CCENT/CCNA ICND1
640-822 Official Cert Guide
Third Edition

Wendell Odom, CCIE No. 1624

Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA
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 Dushimer
Executive Editor: Brett Bartow
Managing Editor: Sandra Schroeder
Project Editor: Mandie Frank
Editorial Assistant: Vanessa Evans
Composition: Mark Shirar
Proofreader: Sarah Kearns

Manager Global Certification: Erik Ullanderson
Business Operation Manager, Cisco Press: Anand Sundaram
Technical Editors: Elan Beer, Teri Cook, Brian D’Andrea, Steve Kalman
Copy Editor: Sheri Cain
Book and Cover Designer: Gary Adair
Indexer: Larry Sweazy

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.
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 among the first to obtain Cisco’s Certified System Instructor (CCSI) certification, and in 1996, Elan was among 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 ten years of experience in the IT industry. She has worked with different types of organizations in 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 who uses real-world experience to present complex networking technologies. As an IT instructor, Teri has been teaching Cisco classes for more than five years.

Brian D’Andrea (CCNA, CCDA, MCSE, A+, and Net+) has 11 years of IT experience in both medical and financial environments, where planning and supporting critical networking technologies were his primary responsibilities. For the last five years, he has dedicated himself to technical training. Brian spends most of his time with The Training Camp, an IT boot camp provider. Using his real-world experience and his ability to break difficult concepts into a language that students can understand, Brian has successfully trained hundreds of students for both work and certification endeavors.

Stephen Kalman is a data security trainer. He is 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, the best daughter I could ask for. 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, Kourtneye, 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 *ICND2*. The nature of this project plus the ICND2 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 question, 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 revved, 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

Part I: Networking Fundamentals 3
Chapter 1 Introduction to Computer Networking 5
Chapter 2 The TCP/IP and OSI Networking Models 17
Chapter 3 Fundamentals of LANs 47
Chapter 4 Fundamentals of WANs 77
Chapter 5 Fundamentals of IPv4 Addressing and Routing 99

Part II: LAN Switching 171
Chapter 7 Ethernet LAN Switching Concepts 173
Chapter 8 Operating Cisco LAN Switches 203
Chapter 9 Ethernet Switch Configuration 237
Chapter 10 Ethernet Switch Troubleshooting 273
Chapter 11 Wireless LANs 305

Part III: IPv4 Addressing and Subnetting 335
Chapter 12 Perspectives on IPv4 Subnetting 337
Chapter 13 Analyzing Classful IPv4 Networks 367
Chapter 14 Converting Subnet Masks 383
Chapter 15 Analyzing Existing Subnet Masks 397
Chapter 16 Designing Subnet Masks 411
Chapter 17 Analyzing Existing Subnets 427
Chapter 18 Finding All Subnet IDs 459

Part IV: IPv4 Routing 479
Chapter 19 Operating Cisco Routers 481
Chapter 20 Routing Protocol Concepts and Configuration 517
Chapter 21 Troubleshooting IP Routing 553

Part V: Wide-Area Networks 591
Chapter 22 WAN Concepts 593
Chapter 23 WAN Configuration 621
Part VI: Final Preparation 645
Chapter 24 Final Preparation 647

Part VII: Appendixes 657
Appendix A Answers to the “Do I Know This Already?” Quizzes 659
Appendix B Numeric Reference Tables 681
Appendix C ICND1 Exam Updates: Version 1.0 689
Glossary 693
Index 718

Part VIII: DVD-Only
Appendix D Practice for Chapter 13: Analyzing Classful IPv4 Networks
Appendix E Practice for Chapter 14: Converting Subnet Masks
Appendix F Practice for Chapter 15: Analyzing Existing Subnet Masks
Appendix G Practice for Chapter 16: Designing Subnet Masks
Appendix H Practice for Chapter 17: Analyzing Existing Subnets
Appendix I Practice for Chapter 18: Finding All Subnet IDs
Appendix J Additional Scenarios
Appendix K Subnetting Video Reference
Appendix L Memory Tables
Appendix M Memory Tables Answer Key
Appendix N ICND1 Open-Ended Questions
# Contents

Introduction xxvii

Part I: Networking Fundamentals 3

Chapter 1 Introduction to Computer Networking 5
  Perspectives on Networking 5
  The Flintstones Network: The First Computer Network? 8

Chapter 2 The TCP/IP and OSI Networking Models 17
  “Do I Know This Already?” Quiz 17
  Foundation Topics 21
  TCP/IP Networking Model 21
  History Leading to TCP/IP 21
  Overview of the TCP/IP Networking Model 23
  TCP/IP Application Layer 24
    HTTP Overview 25
    HTTP Protocol Mechanisms 25
  TCP/IP Transport Layer 26
    TCP Error Recovery Basics 27
    Same Layer and Adjacent Layer Interactions 28
  TCP/IP Internet Layer 29
    Internet Protocol and the Postal Service 29
    Internet Protocol Addressing Basics 31
    IP Routing Basics 32
  TCP/IP Network Access Layer 33
  TCP/IP Model and Terminology 34
    Comparing the Two TCP/IP Models 34
    Data Encapsulation Terminology 35
    Names of TCP/IP Messages 36
  OSI Networking Model 37
    Comparing OSI and TCP/IP 37
    Describing Protocols by Referencing the OSI Layers 38
    OSI Layers and Their Functions 39
    OSI Layering Concepts and Benefits 41
    OSI Encapsulation Terminology 42

Exam Preparation Tasks 43
  Review All the Key Topics 43
  Complete the Tables and Lists from Memory 43
  Definitions of Key Terms 43
  OSI Reference 44
Chapter 3  Fundamentals of LANs  47
“Do I Know This Already?” Quiz  47
Foundation Topics  51
An Overview of Modern Ethernet LANs  51
A Brief History of Ethernet  54
The Original Ethernet Standards: 10BASE2 and 10BASE5  54
Repeaters  56
Building 10BASE-T Networks with Hubs  57
Ethernet UTP Cabling  58
UTP Cables and RJ-45 Connectors  58
Transmitting Data Using Twisted Pairs  60
UTP Cabling Pinouts for 10BASE-T and 100BASE-TX  61
1000BASE-T Cabling  64
Improving Performance by Using Switches Instead of Hubs  64
Increasing Available Bandwidth Using Switches  67
Doubling Performance by Using Full-Duplex Ethernet  68
Ethernet Layer 1 Summary  69
Ethernet Data-Link Protocols  69
Ethernet Addressing  70
Ethernet Framing  71
Identifying the Data Inside an Ethernet Frame  73
Error Detection  74
Exam Preparation Tasks  75
Review All the Key Topics  75
Complete the Tables and Lists from Memory  75
Definitions of Key Terms  75
Chapter 4  Fundamentals of WANs  77
“Do I Know This Already?” Quiz  77
Foundation Topics  80
OSI Layer 1 for Point-to-Point WANs  80
WAN Connections from the Customer Viewpoint  83
WAN Cabling Standards  84
Clock Rates, Synchronization, DCE, and DTE  86
Building a WAN Link in a Lab  87
Link Speeds Offered by Telcos  88
OSI Layer 2 for Point-to-Point WANs  89
HDLC  89
Point-to-Point Protocol  91
Point-to-Point WAN Summary  91
Frame Relay and Packet-Switching Services  92
The Scaling Benefits of Packet Switching  92
Frame Relay Basics  93
Exam Preparation Tasks 97
Review All the Key Topics 97
Complete the Tables and Lists from Memory 97
Definitions of Key Terms 97

Chapter 5 Fundamentals of IPv4 Addressing and Routing 99
“Do I Know This Already?” Quiz 99
Foundation Topics 104
Overview of Network Layer Functions 104
Routing (Forwarding) 105
PC1’s Logic: Sending Data to a Nearby Router 106
R1 and R2’s Logic: Routing Data Across the Network 106
R3’s Logic: Delivering Data to the End Destination 106
Network Layer Interaction with the Data Link Layer 107
IP Packets and the IP Header 108
Network Layer (Layer 3) Addressing 109
Routing Protocols 110
IP Addressing 111
IP Addressing Definitions 111
How IP Addresses Are Grouped 112
Classes of Networks 113
The Actual Class A, B, and C Network Numbers 115
IP Subnetting 116
IP Routing 120
Host Routing 120
Router Forwarding Decisions and the IP Routing Table 121
IP Routing Protocols 124
Network Layer Utilities 127
Address Resolution Protocol and the Domain Name System 127
DNS Name Resolution 128
The ARP Process 128
Address Assignment and DHCP 129
ICMP Echo and the ping Command 131
Exam Preparation Tasks 132
Review All the Key Topics 132
Complete the Tables and Lists from Memory 133
Definitions of Key Terms 133

“Do I Know This Already?” Quiz 135
Foundation Topics 139
TCP/IP Layer 4 Protocols: TCP and UDP 139
Transmission Control Protocol 140
Multiplexing Using TCP Port Numbers 141
Popular TCP/IP Applications 144
Error Recovery (Reliability) 146
Flow Control Using Windowing 147
Connection Establishment and Termination 148
Data Segmentation and Ordered Data Transfer 150
User Datagram Protocol 151
TCP/IP Applications 152
QoS Needs and the Impact of TCP/IP Applications 152
The World Wide Web, HTTP, and SSL 155
Universal Resource Locators 156
Finding the Web Server Using DNS 156
Transferring Files with HTTP 158
Network Security 159
Perspectives on the Sources and Types of Threats 160
Firewalls and the Cisco Adaptive Security Appliance (ASA) 164
Anti-x 166
Intrusion Detection and Prevention 166
Virtual Private Networks (VPN) 167
Exam Preparation Tasks 169
Review All the Key Topics 169
Complete the Tables and Lists from Memory 169
Definitions of Key Terms 169

Part II: LAN Switching 171

Chapter 7 Ethernet LAN Switching Concepts 173
“Do I Know This Already?” Quiz 173

Foundation Topics 177
LAN Switching Concepts 177
Historical Progression: Hubs, Bridges, and Switches 177
Switching Logic 180
The Forward Versus Filter Decision 181
How Switches Learn MAC Addresses 183
Flooding Frames 184
Avoiding Loops Using Spanning Tree Protocol 185
Internal Processing on Cisco Switches 186
LAN Switching Summary 188

LAN Design Considerations 189
Collision Domains and Broadcast Domains 189
Collision Domains 189
Broadcast Domains 190
The Impact of Collision and Broadcast Domains on LAN Design 191
Virtual LANs (VLAN) 193
Campus LAN Design Terminology 194
Ethernet LAN Media and Cable Lengths 197
### Exam Preparation Tasks 200
- Review All the Key Topics 200
- Complete the Tables and Lists from Memory 200
- Definitions of Key Terms 201

### Chapter 8 Operating Cisco LAN Switches 203
- “Do I Know This Already?” Quiz 203

#### Foundation Topics 206
- Accessing the Cisco Catalyst 2960 Switch CLI 206
  - Cisco Catalyst Switches and the 2960 Switch 207
  - Switch Status from LEDs 208
- Accessing the Cisco IOS CLI 211
  - CLI Access from the Console 212
  - Accessing the CLI with Telnet and SSH 214
  - Password Security for CLI Access 214
- User and Enable (Privileged) Modes 216
- CLI Help Features 217
- The debug and show Commands 219

#### Configuring Cisco IOS Software 220
- Configuration Submodes and Contexts 221
- Storing Switch Configuration Files 223
- Copying and Erasing Configuration Files 226
- Initial Configuration (Setup Mode) 227

### Exam Preparation Tasks 232
- Review All the Key Topics 232
- Complete the Tables and Lists from Memory 232
- Definitions of Key Terms 232
- Command References 232

### Chapter 9 Ethernet Switch Configuration 237
- “Do I Know This Already?” Quiz 237

#### Foundation Topics 241
- Configuration of Features in Common with Routers 241
  - Securing the Switch CLI 241
    - Configuring Simple Password Security 242
    - Configuring Usernames and Secure Shell (SSH) 245
    - Password Encryption 248
    - The Two Enable Mode Passwords 250
- Console and vty Settings 251
  - Banners 251
  - History Buffer Commands 252
  - The logging synchronous and exec-timeout Commands 253

#### LAN Switch Configuration and Operation 254
- Configuring the Switch IP Address 254
- Configuring Switch Interfaces 257
Deploying WLANs 321

Wireless LAN Implementation Checklist 321

Step 1: Verify the Existing Wired Network 322
Step 2: Install and Configure the AP’s Wired and IP Details 323
Step 3: Configure the AP’s WLAN Details 323
Step 4: Install and Configure One Wireless Client 324
Step 5: Verify That the WLAN Works from the Client 325

Wireless LAN Security 326

WLAN Security Issues 326

The Progression of WLAN Security Standards 328

Wired Equivalent Privacy (WEP) 328
SSID Cloaking and MAC Filtering 329
The Cisco Interim Solution Between WEP and 802.11i 330
Wi-Fi Protected Access (WPA) 331
IEEE 802.11i and WPA-2 331

Exam Preparation Tasks 333

Review All the Key Topics 333
Complete the Tables and Lists from Memory 333
Definitions of Key Terms 333

Part III: IPv4 Addressing and Subnetting 335

Chapter 12 Perspectives on IPv4 Subnetting 337

“Do I Know This Already?” Quiz 337

Foundation Topics 340

Introduction to Subnetting 340

Subnetting Defined Through a Simple Example 340
Operational View Versus Design View of Subnetting 341

Analyze Subnetting and Addressing Needs 342

Rules About Which Hosts Are in Which Subnet 342
Determining the Number of Subnets 344
Determining the Number of Hosts per Subnet 345
One Size Subnet Fits All—or Not 346

