Assign and verify valid IP addresses to hosts, servers, and networking devices in a LAN environment</td>
</tr>
<tr>
<td>23</td>
<td>IV</td>
<td>Explain the basic uses and operation of NAT in a small network connecting to one ISP</td>
</tr>
<tr>
<td>24</td>
<td>I, IV</td>
<td>Describe and verify DNS operation</td>
</tr>
<tr>
<td>25</td>
<td>III</td>
<td>Describe the operation and benefits of using private and public IP addressing</td>
</tr>
<tr>
<td>26</td>
<td>III, V</td>
<td>Enable NAT for a small network with a single ISP and connection using SDM and verify operation using CLI and ping</td>
</tr>
<tr>
<td>27</td>
<td>IV</td>
<td>Configure, verify, and troubleshoot DHCP and DNS operation on a router (including CLI/SDM)</td>
</tr>
<tr>
<td>28</td>
<td>IV</td>
<td>Implement static and dynamic addressing services for hosts in a LAN environment</td>
</tr>
<tr>
<td>29</td>
<td>III</td>
<td>Identify and correct IP addressing issues</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Implement a small routed network</strong></td>
</tr>
<tr>
<td>30</td>
<td>I, III, IV</td>
<td>Describe basic routing concepts (including packet forwarding, router lookup process)</td>
</tr>
<tr>
<td>31</td>
<td>IV</td>
<td>Describe the operation of Cisco routers (including router bootup process, POST, router components)</td>
</tr>
<tr>
<td>32</td>
<td>I, IV</td>
<td>Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts</td>
</tr>
<tr>
<td>33</td>
<td>IV</td>
<td>Configure, verify, and troubleshoot RIPv2</td>
</tr>
<tr>
<td>34</td>
<td>IV</td>
<td>Access and utilize the router CLI to set basic parameters</td>
</tr>
<tr>
<td>35</td>
<td>IV</td>
<td>Connect, configure, and verify operation status of a device interface</td>
</tr>
<tr>
<td>36</td>
<td>IV</td>
<td>Verify device configuration and network connectivity using ping, traceroute, telnet, SSH, or other utilities</td>
</tr>
<tr>
<td>Reference Number</td>
<td>Book Parts (ICND1 Book)</td>
<td>Exam Topic</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>37</td>
<td>IV</td>
<td>Perform and verify routing configuration tasks for a static or default route given specific routing requirements</td>
</tr>
<tr>
<td>38</td>
<td>IV</td>
<td>Manage IOS configuration files (including save, edit, upgrade, restore)</td>
</tr>
<tr>
<td>39</td>
<td>IV</td>
<td>Manage Cisco IOS</td>
</tr>
<tr>
<td>40</td>
<td>IV</td>
<td>Implement password and physical security</td>
</tr>
<tr>
<td>41</td>
<td>IV</td>
<td>Verify network status and router operation using basic utilities (including ping, traceroute, telnet, SSH, arp, ipconfig), <code>show</code> and <code>debug</code> commands</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Explain and select the appropriate administrative tasks required for a WLAN</strong></td>
</tr>
<tr>
<td>42</td>
<td>II</td>
<td>Describe standards associated with wireless media (including IEEE, WI-FI Alliance, ITU/FCC)</td>
</tr>
<tr>
<td>43</td>
<td>II</td>
<td>Identify and describe the purpose of the components in a small wireless network (including SSID, BSS, ESS)</td>
</tr>
<tr>
<td>44</td>
<td>II</td>
<td>Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point</td>
</tr>
<tr>
<td>45</td>
<td>II</td>
<td>Compare and contrast wireless security features and capabilities of WPA security (including open, WEP, WPA-1/2)</td>
</tr>
<tr>
<td>46</td>
<td>II</td>
<td>Identify common issues with implementing wireless networks</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Identify security threats to a network and describe general methods to mitigate those threats</strong></td>
</tr>
<tr>
<td>47</td>
<td>I</td>
<td>Explain today’s increasing network security threats and the need to implement a comprehensive security policy to mitigate the threats</td>
</tr>
<tr>
<td>48</td>
<td>I</td>
<td>Explain general methods to mitigate common security threats to network devices, hosts, and applications</td>
</tr>
<tr>
<td>49</td>
<td>I</td>
<td>Describe the functions of common security appliances and applications</td>
</tr>
<tr>
<td>50</td>
<td>I, II, IV</td>
<td>Describe security recommended practices including initial steps to secure network devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Implement and verify WAN links</strong></td>
</tr>
<tr>
<td>51</td>
<td>V</td>
<td>Describe different methods for connecting to a WAN</td>
</tr>
<tr>
<td>52</td>
<td>V</td>
<td>Configure and verify a basic WAN serial connection</td>
</tr>
</tbody>
</table>
ICND2 Exam Topics
Table I-2 lists the exam topics for the ICND2 (640-816) exam, along with the book parts in the *CCNA ICND2 Official Exam Certification Guide* in which each topic is covered.

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Book Parts</th>
<th>Exam Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure, verify, and troubleshoot a switch with VLANs and interswitch communications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>101</td>
<td>I</td>
<td>Describe enhanced switching technologies (including VTP, RSTP, VLAN, PVSTP, 802.1q)</td>
</tr>
<tr>
<td>102</td>
<td>I</td>
<td>Describe how VLANs create logically separate networks and the need for routing between them</td>
</tr>
<tr>
<td>103</td>
<td>I</td>
<td>Configure, verify, and troubleshoot VLANs</td>
</tr>
<tr>
<td>104</td>
<td>I</td>
<td>Configure, verify, and troubleshoot trunking on Cisco switches</td>
</tr>
<tr>
<td>105</td>
<td>II</td>
<td>Configure, verify, and troubleshoot interVLAN routing</td>
</tr>
<tr>
<td>106</td>
<td>I</td>
<td>Configure, verify, and troubleshoot VTP</td>
</tr>
<tr>
<td>107</td>
<td>I</td>
<td>Configure, verify, and troubleshoot RSTP operation</td>
</tr>
<tr>
<td>108</td>
<td>I</td>
<td>Interpret the output of various <em>show</em> and <em>debug</em> commands to verify the operational status of a Cisco switched network</td>
</tr>
<tr>
<td>109</td>
<td>I</td>
<td>Implement basic switch security (including port security, unassigned ports, trunk access, etc.)</td>
</tr>
<tr>
<td>110</td>
<td>II</td>
<td>Calculate and apply a VLSM IP addressing design to a network</td>
</tr>
<tr>
<td>111</td>
<td>II</td>
<td>Determine the appropriate classless addressing scheme using VLSM and summarization to satisfy addressing requirements in a LAN/WAN environment</td>
</tr>
<tr>
<td>112</td>
<td>V</td>
<td>Describe the technological requirements for running IPv6 (including protocols, dual stack, tunneling, etc.)</td>
</tr>
<tr>
<td>113</td>
<td>V</td>
<td>Describe IPv6 addresses</td>
</tr>
<tr>
<td>114</td>
<td>II, III</td>
<td>Identify and correct common problems associated with IP addressing and host configurations</td>
</tr>
<tr>
<td>115</td>
<td>III</td>
<td>Compare and contrast methods of routing and routing protocols</td>
</tr>
<tr>
<td>116</td>
<td>III</td>
<td>Configure, verify, and troubleshoot OSPF</td>
</tr>
<tr>
<td>117</td>
<td>III</td>
<td>Configure, verify, and troubleshoot EIGRP</td>
</tr>
<tr>
<td>118</td>
<td>II, III</td>
<td>Verify configuration and connectivity using ping, traceroute, and telnet or SSH</td>
</tr>
<tr>
<td>119</td>
<td>II, III</td>
<td>Troubleshoot routing implementation issues</td>
</tr>
</tbody>
</table>
The CCNA 640-802 exam actually covers everything from both the ICND1 and ICND2 exams, at least based on the published exam topics. As of publication, the CCNA exam topics include all topics in Tables I-1 and I-2, except those topics that are highlighted in light gray in those tables. However, note that the gray topics are still covered on the CCNA 640-802 exam; those topics are just not listed in the CCNA exam topics because one of the other exam topics refers to the same topic. In short, CCNA = ICND1 + ICND2.

### ICND1 and ICND2 Course Outlines

Another way to get some direction about the topics on the exams is to look at the course outlines for the related courses. Cisco offers two authorized CCNA-related courses:
Interconnecting Cisco Network Devices 1 (ICND1) and Interconnecting Cisco Network Devices 2 (ICND2). Cisco authorizes Certified Learning Solutions Providers (CLSP) and Certified Learning Partners (CLP) to deliver these classes. These authorized companies can also create unique custom course books using this material, in some cases to teach classes geared toward passing the CCNA exam.

**About the CCNA ICND1 Official Cert Guide and CCNA ICND2 Official Cert Guide**

As previously mentioned, Cisco separated the content covered by the CCNA exam into two parts: topics typically used by engineers that work in a small enterprise network (ICND1), with the additional topics commonly used by engineers in medium-sized enterprises being covered by the ICND2 exam. Likewise, the Cisco Press CCNA Exam Certification Guide series includes two books for CCNA: the *CCENT/CCNA ICND1 Official Cert Guide* and the *CCNA ICND2 Official Cert Guide*. These books cover the breadth of topics on each exam, typically a bit more in-depth than what is required for the exams, just to ensure the books prepare you for the more difficult exam questions.

This section lists the variety of book features in both this book and the *CCENT/CCNA ICND1 Official Cert Guide*. Both books have the same basic features, so if you are reading both this book and the ICND1 book, there is no need to read the Introduction to that book. Also, for those of you using both books to prepare for the CCNA 640-802 exam (rather than taking the two-exam option), the end of this Introduction lists a suggested reading plan.

**Objectives and Methods**

The most important and somewhat obvious objective of this book is to help you pass the ICND2 exam or the CCNA exam. In fact, if the primary objective of this book were different, the book’s title would be misleading! However, the methods used in this book to help you pass the exams are also designed to make you much more knowledgeable about how to do your job.

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. So, this book does not try to help you pass the exams only by memorization, but by truly learning and understanding the topics. The CCNA certification is the foundation for many of the Cisco professional certifications, and it would be a disservice to you if this book did not help you
truly learn the material. Therefore, this book helps you pass the CCNA exam by using the following methods:

- Helping you discover which exam topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the DVD

**Book Features**

To help you customize your study time using these books, the core chapters 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 determine the amount of time you need to spend studying that chapter.
- **Foundation Topics**—These are the core sections of each chapter. They explain the protocols, concepts, and configuration for the topics in that chapter.
- **Exam Preparation Tasks**—At the end of the “Foundation Topics” section of each chapter, the “Exam Preparation Tasks” section lists a series of study activities that should be done at the end of the chapter. Each chapter includes the activities that make the most sense for studying the topics in that chapter. The activities include
  - **Key Topics Review**: The Key Topics icon is shown next to the most important items in the “Foundation Topics” section of the chapter. The Key Topics Review activity lists the Key Topics from the chapter and their corresponding page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic.
  - **Complete Tables and Lists from Memory**: To help you exercise your memory and memorize some lists of facts, many of the more important lists and tables from the chapter are included in a document on the DVD. This document lists only partial information, which allows you to complete the table or list.
  - **Definition of Key Terms**: Although the exams may be unlikely to ask a question like, “Define this term,” the CCNA exams require that you learn and know a lot of networking terminology. This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the Glossary at the end of the book.
— **Command Reference Tables**: Some book chapters cover a large amount of configuration and EXEC commands. These tables list the commands introduced in the chapter, along with an explanation. For exam preparation, use it for reference, but also read the table once when performing the Exam Preparation Tasks to make sure you remember what all the commands do.

In addition to the features in each of the core chapters, this book, as a whole, has additional study resources, including

- **DVD-based practice exam**: The companion DVD contains the powerful Pearson IT Certification Practice Test exam engine. You can take simulated ICND2 exams, as well as simulated CCNA exams, with the DVD and activation code included in this book. (You can take simulated ICND1 and CCNA exams with the DVD in *CCENT/CCNA ICND1 Official Cert Guide*.)

- **CCNA Simulator Lite**: This lite version of the best-selling CCNA Network Simulator from Pearson provides you with a means, right now, to experience the Cisco command-line interface (CLI). No need to go buy real gear or buy a full simulator to start learning the CLI. Just install it from the DVD in the back of this book. (Note: To determine when to use each lab, refer to this book's web page, and look for the link for Simulator. www.ciscopress.com/title/15872044355 )

- **eBook**: If you are interested in obtaining an eBook version of this title, we have included a special offer on a coupon card inserted in the DVD sleeve in the back of the book. This offer allows you to purchase the *CCNA ICND2 640-816 Official Cert Guide Premium Edition* eBook and Practice Test at a 70 percent discount off the list price. In addition to two versions of the eBook (PDF and EPUB), you will also receive additional practice test questions and enhanced practice test features.

- **Subnetting videos**: The companion DVD contains a series of videos that show how to calculate various facts about IP addressing and subnetting, in particular using the shortcuts described in this book.

- **VLSM, summarization, and ACL practice**: The companion DVD contains three appendices (D through F) that correspond to Chapters 5, 6, and 7, respectively. Each appendix contains a set of practice problems related to a corresponding chapter.

- **ICND1 subnetting chapters**: The DVD also includes a menu section that lists copies of all the subnetting elements from *CCENT/CCNA ICND1 640-822 Official Cert Guide*. These include the printed subnetting chapters from that book and the DVD-only practice appendices from that book.
DVD-based practice scenarios: Appendix G, “Additional Scenarios,” on the companion DVD, contains several networking scenarios for additional study. These scenarios describe various networks and requirements, taking you through conceptual design, configuration, and verification. These scenarios are useful for building your hands-on skills, even if you do not have lab gear.

Companion website: The website www.ciscopress.com/title/1587204355 posts up-to-the-minute materials that further clarify complex exam topics. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exam.

If you are looking for more hands-on practice, you might want to consider purchasing the CCNA 640-802 Network Simulator. You can purchase a copy of this software from Pearson at www.pearsonitcertification.com/networksimulator or other retail outlets. To help you with your studies, I have created a mapping guide that maps each of the 250 labs in the simulator to the specific sections in these CCNA Cert Guides. You can get this mapping guide for free on the "Extras" tab of the companion website.

Author’s website and blogs: The author maintains a website that hosts tools and links useful when studying for CCENT and CCNA. The site lists information to help you build your own lab, study pages that correspond to each chapter of this book and the ICND1 book, and links to the author’s CCENT Skill blog and CCNA Skills blog. Start at www.certskills.com; check the tabs for study and blogs in particular.

How This Book Is Organized
This book contains 20 core chapters—Chapters 1 through 20, with Chapter 20 including some summary materials and suggestions for how to approach the actual exams. Each core chapter covers a subset of the topics on the ICND2 exam. The core chapters are organized into sections. The core chapters cover the following topics:

Part I: LAN Switching

- **Chapter 1, “Virtual LANs,”** explains the concepts and configuration surrounding virtual LANs, including VLAN trunking and VLAN Trunking Protocol.