Defining the Size of a Subnet 346
One Size Subnet Fits All 347

Multiple Subnet Sizes (Variable Length Subnet Masks) 348
This Book: One Size Subnet Fits All 349

Make Design Choices 349

Choose a Classful Network 350
Public IP Networks 350
Growth Exhausts the Public IP Address Space 351
Private IP Networks 352
Choosing an IP Network During the Design Phase 353
Choose the Mask 354
Classful IP Networks Before Subnetting 354
Borrowing Host Bits to Create Subnet Bits 355
Choosing Enough Subnet and Host Bits 355
Example Design: 172.16.0.0, 200 Subnets, 200 Hosts 357
Masks and Mask Formats 358
Build a List of All Subnets 359
Plan the Implementation 360
Assigning Subnets to Different Locations 361
Choose Static and Dynamic Ranges per Subnet 362

Exam Preparation Tasks 364
Review All the Key Topics 364
Complete the Tables and Lists from Memory 364
Definitions of Key Terms 364

Chapter 13 Analyzing Classful IPv4 Networks 367
“Do I Know This Already?” Quiz 367

Foundation Topics 369
Classful Network Concepts 369
IPv4 Network Classes and Related Facts 369
Actual Class A, B, and C Networks 370
Address Formats 371
Default Masks 372
Number of Hosts per Network 373
Deriving the Network ID and Related Numbers 373
Unusual Network IDs and Network Broadcast Addresses 375
Practice with Classful Networks 376
Practice Deriving Key Facts Based on an IP Address 377
Practice Remembering the Details of Address Classes 377
Additional Practice 378

Exam Preparation Tasks 379
Review All the Key Topics 379
Complete the Tables and Lists from Memory 379
Definitions of Key Terms 379
Practice 379
Answers to Earlier Practice Problems 380
Answers to Practice Problem 7 380
Answers to Practice Problem 8 381
Answers to Practice Problem 9 381

Chapter 14 Converting Subnet Masks 383
“Do I Know This Already?” Quiz 383

Foundation Topics 366
Subnet Mask Conversion 386
Three Mask Formats 386
Converting Between Binary and Prefix Masks 387
Converting Between Binary and DDN Masks 388
Converting Between Prefix and DDN Masks 390
Part IV: IPv4 Routing 479

Chapter 19 Operating Cisco Routers 481

“Do I Know This Already?” Quiz 481

Foundation Topics 485

Installing Cisco Routers 485

Installing Enterprise Routers 485

Cisco Integrated Services Routers 487

Physical Installation 488

Installing Internet Access Routers 489

A SOHO Installation with a Separate Switch, Router, and Cable Modem 489

A SOHO Installation with an Integrated Switch, Router, and DSL Modem 490

Regarding the SOHO Devices Used in This Book 491

Cisco Router IOS CLI 491

Comparisons Between the Switch CLI and Router CLI 492

Router Interfaces 493

Interface Status Codes 495

Router Interface IP Addresses 496

Bandwidth and Clock Rate on Serial Interfaces 497

Router Auxiliary (Aux) Port 499

Initial Configuration (Setup Mode) 499

Upgrading Cisco IOS Software and the Cisco IOS Software Boot Process 502

Upgrading a Cisco IOS Software Image into Flash Memory 502

The Cisco IOS Software Boot Sequence 505

The Three Router Operating Systems 507

The Configuration Register 507

How a Router Chooses Which OS to Load 508

The show version Command and Seeing the Configuration Register’s Value 511

Exam Preparation Tasks 513

Review All the Key Topics 513

Complete the Tables and Lists from Memory 513
Definitions of Key Terms 514
Read Appendix J Scenario 2 514
Command References 514

Chapter 20  Routing Protocol Concepts and Configuration 517
“Do I Know This Already?” Quiz 517
Foundation Topics 521
Connected and Static Routes 521
Connected Routes 521
Static Routes 524
Extended ping Command 526
Default Routes 528
Routing Protocol Overview 530
RIP-2 Basic Concepts 531
Comparing and Contrasting IP Routing Protocols 532
Interior and Exterior Routing Protocols 533
Routing Protocol Types/Algorithms 534
Metrics 534
Autosummarization and Manual Summarization 536
Classless and Classful Routing Protocols 536
Convergence 537
Miscellaneous Comparison Points 537
Summary of Interior Routing Protocols 537
Configuring and Verifying RIP-2 538
RIP-2 Configuration 538
Sample RIP Configuration 539
RIP-2 Verification 540
Interpreting the Output of the show ip route Command 542
Administrative Distance 543
The show ip protocols Command 544
Examining RIP Messages with debug 546

Exam Preparation Tasks 549
Review All the Key Topics 549
Complete the Tables and Lists from Memory 549
Definitions of Key Terms 550
Command References 550

Chapter 21  Troubleshooting IP Routing 553
“Do I Know This Already?” Quiz 553
Foundation Topics 557
IP Troubleshooting Tips and Tools 557
IP Addressing 557
Avoiding Reserved IP Addresses 557
One Subnet, One Mask, for Each LAN 558
Summary of IP Addressing Tips 560
Exam Preparation Tasks  618
Review All the Key Topics  618
Complete the Tables and Lists from Memory  618
Definitions of Key Terms  619

Chapter 23  WAN Configuration  621
“Do I Know This Already?” Quiz  621

Foundation Topics  624
Configuring Point-to-Point WANs  624
Configuring HDLC  624
Configuring PPP  627
Configuring and Troubleshooting Internet Access Routers  628
Internet Access Router: Configuration Steps  629
  Step 1: Establish IP Connectivity  629
  Step 2: Install and Access SDM  630
  Step 3: Configure DHCP and PAT  631
  Step 4: Plan for DHCP Services  636
  Step 5: Configure the DHCP Server  638
Internet Access Router Verification  639

Exam Preparation Tasks  642
Review All the Key Topics  642
Complete the Tables and Lists from Memory  642
Definitions of Key Terms  642
Command References  642

Part VI:  Final Preparation  645

Chapter 24  Final Preparation  647
Tools for Final Preparation  647
Pearson Cert Practice Test Engine and Questions on the DVD  647
Install the Software from the DVD  648
Activate and Download the Practice Exam  649
Activating Other Exams  649
Premium Edition  650
The Cisco Learning Network  650
Subnetting Preparation Tools  650
Scenarios  651
Study Plan  651
Recall the Facts  652
Practice Subnetting  652
Build Troubleshooting Skills Using Scenarios  654
Studying for ICND1  640-822 or CCNA  640-802  654
Summary  655
Part VII: Appendixes 657
Appendix A Answers to the “Do I Know This Already?” Quizzes 659
Appendix B Numeric Reference Tables 681
Appendix C ICND1 Exam Updates: Version 1.0 689
Glossary 693
Index 718

Part VIII: DVD-Only
Appendix D Practice for Chapter 13: Analyzing Classful IPv4 Networks
Appendix E Practice for Chapter 14: Converting Subnet Masks
Appendix F Practice for Chapter 15: Analyzing Existing Subnet Masks
Appendix G Practice for Chapter 16: Designing Subnet Masks
Appendix H Practice for Chapter 17: Analyzing Existing Subnets
Appendix I Practice for Chapter 18: Finding All Subnet IDs
Appendix J Additional Scenarios
Appendix K Subnetting Video Reference
Appendix L Memory Tables
Appendix M Memory Tables Answer Key
Appendix N ICND1 Open-Ended Questions
Icons Used in This Book

![Icons](image)

Command Syntax Conventions

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

- **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, were called INTRO and ICND.) 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 a more cost-effective certification path 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](image)

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 or the exam numbers. The previous editions (Editions 2, 2007) still work well and 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 ICND1 640-822 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 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 this new book, and the new library (that holds this book and the ICND2 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 re-written 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 re-organized 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 takes 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 24, “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 the Cisco website (www.cisco.com/go/ccna). If Cisco does happen to add exam topics at a later date, note that
Appendix C, “ICND1 Exam Updates: Version 1.0,” describes how to go to www.ciscopress.com and download additional information about those newly added topics.

### Table I-1  ICND1 Exam Topics

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Book Parts</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>Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network</td>
</tr>
<tr>
<td>4</td>
<td>I</td>
<td>Describe common networking applications including web applications</td>
</tr>
<tr>
<td>5</td>
<td>I</td>
<td>Describe the purpose and basic operation of the protocols in the OSI and TCP models</td>
</tr>
<tr>
<td>6</td>
<td>I</td>
<td>Describe the impact of applications (Voice over IP and Video over IP) on a network</td>
</tr>
<tr>
<td>7</td>
<td>I–V</td>
<td>Interpret network diagrams</td>
</tr>
<tr>
<td>8</td>
<td>I–V</td>
<td>Determine the path between two hosts across a network</td>
</tr>
<tr>
<td>9</td>
<td>I, III, IV, V</td>
<td>Describe the components required for network and Internet communications</td>
</tr>
<tr>
<td>10</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>11</td>
<td>II, III, IV</td>
<td>Differentiate between LAN/WAN operation and features</td>
</tr>
</tbody>
</table>

**Implement a small switched network**

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Book Parts</th>
<th>Exam Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</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>13</td>
<td>II</td>
<td>Explain the technology and media access control method for Ethernet technologies</td>
</tr>
<tr>
<td>14</td>
<td>II</td>
<td>Explain network segmentation and basic traffic management concepts</td>
</tr>
<tr>
<td>15</td>
<td>II</td>
<td>Explain the operation of Cisco switches and basic switching concepts</td>
</tr>
<tr>
<td>16</td>
<td>II</td>
<td>Perform, save, and verify initial switch configuration tasks including remote access management</td>
</tr>
<tr>
<td>17</td>
<td>II</td>
<td>Verify network status and switch operation using basic utilities (including ping, traceroute, telnet, SSH, arp, and ipconfig), <strong>show</strong> and <strong>debug</strong> commands</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>Reference Number</td>
<td>Book Parts</td>
<td>Exam Topic</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td>20</td>
<td>I, III</td>
<td>Implement an IP addressing scheme and IP services to meet network requirements for a small branch office</td>
</tr>
<tr>
<td>21</td>
<td>I, III</td>
<td>Describe the need and role of addressing in a network</td>
</tr>
<tr>
<td>22</td>
<td>III, IV</td>
<td>Create and apply an addressing scheme to a network</td>
</tr>
<tr>
<td>23</td>
<td>IV</td>
<td>Assign and verify valid IP addresses to hosts, servers, and networking devices in a LAN environment</td>
</tr>
<tr>
<td>24</td>
<td>I, IV</td>
<td>Explain the basic uses and operation of NAT in a small network connecting to one ISP</td>
</tr>
<tr>
<td>25</td>
<td>III</td>
<td>Describe the need and role of addressing in a network</td>
</tr>
<tr>
<td>26</td>
<td>III, V</td>
<td>Create and apply an addressing scheme to a network</td>
</tr>
<tr>
<td>27</td>
<td>IV</td>
<td>Assign and verify valid IP addresses to hosts, servers, and networking devices in a LAN environment</td>
</tr>
<tr>
<td>28</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>29</td>
<td>III</td>
<td>Describe and verify DNS operation</td>
</tr>
<tr>
<td>30</td>
<td>I, III, IV</td>
<td>Describe the operation and benefits of using private and public IP addressing</td>
</tr>
<tr>
<td>31</td>
<td>IV</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>32</td>
<td>IV</td>
<td>Configure, verify, and troubleshoot DHCP and DNS operation on a router (including CLI/SDM)</td>
</tr>
<tr>
<td>33</td>
<td>IV</td>
<td>Implement static and dynamic addressing services for hosts in a LAN environment</td>
</tr>
<tr>
<td>34</td>
<td>III</td>
<td>Identify and correct IP addressing issues</td>
</tr>
<tr>
<td>35</td>
<td>III</td>
<td>Implement a small routed network</td>
</tr>
<tr>
<td>36</td>
<td>III</td>
<td>Describe basic routing concepts (including packet forwarding, router lookup process)</td>
</tr>
<tr>
<td>37</td>
<td>IV</td>
<td>Describe the operation of Cisco routers (including router bootstrap process, POST, and router components)</td>
</tr>
<tr>
<td>38</td>
<td>IV</td>
<td>Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts</td>
</tr>
<tr>
<td>39</td>
<td>IV</td>
<td>Configure, verify, and troubleshoot RIPv2</td>
</tr>
<tr>
<td>40</td>
<td>IV</td>
<td>Access and utilize the router CLI to set basic parameters</td>
</tr>
<tr>
<td>41</td>
<td>IV</td>
<td>Connect, configure, and verify operation status of a device interface</td>
</tr>
<tr>
<td>42</td>
<td>IV</td>
<td>Verify device configuration and network connectivity using ping, traceroute, telnet, SSH, or other utilities</td>
</tr>
<tr>
<td>43</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>44</td>
<td>IV</td>
<td>Manage IOS configuration files (including save, edit, upgrade, and restore)</td>
</tr>
<tr>
<td>45</td>
<td>IV</td>
<td>Manage Cisco IOS</td>
</tr>
<tr>
<td>Reference Number</td>
<td>Book Parts</td>
<td>Exam Topic</td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</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, and ipconfig), <strong>show</strong> and <strong>debug</strong> 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, and 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, and 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, and 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>

Table I-1  *ICND1 Exam Topics (Continued)*
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 Cert Guide* in which each topic is covered.