- **Chapter 2, “Spanning Tree Protocol,”** dives deeply into the concepts behind the original Spanning Tree Protocol (STP), as well as the newer Rapid STP (RSTP), including concepts, configuration, and troubleshooting.

- **Chapter 3, “Troubleshooting LAN Switching,”** explains some general ideas about how to troubleshoot networking problems, with most of the chapter focusing on the forwarding process used by LAN switches.
Part II: IP Routing

- Chapter 4, “IP Routing: Static and Connected Routes,” examines how routers add both static routes and connected routes to the routing table, while also reviewing the concepts behind how routers route, or forward, packets.

- Chapter 5, “Variable Length Subnet Masks,” defines VLSM and explains the common pitfalls that may occur when designing and deploying IP addresses when using different masks in the same network.

- Chapter 6, “Route Summarization,” examines the idea of manual route summarization, with which an engineer can make a router advertise a route for one larger subnet rather than multiple routes for many smaller subnets. It also discusses the idea of automatic route summarization at the boundaries between classful networks.

- Chapter 7, “Basic IP Access Control Lists,” examines how standard IP ACLs can filter packets based on the source IP address so that a router will not forward the packet.

- Chapter 8, “Advanced IP Access Control Lists,” examines both named and numbered ACLs, emphasizing how extended IP ACLs can match packets based on both source and destination IP address, and by matching source and destination TCP and UDP port numbers.

- Chapter 9, “Troubleshooting IP Routing,” shows a structured plan for how to isolate problems related to two hosts that should be able to send packets to each other, but cannot. The chapter also includes a variety of tips and tools for helping attack routing problems.

Part III: Routing Protocols


- Chapter 11, “OSPF,” examines OSPF, including more detail about link-state theory as implemented by OSPF, and OSPF configuration.

- Chapter 12, “EIGRP,” examines EIGRP, including a description of the theory behind EIGRP, as well as EIGRP configuration and verification.

- Chapter 13, “Troubleshooting Routing Protocols,” explains some of the typical reasons why routing protocols fail to exchange routing information, showing specific examples of common problems with both OSPF and EIGRP.
Part IV: Wide-Area Networks

- **Chapter 14, “Point-to-Point WANs,”** reviews the basics of WANs and examines PPP, including CHAP, in more detail.

- **Chapter 15, “Frame Relay Concepts,”** focuses on the terminology and theory behind the Frame Relay protocol, including the IP addressing options when using Frame Relay.

- **Chapter 16, “Frame Relay Configuration,”** shows a variety of configuration options for Frame Relay, including both point-to-point and multipoint subinterfaces. It also explains how to best use `show` commands to isolate the root cause of common Frame Relay problems.

- **Chapter 17, “Virtual Private Networks,”** examines the concepts and protocols used to create secure VPNs over the Internet. This chapter includes the basics of IPsec.

Part V: Scaling the IP Address Space

- **Chapter 18, “Network Address Translation,”** closely examines the concepts behind the depletion of the IPv4 address space, and how NAT, in particular the Port Address Translation (PAT) option, helps solve the problem. The chapter also shows how to configure NAT on routers using the IOS CLI.

- **Chapter 19, “IP Version 6,”** introduces the basics of IPv6, including the 128-bit address format, OSPF and EIGRP support for IPv6, and basic native IPv6 configuration. It also introduces the concept of IPv6 tunneling and migration strategies.

Part VI: Final Preparation

- **Chapter 20, “Final Preparation,”** suggests a plan for final preparation after you have finished the core parts of the book (in particular, explaining the many study options available in the book).

Part VII: Appendixes (In Print)

- **Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes,”** includes the answers to all the questions from Chapters 1 through 19.

- **Appendix B, “Numeric Reference Tables,”** lists several tables of numeric information, including a binary-to-decimal conversion table and a list of powers of 2.
Appendix C, “ICND2 Exam Updates: Version 1.0,” covers a variety of short topics that either clarify or expand upon topics covered earlier in this book. This appendix is updated from time to time and posted at www.ciscopress.com/ccna, with the most recent version available at the time of printing included here as Appendix C. (The first page of the appendix includes instructions on how to check whether a later version of Appendix C is available online.)

The Glossary contains definitions for all the terms listed in the “Definitions of Key Terms” section at the conclusion of Chapters 1–19.

Part VIII: Appendices (on the DVD)

The following appendixes are available in PDF format on the DVD that accompanies this book:

- Appendix D, “Practice for Chapter 5: Variable Length Subnet Masks,” lists extra practice problems related to VLSM, as originally explained in Chapter 5.

- Appendix E, “Practice for Chapter 6: Route Summarization,” lists extra practice problems related to manual route summarization, as originally explained in Chapter 6.

- Appendix F, “Practice for Chapter 7: Basic IP Access Control Lists,” lists extra practice problems related to IP ACLs, as originally explained in Chapter 7.

- Appendix G, “Additional Scenarios”—One method to improve your troubleshooting and network analysis skills is to examine as many unique network scenarios as is possible, think about them, and then get some feedback as to whether you came to the right conclusions. This appendix provides several such scenarios.

- Appendix H, “Video Reference”—The DVD includes several subnetting videos that show how to perform various subnetting tasks. This appendix contains copies of the key elements from those videos, which can be useful when watching the videos (so that you do not have to keep moving back and forth in the video).

- Appendix I, “ICND1 Chapter 23: WAN Configuration,” is a duplicate of Chapter 23 from CCENT/CCNA ICND1 Official Cert Guide. Chapter 14 of this book (ICND2), “Point-to-Point WANs,” suggests to review a few prerequisite points as listed in this chapter. This chapter is included in this book for those of you who do not have a copy of CCENT/CCNA ICND1 Official Cert Guide.

- Appendix J, “Memory Tables,” holds the key tables and lists from each chapter, with some of the content removed. You can print this appendix and, as a memory exercise, complete the tables and lists. The goal is to help you memorize facts that can be useful on the exams.
Appendix K, “Memory Tables Answer Key,” contains the answer key for the exercises in Appendix J.

Appendix L, “ICND2 Open-Ended Questions,” is a holdover from previous editions of this book. The older edition had some open-ended questions for the purpose of helping you study for the exam, but the newer features make these questions unnecessary. For convenience, the old questions are included here, unedited since the last edition.

Note that in addition to the appendices listed here, the DVD also includes a menu section that lists copies of all the subsetting elements from *CCENT/CCNA ICND1 640-822 Official Cert Guide*. These include the printed subsetting chapters from that book and the DVD-only practice appendices from that book.

**How to Use This Book to Prepare for the ICND2 and CCNA Exams**

This book was designed with two primary goals in mind: to help you study for the ICND2 exam and to help you study for the CCNA exam by using both this book and the *ICND1 Official Cert Guide*. Using this book to prepare for the ICND2 exam is pretty straightforward: read each chapter in succession, and follow the study suggestions in Chapter 20.

For the core chapters of this book (Chapters 1–19), you have some choices as to how much of the chapter you read. In some cases, you may already know most or all of the information covered in a given chapter. To help you decide how much time to spend on each chapter, the chapters begin with a “Do I Know This Already?” quiz. If you get all the quiz questions correct, or just miss one question, you may want to skip to the end of the chapter and the “Exam Preparation Tasks” section, and do those activities. Figure I-2 shows the overall plan.

**Figure I-2  How to Approach Each Chapter of This Book**

1. **Take the “Do I Know This Already Quiz”**
   - Miss more than 1:
     - Read “Foundation Topics” Section
   - Miss 1 or less, but want more study:
     - Read “Foundation Topics” Section
   - Miss 1 or less, want to move on:
     - Read/do “Exam Preparation Tasks”
2. **To Next Chapter**
When you complete Chapters 1–19, you can then use the guidance listed in Chapter 20 to
detail the rest of the exam preparation tasks. That chapter includes the following suggestions:

- Check www.ciscopress.com for the latest copy of Appendix C, which may include
  additional topics for study.
- Practice subnetting using the tools available in the DVD appendices.
- Repeat the tasks in all chapters’ “Exam Preparation Tasks” chapter-ending sections.
- Review the scenarios in DVD Appendix G.
- Review all “Do I Know This Already?” questions using the exam engine.
- Practice the exam using the exam engine.

How to Use These Books to Prepare for the CCNA
640-802 Exam

If you plan to get your CCNA certification using the one-exam option of taking the CCNA
640-802 exam, you can use this book with the CCENT/CCNA ICND1 Official Cert Guide.
If you’ve not yet bought either book, you can generally get the pair cheaper by buying both
books as a two-book set, called the CCNA Certification Library.

These two books were designed to be used together when studying for the CCNA exam.
There are basically two good options for the order in which to read the two books. The first
and most obvious option is to read the ICND1 book first, and then read this book. The other
option is to read all of ICND1’s coverage of one topic area, and then read ICND2’s
coverage of the same topics, and then go back to ICND1 again. Figure I-3 outlines my
suggested option for reading the two books.

Figure I-3  Reading Plan When Studying for CCNA Exam
Both reading plan options have some benefits. Moving back and forth between books helps you to focus on one general topic at a time. However, there is some overlap between the two exams, so there is some overlap between the two books. From reader comments about the previous edition of these books, those readers new to networking tended to do better by completing the first book, and then moving on to the second, while readers who had more experience and knowledge before starting the books tended to prefer to follow a reading plan like the one shown in Figure I-3.

Note that, for final preparation, you can use the final chapter (Chapter 24) of the ICND1 book instead of Chapter 20 of this book. Both of these chapters mention the same details.

In addition to the flow shown in Figure I-3, when studying for the CCNA exam (rather than the ICND1 and ICND2 exams), it is important to study and practice IP subnetting before moving on to the IP routing and routing protocol parts of this book. This book does not review subnetting or the underlying math, assuming that you know how to find the answers. Some chapters in this book, particularly Chapter 5, “Variable Length Subnet Masks,” will be much easier to understand if you can do the related subnetting math pretty easily.

For More Information

If you have any comments about the book, submit them via www.ciscopress.com. Just go to the website, select Contact Us, and type your message.

Cisco might make changes that affect the CCNA certification from time to time. You should always check www.cisco.com/go/ccna and www.cisco.com/go/ccent for the latest details.

The CCNA certification is arguably the most important Cisco certification, with the newer CCENT certification slowly gaining in popularity. CCNA certainly is the most popular Cisco certification, is required for several other certifications, and is the first step in distinguishing yourself as someone who has proven knowledge of Cisco.

The CCNA ICND2 Official Cert Guide helps you attain CCNA certification. This is the CCNA ICND2 certification book from the only Cisco-authorized publisher. We at Cisco Press believe that this book certainly can help you achieve CCNA certification, but the real work is up to you! I trust that your time will be well spent.
Cisco Published ICND2 Exam Topics*
Covered in This Part

- Configure, verify, and troubleshoot a switch with VLANs and interswitch communications
- Describe enhanced switching technologies (including: VTP, RSTP, VLAN, PVSTP, 802.1q)
- Describe how VLANs create logically separate networks and the need for routing between them
- Configure, verify, and troubleshoot VLANs
- Configure, verify, and troubleshoot trunking on Cisco switches
- Configure, verify, and troubleshoot VTP
- Configure, verify, and troubleshoot RSTP operation
- Interpret the output of various show and debug commands to verify the operational status of a Cisco switched network
- Implement basic switch security (including: port security, unassigned ports, trunk access, etc.)

* Always recheck Cisco.com for the latest posted exam topics.
This chapter covers the following subjects:

**VLSM Concepts and Configuration:** This section explains the issues and solutions when designing an internetwork that uses VLSM.

**Finding VLSM Overlaps:** This section is the first of three that focus on applying VLSM concepts in a particular way. In this case, it focuses on analyzing a deployed internetwork to find cases in which the subnets’ address ranges overlap, which causes IP routing problems.

**Adding New Subnets to an Existing VLSM Design:** This section examines how to choose new subnets, based on an existing design plus the requirements for the new subnets. This section emphasizes how to avoid mistakenly choosing subnets that overlap.

**Designing a Subnetting Plan Using VLSM:** This section discusses cases in which you start with no design at all, but instead with a set of requirements and an IP network. Your job: choose a number of masks, the number of subnets that use each mask, and the specific subnet IDs to use with each mask.
Most of the IP addresses and subnetting content sits inside the ICND1 part of the CCNA puzzle. This chapter explores the one pure addressing topic in the ICND2 part of the mix: variable length subnet masks (VLSM).

VLSM builds on the subnetting concepts in ICND1. If you have a good handle on those details, great! If you are still a little unsure, it may be a good time to review and practice subnetting. For instance, to do some of the exercises in this chapter, you need to remember how and why you would pick a particular mask, given the need for a subnet to support some number of host IP addresses. You also need to be able to find all the subnet IDs of a single classful network when using a single mask. Using both sets of skills, this chapter expands on those concepts when using multiple masks. Look at this chapter as an opportunity to learn VLSM, as well as to review and strengthen your subnetting skills.

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz allows you to assess whether you should read the entire chapter. If you miss no more than one of these six self-assessment questions, you might want to move ahead to the section, “Exam Preparation Tasks.” Table 5-1 lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so that you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes.”

Table 5-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

<table>
<thead>
<tr>
<th>Foundations Topics Section</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLSM Concepts and Configuration</td>
<td>1, 2</td>
</tr>
<tr>
<td>Finding VLSM Overlaps</td>
<td>3, 4</td>
</tr>
<tr>
<td>Adding a New Subnet to an Existing VLSM Design</td>
<td>5</td>
</tr>
<tr>
<td>Designing a Subnetting Plan Using VLSM</td>
<td>6</td>
</tr>
</tbody>
</table>
1. Which of the following routing protocols support VLSM?
   a. RIP-1
   b. RIP-2
   c. EIGRP
   d. OSPF
2. What does the acronym VLSM stand for?
   a. Variable length subnet mask
   b. Very long subnet mask
   c. Vociferous longitudinal subnet mask
   d. Vector-length subnet mask
   e. Vector loop subnet mask
3. R1 has configured interface Fa0/0 with the `ip address 10.5.48.1 255.255.240.0` command. Which of the following subnets, when configured on another interface on R1, would not be considered an overlapping VLSM subnet?
   a. 10.5.0.0 255.255.240.0
   b. 10.4.0.0 255.254.0.0
   c. 10.5.32.0 255.255.224.0
   d. 10.5.0.0 255.255.128.0
4. R4 has a connected route for 172.16.8.0/22. Which of the following answers lists a subnet that overlaps with this subnet?
   a. 172.16.0.0/21
   b. 172.16.6.0/23
   c. 172.16.16.0/20
   d. 172.16.11.0/25
5. A design already includes subnets 192.168.1.0/26, 192.168.1.128/30, and 192.168.1.160/29. Which of the following subnets is the numerically lowest subnet ID that could be added to the design, if you wanted to add a subnet that uses a /28 mask?

a. 192.168.1.144/28
b. 192.168.1.112/28
c. 192.168.1.64/28
d. 192.168.1.80/28
e. 192.168.1.96/28

6. An engineer is following a VLSM design process of allocating the largest subnets first, as the numerically lowest subnets, and then subdividing the next subnet into smaller pieces for the next smaller size of subnet. In this case, the engineer has reserved the first three /20 subnets of 172.16.0.0 to be used in an internetwork: 172.16.0.0/20, 172.16.16.0/20, and 172.16.32.0/20. The next smaller size subnets to be allocated will be subnets with mask /25; this design requires 10 such subnets. Assuming the engineer continues to allocate subnets in sequence, which answers lists the tenth of these /25 subnets?

a. 172.16.48.0/25
b. 172.16.64.0/25
c. 172.16.52.128/25
d. 172.16.68.128/25
Foundation Topics

VLSM Concepts and Configuration

VLSM occurs when an internetwork uses more than one mask for different subnets of a single Class A, B, or C network. Figure 5-1 shows an example of VLSM used in Class A network 10.0.0.0.

Figure 5-1  VLSM in Network 10.0.0.0: Masks /24 and /30

Figure 5-1 shows a typical choice of using a /30 prefix (mask 255.255.255.252) on point-to-point serial links, with mask /24 (255.255.255.0) on the LAN subnets. All subnets are of Class A network 10.0.0.0, with two masks being used, therefore meeting the definition of VLSM.

Oddly enough, a common mistake occurs when people think that VLSM means “using more than one mask in some internetwork,” rather than “using more than one mask in a single classful network.” For example, if in one internetwork diagram, all subnets of network 10.0.0.0 use a 255.255.240.0 mask, and all subnets of network 11.0.0.0 use a 255.255.255.0 mask, the design uses two different masks. However, Class A network 10.0.0.0 uses only one mask, and Class A network 11.0.0.0 uses only one mask. In that case, the design does not use VLSM.

VLSM provides many benefits for real networks, mainly related to how you allocate and use your IP address space. Because a mask defines the size of the subnet (the number of host addresses in the subnet), VLSM allows engineers to better match the need for addresses with the size of the subnet. For example, for subnets that need fewer addresses, the engineer uses a mask with fewer host bits, so the subnet has fewer host IP addresses. This flexibility reduces the number of wasted IP addresses in each subnet. By wasting fewer addresses, more space remains to allocate more subnets.

VLSM can be helpful for both public and private IP addresses, but the benefits are more dramatic with public networks. With public networks, the address savings help engineers
avoid having to obtain another registered IP network number from regional IP address assignment authorities. With private networks, as defined in RFC 1918, running out of addresses is not as big a negative, because you can always grab another private network from RFC 1918 if you run out.

**Classless and Classful Routing Protocols**

Before you can deploy a VLSM design created on paper, you must first use a routing protocol that supports VLSM. To support VLSM, the routing protocol must advertise the mask along with each subnet. Without mask information, the router receiving the update would be confused.

For instance, if a router learned a route for 10.1.8.0, but with no mask information, what does that mean? Is that subnet 10.1.8.0/24? 10.1.8.0/23? 10.1.8.0/30? The dotted-decimal number 10.1.8.0 happens to be a valid subnet number with a variety of masks, and because multiple masks may be used with VLSM, the router has no good way to make an educated guess. To effectively support VLSM, the routing protocol needs to advertise the correct mask along with each subnet, so the receiving router knows the exact subnet that is being advertised.

By definition, *classless routing protocols* advertise the mask with each advertised route, and *classful routing protocols* do not. The classless routing protocols, as noted in Table 5-2, are the newer, more advanced routing protocols. And not only do these more advanced classless routing protocols support VLSM, they also support manual route summarization, a feature discussed in Chapter 6, “Route Summarization.”

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP-1</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IGRP</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>RIP-2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EIGRP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Beyond VLSM itself, the routing protocols do not have to be configured to support VLSM or to be classless. There is no command to enable or disable the fact that classless routing protocols include the mask with each route. The only configuration choice you must make
is to use a classless routing protocol, which among the IGPs discussed for CCNA, are RIP-2, EIGRP, and OSPF.

**VLSM Configuration and Verification**

Cisco routers do not configure VLSM, enable or disable it, or need any configuration to use it. From a configuration perspective, VLSM is simply a side effect of the `ip address` interface subcommand. Routers collectively configure VLSM by virtue of having IP addresses in the same classful network but with different masks.

For instance, Example 5-1 shows a simple example with two of the interfaces from router Yosemite from Figure 5-1. The example shows the IP address assignments on two interfaces, one with a /24 mask and one with a /30 mask, both with IP addresses in Class A network 10.0.0.0.

**Example 5-1  Configuring Two Interfaces on Yosemite, Resulting in VLSM**

```plaintext
Yosemite(config)#configure terminal
Yosemite(config)#interface Fa0/0
Yosemite(config-if)#ip address 10.2.1.1 255.255.255.0
Yosemite(config-if)#interface S0/1
Yosemite(config-if)#ip address 10.1.4.1 255.255.255.252
```

When a router detects VLSM being used in a network, IOS lists the mask per route in the output of the `show ip route` command, rather than simply listing the mask only in the header line for that network. Example 5-2 lists an example of the routing table on Albuquerque from Figure 5-1; Albuquerque uses two masks inside network 10.0.0.0, as noted in the highlighted line in the example.