Table I-2  ICND2 Exam Topics

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Book Part (ICND2 Book)</th>
<th>Exam Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Configure, verify and troubleshoot a switch with VLANs and interswitch communications</strong></td>
</tr>
<tr>
<td>101</td>
<td>I</td>
<td>Describe enhanced switching technologies (including VTP, RSTP, VLAN, PVSTP, and 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 <code>show</code> and <code>debug</code> 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></td>
<td></td>
<td><strong>Implement an IP addressing scheme and IP services to meet network requirements in a medium-sized enterprise branch office network</strong></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></td>
<td></td>
<td><strong>Configure and troubleshoot basic operation and routing on Cisco devices</strong></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>
</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.

Table I-2  ICND2 Exam Topics (Continued)

<table>
<thead>
<tr>
<th>Reference Number</th>
<th>Book Part (ICND2 Book)</th>
<th>Exam Topic</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>120</td>
<td>II, III, IV</td>
<td>Verify router hardware and software operation using show and debug commands</td>
</tr>
<tr>
<td>121</td>
<td>II</td>
<td>Implement basic router security</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Implement, verify, and troubleshoot NAT and ACLs in a medium-size enterprise branch office network</strong></td>
</tr>
<tr>
<td>122</td>
<td>II</td>
<td>Describe the purpose and types of access control lists</td>
</tr>
<tr>
<td>123</td>
<td>II</td>
<td>Configure and apply access control lists based on network filtering requirements</td>
</tr>
<tr>
<td>124</td>
<td>II</td>
<td>Configure and apply an access control list to limit telnet and SSH access to the router</td>
</tr>
<tr>
<td>125</td>
<td>II</td>
<td>Verify and monitor ACL’s in a network environment</td>
</tr>
<tr>
<td>126</td>
<td>II</td>
<td>Troubleshoot ACL implementation issues</td>
</tr>
<tr>
<td>127</td>
<td>V</td>
<td>Explain the basic operation of NAT</td>
</tr>
<tr>
<td>128</td>
<td>V</td>
<td>Configure Network Address Translation for given network requirements using CLI</td>
</tr>
<tr>
<td>129</td>
<td>V</td>
<td>Troubleshoot NAT implementation issues</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Implement and verify WAN links</strong></td>
</tr>
<tr>
<td>130</td>
<td>IV</td>
<td>Configure and verify Frame Relay on Cisco routers</td>
</tr>
<tr>
<td>131</td>
<td>IV</td>
<td>Troubleshoot WAN implementation issues</td>
</tr>
<tr>
<td>132</td>
<td>IV</td>
<td>Describe VPN technology (including importance, benefits, role, impact, and components)</td>
</tr>
<tr>
<td>133</td>
<td>IV</td>
<td>Configure and verify the PPP connection between Cisco routers</td>
</tr>
</tbody>
</table>

CCNA 640-802 Exam Topics
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 CCNA ICND2 Official Cert Guide. Both books have the same basic features, so if you are reading both this book and the ICND2 book, there is no need to read the Introduction to the second 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 ICND1 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 the following:
  
  — **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, allowing 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 ICND1 exams, as well as simulated CCNA exams, with the DVD and activation code included in this book. (You can take simulated ICND2 and CCNA exams with the DVD in the *CCNA ICND2 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.

- **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 *CCENT/CCNA ICND1 640-822 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 you how to calculate various facts about IP addressing and subnetting (in particular, using the shortcuts described in this book).

- **Subnetting practice**—The companion DVD contains six appendices (D through I) that correspond to Chapters 13 through 18, respectively. Each appendix contains a set of subnetting practice problems, with the answers, and with explanations of how the answers were found. This is a great resource to get ready to do subnetting well and fast.
DVD-based practice scenarios—Appendix J, “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/1587204258 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 http://www.ciscopress.com/series/series.asp?ser=2538752 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 ICND2 book, and links to the author’s CCENT Skills 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 24 core chapters—Chapters 1 through 24, with Chapter 24 including some summary materials and suggestions for how to approach the actual exams. Each core chapter covers a subset of the topics on the ICND1 exam. The core chapters are organized into sections. The core chapters cover the following topics:

Part I: Networking Fundamentals

Chapter 1, “Introduction to Computer Networking,” provides a basic introduction for those who are brand new to networking.

Chapter 2, “The TCP/IP and OSI Networking Models,” introduces the terminology surrounding two different networking architectures, namely Transmission Control Protocol/Internet Protocol (TCP/IP) and Open Systems Interconnection (OSI).

Chapter 3, “Fundamental of LANs,” covers the concepts and terms used for the most popular option for the data link layer for local-area networks (LAN), namely Ethernet.
Chapter 4, “Fundamentals of WANs,” covers the concepts and terms used for the most popular options for the data link layer for wide-area networks (WAN), including High-Level Data Link Control (HDLC), the Point-to-Point Protocol (PPP), and Frame Relay.

Chapter 5, “Fundamentals of IPv4 Addressing and Routing,” The Internet Protocol (IP) is the main network layer protocol for TCP/IP. This chapter introduces the basics of IP, including IP addressing and routing.

Chapter 6, “Fundamentals of TCP/IP Transport, Applications, and Security,” The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are the main transport layer protocols for TCP/IP. This chapter introduces the basics of TCP and UDP.

Part II: LAN Switching

Chapter 7, “Ethernet LAN Switching Concepts,” deepens and expands the introduction to LANs from Chapter 3, completing most of the conceptual materials for Ethernet in this book.

Chapter 8, “Operating Cisco LAN Switches,” explains how to access, examine, and configure Cisco Catalyst LAN switches.

Chapter 9, “Ethernet Switch Configuration,” shows how to configure a variety of switch features, including duplex and speed, port security, securing the CLI, and the switch IP address.

Chapter 10, “Ethernet Switch Troubleshooting,” focuses on how to tell if the switch is doing what it is supposed to be doing, mainly through the use of show commands.

Chapter 11, “Wireless LANs,” explains the basic operation concepts of wireless LANs, along with addressing some of the most common security concerns.

Part III: IPv4 Addressing and Subnetting

Chapter 12, “Perspectives on IPv4 Subnetting,” walks through the entire concept of subnetting, from starting with a Class A, B, or C network, analyzing requirements, making choices, calculating the resulting subnets, assigning those on paper, all in preparation to deploy and use those subnets by configuring the devices.

Chapter 13, “Analyzing Classful IPv4 Networks,” IPv4 addresses originally fell into several classes, with unicast IP addresses being in Class A, B, and C. This chapter explores all things related to address classes and the IP network concept created by those classes.
Chapter 14, “Converting Subnet Masks,” Math, and only the math, with subnet masks. Subnet masks come in three formats. This chapter discusses how to quickly and easily convert between the formats, so you can practice before having to think more about what the mask does in the next two chapters.

Chapter 15, “Analyzing Existing Subnet Masks,” In most jobs, someone else came before you and chose the subnet mask used in a network. What does that mean? What does that mask do for you? This chapter focuses on how to look at the mask (and IP network) to discover key facts, like the size of a subnet (number of hosts) and the number of subnets in the network.

Chapter 16, “Designing Subnet Masks,” reverses the approach from Chapter 15, looking at subnet masks from a design perspective. If you could pick a mask to use in a network, what mask would you choose? What questions should you be asking in order to make a good choice? This chapter explores the questions, and the math to solve the problems.

Chapter 17, “Analyzing Existing Subnets,” Most troubleshooting of IP connectivity problems starts with an IP address and mask. This chapter takes that paired information and shows you how to find and analyze the subnet in which that IP address resides, including finding the subnet ID, range of addresses in the subnet, and subnet broadcast address.

Chapter 18, “Finding All Subnet IDs,” As part of the subnet design process, someone chose a network number and a mask. Then someone calculated and wrote down all the subnet IDs implied by those choices. This chapter shows you how to do the same thing: how to find all those subnet IDs, given a network number and a single mask used throughout the network.

Part IV: IPv4 Routing

Chapter 19, “Operating Cisco Routers,” is like Chapter 8, but it focuses on routers instead of switches.

Chapter 20, “Routing Protocol Concepts and Configuration,” explains how routers work to find all the best routes to each subnet. This chapter also shows how to configure IP addresses, static routes, and one routing protocol: RIP Version 2.

Chapter 21, “Troubleshooting IP Routing,” discusses several tools useful when troubleshooting IP routing issues. This chapter also features a scenario that examines the IP packet forwarding process.
Part V: Wide-Area Networks

- **Chapter 22, “WAN Concepts,”** completes the conceptual materials for WANs for this book, continuing the coverage in Chapter 4, by touching on Internet access technologies like DSL and cable. It also covers the concepts of Network Address Translation (NAT).

- **Chapter 23, “WAN Configuration,”** completes the main technical topics of the book, focusing on a few small WAN configuration tasks, plus NAT configuration using Cisco Security Device Manager (SDM).

Part VI: Final Preparation

- **Chapter 24, “Final Preparation,”** suggests a plan for final preparation once 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 2 through 23.

- **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, “ICND1 Exam Updates: Version 1.0,”** covers a variety of short topics that either clarify or expand upon topics covered earlier in the 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 to see if a later version of Appendix C is available online.)

  http://www.pearsonitcertification.com/title/0132903822

- The **Glossary** contains definitions for all of the terms listed in the “Definitions of Key Terms” section at the conclusion of Chapters 1–23.

Part VIII: Appendices (on the DVD)

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

- **Appendix D, “Practice for Chapter 13: Analyzing Classful IPv4 Networks,”** lists practice problems associated with Chapter 13. In particular, the practice questions ask you to find the classful network number in which an address resides, and all other facts about that network.
Appendix E, “Practice for Chapter 14: Converting Subnet Masks,” lists practice problems associated with Chapter 14. In particular, the practice questions ask you to convert masks between the three formats.

Appendix F, “Practice for Chapter 15: Analyzing Existing Subnet Masks,” lists practice problems associated with Chapter 15. In particular, the practice questions ask you to examine an existing mask, determine the structure of the IP addresses, and calculate the number of hosts/subnet and number of subnets.

Appendix G, “Practice for Chapter 16: Designing Subnet Masks,” lists practice problems associated with Chapter 16. In particular, the practice questions ask you to examine a set of requirements, determine which mask (if any) meets those requirements, and choose the best mask based on the requirements.

Appendix H, “Practice for Chapter 17: Analyzing Existing Subnets,” lists practice problems associated with Chapter 17. In particular, the practice questions ask you to take an IP address and mask, and find the subnet ID, subnet broadcast address, and range of IP addresses in the subnet.

Appendix I, “Practice for Chapter 18: Finding All Subnet IDs,” lists practice problems associated with Chapter 18. In particular, the practice questions ask you to find all the subnet IDs in a classful network when given a single mask used throughout the network.

Appendix J, “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 K, “Video Reference”—The DVD includes several subnetting videos that show how to use the processes covered in Chapter 12. This appendix contains copies of the key elements from those videos, which may be useful when watching the videos (so you do not have to keep moving back and forth in the video).

Appendix L, “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 M, “Memory Tables Answer Key,” contains the answer key for the exercises in Appendix L.

Appendix N, “ICND1 Open-Ended Questions,” is a hold-over 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.
How to Use This Book to Prepare for the ICND1 and CCNA Exams

This book was designed with two primary goals in mind: to help you study for the ICND1 exam and to help you study for the CCNA exam by using both this book and the ICND2 Exam Certification Guide. Using this book to prepare for the ICND1 exam is pretty straight-forward: read each chapter in succession and follow the study suggestions in Chapter 24.

For the core chapters of this book (Chapters 1–23), 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.

When you complete Chapters 1–23, you can then use the guidance listed in Chapter 24 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 J.

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 CCNA ICND2 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 this book, and then move on to the ICND2 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 these two books.

![Figure I-3 Reading Plan When Studying for CCNA Exam](image-url)

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 as well. 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 20) of the ICND2
book instead of Chapter 24 of this book. Chapter 20 of ICND2 tells you about the same
basic activities as does this book’s Chapter 24, with reminders of any exam-prep materials
from this book that should be useful.

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 the ICND2 book. The ICND2
book does not review subnetting or the underlying math, assuming that you know how to
find the answers. Those ICND2 chapters, particularly Chapter 5, “Variable Length Subnet
Masks,” will be 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

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 **CCENT/CCNA ICND1 Official Cert Guide** helps you attain both CCENT and CCNA
certifications. This is the CCENT/CCNA ICND1 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.
The TCP/IP and OSI Networking Models

You can think of a networking model as you think of a set of architectural plans for building a house. Sure, you can build a house without the architectural plans, but it will work better if you follow the plans. And because you probably have a lot of different people working on building your house, such as framers, electricians, bricklayers, painters, and so on, it helps if they can all reference the same plan. Similarly, you could build your own network, write your own software, build your own networking cards, and create a network without using any existing networking model. However, it is much easier to simply buy and use products that already conform to some well-known networking model. Because the networking product vendors use the same networking model, their products should work well together.

The CCNA exams include detailed coverage of one networking model: Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP is the most pervasively used networking model in the history of networking. You can find support for TCP/IP on practically every computer operating system (OS) in existence today, from mobile phones to mainframe computers. Every network built using Cisco products today supports TCP/IP. And not surprisingly, the CCNA exams focus heavily on TCP/IP.

The ICND1 exam, and the ICND2 exam to a small extent, also covers a second networking model, called the Open System Interconnection (OSI) reference model. Historically, OSI was the first large effort to create a vendor-neutral networking model. Because of that timing, many of the terms used in networking today come from the OSI model, so this chapter’s section on OSI discusses OSI and the related terminology.

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz allows you to assess if you should read the entire chapter. If you miss no more than one of these ten self-assessment questions, you might want to move ahead to the “Exam Preparation Tasks” section. Table 2-1 lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so 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 2-1  Do I Know This Already?  Foundation Topics Section-to-Question Mapping

<table>
<thead>
<tr>
<th>Foundation Topics Section</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/IP Networking Model</td>
<td>1–6</td>
</tr>
<tr>
<td>OSI Networking Model</td>
<td>7–10</td>
</tr>
</tbody>
</table>

1. Which of the following protocols are examples of TCP/IP transport layer protocols? (Choose two answers.)
   a. Ethernet
   b. HTTP
   c. IP
   d. UDP
   e. SMTP
   f. TCP

2. Which of the following protocols are examples of TCP/IP network access layer protocols? (Choose two answers.)
   a. Ethernet
   b. HTTP
   c. IP
   d. UDP
   e. SMTP
   f. TCP
   g. PPP

3. The process of HTTP asking TCP to send some data and making sure that it is received correctly is an example of what?
   a. Same-layer interaction
   b. Adjacent-layer interaction
   c. OSI model
   d. All of these answers are correct.
4. The process of TCP on one computer marking a TCP segment as segment 1, and the receiving computer then acknowledging the receipt of TCP segment 1 is an example of what?
   a. Data encapsulation
   b. Same-layer interaction
   c. Adjacent-layer interaction
   d. OSI model
   e. All of these answers are correct.

5. The process of a web server adding a TCP header to the contents of a web page, followed by adding an IP header, and then adding a data link header and trailer is an example of what?
   a. Data encapsulation
   b. Same-layer interaction
   c. OSI model
   d. All of these answers are correct.

6. Which of the following terms is used specifically to identify the entity created when encapsulating data inside data link layer headers and trailers?
   a. Data
   b. Chunk
   c. Segment
   d. Frame
   e. Packet
   f. None of these—there is no encapsulation by the data link layer.

7. Which OSI layer defines the functions of logical network-wide addressing and routing?
   a. Layer 1
   b. Layer 2
   c. Layer 3
   d. Layer 4
   e. Layer 5
   f. Layer 6
   g. Layer 7
8. Which OSI layer defines the standards for cabling and connectors?
   a. Layer 1
   b. Layer 2
   c. Layer 3
   d. Layer 4
   e. Layer 5
   f. Layer 6
   g. Layer 7

9. Which OSI layer defines the standards for data formats and encryption?
   a. Layer 1
   b. Layer 2
   c. Layer 3
   d. Layer 4
   e. Layer 5
   f. Layer 6
   g. Layer 7

10. Which of the following terms are not valid terms for the names of the seven OSI layers? (Choose two answers.)
   a. Application
   b. Data link
   c. Transmission
   d. Presentation
   e. Internet
   f. Session
TCP/IP Networking Model

A networking model, sometimes also called either a networking architecture or networking blueprint, refers to a comprehensive set of documents. Individually, each document describes one small function required for a network; collectively, these documents define everything that should happen for a computer network to work. Some documents define a protocol, which is a set of logical rules that devices must follow to communicate. Other documents define some physical requirements for networking. For example, a document could define the voltage and current levels used on a particular cable when transmitting data.

You can think of a networking model as you think of an architectural blueprint for building a house. Sure, you can build a house without the blueprint. However, the blueprint can ensure that the house has the right foundation and structure so it will not fall down, and it has the correct hidden spaces to accommodate the plumbing, electrical, gas, and so on. Also, the many different people that build the house using the blueprint—such as framers, electricians, bricklayers, painters, and so on—know that if they follow the blueprint, their part of the work should not cause problems for the other workers.

Similarly, you could build your own network—write your own software, build your own networking cards, and so on—to create a network. However, it is much easier to simply buy and use products that already conform to some well-known networking model or blueprint. Because the networking product vendors build their products with some networking model in mind, their products should work well together.

History Leading to TCP/IP

Today, the world of computer networking uses one networking model: TCP/IP (Transmission Control Protocol / Internet Protocol). However, the world has not always been so simple. Once upon a time, there were no networking protocols, including TCP/IP. Vendors created the first networking protocols; these protocols supported only that vendor’s computers. For instance, IBM published its Systems Network Architecture (SNA) networking model in 1974. Other vendors also created their own proprietary networking models. As a result, if your company bought computers from three vendors, network engineers often had to create three different networks based on the networking models created by each company, and then somehow connect those networks, making the combined networks much more complex. The left side of Figure 2-1 shows the general idea of what a company’s enterprise network might have looked back in the 1980s, before TCP/IP became common in enterprise internetworks.
Although vendor-defined proprietary networking models often worked well, having an open, vendor-neutral networking model would aid competition and reduce complexity. The International Organization for Standardization (ISO) took on the task to create such a model, starting as early as the late 1970s, beginning work on what would become known as the Open System Interconnection (OSI) networking model. ISO had a noble goal for the OSI model: to standardize data networking protocols to allow communication between all computers across the entire planet. ISO worked toward this ambitious and noble goal, with participants from most of the technologically developed nations on Earth participating in the process.

A second, less formal effort to create an open, vendor-neutral, public networking model sprouted forth from a U.S. Department of Defense (DoD) contract. Researchers at various universities volunteered to help further develop the protocols surrounding the original DoD work. These efforts resulted in a competing open networking model called TCP/IP.

During the 1990s, companies began adding OSI, TCP/IP, or both to their enterprise networks. However, by the end of the 1990s, TCP/IP had become the common choice, and OSI fell away. The center part of Figure 2-1 shows the general idea behind enterprise networks in that decade—still with networks built upon multiple networking models, but including TCP/IP.

Here in the 21st century, TCP/IP dominates. Proprietary networking models still exist, but they have mostly been discarded in favor of TCP/IP. The OSI model, whose development suffered in part because of a slower formal standardization process as compared with TCP/IP, never succeeded in the marketplace. And TCP/IP, the networking model originally created almost entirely by a bunch of volunteers, has become the most prolific network model ever, as shown on the right side of Figure 2-1.
In this chapter, you will read about some of the basics of TCP/IP. Although you will learn some interesting facts about TCP/IP, the true goal of this chapter is to help you understand what a networking model or networking architecture really is and how it works.

Also in this chapter, you will learn about some of the jargon used with OSI. Will any of you ever work on a computer that is using the full OSI protocols instead of TCP/IP? Probably not. However, you will often use terms relating to OSI. Also, the ICND1 exam covers the basics of OSI, so this chapter also covers OSI to prepare you for questions about it on the exam.

**Overview of the TCP/IP Networking Model**

The TCP/IP model both defines and references a large collection of protocols that allow computers to communicate. To define a protocol, TCP/IP uses documents called Requests for Comments (RFC). (You can find these RFCs using any online search engine.) The TCP/IP model also avoids repeating work already done by some other standards body or vendor consortium by simply referring to standards or protocols created by those groups. For example, the Institute of Electrical and Electronic Engineers (IEEE) defines Ethernet LANs; the TCP/IP model does not define Ethernet in RFCs, but refers to IEEE Ethernet as an option.

An easy comparison can be made between telephones and computers that use TCP/IP. You go to the store and buy a phone from one of a dozen different vendors. When you get home and plug in the phone to the same cable in which your old phone was connected, the new phone works. The phone vendors know the standards for phones in their country and build their phones to match those standards.

Similarly, when you buy a new computer today, it implements the TCP/IP model to the point that you can usually take the computer out of the box, plug in all the right cables, turn it on, and it connects to the network. You can use a web browser to connect to your favorite website. How? Well, the OS on the computer implements parts of the TCP/IP model. The Ethernet card, or wireless LAN card, built into the computer implements some LAN standards referenced by the TCP/IP model. In short, the vendors that created the hardware and software implemented TCP/IP.

To help people understand a networking model, each model breaks the functions into a small number of categories called *layers*. Each layer includes protocols and standards that relate to that category of functions. TCP/IP actually has two alternative models, as shown in Figure 2-2.
The two TCP/IP Networking Models

The model on the left, the original TCP/IP model, breaks TCP/IP into four layers. The top layers focus more on the applications that need to send and receive data, whereas the lower layers focus more on the need to somehow transmit the bits from one device to another. The model on the right is a newer version of the model, formed by expanding the network access layer on the left into two separate layers: data link and physical. Note that the model on the right is used more often today.

Many of you will have already heard of several TCP/IP protocols, like the examples listed in Table 2-2. Most of the protocols and standards in this table will be explained in more detail as you work through this book. Following the table, this section takes a closer look at the layers of the TCP/IP model.

<table>
<thead>
<tr>
<th>TCP/IP Architectural Layer</th>
<th>Example Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>HTTP, POP3, SMTP</td>
</tr>
<tr>
<td>Transport</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td>Internet</td>
<td>IP</td>
</tr>
<tr>
<td>Network Access</td>
<td>Ethernet, Point-to-Point Protocol (PPP), T/1</td>
</tr>
</tbody>
</table>

TCP/IP Application Layer

TCP/IP application layer protocols provide services to the application software running on a computer. The application layer does not define the application itself, but it defines services that applications need. For example, application protocol HTTP defines how web browsers can pull the contents of a web page from a web server. In short, the application layer provides an interface between software running on a computer and the network itself.
Arguably, the most popular TCP/IP application today is the web browser. Many major software vendors either have already changed or are changing their application software to support access from a web browser. And thankfully, using a web browser is easy: you start a web browser on your computer and select a website by typing the name of the website, and the web page appears.

HTTP Overview

What really happens to allow that web page to appear on your web browser?

Imagine that Bob opens his browser. His browser has been configured to automatically ask for web server Larry’s default web page, or home page. The general logic looks like Figure 2-3.

Figure 2-3  Basic Application Logic to Get a Web Page

So, what really happened? Bob’s initial request actually asks Larry to send his home page back to Bob. Larry’s web server software has been configured to know that the default web page is contained in a file called home.htm. Bob receives the file from Larry and displays the contents of the file in the web-browser window.

HTTP Protocol Mechanisms

Taking a closer look, this example shows how applications on each endpoint computer—specifically, the web-browser application and web-server application—use a TCP/IP application layer protocol. To make the request for a web page and return the contents of the web page, the applications use the Hypertext Transfer Protocol (HTTP).

HTTP did not exist until the Tim Berners-Lee created the first web browser and web server in the early 1990s. Berners-Lee gave HTTP functions to ask for the contents of web pages, specifically by giving the web browser the ability to request files from the server, and giving the server a way to return the content of those files. The overall logic matches what was shown in Figure 2-3; Figure 2-4 shows the same idea, but with details specific to HTTP.
The full version of most web addresses—also called universal resource locators (URL)—begin with the letters “http,” which means that HTTP is used to transfer the web pages.

Figure 2-4  HTTP Get Request, HTTP Reply, and One Data-Only Message

To get the web page from Larry, at Step 1, Bob sends a message with an HTTP header. Generally, protocols use headers as a place to put information used by that protocol. This HTTP header includes the request to “get” a file. The request typically contains the name of the file (home.htm, in this case), or, if no filename is mentioned, the web server assumes that Bob wants the default web page.

Step 2 in Figure 2-4 shows the response from web server Larry. The message begins with an HTTP header, with a return code (200), which means something as simple as “OK” returned in the header. HTTP also defines other return codes, so the server can tell the browser whether the request worked or not. (As another example: If you ever looked for a web page that was not found, and then received an HTTP 404 “not found” error, you received an HTTP return code of 404.) The second message also includes the first part of the requested file.

Step 3 in Figure 2-4 shows another message from web server Larry to web browser Bob, but this time without an HTTP header. HTTP transfers the data by sending multiple messages, each with a part of the file. Rather than wasting space by sending repeated HTTP headers that list the same information, these additional messages simply omit the header.

TCP/IP Transport Layer

Although many TCP/IP application layer protocols exist, the TCP/IP transport layer includes a smaller number of protocols. The two most commonly used transport layer
protocols are the *Transmission Control Protocol* (TCP) and the *User Datagram Protocol* (UDP).

Transport layer protocols provide services to the application layer protocols that reside one layer higher in the TCP/IP model. How does a transport layer protocol provide a service to a higher layer protocol? This section introduces that general concept by focusing on a single service provided by TCP: error recovery. Later chapters examine the transport layer in more detail, and discuss more functions of the transport layer.

**TCP Error Recovery Basics**

To appreciate what the transport layer protocols do, you must think about the layer above the transport layer, the application layer. Why? Well, each layer provides a service to the layer above it, like the error-recovery service provided to application layer protocols by TCP.

For example, in Figure 2-3, Bob and Larry used HTTP to transfer the home page from web server Larry to Bob’s web browser. But what would have happened if Bob’s HTTP GET request had been lost in transit through the TCP/IP network? Or, what would have happened if Larry’s response, which included the contents of the home page, had been lost? Well, as you might expect, in either case, the page would not have shown up in Bob’s browser.

TCP/IP needs a mechanism to guarantee delivery of data across a network. Because many application layer protocols probably want a way to guarantee delivery of data across a network, the creators of TCP included an error recovery feature. To recover from errors, TCP uses the concept of acknowledgments. Figure 2-5 outlines the basic idea behind how TCP notices lost data and asks the sender to try again.

**Figure 2-5  TCP Error Recovery Services as Provided to HTTP**
Figure 2-5 shows web server Larry sending a web page to web browser Bob, using three separate messages. Note that this figure shows the same HTTP headers as Figure 2-4, but it also shows a TCP header. The TCP header shows a sequence number (SEQ) with each message. In this example, the network has some problem so that the network fails to deliver the segment with sequence number 2. When Bob receives messages with sequence numbers 1 and 3, but does not receive a message with sequence number 2, Bob realizes that message 2 was lost. That realization by Bob’s TCP logic causes Bob to send a TCP segment back to Larry, asking Larry to send message 2 again.