**Example 5-2  Albuquerque Routing Table with VLSM**

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

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 11 subnets, 2 masks
    D 10.2.1.0/24 [90/2172416] via 10.1.4.1, 00:00:34, Serial0/0
    D 10.2.2.0/24 [90/2172416] via 10.1.4.1, 00:00:34, Serial0/0
    D 10.2.3.0/24 [90/2172416] via 10.1.4.1, 00:00:34, Serial0/0
```
So ends the discussion of VLSM as an end to itself. This chapter is devoted to VLSM, but it took a mere 3–4 pages to fully describe it. Why the whole VLSM chapter? Well, to work with VLSM, to find problems with it, to add subnets to an existing design, and to design using VLSM from scratch—in other words, to apply VLSM to real networks—takes skill and practice. To do these same tasks on the exam requires skill and practice. The rest of this chapter examines the skills to apply VLSM and provides some practice for these three key areas:

- Finding VLSM overlaps
- Adding new VLSM subnets without overlaps
- Designing subnetting using VLSM

### Finding VLSM Overlaps

Regardless of whether a design uses VLSM or not, the subnets used in any IP internetwork design should not overlap their address ranges. When subnets in different locations overlap their addresses, a router’s routing table entries overlap. As a result, hosts in different locations may be assigned the same IP address. Routers clearly cannot route packets correctly in these cases. In short, a design that uses overlapping subnets is considered to be an incorrect design and should not be used.

**NOTE** Although I’ve not seen the term used in other places, just to have a term to contrast with VLSM, this book refers to the non-use of VLSM—in other words, using a single mask throughout a classful network—as static length subnet masks (SLSM).

These address overlaps are easier to see when using SLSM than when using VLSM. With SLSM, overlapped subnets have identical subnet IDs, so to find overlaps, you just have to look at the subnet IDs. With VLSM, overlapped subnets may not have the same subnet ID. To find these overlaps, you have to look at the entire range of addresses in each subnet, from

---

**Example 5-2  Albuquerque Routing Table with VLSM (Continued)**

|  | 10.2.4.0/24 [90/2172416] via 10.1.4.1, 00:00:34, Serial0/0 |
|  | 10.3.4.0/24 [90/2172416] via 10.1.6.2, 00:00:56, Serial0/1 |
|  | 10.3.5.0/24 [90/2172416] via 10.1.6.2, 00:00:56, Serial0/1 |
|  | 10.3.6.0/24 [90/2172416] via 10.1.6.2, 00:00:56, Serial0/1 |
|  | 10.3.7.0/24 [90/2172416] via 10.1.6.2, 00:00:56, Serial0/1 |
| C | 10.1.1.0/24 is directly connected, FastEthernet0/0 |
| C | 10.1.6.0/30 is directly connected, Serial0/1 |
| C | 10.1.4.0/30 is directly connected, Serial0/0 |
subnet ID to subnet broadcast address, and compare the range to the other subnets in the design.

**An Example of Finding a VLSM Overlap**

For example, imagine that a practice question for the CCNA exam shows Figure 5-2. It uses a single Class B network (172.16.0.0), with VLSM, because it uses three different masks: /23, /24, and /30.

**Figure 5-2  VLSM Design with Possible Overlap**

Now imagine that the exam question shows you the figure, and either directly or indirectly asks whether overlapping subnets exist. This type of question might simply tell you that some hosts cannot ping each other, or it might not even mention that the root cause could be that some of the subnets overlap. To answer such a question, you could follow this simple but possibly laborious process:

**Step 1** Calculate the subnet ID and subnet broadcast address of each subnet, which gives you the range of addresses in that subnet.

**Step 2** List the subnet IDs in numeric order (along with their subnet broadcast addresses).

**Step 3** Scan the list top to bottom, comparing each pair of adjacent entries, to see if their range of addresses overlaps.
For example, Table 5-3 completes the first two steps based on Figure 5-2, listing the subnet IDs and subnet broadcast addresses, in numeric order based on the subnet IDs.

**Table 5-3** *Subnet IDs and Broadcast Addresses, in Numeric Order, from Figure 5-2*

<table>
<thead>
<tr>
<th>Subnet</th>
<th>Subnet Number</th>
<th>Broadcast Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1 LAN</td>
<td>172.16.2.0</td>
<td>172.16.3.255</td>
</tr>
<tr>
<td>R2 LAN</td>
<td>172.16.4.0</td>
<td>172.16.5.255</td>
</tr>
<tr>
<td>R3 LAN</td>
<td>172.16.5.0</td>
<td>172.16.5.255</td>
</tr>
<tr>
<td>R1-R2 serial</td>
<td>172.16.9.0</td>
<td>172.16.9.3</td>
</tr>
<tr>
<td>R1-R3 serial</td>
<td>172.16.9.4</td>
<td>172.16.9.7</td>
</tr>
</tbody>
</table>

Step 3 states the somewhat obvious step of comparing the address ranges to see whether any overlaps occur. You could just scan the list overall, but if you order the list, you can also methodically scan the list looking at each adjacent pair.

First, look closely just at the subnet number column in Table 5-3. Note that, in this case, none of the subnet numbers are identical, but two entries (highlighted) do overlap.

Next, look closely at the R2 LAN and R3 LAN subnets. All the addresses in the 172.16.5.0/24 subnet are also part of the 172.16.4.0/23 subnet. In this case, the design is invalid because of the overlap, and one of these two subnets would need to be changed.

As far as the three-step process works, note that if two adjacent entries in the list overlap, compare three entries at the next step. The two subnets already marked as overlapped may overlap with the next subnet in the list. For example, imagine a case where you had the following three subnets in a list that you were examining for VLSM overlaps:

- 10.1.0.0/16 (subnet ID 10.1.0.0, broadcast 10.1.255.255)
- 10.1.200.0/24 (subnet ID 10.1.200.0, broadcast 10.1.200.255)
- 10.1.250.0/24 (subnet ID 10.1.250.0, broadcast 10.1.250.255)

If you compare entries 1 and 2, clearly, an overlap occurs, because all the addresses in subnet 10.1.200.0/24 sit inside subnet 10.1.0.0/16. If you then compare only entries 2 and 3, those entries do not overlap. However, entries 1 and 3 do overlap. So what does this mean for the process? Any time you find an overlap, compare all of those overlapped subnets with the next line in the list of subnets until you find one that doesn’t overlap.
Practice Finding VLSM Overlaps

As typical of anything to with applying IP addressing and subnetting, practice helps. To that end, Table 5-4 lists three practice problems. Just start with the five IP addresses listed in a single column, and then follow the three-step process outlined in the previous section to find any VLSM overlaps. The answers can be found near the end of this chapter, in the section, “Answers to Earlier Practice Problems.”

Table 5-4  VLSM Overlap Practice Problems

<table>
<thead>
<tr>
<th>Problem 1</th>
<th>Problem 2</th>
<th>Problem 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.34.9/22</td>
<td>172.16.126.151/22</td>
<td>192.168.1.253/30</td>
</tr>
<tr>
<td>10.1.29.101/23</td>
<td>172.16.122.57/27</td>
<td>192.168.1.113/28</td>
</tr>
<tr>
<td>10.1.23.254/22</td>
<td>172.16.122.33/30</td>
<td>192.168.1.245/29</td>
</tr>
<tr>
<td>10.1.17.1/21</td>
<td>172.16.122.1/30</td>
<td>192.168.1.125/30</td>
</tr>
<tr>
<td>10.1.1.1/20</td>
<td>172.16.128.151/20</td>
<td>192.168.1.122/30</td>
</tr>
</tbody>
</table>

Adding a New Subnet to an Existing VLSM Design

The task described in this section happens frequently in real networks: choosing new subnets to add to an existing design. In real life, you may use tools that help you choose a new subnet so that you do not cause an overlap. However, for both real life and for the CCNA exam, you need to be ready to do the mental process and math of choosing a subnet that both has the right number of host IP addresses and does not create an overlapped VLSM subnet condition. In other words, you need to pick a new subnet and not make a mistake!

For example, consider the internetwork in Figure 5-2, with classful network 172.16.0.0. An exam question might suggest that a new subnet, with a /23 prefix length, needs to be added to the design. The question might also say, “Pick the numerically lowest subnet number that can be used for the new subnet.” In other words, if both 172.16.4.0 and 172.16.6.0 would work, use 172.16.4.0.

So, you really have a couple of tasks: to find all the subnet IDs that could be used, rule out the ones that would cause an overlap, and then check to see if the question guides you to pick either the numerically lowest (or highest) subnet ID. This list outlines the specific steps:
Step 1  Pick the subnet mask (prefix length) for the new subnet, based on the design requirements (if not already listed as part of the question).

Step 2  Calculate all possible subnet numbers of the classful network using the mask from Step 1, along with the subnet broadcast addresses.

Step 3  Make a list of existing subnet IDs and matching subnet broadcast addresses.

Step 4  Rule out overlapping new subnets by comparing the lists from the previous two steps.

Step 5  Choose the new subnet ID from the remaining subnets identified at Step 4, paying attention to whether the question asks for the numerically lowest or numerically highest subnet ID.

An Example of Adding a New VLSM Subnet
For example, Figure 5-3 shows an existing internetwork that uses VLSM. In this case, you need to add a new subnet to support 300 hosts. Imagine that the question tells you to use the smallest subnet (least number of hosts) to meet that requirement. You use some math and logic you learned earlier in your study to choose mask /23, which gives you 9 host bits, for $2^9 - 2 = 510$ hosts in the subnet.

NOTE  If the logic and process in the previous paragraph was unfamiliar, it may be useful to take some time to review the ICND1 book’s Chapter 15, “Analyzing Existing Masks,” and Chapter 16, “Designing Subnet Masks.” These chapters are also on the DVD in the back of this book. Likewise, if finding the subnet ID and subnet broadcast address is unfamiliar, review ICND1 Chapter 17, “Analyzing Existing Subnets,” and Chapter 18, “Finding All Subnet IDs.”

Figure 5-3  Internetwork to Which You Need to Add a /23 Subnet, Network 172.16.0.0

At this point, just follow the steps listed before Figure 5-3. For Step 1, you have already been given the mask (/23). For Step 2, you need to list all the subnet numbers and broadcast
addresses of 172.16.0.0 assuming the /23 mask. You will not use all these subnets, but you need the list for comparison to the existing subnets. Table 5-5 shows the results, at least for the first five possible /23 subnets.

**Table 5-5  First Five Possible /23 Subnets**

<table>
<thead>
<tr>
<th>Subnet</th>
<th>Subnet Number</th>
<th>Subnet Broadcast Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>First (zero)</td>
<td>172.16.0.0</td>
<td>172.16.1.255</td>
</tr>
<tr>
<td>Second</td>
<td>172.16.2.0</td>
<td>172.16.3.255</td>
</tr>
<tr>
<td>Third</td>
<td>172.16.4.0</td>
<td>172.16.5.255</td>
</tr>
<tr>
<td>Fourth</td>
<td>172.16.6.0</td>
<td>172.16.7.255</td>
</tr>
<tr>
<td>Fifth</td>
<td>172.16.8.0</td>
<td>172.16.9.255</td>
</tr>
</tbody>
</table>

Next, at Step 3, list the existing subnet numbers and broadcast addresses, as seen earlier in Figure 5-3. To do so, do the usual math to take an IP address/mask to then find the subnet ID and subnet broadcast address. Table 5-6 summarizes that information, including the locations, subnet numbers, and subnet broadcast addresses.

**Table 5-6  Existing Subnet IDs and Broadcast Addresses from Figure 5-3**

<table>
<thead>
<tr>
<th>Subnet</th>
<th>Subnet Number</th>
<th>Subnet Broadcast Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1 LAN</td>
<td>172.16.2.0</td>
<td>172.16.3.255</td>
</tr>
<tr>
<td>R2 LAN</td>
<td>172.16.4.0</td>
<td>172.16.5.255</td>
</tr>
<tr>
<td>R3 LAN</td>
<td>172.16.6.0</td>
<td>172.16.6.255</td>
</tr>
<tr>
<td>R1-R2 serial</td>
<td>172.16.9.0</td>
<td>172.16.9.3</td>
</tr>
<tr>
<td>R1-R3 serial</td>
<td>172.16.9.4</td>
<td>172.16.9.7</td>
</tr>
</tbody>
</table>

At this point, you have all the information you need to look for the overlap at Step 4. Simply compare the range of numbers for the subnets in the previous two tables. Which of the possible new /23 subnets (Table 5-5) overlap with the existing subnets (Table 5-6)? In this case, the second, third, and fifth subnets in Table 5-5 overlap, so rule those out as candidates to be used. (Table 5-5 denotes those subnets with gray highlights.)

Step 5 has more to do with the exam than with real network design, but it is still worth listing as a separate step. Multiple-choice questions sometimes need to force you into a single answer, and asking for the numerically lowest or highest subnet does that. This
particular example asks for the numerically lowest subnet number, which in this case is 172.16.0.0/23.

**NOTE** The answer, 172.16.0.0/23, happens to be a zero subnet. For the exam, the zero subnet should be avoided if (a) the question implies the use of classful routing protocols, or (b) the routers are configured with the `no ip subnet-zero` global configuration command. Otherwise, assume that the zero subnet can be used.

**Practice Adding New VLSM Subnets**

Your boss wants you to add a subnet to an existing design. The existing design already has these five subnets:

- 10.0.0.0/24
- 10.0.1.0/25
- 10.0.2.0/26
- 10.0.3.0/27
- 10.0.6.0/28

The boss cannot decide among five competing subnet masks. However, the boss wants you to practice VLSM and plan the subnet ID he would use for each of those five possible masks. He tells you that the new subnet ID must be part of class A network 10.0.0.0, that the new subnet must not overlap with the original five subnets, and that the new subnet ID must be the numerically lowest possible subnet ID (without breaking the other rules). Pick the one subnet ID you would plan to use based on each of the following mask choices by the boss:

1. /24
2. /23
3. /22
4. /25
5. /26

You can find the answers in the section, “Answers to Practice Problems.”

**Designing a Subnetting Plan Using VLSM**

*CCENT/CCNA ICND1 Official Cert Guide* explains several important subnetting design concepts and tasks, but they all assume a single subnet mask is used in each classful network. To perform the similar but more involved design work when using VLSM, you need to apply those same skills in new ways.

For instance, you should understand by now how to design or choose a subnet mask so that a subnet supports a stated number of host IP addresses. You should also know how to list
all the subnets of a classful network, assuming one specific mask is used throughout that classful network.

This section discusses how to apply those same concepts when you allow the use of multiple masks.

For example, when assuming SLSM in the ICND1 book, a problem might use Class B network 172.16.0.0, and the design might call for ten subnets, with the largest subnet containing 200 hosts. Mask 255.255.255.0 meets the requirements for that largest subnet, with 8 subnet bits and 8 host bits, supporting 256 subnets and 254 hosts per subnet. (Other masks also meet that requirement.) If using that one mask throughout the network, the subnet numbers would be 172.16.0.0, 172.16.1.0, 172.16.2.0, and so on, counting by one in the third octet.

To create a subnet plan with VLSM, you have to rethink the choice of subnet masks and the choice of allowed subnets. Additionally, you always have to avoid choosing subnets that overlap. This section walks through the VLSM subnet design process, beginning with mask design, and moving on to choosing subnets to use for a particular topology.

**Choosing VLSM Masks**

With SLSM design, you typically choose the one mask based on the needs of the largest subnet—in other words, the subnet that requires the largest number of host IP addresses. With VLSM design, you can instead choose to use many different masks. You could literally use every mask from /8 through /30 inside a single classful network.

Although using a dozen masks might let you save lots of addresses, it would also create extra complexity. So, the VLSM design choice for how many masks to use, and which ones, requires some compromise and tradeoffs between saving addresses while keeping things simple. Many companies settle on somewhere between two and four different masks as a compromise.

To choose the masks in real life, you need to look at the requirements for each subnet in the design. How many host IP addresses do you need in each case? How much growth do you expect? How many subnets do you need of each size?
In the more theoretical world of exam preparation, you can typically expect a cleaner view of the world, which makes the discussion in this book more objective. For instance, consider Figure 5-4, which lists requirements for two ultra-large data center subnets on the left, several branch office LAN subnets on the right, and a number of typical serial links.

Figure 5-4  Requirements that Feed into a VLSM Design

Figure 5-4 shows requirements for the number of host IP addresses; all you have to do then is pick a mask to meet the requirements for each size subnet as a separate problem, and note the number of subnets you need to create for each size. For the exam, the question might give some guidance that leads you to a single answer, like asking you to choose a mask that meets the goal and uses the least host bits. With Figure 5-4, using the least host bits, you would choose these three masks:

- /18: 14 host bits, $2^{14} - 2 = 16,382$ hosts/subnet
- /24: 8 host bits, $2^8 - 2 = 254$ hosts/subnet
- /30: 2 host bits, $2^2 - 2 = 2$ hosts/subnet

In summary, to choose the masks to use in VLSM, analyze the requirements. Find subnets with requirements for similar numbers of hosts, like the three sizes of subnets in Figure 5-4. Then, choose a small number of masks to use for those different sizes of subnets, as summarized in the list for this particular example.

Assigning the Largest Subnet IDs First

VLSM subnet assignment first occurs on paper, when the network engineer looks at a list of subnet IDs and chooses which subnet ID to use for which need in the network topology. For example, Figure 5-4 shows the need for two subnets with a /18 mask, three subnets with a /24 mask, and three subnets with a /30 mask. What specific subnets did the engineer
choose? Which subnets could the engineer have chosen? This section explores how to answer these questions and how to go about choosing subnets.

When assigning subnets, follow this strategy: Choose the largest subnets first.

To show you why, we continue the example based in part on Figure 5-4. In that company, the LAN team will assign the subnets for the /18 and /24 subnets, and the WAN team will assign all the /30 subnets. The WAN team has already deployed some WAN links, and they have the political power and are unwilling to change. The WAN team has already used subnets 172.16.50.0/30, 172.16.100.0/30, 172.16.150.0/30, and 172.16.200.0/30.

Although the four WAN subnets have consumed a mere 16 addresses, unfortunately, those subnets have already busted the VLSM design. The four small subnet assignments have created an overlap with all four possible /18 subnets of network 172.16.0.0. Figure 5-5 shows the idea, with the four possible /18 subnets at the top and the overlapping WAN subnets at the bottom.

When using mask /18, with Class B network 172.16.0.0, only four possible subnets exist: 172.16.0.0, 172.16.64.0, 172.16.128.0, and 172.16.192.0. The four small /30 WAN subnets each overlap with one of these four, as shown in Figure 5-5. How can you avoid making such mistakes? Either assign the smaller subnets from a much tighter range or assign the larger subnet IDs first, as suggested in this chapter. In this case, the LAN team could have allocated the first two /18 subnets first, and made the WAN team avoid using IP addresses from the first half of class B network 172.16.0.0.

Admittedly, the WAN team could not have been any more shortsighted in this contrived example. Regardless, it shows how a small subnet assignment can prevent you from having a larger subnet available. You should always strive to keep large holes open in your address space in anticipation of assigning large subnets in the future.
An Example of VLSM Subnet Design

Other than a general strategy to assign the larger subnets first, what specific steps should you take? Rather than start with a formal process, this section shows an example. In short, the process finds and allocates the largest subnets. Then it takes one of those unused subnets and further subdivides it—sub-subnets it if you prefer—to make the next smaller size of subnets.

NOTE To use this process, you really need to be comfortable with the idea of looking at a classful network number, one subnet mask, and finding all subnet IDs. As previously mentioned, to review the process to find all subnet IDs using a single mask, refer to *CCENT/CCNA ICND1 Official Cert Guide*, Chapter 18, which is found on this book’s DVD.

This example uses the following requirements; they are the same requirements shown earlier in Figure 5-4.

2 subnets with mask /18
3 subnets with /24
3 subnets with /30

To begin, calculate all possible subnets of network 172.16.0.0 using a /18 mask (the largest subnets). Then, pick two subnets, because the requirements say that you need two. Figure 5-6 shows a representation of these four subnets and the fact that two are allocated for use.

![Figure 5-6 Four /18 Subnets Listed, with Two Allocated for Use](image)

The allocation of the first two of these large subnets removes a large set of IP addresses from the pool. When choosing subnets for the next smaller size subnet, you have to avoid the range of addresses in these subnets. In this case, these two subnets consume half the Class B network: addresses 172.16.0.0 – 172.16.127.255. The numerically lowest subnet ID that could possibly be used for the next to-be-allocated subnet, and not overlap, is 172.16.128.0.

For the next step, you take one of the currently free subnets from the list of large subnets and further subdivide it (or “sub-subnet it”) to create the smaller sized subnet. For instance, in this case, the next large subnet ID in sequence is 172.16.128.0/18. You take this range of addresses, and you find all subnets in this range using the next smaller subnet size, which
in this example are the subnets that use the /24 mask. You can find all subnets of Class B network 172.16.0.0 using the /24 mask, but you really only have to start at 172.16.128.0. Figure 5-7 shows the idea of what subnets exist in this range, using /24 masks.

**Figure 5-7** Subdividing 172.16.128.0/18 into 64 Subnets Using /24 Mask

Figure 5-7 shows a representation of the fact that the subnets 172.16.128.0/24, 172.16.129.0/24, 172.16.130.0/24, and so on, through 172.16.191.0/24, all fit inside the range of addresses of the subdivided larger 172.16.128.0/18 subnet. Although the figure does not show all 64 of these /24 subnets because of space constraints, it shows enough to see the pattern.

To summarize what actions we took so far in choosing and assigning subnets on paper in this example, we

- Calculated the four possible subnets of Class B network 172.16.0.0 using mask /18
- Allocated the first two subnets for use in the internetwork
- Marked the third of four /18 subnets (172.16.128.0/18) to be sub-subnetted into smaller subnets
- Listed all subnets using mask /24 that could exist inside 172.16.128.0/18

To continue the exercise, the requirements asked for three /24 subnets, so you need to pick three subnets from the list in Figure 5-7. Using the first three makes sense: 172.16.128.0/24, 172.16.129.0/24, and 172.16.130.0/24.

The process continues until you go through every different mask. In this example, only one other mask was chosen (/30). To proceed, pick one of the currently free /24 subnets, mark it as one to be sub-subnetted, and proceed to subnet it into /30 subnets. Figure 5-8 updates
the idea, showing the three allocated /24 subnets, and the next /24 subnet in sequence
(172.16.131.0/24) marked as the one to subnet further to create the /30 subnets.

**Figure 5-8  The Three Allocated /24 Subnets and the Next Subnet to Divide Further**

The process continues with the same logic as before, subnetting the address range implied
by 172.16.131.0/24 using a /30 mask. That is, finding these possible /30 subnets within this
range:

- 172.16.131.0/30
- 172.16.131.4/30
- 172.16.131.8/30
- 172.16.131.12/30
- And so on, up through 172.16.131.252/30

If you again pick the first three subnets (you pick three because the requirements stated that
you needed three subnets with a /30 mask), you would mark the first three in this list as
allocated or used. At this point, the process is complete, other than picking exactly where
to use each subnet.

**Summary of the Formal VLSM Subnet Design Process**
The process seems long because it takes time to work through each step. However, you
essentially repeat the same process you would use to find and allocate subnets when using
a single mask, just repeating the process for each successively longer mask (in other words,
from the largest subnets to smallest subnets). For completeness, the following list summarizes the steps:

**Step 1** Analyze the requirements for the number of hosts and subnets, choose the masks to use, and list the number of subnets needed using each mask.

**Step 2** For the shortest prefix mask (largest subnets):

a. Calculate, on paper, all possible subnets, using that one mask.

b. Mark some subnets as allocated for use, per the requirements from step 1.

c. Pick an unallocated subnet to be further subdivided by the next step (step 3).

**Step 3** Repeat Step 2 for each mask, moving to the next longer mask (next smaller sized subnet) each time.

**Practice Designing VLSM Subnets**

The biggest hurdle in designing with VLSM subnets is to get through the process of finding all the subnets using each mask, particularly after the first step, when you really only care about a more limited range of subnet numbers. The following practice problems help with that process.

Table 5-7 lists the problems. To answer these problems, choose subnet IDs, lowest to highest, first allocating subnets for the largest subnets, then for the next largest subnets, and so on. Always choose the numerically lowest subnet IDs if you want your answer to match what is listed at the end of this chapter.

**Table 5-7 VLSM Subnet Design Practice Problems**

<table>
<thead>
<tr>
<th>Problem</th>
<th>Classful Network</th>
<th>First Requirement</th>
<th>Second Requirement</th>
<th>Third Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>172.20.0.0</td>
<td>3 subnets, /22</td>
<td>3 subnets, /25</td>
<td>3 subnets, /30</td>
</tr>
<tr>
<td>2</td>
<td>192.168.1.0</td>
<td>3 subnets, /27</td>
<td>3 subnets, /28</td>
<td>3 subnets, /30</td>
</tr>
</tbody>
</table>
Exam Preparation Tasks

Review All the Key Topics

Review the most important topics from this chapter, noted with the Key Topics icon in the outer margin of the page. Table 5-8 lists a reference of these key topics and the page numbers on which each is found.

Table 5-8  Key Topics for Chapter 5

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 5-2</td>
<td>Classless and classful routing protocols listed and compared</td>
<td>203</td>
</tr>
<tr>
<td>List</td>
<td>Steps to analyze an existing design to discover any VLSM overlaps</td>
<td>206</td>
</tr>
<tr>
<td>List</td>
<td>Steps to follow when adding a new subnet to an existing VLSM design</td>
<td>209</td>
</tr>
<tr>
<td>Paragraph</td>
<td>Statement of the main VLSM subnet assignment strategy or assigning the largest subnets first</td>
<td>214</td>
</tr>
<tr>
<td>List</td>
<td>Steps to follow to design a subnet plan using VLSM</td>
<td>218</td>
</tr>
</tbody>
</table>

Complete the Tables and Lists from Memory

Print a copy of Appendix J, “Memory Tables,” (found on the DVD) or at least the section for this chapter, and complete the tables and lists from memory. Appendix K, “Memory Tables Answer Key,” also on the DVD, includes completed tables and lists to check your work.

Definitions of Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

- classful routing protocol
- classless routing protocol
- overlapping subnets
- variable length subnet masks (VLSM)
Read Appendix G Scenarios
Appendix G, “Additional Scenarios,” contains five detailed scenarios that both give you a chance to analyze different designs, problems, and command output and show you how concepts from several different chapters interrelate. Appendix G Scenario 1, Part A, and all of Scenario 5 provide an opportunity to practice and develop skills with VLSM.

Appendix D Practice Problems
Appendix D, “Practice for Chapter 5: Variable Length Subnet Masks,” lists additional practice problems and answers. You can find this appendix on the DVD as a printable PDF.

Answers to Earlier Practice Problems

Answers to Practice Finding VLSM Overlaps
This section lists the answers to the three practice problems in the section, “Practice Finding VLSM Overlaps,” as listed earlier in Table 5-4. Note that the tables that list details of the answer reordered the subnets as part of the process.

In Problem 1, the second and third subnet IDs listed in Table 5-9 happen to overlap. The second subnet’s range completely includes the range of addresses in the third subnet.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Original Address and Mask</th>
<th>Subnet ID</th>
<th>Broadcast Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.1.1.1/20</td>
<td>10.1.0.0</td>
<td>10.1.15.255</td>
</tr>
<tr>
<td>2</td>
<td>10.1.17.1/21</td>
<td>10.1.16.0</td>
<td>10.1.23.255</td>
</tr>
<tr>
<td>3</td>
<td>10.1.23.254/22</td>
<td>10.1.20.0</td>
<td>10.1.23.255</td>
</tr>
<tr>
<td>4</td>
<td>10.1.29.101/23</td>
<td>10.1.28.0</td>
<td>10.1.29.255</td>
</tr>
<tr>
<td>5</td>
<td>10.1.34.9/22</td>
<td>10.1.32.0</td>
<td>10.1.35.255</td>
</tr>
</tbody>
</table>

In Problem 2, again, the second and third subnet IDs (listed in Table 5-10) happen to overlap, and again, the second subnet’s range completely includes the range of addresses in
the third subnet. Also, the second and third subnet IDs are the same value, so the overlap is more obvious.

**Table 5-10  VLSM Overlap Problem 2 Answers (Overlaps Highlighted)**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Original Address and Mask</th>
<th>Subnet ID</th>
<th>Broadcast Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>172.16.122.1/30</td>
<td>172.16.122.0</td>
<td>172.16.122.3</td>
</tr>
<tr>
<td>2</td>
<td>172.16.122.57/27</td>
<td>172.16.122.32</td>
<td>172.16.122.63</td>
</tr>
<tr>
<td>3</td>
<td>172.16.122.33/30</td>
<td>172.16.122.32</td>
<td>172.16.122.35</td>
</tr>
<tr>
<td>4</td>
<td>172.16.126.151/22</td>
<td>172.16.124.0</td>
<td>172.16.127.255</td>
</tr>
<tr>
<td>5</td>
<td>172.16.128.151/20</td>
<td>172.16.128.0</td>
<td>172.16.143.255</td>
</tr>
</tbody>
</table>

In Problem 3, three subnets overlap. Subnet 1’s range completely includes the range of addresses in the second and third subnets. Note that the second and third subnets do not overlap with each other, so for the process in this book to find all the overlaps, after you find that the first two subnets overlap, you should compare the next entry in the table (3) with both of the two known–to-overlap entries (1 and 2).

**Table 5-11  VLSM Overlap Problem 3 Answers (Overlaps Highlighted)**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Original Address and Mask</th>
<th>Subnet ID</th>
<th>Broadcast Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.1.113/28</td>
<td>192.168.1.112</td>
<td>192.168.1.127</td>
</tr>
<tr>
<td>2</td>
<td>192.168.1.122/30</td>
<td>192.168.1.120</td>
<td>192.168.1.123</td>
</tr>
<tr>
<td>3</td>
<td>192.168.1.125/30</td>
<td>192.168.1.124</td>
<td>192.168.1.127</td>
</tr>
<tr>
<td>4</td>
<td>192.168.1.245/29</td>
<td>192.168.1.240</td>
<td>192.168.1.247</td>
</tr>
<tr>
<td>5</td>
<td>192.168.1.253/30</td>
<td>192.168.1.252</td>
<td>192.168.1.255</td>
</tr>
</tbody>
</table>

**Answers to Practice Adding VLSM Subnets**

This section lists the answers to the five practice problems in the section, “Practice Adding VLSM Subnets.”
All five problems for this section used the same set of five pre-existing subnets. Table 5-12 lists those subnet IDs and subnet broadcast addresses, which define the lower and higher ends of the range of numbers in each subnet.