**Same Layer and Adjacent Layer Interactions**

The example in Figure 2-4 also demonstrates a function called *adjacent-layer interaction*, which refers to the concepts of how adjacent layers in a networking model, on the same computer, work together. In this example, the higher-layer protocol (HTTP) needs to do something it cannot do (error recovery). The higher layer asks for the next lower-layer protocol (TCP) to perform the service; the lower layer provides a service to the layer above it.

Figure 2-4 also shows an example of a similar function called *same-layer interaction*. When a particular layer on one computer wants to communicate with the same layer on another computer, the two computers use headers to hold the information that they want to communicate. For example, in Figure 2-4, Larry set the sequence numbers to 1, 2, and 3, so that Bob could notice when some of the data did not arrive. Larry’s TCP process created that TCP header with the sequence number; Bob’s TCP process received and reacted to the TCP segments. This process through which two computers set and interpret the information in the header used by that layer is called *same-layer interaction*, and it occurs between different computers.

Table 2-3 summarizes the key points about how adjacent layers work together on a single computer and how one layer on one computer works with the same networking layer on another computer.

<table>
<thead>
<tr>
<th>Concept</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same-layer interaction on different computers</td>
<td>The two computers use a protocol to communicate with the same layer on another computer. The protocol defined by each layer uses a header that is transmitted between the computers to communicate what each computer wants to do.</td>
</tr>
<tr>
<td>Adjacent-layer interaction on the same computer</td>
<td>On a single computer, one layer provides a service to a higher layer. The software or hardware that implements the higher layer requests that the next lower layer perform the needed function.</td>
</tr>
</tbody>
</table>
TCP/IP Internet Layer
The application layer includes many protocols. The transport layer includes fewer, most notably, TCP and UDP. The TCP/IP Internet layer includes a small number of protocols, but only one major protocol: the Internet Protocol (IP). In fact, the name TCP/IP is simply the names of the two most common protocols (TCP and IP) separated by a /.

IP provides several features, most importantly, addressing and routing. This section begins by comparing IP’s addressing and routing with another commonly known system that uses addressing and routing: the postal service. Following that, this section introduces IP addressing and routing. (More details follow in Chapter 5, “Fundamentals of IPv4 Addressing and Routing.”)

Internet Protocol and the Postal Service
Imagine that you just wrote two letters: one to a friend on the other side of the country and one to a friend on the other side of town. You addressed the envelopes and put on the stamps, so both are ready to give to the postal service. Is there much difference in how you treat each letter? Not really. Typically, you would just put them in the same mailbox, and expect the postal service to deliver both letters.

The postal service, however, must think about each letter separately, and then make a decision of where to send each letter so it is delivered. For the letter sent across town, the people in the local post office probably just need to put the letter on another truck.

For the letter that needs to go across the country, the postal service sends the letter to another post office, then another, and so on, until the letter gets delivered across the country. At each post office, the postal service must process the letter and choose where to send it next.

To make it all work, the postal service has regular routes for small trucks, large trucks, planes, boats, and so on, to move letters between postal service sites. The service must be able to receive and forward the letters, and it must make good decisions about where to send each letter next, as shown in Figure 2-6.

Still thinking about the postal service, consider the difference between the person sending the letter and the work that the postal service does. The person sending the letters expects that the postal service will deliver the letter most of the time. However, the person sending the letter does not need to know the details of exactly what path the letters take. In contrast, the postal service does not create the letter, but they accept the letter from the customer. Then, the postal service must know the details about addresses, postal codes that group addresses into larger groups, and it must have the ability to deliver the letters.
The TCP/IP application and transport layers act like the person sending letters through the postal service. These upper layers work the same way regardless of whether the endpoint host computers are on the same LAN or are separated by the entire Internet. To send a message, these upper layers ask the layer below them, the Internet layer, to deliver the message.

The lower layers of the TCP/IP model, the Internet layer and the network access layer, act more like the postal service to deliver those messages to the correct destinations. To do so, these lower layers must understand the underlying physical network because they must choose how to best deliver the data from one host to another.

So, what does this all matter to networking? Well, the Internet layer of the TCP/IP networking model, primarily defined by the Internet Protocol (IP), works much like the postal service. IP defines addresses so that each host computer can have a different IP address, just as the postal service defines addressing that allows unique addresses for each house, apartment, and business. Similarly, IP defines the process of routing so that devices called routers can work like the post office to forward packets of data so that they are delivered to the correct destinations. Just as the postal service created the necessary infrastructure to be able to deliver letters—post offices, sorting machines, trucks, planes, and personnel—the Internet layer defines the details of how a network infrastructure should be created so that the network can deliver data to all computers in the network.
Internet Protocol Addressing Basics

IP defines addresses for several important reasons. First, each device that uses TCP/IP—each TCP/IP host—needs a unique address so that it can be identified in the network. IP also defines how to group addresses together, just like the postal system groups addresses based on postal codes (like ZIP codes in the U.S.).

To understand the basics, examine Figure 2-7, which shows the familiar web server Larry and web browser Bob; but now, instead of ignoring the network between these two computers, part of the network infrastructure is included.

![Simple TCP/IP Network: Three Routers with IP Addresses Grouped](image)

First, note that Figure 2-7 shows some sample IP addresses. Each IP address has four numbers, separated by periods. In this case, Larry uses IP address 1.1.1.1, and Bob uses 2.2.2.2. This style of number is called a **dotted-decimal notation** (DDN).

Figure 2-7 also shows three groups of address. In this example, all IP address that begin with 1 must be on the upper left, as shown in shorthand in the figure as 1.__.__.__. All addresses that begin with 2 must be on the right, as shown in shorthand as 2.__.__.__. Finally, all IP addresses that begin with 3 must be on the bottom of the figure.

Additionally, Figure 2-7 also introduces icons that represent IP routers. Routers are networking devices that connect the parts of the TCP/IP network together for the purpose of routing (forwarding) IP packets to the correct destination. Routers do the equivalent of the work done by each post office site: they receive IP packets on various physical interfaces, make decisions based on the IP address included with the packet, and then physically forward the packet out some other network interface.
IP Routing Basics

The TCP/IP Internet layer, using the IP protocol, provides a service of forwarding IP packets from one device to another. Any device with an IP address can connect to the TCP/IP network and send packets. This section shows a basic IP routing example for perspective.

**NOTE** The term *IP host* refers to any device, regardless of size or power, that has an IP address and connects to any TCP/IP network.

Figure 2-8 repeats the familiar case in which web server Larry wants to send part of a web page to Bob, but now with details related to IP. On the lower left, note that server Larry has the familiar application data, HTTP header, and TCP header ready to send. Additionally, the message now also contains an IP header. The IP header includes a source IP address of Larry’s IP (1.1.1.1) and a destination IP address of Bob’s IP address (2.2.2.2).

**Figure 2-8 Basic Routing Example**

Step 1, on the left of Figure 2-8, begins with Larry being ready to send an IP packet. Larry’s IP process chooses to send the packet to some router—a nearby router on the same LAN—with the expectation that the router will know how to forward the packet. (This logic is much like you or me sending all of our letters by putting them in a nearby post office box.) Larry doesn’t need to know anything more about the topology or the other routers.

At Step 2, router R1 receives the IP packet, and R1’s IP process makes a decision. R1 looks at the destination address (2.2.2.2), compares that address to its known IP routes, and chooses to forward the packet to router R2. This process of forwarding the IP packet is called *IP routing* (or simply *routing*).

At Step 3, router R2 repeats the same kind of logic used by router R1. R2’s IP process will compare the packet’s destination IP address (2.2.2.2) to R2’s known IP routes and make a choice to forward the packet to the right, on to Bob.
All the CCNA exams cover IP fairly deeply. Practically half the chapters in this book discuss some feature that relates to addressing, IP routing, and how routers perform routing.

**TCP/IP Network Access Layer**

The TCP/IP model’s network access layer defines the protocols and hardware required to deliver data across some physical network. The term *network access* refers to the fact that this layer defines how to access or use the physical media over which data can be transmitted.

Just like every layer in any networking model, the TCP/IP network access layer provides services to the layer above it in the model. When a host or router’s IP process chooses to send an IP packet to another router or host, that host or router then uses network access layer details to send that packet to the next host/router.

Because each layer provides a service to the layer above it, take a moment to think about the IP logic related to Figure 2-8. In that example, host Larry’s IP logic chooses to send the IP packet to a nearby router (R1), with no mention of the underlying Ethernet. The Ethernet network, which implements access layer protocols, must then be used to deliver that packet from host Larry over to router R1. Figure 2-9 shows four steps of what occurs at the network access layer to allow Larry to send the IP packet to R1.

**NOTE** Figure 2-9 depicts the Ethernet as a series of lines. Networking diagrams often use this convention when drawing Ethernet LANs, in cases where the actual LAN cabling and LAN devices are not important to some discussion, as is the case here. The LAN would have cables and devices, like LAN switches, which are not shown in this figure.

![Figure 2-9](image-url) **Larry Using Ethernet to Forward an IP Packet to Router R1**
Figure 2-9 shows four steps. The first two occur on Larry, and the last two occur on router R1, as follows:

**Step 1** Larry encapsulates the IP packet between an Ethernet header and Ethernet trailer, creating an Ethernet *frame*.

**Step 2** Larry physically transmits the bits of this Ethernet frame, using electricity flowing over the Ethernet cabling.

**Step 3** Router R1 physically receives the electrical signal over a cable, and recreates the same bits by interpreting the meaning of the electrical signals.

**Step 4** Router R1 de-encapsulates the IP packet from the Ethernet frame by removing and discarding the Ethernet header and trailer.

By the end of this process, the network access processes on Larry and R1 have worked together to deliver the packet from Larry to router R1.

**NOTE** Protocols define both headers and trailers for the same general reason, but headers exist at the beginning of the message, and trailers exist at the end.

The network access layer includes a large number of protocols and standards. For instance, the network access layer includes all the variations of Ethernet protocols, along with several other LAN standards that were more popular in decades past. The network access layer includes WAN standards for different physical media, which differ significantly compared to LAN standards because of the longer distances involved in transmitting the data. This layer also includes the popular WAN standards that add headers and trailers as shown generally in Figure 2-7, protocols such as the Point-to-Point Protocol (PPP) and Frame Relay. Chapter 3, “Fundamentals of LANs,” and Chapter 4, “Fundamentals of WANs,” further develop these topics for LAN and WAN, respectively.

In short, the TCP/IP network access layer includes two distinct functions: functions related to the physical transmission of the data, plus the protocols and rules that control the use of the physical media. The five layer TCP/IP model simply splits out the network access layer into two layers (Data Link and Physical) to match this logic.

### TCP/IP Model and Terminology

**Before completing this introduction to the TCP/IP model, this section examines a few remaining details of the model and some related terminology.**

### Comparing the Two TCP/IP Models

The functions defined in the network access layer can be broken into two major categories: functions related directly to the physical transmission of data and those only indirectly
related to the physical transmission of data. For instance, in the four steps shown around Figure 2-9, Steps 2 and 3 were specific to sending the data, but Steps 1 and 4—encapsulation and de-encapsulation—were only indirectly related. This division will become clearer as you read about additional details of each protocol and standard.

The two alternative TCP/IP models exist. Comparing the two, the upper layers are identical. The lower layers differ in that the single network access layer in one model is split into two layers to match the division of physical transmission details from the other functions. Figure 2-10 shows the two models again, with emphasis on these distinctions.

**Data Encapsulation Terminology**

As you can see from the explanations of how HTTP, TCP, IP, and Ethernet do their jobs, each layer adds its own header (and sometimes trailer) to the data supplied by the higher layer. The term *encapsulation* refers to the process of putting headers (and sometimes trailers) around some data.

Many of the examples in this chapter show the encapsulation process. For instance, web server Larry encapsulated the contents of the home page inside an HTTP header in Figure 2-4. The TCP layer encapsulated the HTTP headers and data inside a TCP header in Figure 2-5. IP encapsulated the TCP headers and the data inside an IP header in Figure 2-7. Finally, the Ethernet network access layer encapsulated the IP packets inside both a header and a trailer in Figure 2-9.

The process by which a TCP/IP host sends data can be viewed as a five-step process. The first four steps relate to the encapsulation performed by the four TCP/IP layers, and the last step is the actual physical transmission of the data by the host. In fact, if you use the
five-layer TCP/IP model, one step corresponds to the role of each layer. The steps are summarized in the following list:

**Step 1** Create and encapsulate the application data with any required application layer headers. For example, the HTTP OK message can be returned in an HTTP header, followed by part of the contents of a web page.

**Step 2** Encapsulate the data supplied by the application layer inside a transport layer header. For end-user applications, a TCP or UDP header is typically used.

**Step 3** Encapsulate the data supplied by the transport layer inside an Internet layer (IP) header. IP defines the IP addresses that uniquely identify each computer.

**Step 4** Encapsulate the data supplied by the Internet layer inside a data link layer header and trailer. This is the only layer that uses both a header and a trailer.

**Step 5** Transmit the bits. The physical layer encodes a signal onto the medium to transmit the frame.

The numbers in Figure 2-11 correspond to the five steps in this list, graphically showing the same concepts. Note that because the application layer often does not need to add a header, the figure does not show a specific application layer header.

**Figure 2-11  Five Steps of Data Encapsulation: TCP/IP**

**Names of TCP/IP Messages**

Finally, take particular care to remember the terms segment, packet, and frame, and the meaning of each. Each term refers to the headers and possibly trailers defined by a particular layer, and the data encapsulated following that header. Each term, however, refers
to a different layer: segment for the transport layer, packet for the Internet layer, and frame for the network access layer. Figure 2-12 shows each layer along with the associated term.