**Table 5-12  Pre-Existing Subnets for the Add a VLSM Subnet Problems in This Chapter**

<table>
<thead>
<tr>
<th>Subnet</th>
<th>Subnet Number</th>
<th>Broadcast Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.0.0.0/24</td>
<td>10.0.0.255</td>
</tr>
<tr>
<td>2</td>
<td>10.0.1.0/25</td>
<td>10.0.1.127</td>
</tr>
<tr>
<td>3</td>
<td>10.0.2.0/26</td>
<td>10.0.2.63</td>
</tr>
<tr>
<td>4</td>
<td>10.0.3.0/27</td>
<td>10.0.3.31</td>
</tr>
<tr>
<td>5</td>
<td>10.0.6.0/28</td>
<td>10.0.6.15</td>
</tr>
</tbody>
</table>

The rest of the explanations follow the five-step process outlined earlier in the section, “Adding New Subnets to an Existing VLSM Design,” except that the explanations ignore Step 3 because Step 3’s results in each case are already listed in Table 5-12.

**Problem 1**

**Step 1** The problem statement tells us to use /24.

**Step 2** The subnets would be 10.0.0.0, 10.0.1.0, 10.0.2.0, 10.0.3.0, 10.0.4.0, 10.0.5.0, and so on, counting by 1 in the third octet.

**Step 4** The first four new possible subnets (10.0.0.0/24, 10.0.1.0/24, 10.0.2.0/24, and 10.0.3.0/24) all overlap with the existing subnets (see Table 5-12). 10.0.6.0/24 also overlaps.

**Step 5** 10.0.4.0/24 is the numerically lowest new subnet number that does not overlap with the existing subnets.

**Problem 2**

**Step 1** The problem statement tells us to use /23.

**Step 2** The subnets would be 10.0.0.0, 10.0.2.0, 10.0.4.0, 10.0.6.0, 10.0.8.0, and so on, counting by 2 in the third octet.

**Step 4** Three of the first four new possible subnets (10.0.0.0/23, 10.0.2.0/23, and 10.0.6.0/23) all overlap with existing subnets.

**Step 5** 10.0.4.0/23 is the numerically lowest new subnet number that does not overlap with the existing subnets.

**Problem 3**

**Step 1** The problem statement tells us to use /22.
Step 2  The subnets would be 10.0.0.0, 10.0.4.0, 10.0.8.0, 10.0.12.0, and so on, counting by 4 in the third octet.

Step 4  The first two new possible subnets (10.0.0.0/22, 10.0.4.0/22) overlap with existing subnets.

Step 5  10.0.8.0/22 is the numerically lowest new subnet number that does not overlap with the existing subnets.

Problem 4

The answer for this problem requires more detail than others, because the /25 mask creates a larger number of subnets that might overlap with the pre-existing subnets. For this problem, at Step 1, you already know to use mask /25. Table 5-13 shows the results of Step 2, listing the first 14 subnets of network 10.0.0.0 when using mask /25. For Step 4, Table 5-13 highlights the overlapped subnets. To complete the task at Step 5, search the table sequentially and find the first non-grayed subnet, 10.0.1.128/25.

Table 5-13  First 14 Subnets of Network 10.0.0.0, Using /25 Mask

<table>
<thead>
<tr>
<th>Reference</th>
<th>Subnet Number</th>
<th>Broadcast Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.0.0.0</td>
<td>10.0.0.127</td>
</tr>
<tr>
<td>2</td>
<td>10.0.0.128</td>
<td>10.0.0.255</td>
</tr>
<tr>
<td>3</td>
<td>10.0.1.0</td>
<td>10.0.1.127</td>
</tr>
<tr>
<td>4</td>
<td>10.0.1.128</td>
<td>10.0.1.255</td>
</tr>
<tr>
<td>5</td>
<td>10.0.2.0</td>
<td>10.0.2.127</td>
</tr>
<tr>
<td>6</td>
<td>10.0.2.128</td>
<td>10.0.2.255</td>
</tr>
<tr>
<td>7</td>
<td>10.0.3.0</td>
<td>10.0.3.127</td>
</tr>
<tr>
<td>8</td>
<td>10.0.3.128</td>
<td>10.0.3.255</td>
</tr>
<tr>
<td>9</td>
<td>10.0.4.0</td>
<td>10.0.4.127</td>
</tr>
<tr>
<td>10</td>
<td>10.0.4.128</td>
<td>10.0.4.255</td>
</tr>
<tr>
<td>11</td>
<td>10.0.5.0</td>
<td>10.0.5.127</td>
</tr>
<tr>
<td>12</td>
<td>10.0.5.128</td>
<td>10.0.5.255</td>
</tr>
<tr>
<td>13</td>
<td>10.0.6.0</td>
<td>10.0.6.127</td>
</tr>
<tr>
<td>14</td>
<td>10.0.6.128</td>
<td>10.0.6.255</td>
</tr>
</tbody>
</table>
Problem 5
Like Problem 4, the answer for Problem 5 requires more detail, because the /26 mask creates a larger number of subnets that might overlap with the pre-existing subnets. For this problem, at Step 1, you already know to use mask /26. Table 5-14 shows the results of Step 2, listing the first 12 subnets of network 10.0.0.0 when using mask /26. For Step 4, Table 5-14 highlights the overlapped subnets. To complete the task at Step 5, search the table sequentially and find the first non-grayed subnet, 10.0.1.128/26.

Table 5-14 First 12 Subnets of Network 10.0.0.0, Using /26 Mask

<table>
<thead>
<tr>
<th>Reference</th>
<th>Subnet Number</th>
<th>Broadcast Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.0.0.0</td>
<td>10.0.0.63</td>
</tr>
<tr>
<td>2</td>
<td>10.0.0.64</td>
<td>10.0.0.127</td>
</tr>
<tr>
<td>3</td>
<td>10.0.0.128</td>
<td>10.0.0.191</td>
</tr>
<tr>
<td>4</td>
<td>10.0.0.192</td>
<td>10.0.0.255</td>
</tr>
<tr>
<td>5</td>
<td>10.0.1.0</td>
<td>10.0.1.63</td>
</tr>
<tr>
<td>6</td>
<td>10.0.1.64</td>
<td>10.0.1.127</td>
</tr>
<tr>
<td>7</td>
<td>10.0.1.128</td>
<td>10.0.1.191</td>
</tr>
<tr>
<td>8</td>
<td>10.0.1.192</td>
<td>10.0.1.255</td>
</tr>
<tr>
<td>9</td>
<td>10.0.2.0</td>
<td>10.0.2.63</td>
</tr>
<tr>
<td>10</td>
<td>10.0.2.64</td>
<td>10.0.2.127</td>
</tr>
<tr>
<td>11</td>
<td>10.0.2.128</td>
<td>10.0.2.191</td>
</tr>
<tr>
<td>12</td>
<td>10.0.2.192</td>
<td>10.0.2.255</td>
</tr>
</tbody>
</table>

Answers to Practice Designing VLSM Subnets
This section lists the answers to the two practice problems in the section, “Practice Designing VLSM Subnets.”

Answers for VLSM Subnet Design, Problem 1
For Problem 1, subnetting network 172.20.0.0 with mask /22 means that the subnets will all be multiples of 4 in the third octet: 172.20.0.0, 172.20.4.0, 172.20.8.0, and so on, through 172.20.252.0. Following the rule to choose the numerically lowest subnet IDs, you would allocate or use 172.20.0.0/22, 172.20.4.0/22, and 172.20.8.0/22. You would also then mark the next subnet, 172.20.12.0/22, to be sub-subnetted.
For the next mask, /25, all the subnet IDs will be either 0 or 128 in the last octet, and increments of 1 in the third octet. Starting at 172.20.12.0 per the previous paragraph, the first four such subnets are 172.20.12.0/25, 172.20.12.128/25, 172.20.13.0/25, and 172.20.13.128/25. Of these, you need to use three, so mark the first three as used. The fourth will be sub-subnetted at the next step.

For the third and final mask, /30, all the subnet IDs will increment by 4 in the fourth octet. Starting with the subnet ID that will be sub-subnetted (172.20.13.128), the next /30 subnet IDs are 172.20.13.128, 172.20.13.132, 172.20.13.136, 172.20.13.140, and so on. The first three in this list will be the three used per the requirements and rules for Problem 1.

Answers for VLSM Subnet Design, Problem 2

For Problem 2, subnetting network 192.168.1.0 with mask /27 means that the subnets will all be multiples of 32 in the fourth octet: 192.168.1.0, 192.168.1.32, 192.168.1.64, 192.168.1.96, and so on, through 192.168.1.224. Following the rule to choose the numerically lowest subnet IDs, you would allocate or use 192.168.1.0/27, 192.168.1.32/27, and 192.168.1.64/27. You would also then mark the next subnet, 192.168.1.96/27, to be sub-subnetted.

For the next mask, /28, all the subnet IDs will be multiples of 16 in the last octet. Starting at 192.168.1.96 per the previous paragraph, the first four such subnets are 192.168.1.96, 192.168.1.112, 192.168.1.128, and 192.168.1.144. Of these, you need to use three, so mark the first three as used. The fourth will be sub-subnetted at the next step.

For the third and final mask, /30, all the subnet IDs will increment by 4 in the fourth octet. Starting with the subnet ID that will be sub-subnetted (192.168.1.144), the next /30 subnet IDs are 192.168.1.144, 192.168.1.148, 192.168.1.152, 192.168.1.156, and so on. The first three in this list will be the three used per the requirements and rules for Problem 2.
Index

A
access
   interfaces, 28
   links
      AR, 499
      Frame Relay, 499, 549-550
      VPN, 570
access-class command, 295
access-list commands, 260-264
   building, 268-269, 288-291
   extended IP ACLs, 284
access-list remark parameters, 268
ACLs (Access Control Lists), 251, 268-269
   advanced IP, 275
      extended numbered, 278-288
      implementing, 294-300
      named, 288-294
   creating, 296
   dynamic, 299-300
   editing, 288-294
   IP
      extended, 283-287
      troubleshooting, 334-336
   overview of, 254-257
   reflexive, 297-298
   reverse engineering, 269-270
   SSH, 295-297
   standard numbered IPv4, 257-267
   telnet, 295-297
   time-based, 300
adding subnets to VLSMs, 208-211
Additional ACL Numbers, 256
   static mapping, 536
addresses
   IP, 260
   mapping
      Frame Relay, 532-534
      Inverse ARP, 535
   matching, 263
   ranges, reverse engineering ACLs, 269-270
   subsets, matching, 260-262
   VLSMs, 199
      adding subnets, 208-211
      configuring, 202-205
      overlaps, 205-208
      planning subnets, 211-218
administrative distance, 352-353
Administrative mode (VLAN), 29, 33
advanced IP ACLs, 275
   extended numbered, 278-288
   implementing, 294-300
   named, 288-294
advertisement request messages (VTP), 19
AH security protocol, IPsec VPN, 576
any keyword, 263
AR (Access Rates), 499
area authentication command, 408
areas (OSPF), 394-396
   multiple area configurations, 400-402
   single-area configurations, 398-400
ARP (Address Resolution Protocol)
   Inverse ARP, 535
   IP routing, 171-173
ASA (Adaptive Security Appliances), 571
ASN (AS numbers), 348
assigning subnet IDs, 213-216
authentication
   CHAP, troubleshooting serial link failures, 485-486
   EIGRP, 433-435
   IPsec VPN, 574-576
   OSPF, 406-408
   PAP, troubleshooting serial link failures, 485-486
   PPP, 476-477
autoconfiguring IPv6 host addresses, 637
auto-cost reference-bandwidth command, 398, 405
automatic sequence numbering, 292
autosummarization, 239
discontiguous classful networks, 241-243
example of, 240-241
IP routing, troubleshooting, 333
support for, 243-244
auto-summary command, 244

B
backup ports, STP, 82
bandwidth
commands, 397, 405, 421, 437
EIGRP metric calculation, 421
BECN (Backward Error Congestion Notification), 517-518
BID (Bridge ID), 66, 89
binary wildcard masks, 262
Blocking State (STP), 63-65
BPDUs (Bridge Protocol Data Units), 66
BPDU Guard, 77, 95
broadcast storms, STP, 61-63
building access-list commands, 288, 291

C
cabling pinouts, troubleshooting LAN switching, 123-124
can't fragment codes (Destination Unreachable ICMP messages), 309
CDP (Cisco Discovery Protocol), 119-121, 138-139
channel-group command, EtherChannel configuration, 96
CHAP (Challenge Handshake Authentication Protocol)
authentication failures, 485-486
PPP configurations, 479-480
checking for updated information, 693-694
CIDR (Classless Interdomain Routing), 590-591
CIR (Committed Information Rates), 499
Cisco CCNA Prep Center, 662
Class A, B, or C networks, 202
classful networks
contiguous networks, 241-243
contiguous networks, 241-243
classful routing
protocols, 203-204
static routes, 190-193
classless routing
protocols, 203-204
static routes, 190-193
clear commands
clear ip nat translation command, 597, 608
clear ip ospf process command, 403
Client mode (VTP), configuring, 17-19, 38-42
commands
access-class, 295
access-list, 260-264
building, 268-269, 288-291
extended IP ACLs, 284
ACLs, configuring, 255
auto-summary, 244
delete vtp, 54-55
deny, 289
ip commands
ip access-group, 284, 297
ip access-group 1, 265
ip access-list, 289
ip access-list 101 permit tcp any any eq 80, 291
ip access-list extended barney, 290
ip address interface, 204
ip summary-address, 234
no access-list number, 296
no auto-summary, 244
no ip access-group, 296
no ip access-list 101 permit tcp any any eq 80, 291
no ip subnet-zero global configuration, 211
permit, 289
ping, 182, 184
remark, 289
show commands, 263-265
show ip access-list, 294
show ip interfaces, 266
show ip route, 181, 184, 240
show running-config, 265, 291-293
syntax, 260
concentrators (VPN), 571
configuration
ACL commands, 255
databases (VLAN), 20-21
EIGRP, 425
authentication, 433-435
basic configuration, 426-428
feasible successors, 430-432
maximum-paths, 435, 437
metrics, 428-430
tuning metric calculation, 437-438
variance, 436
extended IP ACLs, 283-287
Frame Relay
address mapping, 532-536
encapsulation, 531-532
fully meshed networks with one IP subnet, 529-530
LMI, 531-532
partially meshed networks, 537-546
planning configurations, 527-529
self-assessment, 523-526
verification, 541-542
IP addresses, 183-184
IPv6, 645-648
stateless autoconfiguration, 637
static addresses, 636-637
manual route summarization, 233-234
NAT
Dynamic NAT, 604-607
Static NAT, 602-604
OSPF, 397
authentication, 406-408
dead timers, 403-405
hello timers, 403-405
load balancing, 408
metrics (cost), 405-406
multiple area configurations, 400-402
RID, 402-403
single-area configurations, 398-400
PPP
basic configurations, 478-479
CHAP configurations, 479-480
RID (router ID), OSPF, 402-403
RSTP, 97
static routes, IP routing, 182-183
STP, 86
BID, 89
BPDU Guard, 95
EtherChannel, 95-97
multiple instances, 87-88
option summary, 90
per-VLAN costs, 89
port costs, 92-94
PortFast, 95
switch priority, 92-94
system ID extension, 89
VLAN, 24
allowed VLAN lists, 33-36
full configuration, 25-27
shorter configurations, 28-29
storing configurations, 20-21
trunking configuration, 29-33
VLSMs, 202-205
VTP
Client mode, 38-42
default behaviors, 42-43
Server mode, 38-42
Transparent mode, 43
Configuration mode (VLAN), 25
contiguous classful networks, 241-243
control plane analysis, LAN switching, 113
corvergence
IP routing, 346
link-state routing protocol, 373
RSTP, 78-85
STP, 64, 74
delays, 75
troubleshooting, 104
criteria for STP forwarding state activation, 66
data plane analysis, LAN switching, 111-113
databases
  configuration revision numbers (VLAN), 17
  exchange (OSPF)
    DR, choosing, 388-390
    LSDB maintenance, 391
  overview of, 388
Database mode (VLAN), 25
DE (Discard Eligibility) bit, Frame Relay
clouds, 518
dead timers, OSPF configurations, 403-405
debug commands
  debug eigrp packets command, 435
  debug frame-relay lmi command, 542
  debug ip nat command, 608
  debug ip ospf adj command, 460-461
  debug ip ospf hello command, 461-462
  debug ppp authentication command, 485
  debug spanning-tree events command, 94
delay command, 437
delete vtp command, 54-55
deleting single lines, 292
deny all statements, 259
deny command, 289
deny keyword, 256, 260, 278
design, VSLMs, 206
destination IPs, matching, 278-280
Destination Unreachable ICMP messages
  can't fragment codes, 309
  host unreachable codes, 309
  network unreachable codes, 309
  port unreachable codes, 309
  protocol unreachable codes, 309
  troubleshooting IP routing, 307-310
DHCP (Dynamic Host Configuration Protocol)
  IP routing, 171-172
  IPv6, 633
Dijkstra SPF (Shortest Path First) algorithm, 371-372
disabling ACLs, 291
  discontiguous classful networks, 241-243
discontiguous networks, troubleshooting IP routing, 333
distance vector loops
  link-state routing protocol versus, 373-374
  preventing, 356
    counting to infinity, 358-366
    counting to infinity over single links, 358-359
    holddown process, 366-368
    poison reverse, 362-363
    route poisoning, 357-358
    split horizons, 360-363
    triggered updates, 362
distance vector routing protocols, 354-356, 368
DKE (Dynamic Key Exchange), 574
DLCI (data-link connection identifiers)
  assigning to particular subinterfaces, 540
  Frame Relay, 498-499
DNS (Domain Name System)
  IP routing, 172
  IPv6 addresses, finding, 639
Down neighbor state (OSPF neighbors), 391
Down state (OSPF neighbors), 387
DP (designated ports)
  Forwarding State (STP), 65
  LAN segments, determining for STP, 102-104
DR (Designated Routers), 388-390
DTE (data communications equipment)
  access links, 499
  Frame Relay, 498-499, 505, 511-512
DUAL (Diffusing Update Algorithm), 423
dual stacks (IPv4/IPv6), 649
dynamic 6to4 tunnels, IPv6, 651
dynamic ACLs, 299-300
Dynamic NAT (Network Address Translation), 596-597
  configuring, 604-607
  overloading NAT with PAT, 598-599
  translating overlapping addresses, 600-601
  verifying configurations, 607-608
dynamic routing protocol, 345
  administrative distance, 352-353
  convergence, 346
  EGP, 347
  functions of, 346
  IGP, 347
    comparison chart, 351-352
    metrics, 350-351
    routing protocol algorithms, 349
  path selection, 345
Echo Reply messages (ICMP), 307
Echo Request messages (ICMP), 172, 307
edges (RSTP), 79-80
editing ACLs, 288-294
EIGRP (Enhanced Interior Gateway Routing Protocol), 349, 413
authentication, 433-435
configuring, 425
  authentication, 433-435
  basic configuration, 426-428
  feasible successors, 430-432
  maximum-paths, 435-437
  metrics, 428-430
  tuning metric calculations, 437-438
  variance, 436
convergence, 421
  query/reply process, 424
  successors, 422-432
DUAL, 423
IGP comparison chart, 351-352
loop avoidance, 421-424
metric calculation, 418-420, 428-430
  bandwidth, 421
  FD, 420
  RD, 420
  tuning, 437-438
metrics, 350
neighbors, 416-418, 454-457
OSPF versus, 424-425
self-assessment, 413-415
topology information, exchanging, 417-418
update messages, 417
eigrp router-id command, 428
encapsulation
  end-to-end, 559
  Frame Relay, 531-532
encapsulation command, 179, 549
encapsulation frame-relay command, 527-530, 550
encryption, IPsec VPNs, 572-573
data 21 parameters, 282
derror detection, LCP, 475
ESP security protocol, IPsec VPNs, 576
EtherChannel, 76
  STP configuration, 95-97
EUI-64, IPv6, 634
existing VLSMs, adding subnets to, 208-211
extended IP ACLs, configuring, 283-287
Extended Numbered ACLs, 256
extended numbered IP ACLs, 278-288
extended ping command, 183-185
Extranets, VPN, 570
FD (Feasible Distance), EIGRP metric calculation, 420
feasible successors (EIGRP), 422-424, 428-429
  converging via, 432
  creating/viewing, 430-431
FECN (Forward Error Congestion Notification), 517-518
filters
  IP ACLs, 251, 268-269
  overview of, 254-257
  standard numbered IPv4, 257-267
LAN switching, troubleshooting, 127-131, 141-143
  packets, 281-282
final preparation for ICND2 exam, 659
firewalls, 571
formatting ACLs, 296
Forward Delay timers (STP), 73
Forwarding State (STP), 63-65
forwarding unicast frames, troubleshooting
  LAN switching, 151-154
fragmentation, IP routing, 173-174
Frame Relay, 493
  access links, 499
  Layer 1 issues, troubleshooting, 549
  Layer 2 issues, troubleshooting, 549-550
AR, 499
clouds, 516
  BECN, 517-518
  DE bit, 518
  FECN, 517-518
configuring
  address mapping, 532-536
  encapsulation, 531-532
  fully meshed networks with one IP subnet, 529-530
  LMI, 531-532
partially meshed networks, 537-546
planning configurations, 527-529
self-assessment, 523-526
verification, 541-542
DCE, 499
DLCI, 498-499
DTE, 498-499, 505, 511-512
Layer 3 addressing
  broadcast handling, 515
  hybrid alternative, 514-515
  one subnet per VC, 512-513
  single subnets containing all DTE, 511-512
LMI, 498-499, 503-505, 549
NBMA networks, 497-499
overview, 497-499
protocol specifications, 500
PVC, 499
  status codes, 555-556
  subinterface status, 556-557
  troubleshooting, 551-557
self-assessment, 493-496
SVC, 499
troubleshooting
  end-to-end encapsulation, 559
  example of, 547-548
  Layer 1 issues on access links, 549
  Layer 2 issues on access links, 549-550
  mapping issues, 558-559
  mismatched subnet numbers, 559
  PVC problems, 551-557
  self-assessment, 523-526
VC, 498-502
  layer 3 addressing, 512-513
  partially meshed networks with one IP
  subnet per VC, 537-540
frame-relay commands
  frame-relay interface-dlci command, 528, 532, 539-545, 555-557
  frame-relay lmi-type ansi command, 532, 550
  frame-relay lmi-type command, 528
  frame-relay map command, 528, 537, 557
ftp keyword, 285
Full neighbor state (OSPF neighbors), 390-391

G-H
global addressing, Frame Relay
configurations, 540
Hello messages, OSPF, 384-385
hello timers
  OSPF configuration, 403-405
  STP, 73
hosts
  keyword, 260, 279
  unreachable codes (Destination
  Unreachable ICMP messages), 309
I-J
ICMP (Internet Control Message Protocol)
  Echo Requests, 172
  IP routing, 172
troubleshooting IP routing, 306
  Destination Unreachable ICMP
  messages, 307-310
  Echo Reply messages, 307
  Echo Request messages, 307
  ICMP Time Exceeded messages, 310-311
  Redirect ICMP messages, 310
  Time Exceeded messages, 310-311
icmp keyword, 278
IDs, assigning to subnets, 213-216
IEEE (Institute of Electronic and Electrical
Engineers), 802.1Q, 13-15
IGP (Interior Gateway Protocols), 347
  comparison chart, 351-352
  metrics, 350-351
  routing protocol algorithms, 349
IKE (Internet Key Exchange), 574
implementation
  IP ACLs, 294-300
  standard IP ACLs, 264-267
Improved Editing with Sequence Numbers,
257
infinity metric values, route poisoning, 357
Init neighbor state (OSPF neighbors), 391
Init state (OSPF neighbors), 387
inserting new lines, 292
inside global addresses, NAT, 595-596
inside local addresses, NAT, 595-596

interface commands
  interface loopback command, 403
  interface serial 0/0/0/1 point-to-point command, 539
interface IDs, IPv6, 634
interfaces, disabling ACLs, 291
Intranets, VPN, 570
Inverse ARP, Frame Relay address mapping, 535
IP (Internet Protocol)
  ACLs, 251, 256-257, 268-269
    advanced, 275
    extended, 283-287
    extended numbered, 278-288
    implementing, 294-300
    named, 288-294
    overview of, 254-257
  interfaces, matching exact, 260
  configuring, 183-184
routings
  ARP, 171-173
  connected routes, 175-180
  DHCP, 171-172
  distance vector routing protocols,
    354-363, 368, 373-374
  DNS, 172
  dynamic routing protocol, 345-353
  fragmentation, 173-174
  ICMP, 172
  IP addressing and, 162, 166-171
  LAN switches, 325-326
  link-state routing protocols, 369-374
  MTU, 173-174
  process overview, 162-166
  self-assessment, 159-161, 341-344
  static routes, 180-193
  tables, 392-394
  troubleshooting, 305-314, 324-336
secondary IP addressing, 175-177
subnetting, practicing, 662-665
VLANs, 16
ip access-group commands
  ip access-group 1 in command, 265
  ip access-group command, 284, 297
  ip access-group number {in | out} interface subcommand, 264
ip access-list 101 permit tcp any any eq 80 command, 291
ip access-list command, 289
ip access-list extended barney command, 290
ip address commands
  ip address command, 175-178, 329-331, 634
  ip address interface command, 204
ip authentication commands
  ip authentication key-chain eigrp command, 433
  ip authentication mode eigrp command, 433
ip default-network commands, 188-189
ip domain-lookup command, 648
ip hello-interval eigrp command, 425
ip hold-time eigrp command, 425
ip keyword, 279
ip mtu command, 174
ip nat commands
  ip nat inside source command, 606
  ip nat inside source list 1 interface serial 0/0 overload, 611
  ip nat inside source list command, 608, 612
  ip nat inside source static command, 602-604
  ip nat outside command, 602, 604-605, 609, 611
  ip nat pool command, 606
  ip nat pool mask command, 605
  ip nat source list interface overload command, 609
  ip nat source list pool command, 605
  ip nat source static command, 612
ip ospf commands
  ip ospf authentication command, 408
  ip ospf cost command, 397, 405
  ip ospf dead-interval command, 397, 405
  ip ospf hello-interval command, 397, 405
  ip ospf network command, 388
IP phones, VLAN trunking, 36-37
ip route command, 181-183, 186-187
ip subnet-zero command, 177
ip summary-address command, 234
ipconfig/displaydns command, 172
IPsec (IP Security), 571
  authentication, 574-576
  encryption, 572-573
implementing, 577
key exchange, 573-574
message integrity, 574-576
IPv4 (Internet Protocol version 4)
NAT scalability, 589
CIDR, 590-591
private addressing, 592
standard numbered ACLs, 257-267
transitions
IPv4/IPv6 dual stacks, 649
NAT-PT, 651
IPv6 (Internet Protocol version 6), 617
addresses
conventions, 624-625
summaries, 643-644
configuring, 645-648
default routers, finding via NDP, 639
DHCP, 633
DNS server addresses, finding, 639
global route aggregation, 622-624
host address assignment, 634
configuration summary, 638
EUI-64, 634
interface ID, 634
RA, 637
stateless autoconfiguration, 637
static address configuration, 636-637
multicast addresses, 642-643
prefixes
conventions, 625-627
global unicast prefix assignment
example, 628-630
site prefixes, 630
subnet prefixes, 630
terminology of, 632
routing protocols, 644-645
self-assessment, 617-619
subnetting, 630-632
transitions
NAT-PT, 651
summary of, 652
tunneling, 649-651
transitionsIPv4/IPv6 dual stacks, 649
unicast addresses, 640-641
ipv6 commands
ipv6 address command, 636
ipv6 router rip command, 647
ISATAP (Intra-site Automatic Tunnel Addressing Protocol), 651

IS-IS (Intermediate System-to-Intermediate System), 351-352
ISL (Inter-Switch Links)
802.1Q versus, 14-15
IP routing, connected routes, 178-180
VLAN trunking, 13

K-L

keepalive failures, troubleshooting serial links, 484

key exchanges
DKE, 574
IKE, 574
IPsec VPN, 573-574

keywords, 256, 260, 263, 278

LANs (local area networks)
segments
designated ports, 70-72
DP, determining for STP, 102-104
switches, IP support, 325-326
troubleshooting, 109-110
analyzing/predicting normal operation, 111-114
cabling pinouts, 123-124
core plane analysis, 113
data plane analysis, 111-113
duplex issues, 124-127
exam tips, 116
example of, 136-146
forwarding, 117-119, 151-154
interface speeds, 124-127
interface status codes, 122
isolate filtering/port security
problems, 127-131, 141-143
isolate interface problems, 121-127, 139-141
isolate VLAN/trunking problems, 132-135, 143-146
network diagram confirmation via CDP, 119-121, 138-139
notconnect state, 123-124
PC1 broadcasts in VLAN 1, 147-150
predicting normal operation, 147-150
problem isolation, 114-115
root cause analysis, 115-116
self-assessment, 109
LCP (Link Control Protocol), 473
  error detection, 475
  looped link detection, 474
  multilink PPP, 475-476
  PPP authentication, 476-477
Learning State (RSTP), 83
link LSA (link-state advertisements), 369, 392
link-state routing protocols, 369
  convergence, 373
  Dijkstra SPF algorithm, 371-372
  distance vector routing protocol versus, 373-374
  LSA, 369-370
  LSDB, building on routers, 369-370
  OSPF, 369
links (RSTP), 79-80
Listening state
  RSTP, 83
  STP, 75
lists, logic with IP ACLs, 258-260
LMI (Local Management Interface), 499, 503-505
  encapsulation command, 549
  Frame Relay, configuring, 531-532
  protocol, 498
load balancing, OSPF, 408
local addressing, Frame Relay
  configurations, 540
locations, ACLs, 254-255
Lock-and-Key Security, 299
logic
  lists with IP ACLs, 258-260
  matching, 260
loops
  avoidance, STP, 64
  distance vector loops, 356
    counting to infinity in redundant networks, 363-366
    counting to infinity over single links, 358-359
    holddown process, 366-368
    poison reverse, 362-363
    route poisoning, 357-358
    split horizons, 360-363
    triggered updates, 362
  EIGRP, avoiding in, 421-424
  link detection, LCP, 474
LSA (link-state advertisements), 370
  link LSA, 369, 392
  router LSA, 369, 391
LSDB (link-state databases)
  building, 369-370
  OSPF topology database exchange, maintaining for, 391
M
MAC (Media Access Control) tables, STP, 62-63
manual route summarization, 230-231
  configuring, 233-234
  strategies for, 235-238
  verification, 232-233
mapping addresses, Frame Relay, 532-534
  Inverse ARP, 535
  static mapping, 536
masks
  binary wildcard, 262
  SLSMs, 212
  VLSMs, 199
    adding subnets, 208-211
    configuring, 202-205
    overlaps, 205-208
    planning subnets, 211-218
    selecting, 212-213
  WC, 261
  wildcard, selecting, 263
matching
  addresses, 263
  exact IP addresses, 260
  logic, 260
  packets, 255-256
  parameters, 297
  protocols, 278-280
  subnets, selecting wildcard masks, 263
  TCP numbers, 280-283
  UDP numbers, 280-283
Max Age timers (STP), 73
maximum-paths command, 408, 426, 435-437
MCT (Manually Configured Tunnels), IPv6, 651
message integrity, IPsec VPNs, 574-576
metric calculations (EIGRP), 418-420, 428-430
  bandwidth, 421
  FD, 420
RD, 420
RIP, 233
tuning, 437-438

MIST (Multiple Instances of Spanning Trees), 88
MST (Multiple Spanning Trees), 88
MTU (maximum transmission units), 173-174, 463
mtu command, 174
multicast IPv6 addresses, 642-643
multilink PPP (Point-to-Point Protocol), 475-476

N
named ACLs, 257, 288-294
NAT (Network Address Translation), 275, 585, 593
Dynamic NAT, 596-597
configuring, 604-607
overloading NAT with PAT, 598-599
translating overlapping addresses, 600-601
verifying configurations, 607-608
inside global addresses, 595-596
inside local addresses, 595-596
IPv4 address scalability, 589
CIDR, 590-591
private addressing, 592
outside global addresses, 595-596
outside local addresses, 595-596
overload (PAT) NAT, 608-611
self-assessment, 585-587
Static NAT, 593-596, 602-604
troubleshooting, 611-612
NAT-PT (Network Address Translation-Protocol Translation), 651
NBMA (nonbroadcast multiaccess) networks, 497-499
NDP (Non-designated Port), IPv6 default routers, 639
neighbors
  EIGRP, 416-418, 454-457
  OSPF, 383
  Down neighbor state, 391
  Down state, 387
  Full neighbor state, 390-391
  Hello messages, 384-385
  Init neighbor state, 391
  Init state, 387
  OSPF RID, 384
  potential problems with, 385-386
  routing protocols, troubleshooting, 454-463
  states of, 386-387
  summary of states, 391
  Two-way neighbor state, 391

network area command, 397
network command, 399, 425, 428, 446
networks
diagrams, 119-121, 138-139
discontiguous networks, troubleshooting
IP routing, 333
unreachable codes (Destination
Unreachable ICMP messages), 309
new lines, inserting, 292
no commands
no access-list number command, 296
no auto-summary command, 244
no frame-relay lmi-type command, 551
no ip access-group command, 296
no ip access-list 101 permit tcp any any eq
80 commands, 291
no ip subnet-zero command, 178
no ip subnet-zero global configuration
command, 211
no keepalive command, 542
no shutdown command, 129-130, 143, 326
no shutdown vlan command, 134
nonroot switches, 100-102
notconnect state, troubleshooting, 123-124
numbers
ports, 282
sequences
  automatic, 292
  editing ACLs, 291-294
  automatic, 292
TCP, matching, 280-283
UDP, matching, 280-283

O
OSPF (Open Shortest Path First), 369, 379
areas
  multiple area configurations, 400-402
  single-area configurations, 398-400
authentication, 406-408
configuring, 397
  authentication, 406-408
dead timers, 403-405
hello timers, 403-405
load balancing, 408
metrics (cost), 405-406
multiple area configurations, 400-402
RID, 402-403
  single-area configurations, 398-400
EIGRP versus, 424-425
IGP comparison chart, 351-352
IP routing tables, building, 392-393
load balancing, 408
neighbors, 383
  Down state, 387, 391
  Full neighbor state, 390-391
  Hello messages, 384-385
  Init state, 387, 391
OSPF RID, 384
  potential problems with, 385-386
  states of, 386-387
  summary of states, 391
  troubleshooting routing protocols, 454-463
  Two-way neighbor state, 391
RID, configuring, 402-403
routing protocols, troubleshooting, 446, 451-463
scaling via hierarchical design, 393
  areas, 394-396
  design terminology table, 396
self-assessment, 379-381
topology database exchange
  choosing DR, 388-390
  LSDB maintenance, 391
  overview of, 388
OSPF RID (OSPF router ID), 384
out keyword, 295
outside global addresses, NAT, 595-596
outside local addresses, NAT, 595-596
overlaps, VLSMs, 205-208

P
  p access-group interface subcommand, 266
packets
  filters
    destination ports, 281
    source ports, 282
forwarding
  host-related problems, 314-315
  router-related problems, 316-324
IP ACLs, 251, 268-269
  overview of, 254-257
  standard numbered IPv4, 257-267
matching, 255-256
PAP (Password Authentication Protocol), 485-486
parameters
  access-list remark, 268
  eq 21, 282
  matching, 297
  protocols, 285
  source, 262
  passive-interface command, 446-447, 451
PAT (Port Address Translation)
  NAT overload configuration, 608-611
  overloading NAT, 598-599
path selection, 345
PC1 broadcasts, 147-150
permit command, 289
permit keyword, 256, 260, 278, 289
permit subcommands, 289
ping command, 182-184, 316-317, 322
  extended ping command, 183-185
  IP
    connectivity, testing, 181-182
    routing, troubleshooting, 324
remote host route tests, 172-173
troubleshooting IP routing, 306
  Destination Unreachable ICMP messages, 307-310
  ICMP Echo Reply messages, 307
  ICMP Echo Request messages, 307
  ICMP Time Exceeded messages, 310-311
  Redirect ICMP messages, 310
pinouts (cabling), 123-124
PIX firewalls, 571
planning subnets, VLSMs, 211-218
poison reverse, distance vector loops, 362-363
PortFast, 77
  RSTP, 83
  STP configuration, 95
ports
  backup ports, STP, 82
  numbers, 282
  PAT, overloading NAT, 598-599
security, troubleshooting, 127-131, 141-143