**Figure 2-12**  
*Perspectives on Encapsulation and “Data”*

```
+----------------+  +----------------+  +----------------+
| TCP  | Data | Segment         |
| IP   | Data | Packet          |
| LH   | Data | Frame           |
| LT   |      |                 |
```

*The letters LH and LT stand for link header and link trailer, respectively, and refer to the data link layer header and trailer.*

Figure 2-12 also shows the encapsulated data as simply “data.” When focusing on the work done by a particular layer, the encapsulated data typically is unimportant. For example, an IP packet may indeed have a TCP header after the IP header, an HTTP header after the TCP header, and data for a web page after the HTTP header. However, when discussing IP, you probably just care about the IP header, so everything after the IP header is just called “data.” So, when drawing IP packets, everything after the IP header is typically shown simply as “data.”

**OSI Networking Model**

At one point in the history of the OSI model, many people thought OSI would win the battle of the networking models discussed earlier. If that had occurred, instead of running TCP/IP on every computer in the world, those computers would be running with OSI.

However, OSI did not win that battle. In fact, OSI no longer exists as a networking model that could be used instead of TCP/IP, although some of the original protocols referenced by the OSI model still exist.

So, why is OSI even in this book? Terminology. During those years in which many people thought the OSI model would become commonplace in the world of networking (mostly in the late 1980s and early 1990s), many vendors and protocol documents started using terminology from the OSI model. That terminology remains today. So, while you will never need to work with a computer that uses OSI, to understand modern networking terminology, you need to understand something about OSI.

**Comparing OSI and TCP/IP**

The OSI model has many similarities to the TCP/IP model from a basic conceptual perspective. It has (seven) layers, and each layer defines a set of typical networking
functions. As with TCP/IP, the OSI layers each refer to multiple protocols and standards that implement the functions specified by each layer. In other cases, just as for TCP/IP, the OSI committees did not create new protocols or standards, but instead referenced other protocols that were already defined. For instance, the IEEE defines Ethernet standards, so the OSI committees did not waste time specifying a new type of Ethernet; it simply referred to the IEEE Ethernet standards.

Today, the OSI model can be used as a standard of comparison to other networking models. Figure 2-13 compares the seven-layer OSI model with both the four-layer and five-layer TCP/IP models.

![Figure 2-13 OSI Model Compared to the Two TCP/IP Models](image)

Next, this section will examine two ways in which we still use OSI terminology today: to describe other protocols and to describe the encapsulation process. Along the way, the text will briefly examine each layer of the OSI model.

**Describing Protocols by Referencing the OSI Layers**

Even today, networking documents often describe TCP/IP protocols and standards by referencing OSI layers, both by layer number and layer name. For instance, a common description of a LAN switch is “layer 2 switch,” with “layer 2” referring to OSI layer 2. Because OSI did have a well-defined set of functions associated with each of its seven layers, if you know those functions, you can understand what people mean when they refer to a product or function by its OSI layer.

For another example, TCP/IP’s Internet layer, as implemented mainly by IP, equates most directly to the OSI network layer. So, most people say that IP is a network layer protocol, or a Layer 3 protocol, using OSI terminology and numbers for the layer. Of course, if you numbered the TCP/IP model, starting at the bottom, IP would be either Layer 2 or 3, depending on what version of the TCP/IP model you care to use. However, even though IP is a TCP/IP protocol, everyone uses the OSI model layer names and numbers when describing IP or any other protocol for that matter.
Although Figure 2-13 seems to imply that the OSI network layer and the TCP/IP Internet layer are at least similar, the figure does not point out why they are similar. To appreciate why the TCP/IP layers correspond to a particular OSI layer, you need to have a better understanding of the OSI layers. For example, the OSI network layer defines logical addressing and routing, as does the TCP/IP Internet layer. Although the details differ significantly, the TCP/IP Internet layer matches the overall goals and intent of the OSI network layer.

As another example, you may recall that the TCP/IP transport layer defines many functions, including error recovery. The OSI transport layer also defines these same functions as well, although with different details and different specific protocols. As a result, the networking industry refers to TCP as a Layer 4 protocol or a transport layer protocol, again based on the OSI layer number and name.

**OSI Layers and Their Functions**
Cisco requires that CCNAs demonstrate a basic understanding of the functions defined by each OSI layer, as well as remembering the names of the layers. It is also important that, for each device or protocol referenced throughout the book, you understand which layers of the OSI model most closely match the functions defined by that device or protocol.

Today, because most people happen to be much more familiar with TCP/IP functions than with OSI functions, one of the best ways to learn about the function of different OSI layers is to think about the functions in the TCP/IP model, and correlate those with the OSI model. If you use the five-layer TCP/IP model, the bottom four layers of OSI and TCP/IP map closely together. The only difference in these bottom four layers is the name of OSI Layer 3 (network) compared to TCP/IP (Internet). The upper three layers of the OSI reference model (application, presentation, and session—Layers 7, 6, and 5) define functions that all map to the TCP/IP application layer. Table 2-4 defines the functions of the seven layers.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Functional Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Layer 7 provides an interface between the communications software and any applications that need to communicate outside the computer on which the application resides. It also defines processes for user authentication.</td>
</tr>
<tr>
<td>6</td>
<td>This layer’s main purpose is to define and negotiate data formats, such as ASCII text, EBCDIC text, binary, BCD, and JPEG. Encryption is also defined by OSI as a presentation layer service.</td>
</tr>
<tr>
<td>5</td>
<td>The session layer defines how to start, control, and end conversations (called sessions). This includes the control and management of multiple bidirectional messages so that the application can be notified if only some of a series of messages are completed. This allows the presentation layer to have a seamless view of an incoming stream of data.</td>
</tr>
</tbody>
</table>
Table 2-4  *OSI Reference Model Layer Definitions (Continued)*

<table>
<thead>
<tr>
<th>Layer</th>
<th>Functional Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Layer 4 protocols provide a large number of services, as described in Chapter 6, “Fundamentals of TCP/IP Transport, Applications, and Security.” Although OSI Layers 5 through 7 focus on issues related to the application, Layer 4 focuses on issues related to data delivery to another computer (for instance, error recovery and flow control).</td>
</tr>
<tr>
<td>3</td>
<td>The network layer defines three main features: logical addressing, routing (forwarding), and path determination. Routing defines how devices (typically routers) forward packets to their final destination. Logical addressing defines how each device can have an address that can be used by the routing process. Path determination refers to the work done by routing protocols to learn all possible routes, and choose the best route.</td>
</tr>
<tr>
<td>2</td>
<td>The data link layer defines the rules that determine when a device can send data over a particular medium. Data link protocols also define the format of a header and trailer that allows devices attached to the medium to successfully send and receive data.</td>
</tr>
<tr>
<td>1</td>
<td>This layer typically refers to standards from other organizations. These standards deal with the physical characteristics of the transmission medium, including connectors, pins, use of pins, electrical currents, encoding, light modulation, and the rules for how to activate and deactivate the use of the physical medium.</td>
</tr>
</tbody>
</table>

Table 2-5 lists most of the devices and protocols covered in the CCNA exams and their comparable OSI layers. Note that many network devices must actually understand the protocols at multiple OSI layers, so the layer listed in Table 2-5 actually refers to the highest layer that the device normally thinks about when performing its core work. For example, routers need to think about Layer 3 concepts, but they must also support features at both Layers 1 and 2.

Table 2-5  *OSI Reference Model—Example Devices and Protocols*

<table>
<thead>
<tr>
<th>Layer Name</th>
<th>Protocols and Specifications</th>
<th>Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application, presentation, session (Layers 5–7)</td>
<td>Telnet, HTTP, FTP, SMTP, POP3, VoIP, SNMP</td>
<td>Firewall, intrusion detection systems, hosts</td>
</tr>
<tr>
<td>Transport (Layer 4)</td>
<td>TCP, UDP</td>
<td>Hosts, firewalls</td>
</tr>
<tr>
<td>Network (Layer 3)</td>
<td>IP</td>
<td>Router</td>
</tr>
<tr>
<td>Data link (Layer 2)</td>
<td>Ethernet (IEEE 802.3), HDLC, Frame Relay, PPP</td>
<td>LAN switch, wireless access point, cable modem, DSL modem</td>
</tr>
<tr>
<td>Physical (Layer 1)</td>
<td>RJ-45, EIA/TIA-232, V.35, Ethernet (IEEE 802.3)</td>
<td>LAN hub, LAN repeater, cables</td>
</tr>
</tbody>
</table>

Besides remembering the basics of the features of each OSI layer (as in Table 2-4), and some example protocols and devices at each layer (as in Table 2-5), you should also
memorize the names of the layers. You can simply memorize them, but some people like to use a mnemonic phrase to make memorization easier. In the following three phrases, the first letter of each word is the same as the first letter of an OSI layer name, in the order specified in parentheses:

- All People Seem To Need Data Processing (Layers 7 to 1)
- Please Do Not Take Sausage Pizzas Away (Layers 1 to 7)
- Pew! Dead Ninja Turtles Smell Particularly Awful (Layers 1 to 7)

**OSI Layering Concepts and Benefits**

While networking models use layers to help humans categorize and understand the many functions in a network, networking models use layers for many reasons. For example, consider another postal service analogy. A person writing a letter does not have to think about how the postal service will deliver a letter across the country. The postal worker in the middle of the country does not have to worry about the contents of the letter. Likewise, networking models that divide functions into different layers enables one software package or hardware device to implement functions from one layer, and assume that other software/hardware will perform the functions defined by the other layers.

The following list summarizes the benefits of layered protocol specifications:

- **Less complex**: Compared to not using a layered model, network models break the concepts into smaller parts.

- **Standard interfaces**: The standard interface definitions between each layer allow for multiple vendors to create products that fill a particular role, with all the benefits of open competition.

- **Easier to learn**: Humans can more easily discuss and learn about the many details of a protocol specification.

- **Easier to develop**: Reduced complexity allows easier program changes and faster product development.

- **Multivendor interoperability**: Creating products to meet the same networking standards means that computers and networking gear from multiple vendors can work in the same network.

- **Modular engineering**: One vendor can write software that implements higher layers—for example, a web browser—and another vendor can write software that implements the lower layers—for example, Microsoft’s built-in TCP/IP software in its OSs.
OSI Encapsulation Terminology

Like TCP/IP, each OSI layer asks for services from the next lower layer. To provide the services, each layer makes use of a header, and possibly a trailer. The lower layer encapsulates the higher layer’s data behind a header. The final topic of this chapter explains some of the terminology and concepts related to OSI encapsulation.

The TCP/IP model uses terms such as *segment*, *packet*, and *frame* to refer to various layers and their respective encapsulated data (refer to Figure 2-11). OSI uses a more generic term: *protocol data unit (PDU)*.

A PDU represents the bits that include the headers and trailers for that layer, as well as the encapsulated data. For instance, an IP packet, as shown in Figure 2-10, using OSI terminology, is a PDU. In fact, an IP packet is a *Layer 3 PDU* (abbreviated L3PDU) because IP is a Layer 3 protocol. So, rather than use the terms *segment*, *packet*, or *frame*, OSI simply refers to the “Layer x PDU” (LxPDU), with “x” referring to the number of the layer being discussed.

Figure 2-14 represents the typical encapsulation process, with the top of the figure showing the application data and application layer header and the bottom of the figure showing the L2PDU that is transmitted onto the physical link.
Exam Preparation Tasks

Review All the Key Topics
Review the most important topics from inside the chapter, noted with the key topics icon in the outer margin of the page. Table 2-6 lists a reference of these key topics and the page number on which each is found.

Table 2-6  Key Topics for Chapter 2

<table>
<thead>
<tr>
<th>Key Topic Elements</th>
<th>Description</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 2-3</td>
<td>Provides definitions of same-layer and adjacent-layer interaction</td>
<td>28</td>
</tr>
<tr>
<td>Figure 2-8</td>
<td>Shows the general concept of IP routing</td>
<td>32</td>
</tr>
<tr>
<td>Figure 2-9</td>
<td>Depicts the data-link services provided to IP for the purpose of delivering IP packets from host to host</td>
<td>33</td>
</tr>
<tr>
<td>Figure 2-12</td>
<td>Shows the meaning of the terms segment, packet, and frame</td>
<td>37</td>
</tr>
<tr>
<td>Figure 2-13</td>
<td>Compares the OSI and TCP/IP network models</td>
<td>38</td>
</tr>
<tr>
<td>List</td>
<td>Lists the benefits of using a layered networking model</td>
<td>41</td>
</tr>
</tbody>
</table>

Complete the Tables and Lists from Memory
Print a copy of Appendix L, “Memory Tables,” (found on the DVD) or at least the section for this chapter, and complete the tables and lists from memory. Appendix M, “Memory Tables Answer Key,” 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:

adjacent-layer interaction, decapsulation, encapsulation, frame, networking model, packet, protocol data unit (PDU), same-layer interaction, segment
OSI Reference

You should memorize the names of the layers of the OSI model. Table 2-7 summarizes the OSI functions at each layer, along with some sample protocols at each layer.

Table 2-7  OSI Functional Summary

<table>
<thead>
<tr>
<th>Layer</th>
<th>Functional Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application (7)</td>
<td>Interfaces between network and application software. Also includes authentication services.</td>
</tr>
<tr>
<td>Presentation (6)</td>
<td>Defines the format and organization of data. Includes encryption.</td>
</tr>
<tr>
<td>Session (5)</td>
<td>Establishes and maintains end-to-end bidirectional flows between endpoints. Includes managing transaction flows.</td>
</tr>
<tr>
<td>Transport (4)</td>
<td>Provides a variety of services between two host computers, including connection establishment and termination, flow control, error recovery, and segmentation of large data blocks into smaller parts for transmission.</td>
</tr>
<tr>
<td>Network (3)</td>
<td>Logical addressing, routing, and path determination.</td>
</tr>
<tr>
<td>Data link (2)</td>
<td>Formats data into frames appropriate for transmission onto some physical medium. Defines rules for when the medium can be used. Defines means by which to recognize transmission errors.</td>
</tr>
<tr>
<td>Physical (1)</td>
<td>Defines the electrical, optical, cabling, connectors, and procedural details required for transmitting bits, represented as some form of energy passing over a physical medium.</td>
</tr>
</tbody>
</table>
Index

**Numerics**
- 10BASE2 Ethernet, 54
- 10BASE5 Ethernet, 55–56
- 10BASE-T, 177
- bridges, 178
- building, 57–58
- cabling pinouts, 61–64
- hubs, 178
- switches, 179–180
- 100BASE-TX, cabling pinouts, 61–64
- 1000BASE-T cabling, 64

**A**
- access points. See APs
- accessing
  - attacks, 161
  - CLI on Cisco IOS Software, 211
    - enable mode, 217
    - from console port, 212–214
    - password security, 214–216
    - user EXEC mode, 216
    - with SSH, 214
    - with Telnet, 214
  - links, 93
  - setup mode, 228
  - switches, 195
- ACK flags (TCP), 149
- acknowledgements, 27
- AD (administrative distance), 543–544, 598
- ad hoc WLANs, 311
- Address field (HDLC), 89
- addresses
  - broadcasts, 375–376
  - classes, 377
  - formats, 371–372
  - IP, 31
    - applying rules, 349-360
    - unicast, 430
- IPv4
  - calculating, 403–405
  - classless/classful, 403
  - defining, 400
  - dividing, 401–403
  - network layer, 109–110
  - ranges of
    - searching, 442
    - of usable, 434
  - searching, 442
  - subnets, managing, 342-349
  - translation
    - NAT, 613–617
    - PAT, 613–617
- adjacent-layer interaction, 28
- AES (Advanced Encryption Standard), 332
- analog modems, 599, 601
- analyzing
  - classless IPv4 networks, 367–376
  - deriving IDs/numbers, 373–375
  - number of hosts per, 373
  - unusual network IDs, 375–376
  - easy masks, 443–444
  - Layer 2 forwarding path, 295–299
  - subnets, 342-349, 427
    - binary, 434–442
    - decimal, 442–449
    - existing, 451–452
    - masks, existing, 397, 400–405
- ANSI (American National Standards Institute), 85
- anti-X, 166
- applications
  - layers, 24–26
  - TCP/IP, 144
    - DNS, 145
    - FTP, 145
    - QoS needs, 152–153
    - SNMP, 145
TCP, 145
well-known port numbers, 145
WWW, 145, 155–158
applying classful IPv4 networks, 376–378
APs (access points), 309
configuring, 323–324
rogue APs, 326
transmit power, 317
architecture
OSI networking models, 37
benefits of, 41
comparing to TCP/IP, 37–38
encapsulation, 42
functions, 39–41
referencing layers, 38–39
SNA, 21
TCP/IP networking models, 21
application layers, 24–26
history of, 21–23
Internet layers, 29–32
network access layers, 33–34
overview of, 23–24
terminology, 34–37
transport layers, 26–28
ARIN (American Registry for Internet Numbers), 116
ARP, 108, 128–129
ASN (autonomous system number), 533
asymmetric DSL, 603
ATM (Asynchronous Transfer Mode), 607
cells, 608
PVCs, 608
SAR, 609
versus Frame Relay, 608
attacks
anti-x, 166
tools used to generate, 163
attenuation, 56
autonegotiation, troubleshooting, 291–293
autonomous systems, 533
autosummarization, 536
Aux ports, 499
avoiding reserved IP addresses, 557–558
B
back-to-back serial connections, 87
balanced hybrid routing protocols, 534
bandwidth
commands, 535
on interfaces, configuring, 353, 497–499
banners, configuring on Cisco Catalyst switches, 251–252
benefits of OSI layers, 41
Berners-Lee, Tim, 25
BGP (Border Gateway Protocol), 533
BIAs (burned-in addresses, 70
binary math, 438–440
binary processes, 440–441
binary subnet masks
analyzing, 434–442
converting, 387–389
rules, 386
bits
borrowing, 355–356
calculating, 403
converting, 436
default masks, 372
exactly 8 subnet, 469
hosts, 346
less than 8 subnet, 464–468
more than 8 subnet, 469–472
subnets, selecting, 414, 416
blocking state (STP), 185
blocks, subnets, 470
blueprints, 21. See also networking models
Boolean Algebra, 442
Boolean math, 442
boot sequence of Cisco IOS Software, 505
configuration registers, 507, 511–512
OS selection process, 508–511
boot system commands, 510
borrowing host bits, 355–356
bridges, 178
broadcasts
addresses, 71, 180–181, 375–376
subnets, 433–434
searching, 449–451
domains, 190–192
subnets, 467. See also subnets
BSS (Basic Service Set), 312–313, 323
building
10BASE-T networks, 57–58
WANs for practice lab, 87
bytes, 112
C
cable Internet, 605–606
cabling
1000BASE-T, 64
crossover cabling, 63
distance limitations on campus LANs, 197–199
fiber-optic, 50
serial cabling, 84, 87
straight-through cables, 62
twisted pair encoding schemes, 60
UTP, 51, 58–59
calculations
hosts, 400
IPv4 addresses, 403–405
magic numbers, 464
masks, searching, 420
subnets, 356, 401
campus LANs, 194
access switches, 195
core switches, 197
distribution switches, 196
maximum cable lengths, 197–199
Cat OS (Catalyst Operating System), 208
Catalyst switches
banners, configuring, 251–252
CLI
EXEC mode, 250–251
securing, 241–242
passwords
encryption, 248–249
security, configuring, 242–244
SSH, configuring, 245–248
usernames, configuring, 245–248
CCX (Cisco Compatibile Extensions Program), 324
CDP (Cisco Discovery Protocol), troubleshooting tools, 283–288
cells, 608–609
checking for updated information, 689–690
CIDR (Classless Interdomain Routing), 387
CIR (committed information rate), 96
circuit switching, 609
Cisco ASA hardware, 165–166
Cisco Catalyst switches
CLI
comparing to router CLI, 492–493
history buffer commands, 252
interaces
configuring, 257–258
securing, 265–266
IP address, configuring, 254–257
LEDs, 209–210
mode button, 210
ports
LED modes, switching between, 210
security, configuring, 259–262
VLANs, configuring, 262–265
Cisco CCNA Prep Center, 650
Cisco IOS Software
boot sequence, 505–507
configuration registers, 507, 511–512
OS selection process, 508–511
CLI, 492–493
Aux port, 499
commands, recalling, 217–218
router interfaces, 493–495
configuring, 220–223
images, upgrading into Flash memory, 502–505
interfaces
bandwidth, configuring, 353, 497–499
clock rate, configuring, 353, 497–499
IP addresses, configuring, 496
status codes, 495–496
setup mode, 227–231, 499–502
Cisco ISRs (Integrated Services Routers)
installing, 487
physical installation, 488
Cisco Learning Network. See CLN
Cisco routers
   enterprise routers, installing, 485–488
   Internet access routers, installing, 489–490
   operating systems, 507
Cisco switches
   CLI
      accessing, 211–214
      enable mode, 217
      password security, 214–216
      user EXEC mode, 216
   memory, types of, 223
   reloading, 226
   supported operating systems, 208
CiscoWorks software, 145
Class A, B, and C networks,
   340, 370–371, 462
classes
   addresses, 377
   IP address, 113–120
   IPv4 networks, 369–370
classful addresses, 119, 403
classful networks, IPv4
   analyzing, 367–376
   applying, 376–378
   deriving IDs/numbers, 373–375
   number of hosts per, 373
   subnets, 354-355, 430–434
   unusual network IDs, 375–376
classful routing, 403, 536
classless addresses, 119, 403
Classless Interdomain Routing. See CIDR
classless routing protocols, 403, 536
clear ip nat translation * command, 641
CLI (command-line interface), 206
   accessing on Cisco switches, 211
      from console port, 212–214
      password security, 214–216
      with SSH, 214
      with Telnet, 214
   banners, configuring, 251–252
   configuration mode, 218
   enable mode, 217
   EXEC mode, 250–251
   help system, recalling commands, 217–218
   history buffer commands, 252
   passwords
      encryption, 248–249
      security, 242–244
   securing, 241–242
   SSH, configuring, 245–248
   user EXEC mode, 216, 250–251
   usernames, configuring, 245–248
CLN (Cisco Learning Network), 388
clocks, 497
   rates on interfaces configuring, 88, 353,
      497–499
   sources, 91
   speed
      CIR, 96
      synchronization, 86
clouds, 7
CO (central office), 83
collisions
   domains, 67, 178, 189
   full-duplex Ethernet, 68–69
   impact on LAN design, 191–192
   troubleshooting, 294–295
   between WLAN devices, 320
commands, 611
   boot system, 510
   clear ip nat translation, 641
   clock rate, 88
   configure terminal, 244
   context-setting, 221
   copy, 226
   copy running-config startup-config, 226
   debug, 219–220
   debug ip rip, 546, 548
   enable, 241
   enable secret, 244
   encapsulation ppp, 627
   exec-timeout, 253
   exit, 245
   extended ping, 526–528
   history buffer-related, 252
   interface, 221
   interface range, 258
   ip address, 624
   ip route, 525
   logging synchronous, 253
   Microsoft Windows XP network command
      reference, 561
   ping, 524–526, 561
   recalling, 217–218
   resume, 572
   service password-encryption, 248
   show, 219–220
show cdp, 284, 287–288
show dhcp server, 637
show interfaces status, 289–290
show ip arp, 567
show ip dhcp binding, 640–641
show ip interface brief, 524
show ip nat translations, 641
show ip protocols, 544–548
show ip route, 542
show mac address-table, 295
show running-config, 245, 625–626
show sessions, 572
show ssh, 572
show users, 572
show version, 511–512
show vlan brief, 298–299
subcommands, 221
telnet, 569
traceroute, 568–569

comparing
Ethernet LANs and WLANs, 309
interior routing protocols, 537
LANs and WANs, 82
OSI/TCP/IP models, 37–38
switch and router CLI, 492–493

configuration
Cisco Catalyst switches
banners, 251–252
CLI, securing, 241–242
interfaces, 257–258
IP address, 254–257
password encryption, 248–249
password recovery, 242–244
passwords, 250–251
port security, 259–262
SSH, 245–248
usernames, 245–248
VLANs, 262–265
Cisco IOS Software, 220–223
context-setting commands, 221
setup mode, 227, 231
default routes, 529–530
files
copying, 226–227
erasing, 226–227
storage on Cisco switches, 224
interfaces, IP address, 496

Internet access routers
connectivity, 629–630
DHCP, 631, 634–636
DHCP server, 638–639
PAT, 634
verifying configuration, 639–641
mask formats, 386–387
modes, 218–222
password protection for console access, 214–216
point-to-point WANs
HDLC, 624–627
PPP, 627–628
registers, 507–512
RIP-2, 538–548
serial interfaces, clock rate, 18, 353, 497–499
subnets
design. See design, subnets
masks, 411
overview of, 340–342
processes, 421–422
selecting masks, 414–421
WLANs
APs, 323–324
wireless clients, 324

connections
establishment and termination, 148–149
routes, 521, 524
connectionless protocols, 150
connection-oriented protocols, 150
connectivity, testing with extended ping command, 526–528
connectors
for WANs, 84
pinouts, 61–64
RJ-48, 85

consoles
inactivity timeouts, defining, 253
line 0, 215
ports, accessing CLIs, 212–214

conventions. See design, subnets
convergence, 125, 537
converting
bits, 436
masks, 404
subnets
IDs, 437
masks, 383, 386–391
copy command, 226
copy running-config startup-config
copying
configuration files, 226–227
images into Flash memory, 502–505
core switches, 197
coverage area (WLANs), 317–318
CPE (customer premises equipment), 84
crashers, 161
crossover cables, 63, 80
CSMA/CA (Carrier Sense Multiple
Access / Collision Avoidance), 320
CSMA/CD (Carrier Sense Multiple
Access / Collision Detection), 55, 66, 309
CSU/DSU (channel service unit/data service
unit), 83, 91
clocking the link, 86
internal versus external, 85
synchronization, 86
cut-through processing, 187
definitions
IPv4 addresses, 400
calculating, 403–405
classful/classless addressing, 403
dividing, 401–403
subnets, 430–434
demarc (demarcation point), 84
demodulation, 599
deploying WLANs, 321–326
design, subnets
analyzing, 342–349
applying addressing rules, 349-360
mask, 411
overview of, 340–342
planning, 360–363
processes, 421–422
selecting masks, 414–421
destination port numbers, 142
development, OSI layers, 41
devices
hubs, 57–58
performance issues, 64–66
repeaters, 56
switches, 67
DHCP (Dynamic Host Configuration
Protocol), 129–131
configuring on Internet access router, 631,
634–636
IP address, configuring on Cisco Catalyst
switches, 254–257
planning for on Internet access router, 636
servers, 638–639
verifying configuration on Internet
access router, 639–641
difficult masks, 443, 446
subnet address masks, searching, 449–451
directed broadcast address, 115
displaying
configuration register value, 511–512
interfaces
information, 494
speed and duplex settings, 290–293
status codes, 289–290
log messages, 253
MAC address table contents, 295
URL link properties, 156
distance vector protocols, RIP-2
configuring, 538–540
verifying configuration, 540–548
distribution switches, 196
dividing IPv4 addresses, 401–403
DIX Ethernet, 54
DLCI (data link connection identifier), 95
DMZs (demilitarized zones), 164
DNS, (Domain Name Service) 128, 145
  resolution, 156–158
documentation, subnet designs, 340
DoS (denial-of-service) attacks, 161
dotted-decimal notation. See DDN
DS0 (digital signal level 0), 88
DS1 (Digital Signal, Level 1) services, 88
DS3 (Digital Signal, Level 3) services, 88
DSL (digital subscriber line), 601–604
DSLAM (DSL access multiplexer), 601–603
DSSS (Direct Sequence Spread Spectrum), 315
DTE (data termination equipment), 87, 94
duplex mismatches, effect on Layer 1
  interface operation, 294
duplex settings, displaying, 290–293
duplex transmission issues, 290–293
dynamic port numbers, 143