states of RSTP, 80
unreachable codes (Destination Unreachable ICMP messages), 309

PPP (Point-to-Point Protocol), 469
configuring
  basic configurations, 478-479
  CHAP configurations, 479-480
LCP, 473
  error detection, 475
  looped link detection, 474
  multilink PPP, 475-476
  PPP authentication, 476-477
Protocol field, 472-473
self-assessment, 469-471
troubleshooting serial links, 480
  CHAP authentication failures, 485-486
  keepalive failures, 484
  Layer 1 problems, 482
  Layer 2 problems, 483-486
  Layer 3 problems, 486, 488
  PAP authentication failures, 485-486

practicing subnetting, 665
preparing
  for ICND1 exams
    Cisco CCNA Prep Center, 662
    recommended study plan, 664-665
    scenarios, 663
    subnetting skills, 662-663
  for ICND2 exams, 659
preventing routing loops
  STP, 64
  RSTP, port states, 80
private addressing, NAT, 592
private IP addresses, 202
processes, ACLs, 258
Protocol field (PPP), 472-473
protocols
  matching, 278-280
  parameters, 285
  routing, classful/classless, 203-204
  unreachable codes (Destination Unreachable ICMP messages), 309
pruning (VTP), 22, 38
pseudocode ACLs, 261
public IP addresses, 202
PVCs (permanent virtual circuits)
  Frame Relay, 499-557
  status codes, 555-556
  subinterface status, 556-557
  PVRST+ (Per-VLAN Rapid Spanning Tree Plus), 87-88

Q-R
QoS (quality of service), 275
RA (router advertisement), 637
ranges of addresses, reverse engineering
  ACLs, 269-270
RD (Reported Distance), EIGRP metric calculations, 420
recommended study plan, 664-665
Redirect ICMP messages, troubleshooting
  IP routing, 310
  reflexive ACLs, 297-298
  remark commands, 289
requirements, VLSMs, 213
reverse engineering ACLs, 269-270
RID (router ID), 384, 402-403
RIP (Routing Information Protocol), 188
distance vector loops, preventing
  counting to infinity in redundant networks, 363-366
  counting to infinity over single links, 358-359
  holddown process, 366-368
  poison reverse, 362-363
  split horizons, 360-363
  triggered updates, 362
IGP comparison chart, 351-352
metrics, 233, 350
steady-state operations, 355-356
Root Guard feature, STP security, 78
root ports, 69-70
root switches, 67-68, 99-100
router commands, 451
  router eigrp command, 425-427
  router ospf command, 397-399
  router-id command, 397
routers
  IPv6 default routers, finding via NDP, 639
  LSA, 369, 392
routes
  aggression, CIDR, 590
  poisoning, 357-358
selecting, 235-238
summarization, 227
  autosummarization, 239-244
  manual route summarization, 230-238

routing
  loops
    preventing with RSTP, 80
    STP, 64
  protocols, 203-204, 444-445
    algorithms (IGP), 349
    EIGRP interfaces, 446-451
    EIGRP neighbors, 454-457
    OSPF interfaces, 446, 451-453
    OSPF neighbors, 454-463
    self-assessment, 443
  tables
    bandwidth, 421
    EIGRP metric calculation, 418-420
    FD, 420
    manual route summarization, 230-234
    RD, 420

RP (root ports)
  Forwarding State (STP), 65
  STP, troubleshooting, 100-102

RSTP (Rapid Spanning Tree Protocol)
  configuring, 97
  convergence, 78-85
  edges, 79-80
  Learning State, 83
  links, 79-80
    link-type point-to-point, 83
    link-type shared links, 83
  Listening State, 83
  ports
    roles, 81
    states, 80
  PortFast, 83
  STA, 82
  synchronization, 85

RTP (Reliable Transport Protocol), 417

S
  scaling, OSPF, 393
    areas, 394-396
    design terminology table, 396
  scenarios, preparing for ICND1 exams, 663
  searching for VLSM overlaps, 205-208
  secondary IP addressing, 175-177

security
  Lock-and-Key Security, 299
  port security, LAN switching, 127-131, 141-143
  STP, 77-78
  VLAN trunking, 37

selecting
  routes, 235-238
  VLSM masks, 212-213
  wildcard masks, 263

self-assessments
  EIGRP, 413-415
  Frame Relay, 493-496
    configuring, 523-526
    troubleshooting, 523-526
  IP routing, 159-161, 305, 341-344
  IPv6, 617-619
  LAN switching, troubleshooting, 109
  NAT, 585-587
  OSPF, 379-381
  PPP, 469-471
  routing protocols, troubleshooting, 443
  STP, 57-60
  VLAN, 5-8
  VPN, 565-567

sequence numbers
  ACLs, editing, 291-294
  automatic, 292

serial links, troubleshooting, 480
  CHAP authentication failures, 485-486
  keepalive failures, 484
  Layer 1 problems, 482
  Layer 2 problems, 483-486
  Layer 3 problems, 486, 488
  PAP authentication failures, 485-486

Server mode (VTP), configuring, 17-19, 38-42

servers, finding IP addresses, 639

service password-encryption command, 408

show commands, 143, 263-265
  show cdp command, 120
  show cdp entry command, 138
  show cdp neighbors command, 48, 120, 138
  show ip route command, 204
  show frame-relay lmi command, 550
  show frame-relay map command, 534-535, 542, 545, 554, 558
  show frame-relay pvc command, 534, 542, 553, 556
  show interface status command, 139
show interface switchport command, 133, 136
show interfaces command, 122-124, 127, 140, 175, 419, 479, 559
show interfaces description command, 122
show interfaces fa0/0 command, 438
show interfaces Fa0/13 command, 126
show interfaces status command, 122-126
show interfaces switchport command, 2-33, 48
show interfaces trunk command, 48-49, 134-135, 146
show ip access-list command, 294
show ip access-lists command, 336
show ip access-lists command, 323
show ip eigrp interface command, 453
show ip eigrp interfaces command, 428, 446, 449-451
show ip eigrp neighbor command, 416
show ip eigrp neighbors command, 428, 435, 456
show ip eigrp topology command, 416, 419, 430-431
show ip interface command, 335
show ip interface brief command, 453, 559
show ip interfaces command, 266
show ip nat statistics command, 604-608, 612
show ip nat translations command, 604-608, 611
show ip ospf interface brief command, 453
show ip ospf interface brief command, 446, 452, 460
show ip ospf interface command, 404-405, 462
show ip ospf neighbor command, 403, 457-458, 463
show ip protocols command, 446, 449-453, 456
show ip route command, 171, 175, 181, 184, 187, 190, 240, 321, 326, 353, 357, 416, 428
show ip route connected command, 175
show ip route eigrp command, 428, 449
show ipv6 interface brief command, 648
show ipv6 interface command, 637, 642
show ipv6 route command, 647
show mac address-table command, 133
show mac address-table dynamic command, 154
show mac address-table vlan 3 command, 154
show port-security command, 142
show port-security interface command, 128-131
show running-config command, 134, 265, 291, 293
show spanning-tree command, 98-99
show spanning-tree root command, 92
show spanning-tree vlan 2 command, 91
show spanning-tree vlan 3 active command, 148
show spanning-tree vlan command, 99, 135
show vlan brief command, 49, 133
show vlan command, 42, 133-134
show vtp password command, 49
show vtp status command, 39, 49
shutdown command, 130, 143
single classful networks, 202
single lines, deleting, 292
site prefixes, IPv6, 630
SLSMs (static length subnet masks), 205, 212
sources
IPs, matching, 278-280
parameters, 262
Spanning Tree, port states, 71
spanning tree commands
spanning-tree mode rapid-pvst command, 97
spanning-tree portfast command, 97
spanning-tree vlan root primary command, 94
spanning-tree vlan root secondary command, 94
split horizons, distance vector loops, 360-363
SSH (Secure Shell), ACLs, 295-297
SSL (Secure Socket Layer), VPN, 578-579
STA (Spanning Tree Algorithm), 65, 82
standard IP ACLs, implementing, 264-267
Standard Numbered ACLs, 256
standard numbered IPv4 ACLs, 257-267
statements, deny all, 259
static address mapping, Frame Relay address mapping, 536
Static NAT (Network Address Translation), 593-596, 602-604
static routes, IP routing, 180-181
   classful/classless routing, 190-193
   configuring for, 182-183
   default routes, 186-190
   extended ping command, 183-185
status codes (PVC), 555-556
storing VLAN configurations, 20-21

STP (Spanning Tree Protocol)
   backup ports, 82
   BID, 66
   Blocking State, 63-65
   BPDU, 66
   broadcast storms, 61-63
   configuring, 86
      BID, 89
      BPDU Guard, 95
      EtherChannel, 95-97
      multiple instances, 87-88
      option summary, 90
      per-VLAN costs, 89
      port costs, 92-94
      PortFast, 95
      switch priority, 92-94
      system ID extension, 89
   convergence, 64, 74
      delays, 75
      troubleshooting, 104
   EtherChannel, 76
   Forwarding State, 63-65
   LAN segments
      choosing designated ports, 70-72
      steady-state networks, 72
   Listening state, 75
   MAC table instability, 62-63
   multiple frame transmission, 62-63
   ports, 80-81
   PortFast, 77
   root ports, choosing, 69-70
   root switches, electing, 67-68
RSTP
   configuring, 97
   convergence, 78-85
   edges, 79-80
   Learning State, 83
   links, 79-80
   link-type point-to-point, 83
   link-type shared links, 83
   Listening State, 83
   port roles, 81

port states, 80
   PortFast, 83
   STA, 82
   synchronization, 85
security, 77-78
self-assessment, 57-60
STA, 65
state comparison table, 75
timers, 73
topology of, 64
troubleshooting, 98
   convergence, 104
   determining LAN segment DP, 102-104
   determining nonroot switches, 100-102
   determining root switches, 99-100
   determining RP, 100-102
   verifying default operation, 90-91

strategies for route selection, 235-238

subinterfaces, 513

subnets
   IDs, assigning, 213-216
   IP
      addressing, 166-171
      routing, connected routes, 175
      secondary IP addressing, 175-177
      subnet zero support, 177-178
      VLAN, 16
   IPv6, 630-632
   matching, selecting wildcard masks, 263
   practicing, 662-665
   SLSMs, 212
   VLSMs, 199
      adding subnets, 208-211
      configuring, 202-205
      overlaps, 205-208
      planning subnets, 211-218

subsets
   addresses, matching, 260-262
   advertisements, 19

successors (EIGRP), 422-423, 428-429
   converging via, 432
   creating/viewing, 430-431

summarization (route), 227
   autosummarization, 239
   discontiguous classful networks, 241-243
example of, 240-241
support for, 243-244
manual route summarization, 230-231
configuring, 233-234
strategies for, 235-238
verification, 232-233
summary advertisements (VTP), 19
SVC (switched virtual circuits), Frame Relay, 499
switchport commands
switchport access vlan 3 command, 144
switchport access vlan command, 133
switchport mode command, 29
switchport mode trunk command, 180
switchport port-security mac-address command, 154
switchport trunk allowed vlan command, 134
switchport trunk encapsulation dot1q command, 180
synchronization
RSTP, 85
VLAN, 19
syntax, commands, 260
system ID extension, STP, 89

tagging (VLAN), 11
TCP (Transmission Control Protocol)
numbers, matching, 280-283
tcp keyword, 278-280
TCP/IP (Transmission Control Protocol/Internet Protocol), 183-184
telnet command, 324
Teredo tunneling, IPv6, 651
terminal commands
terminal monitor command, 460
terminal no monitor command, 460
text, creating ACLs, 296
time-based ACLs, 300
TLS (Transport Layer Security), 578
tools, route summarization, 227
topology database exchange (OSPF)
DR, choosing, 388-390
LSDM maintenance, 391
overview of, 388
ttraceroute command, 316-323
troubleshooting IP routing, 312-314
VLSM, troubleshooting, 331-333
tracert command, troubleshooting IP routing, 314
Traffic Shaping, 517
transitions, IPv6
IPv4/IPv6 dual stacks, 649
NAT-PT, 651
summary of, 652
tunneling, 649-651
Triggered mode (VTP), 20-21, 43
t triggerd updates, distance vector loops, 362
troubleshooting
Frame Relay
d-to-end encapsulation, 559
eof, 547-548
Layer 1 issues on access links, 549
Layer 2 issues on access links, 549-550
mapping issues, 558-559
mismatched subnet numbers, 559
PVC problems, 551-557
self-assessment, 523-526
IP routing
ACL, 334-336
autosummary, 333
discontiguous networks, 333
host routing tools, 324-326
ICMP, 306-311
interface status, 328
packet forwarding, 314-324
ping command, 306-311
self-assessment, 305
show ip route command, 326
traceroute command, 312-314
tracert command, 314
VLSM, 328-333
LAN switching, 110
analyzing/predicting normal operation, 111-114
cabling pinouts, 123-124
control plane analysis, 113
data plane analysis, 111-113
duplex issues, 124-127
exam tips, 116
example of, 136-146
forwarding process overview, 117-119
forwarding unicast frames, 151-154
interface speeds, 124-127
interface status codes, 122
isolate filtering/port security problems, 127-131, 141-143
isolate interface problems, 121-127, 139-141
isolate VLAN/trunking problems, 132-135, 143-146
network diagram confirmation via CDP, 119-121, 138-139
notconnect state, 123-124
PC1 broadcasts in VLAN 1, 147-150
predicting normal operation, 147-150
problem isolation, 114-115
root cause analysis, 115-116
self-assessment, 109
NAT, 611-612
PPP, serial links, 480-488
routing protocols, 444-445
EIGRP interfaces, 446-451
EIGRP neighbors, 454-457
OSPF interfaces, 446, 451-453
OSPF neighbors, 454-463
self-assessment, 443
serial links, 480
CHAP authentication failures, 485-486
keepalive failures, 484
Layer 1 problems, 482
Layer 2 problems, 483-486
Layer 3 problems, 486-488
PAP authentication failures, 485-486
STP, 98
convergence, 104
determining LAN segment DP, 102-104
determining nonroot switches, 100-102
determining root switches, 99-100
determining RP, 100-102
VLSM, 333
configuring overlapping subnets, 329-331
overlapping subnets, 331-332
recognizing VLSM usage, 328
VTP
best practices, 51-52
determining the problem, 44-49
switch connections, 50-51
trunking, 50-51
trunking
interfaces, 28
LAN switching, troubleshooting, 132-135, 143-146
VLANs, 11-12
802.1Q, 13-15
allowed VLAN lists, 33-36
configuring, 29-33
IP phones, 36-37
ISL, 13-15
security, 37
VTP, 16
avoiding via Transparent mode, 20
client mode, 17-19
feature comparison summary, 23
pruning, 22
server mode, 17-19
storing VLAN configurations, 20-21
switch requirements, 19
troubleshooting, 50-51
versions of, 21
trunking (VTP)
IPv6, 649-651
VPN, 569
Two-way neighbor state (OSPF neighbors), 391
U
UDP (User Datagram Protocol), 280-283
udp keyword, 278, 280
unicast frames
forwarding, troubleshooting LAN switching, 151-154
IPv6 addresses, 640-641
updates
for ICND1 exam, 693-694
messages, (EIGRP), 417
triggered updates, distance vector loops, 362
V

variance command, 426, 436

VCs (Virtual Circuits)
CIR, 499
Frame Relay, 498-502, 512-513
partially meshed networks with one IP
subnet per VC, 537-540

verification
Dynamic NAT configurations, 607-608
Frame Relay configurations, 541-542
manual route summarization, 232-233
STP default operations, 90-91
VLSMs, 204-205

VLANs (Virtual LANs), 9-11
Administrative mode, 29, 33
collection database, 20-21
Configuration mode, 25
configuring, 24
allowed VLAN lists, 33-36
full configuration, 25-27
shorter configurations, 28-29
storing, 20
trunking configuration, 29-33
database configuration revision
numbers, 17
Database mode, 25
IP
subnets, 16
routing, 178-180
LAN switching, 132-134, 143-146
self-assessments, 5-8
STP configuration, 89
synchronization, 19
tagging, 11
trunking, 11-12
802.1Q, 13-15
allowed VLAN lists, 33-36
configuring, 29-33
IP phones, 36-37
ISL, 13-15
security, 37
verifying, 33
VLAN ID, 11
VMPS, 25
VTP, 16
best practices, 51-52
Client mode, 17-19, 38-42
configuring, 42-43

VPN (Virtual Private Networks), 565
components of, 571
IPsec, 571
authentication, 574-576
encryption, 572-573
implementing, 577
key exchange, 573-574
message integrity, 574-576
self-assessment, 565-567
SSL, 578-579
tunnels, 569
types of, 570

VTP (VLAN Trunking Protocol), 16
advertisement request messages, 19
best practices, 51-52
client mode, 17-19, 38-42
configuring, 42-43
feature comparison summary, 23
pruning, 22, 38
server mode, 17-19, 38-42
subset advertisements, 19
summary advertisements, 19
switch requirements, 19
Transparent mode, 20-21, 43
troubleshooting
  * determining the problem, 44-49
  * switch connections, 50-51
  * trunking, 50-51

trunking, 50-51
versions of, 21
VLAN configurations, storing, 20-21

**vtp commands**
  * vtp domain command, 38
  * vtp mode command, 38
  * vtp mode transparent command, 43
  * vtp password command, 38
  * vtp pruning command, 38, 135

**W-Z**

**WANs (Wide Area Networks), PPP, 469**
  * configuring, 478-480
  * LCP, 473-477
  * Protocol field, 472-473
  * self-assessment, 469-471
  * troubleshooting, 480-488

**WC (wildcard) masks, 261**

**well-known port numbers, 282**

**wildcards**
  * addresses, 260-262
  * binary masks, 262
  * masks, 263

**www keyword, 285**