e
E1 lines, 88, 92
E3 lines, 88
easy masks, analyzing, 443–444
EGPs (Exterior Gateway Protocols), 533
EIRP (Effective Isotropic Radiated Power), 318
EMIs (Electronic Magnetic Interfaces), 293
enable command, 241
enable mode, 217
enable secret command, 244
encapsulation, 35–36, 42, 107
encapsulation ppp command, 627
encoding
  schemes, 60
  types for WLANs, 315–316
encryption, configuring on Cisco Catalyst
  switches, 248–249
Enterprise networks, 342
  security, 160
  subnets, managing, 342–349
  threats to, 161–162
enterprise routers
  Cisco ISR, 487–488
  installing, 485–487
erasing configuration files, 226–227
errors
  detection, 74, 139
  HTTP, 26
  recovery, 139, 146–147
  TCP, 27–28
ESS (Extended Service Set), 312–313, 323
Ethernet
  10BASE-T cabling, 177
    bridges, 178
    cabling pinouts, 61–64
    hubs, 178
    switches, 179–180
  10BASE-TX cabling, 62–64
  100BASE-T cabling, 64
  data-link protocols, 69
  error detection, 74
  Ethernet addressing, 70–71
    framing, 71–73
  frames, Type fields, 73–74
  full-duplex, 68–69
  header/trailer fields, 72
  history of, 54–56
  hubs, 57–58, 64–66
  IEEE standards, 51
  interfaces, 493–495
  LAN components, 52
  repeaters, 56
  switches, 248. See also Catalyst switches
  switching, 67
  UTP cabling, 58–59
exactly 8 subnet bits, searching, 469
EXEC commands. See commands
EXEC mode, 250–251
exec-timeout command, 253
existing subnet masks
  analyzing, 397, 400–405, 427, 451
  binary, 434–442
decimal, 442–449
exit command, 245
extended ping command, 526–528

F
FCC (Federal Communications Commission)
  regulations, 314–315
FCS (Frame Check Sequence) field, 74
  FCS field (HDLC), 90
FHSS (Frequency Hopping Spread
  Spectrum), 315
fiber-optic cabling, 51
filtering
  versus forwarding, 181–183
  problems, identifying, 300
final preparation for ICND2 exam, 647
finding, See searching
firewalls, 160, 164. See also security
Flintstones example network, 8–15
flooding frames, 184–185
flow control, 147
formatting, See also configuration
  addresses, 371–372
  classful networks, 354
  IPv4 addresses
    calculating, 403–405
    classful/classless addressing, 403
    defining, 400
    dividing, 401–403
    masks, 386–387
    parts, 402
forward acknowledgments, 146
forwarding
  data-link frames, 122–124
  versus filtering, 181–183
  packets, 121
  state (STP), 185
four subnet example, 430–432
four-wire circuits, 92
fragment-free processing, 187
Frame Relay
  access links, 93
  versus ATM, 608
  LAPF, 94
  scaling benefits of, 93
  VCs, 95–96
  WANs, 9
frames, 42, 71–73, 94
  forwarding logic on switches, 180
    flooding, 184–185
    forwarding versus filtering, 181–183
    internal switch processing, 186–187
    loop avoidance, 185–186
    MAC address learning process, 183–184
  HDLC, 89
  PPP, 91
  Type fields, 73–74
frequency bands, 314–315
FTP (File Transfer Protocol), 145
full-duplex Ethernet, 68–69
functions, OSI layers, 39–41. See also commands

G
GBIC (Gigabit Interface Converters), 60
GET request (HTTP), 158
grouping IP addresses, 71, 113

H
hacker tools, 163
half duplex transmission, 66
HDLC (High-Level Data Link Control), 89
  configuring, 624–627
  error detection, 90
  FCS field, 90
  Protocol Type field, 90
head-end, 606
headers
  fields for IPv4, 108–109
  trailer fields (Ethernet), 72
  UDP, 151
history
  buffer commands, 252
  of Ethernets
    10BASE2 networks, 54
    10BASE5 networks, 55–56
  of TCP/IP networking models, 21–23
home pages, 25
hop count, 535
hosts, 397
  bits, 346
    borrowing, 355–356
    selecting, 414–416
  calculating, 400
  IP, 32
  networks
    deriving IDs/numbers, 373–375
    number of per, 373
  portion of IP addresses 113–115
  routing, 120
  selecting, 342
  sizing, 400
  subnets, 401
  troubleshooting, 564–565
HTTP (Hypertext Transfer Protocol), 25, 158
  errors, 26
  GET requests/responses, 158
hubs, 57–58
  10BASE-T topologies, 178
  performance issues, 64–67
hybrid 6500 switches, 208

IBM SNA, 21
ICANN (Internet Corporation for Assigned Names and Numbers), 116, 614
ICMP (Internet Control Message Protocol)
  echoes, 131
identifying filtering problems, 300
IDs
  networks
    deriving, 373–375
    unusual, 375–376
  subnets, 423–433
    binary, searching, 435–437
    decimal, searching, 437–438
    difficult masks, 446
    searching, 459, 462–473
IDSs (intrusion detection systems), 166–167, 327
IEEE (Institute of Electrical and Electronic Engineers), 23
  802.2 committee, 54
  802.3 committee, 54
  802.11 standard, 311
  802.11i standard, 331
  Ethernet standards, 51
  WLAN standards, 310
IGPs (Interior Gateway Protocols), 533
images, upgrading into Flash memory, 502–505
implementing subnet masks
  design, 411
  IPv4 subnets, 360–363
  processes, 421–422
  selecting, 414–421
inactivity timer, 185
increasing size of WLAN coverage area, 318
infrastructure mode WLANs, 311–313
inside local addresses, 616
installing
  enterprise routers, 485–488
  Internet access routers, 489–490
  SDM, 630–631
Institute of Electrical and Electronic Engineers. See IEEE
interesting octets, 445, 464
  predictability in, 444–445
interfaces, 207
  bandwidth, configuring, 353, 497–499
  clock rate, configuring, 353, 497–499
  commands, 221, 258
  configuring on Cisco Catalyst switches, 257–258
  Ethernet, 493–495
  IP addresses, configuring, 496
  Layer 1 problems, troubleshooting, 293–295
  OSI, 41
  serial interfaces, 493–495
  speed issues, troubleshooting, 290–293
  status codes, 288–290, 495–496
  unused, securing, 265–266
interference
  effect on Layer 1 interface operation, 294
  in wireless communication, 317
interior routing protocols, 533, 537
International Organization for Standardization (ISO), 22
Internet access routers
  connectivity, configuring, 629–630
  default routes, 612–613
DHCP
  configuring, 631, 634–636
  servers, 638–639
  services, planning for, 636
  verifying configuration, 639–641
installing, 489–490
  PAT, configuring, 634
Internet layers, 29–32
Internet Protocol. See IP
internetworks, 342
interoperability, 41
IP (Internet Protocol), 29, 104
  addresses, 31
    address assignment on Internet access routers, 611–612
    applying rules, 349-360
classes of, 115–116
configuring on Cisco Catalyst switches, 254–257
DNS resolution, 156–158
dotted-decimal notation, 111–112
grouping, 113
host portion, 113–115
network number, 113–115
on interfaces, configuring, 496
postal service and, 29–30
ranges of usable, 434
reserved, avoiding, 557–558
searching ranges of, 442
subnetting, 116–120, 524, 558–560, 650–653
routng, 32–33
unicast, 430
hosts, 111
networks, 18, 112
ip address command, 611, 624
ip route command, 525
routng
forwarding decisions, 121–124
host routng, 120
matching routes, locating, 565–567
troubleshooting scenario, 573, 575–586
subnet design, 337
IPSs (Intrusion Prevention Systems), 166–167
IPv4 (Internet Protocol version 4)
addresses
calculating, 403–405
classful/classless, 403
defining, 400
dividing, 401–403
classes, 369–370
classful networks
analyzing, 367–376
applying, 376–378
deriving IDs/numbers, 373–375
number of hosts per, 373
unusual network IDs, 375–376
header fields, 108–109
subnetting, 337
analyzing, 342–349
applying addressing rules, 14–25
overview of, 340–342
planning, 360–363
ISM (Industrial, Scientific, Mechanical)
frequency band, 315
ISO (International Organization for Standardization), 22
isolating problems, 280–282
ITU (International Telecommunications Union), 91

J-L
jitter, 154

keystroke logging, 163

L3PDUs (Layer 3 PDUs), 42
LANS (local area networks)
broadcast domains, 190–192
campus LANs, 194
access switches, 195
core switches, 197
distribution switches, 196
maximum cable lengths, 197–199
collision domains, 67, 189–192
comparing to WANs, 82
Ethernet
addressing, 70–71
error detection, 74
framing, 71–73
history of, 54–56
hubs, 57–58
repeaters, 56
required components, 52
UTP cabling, 58–59
frame forwarding logic, 180
flooding, 184–185
forwarding versus filtering, 181–183
internal switch processing, 186–187
loop avoidance, 185–186
MAC address learning process, 183–184
small, uses for, 53
subnets, 341
switching, 67
versus WANs, 81
LAPF (Link Access Procedure – Frame), 94
late collisions, effect on Layer 1 interface operation, 295
Layer 1
- interfaces, troubleshooting, 293–295
- WLAN operations, 313–315

Layer 2
- forwarding path, analyzing, 295–299
- WLAN operations, 320–321

Layer 3, 40
- PDUs, 42
- problem isolation, 281–282

Layer 4, 40
- TCP, 140
  - connection establishment and termination, 148–149
  - data segmentation, 150–151
  - error recovery, 139, 146–147
  - flow control, 147
  - multiplexing using TCP port numbers, 141–143
  - ordered data transfer, 150–151
  - primary function of, 139
- UDP, 151

Layer 6, 39
Layer 7, 39
Layer x PDUs (LxPDUs), 42
layers, 23
- adjacent-layer interaction, 28
- application, 24–26
- Internet, 29–32
- network access, 33–34
- OSI
  - benefits of, 41
  - functions, 39–41
  - problem isolation, 281–282
- transport, 26–28

leased circuits, 82
leased lines, 81
- CSU/DSU synchronization, 86

LEDs on Cisco Catalyst switches, 209–210
legal ownership of point-to-point WAN devices, 84
less than 8 subnet bits, 464–468
lines
- cable Internet, 606
- DSL, 604
- status, verifying on interfaces, 495–496

links, 156
- speeds, 88
- URL properties, displaying, 156

links-state routing protocols, 534
list-all-subnets chart, 464
lists, subnet mask processes, 421–422
LLC (Logical Link Control) sublayer, 51, 54
local loops, 597
locating matching routes in routing table, 565–567
log messages, displaying, 253
logging synchronous command, 253
logic, basic application, 25
logical addressing, 109
loop avoidance, STP, 185–186
LxPDUs (Layer x PDUs), 42

M

MAC (Media Access Control) addresses, 51, 54, 71, 180–181
- contents, displaying, 295
- filtering on WLANs, 330
- Layer 2 forwarding path, analyzing, 295–299
- role in frame forwarding process, 183–184
- sticky secure MAC addresses, 261

magic numbers, 446, 464
malware, 164
MAN (metropolitan-area network), 81
managing subnets, 342–349
manual summarization, 536
masks
- converting, 404
- defaults, 372
- difficult, 443, 446, 449–451
- easy, analyzing, 443–444
- formats, 386–387
- multiple masks meet requirements, 418–421
- no masks meet requirements, 416–417
- one mask meets requirements, 417–418
- searching, 421
- selecting, 354
- slash, 387

subnets
- converting, 383, 386–391
- design, 411
- existing, 397, 400–405
- processes, 421–422
- selecting, 414–421
- VLSMs, 348–349
math
binary, 438–440
Boolean, 442
masks, searching, 420
maximum cable lengths on campus LANs, 197–199
memory on Cisco switches, types of, 223
messages, TCP/IP, 36–37
Metro E (Metropolitan Ethernet), 609–610
microsegmentation, 179
Microsoft Windows XP network command reference, 561
MIMO (multiple input multiple output), 317
mnemonics, 41
mode button on Cisco Catalyst switches, 210
models
networking, 17
OSI, 17
benefits of, 41
comparing to TCP/IP models, 37–38
encapsulation, 42
functions, 39–41
referencing layers, 38–39
TCP/IP, 17
application layers, 24–26
history of, 21–23
Internet layers, 29–32
network access layers, 33–34
overview of, 23–24
terminology, 34–37
transport layers, 26–28
modular engineering, 41
more than 8 subnet bits, searching, 469–472
MOTD (Message-of-the-Day) banners, 251–252
MTU (maximum transmission unit), 150
multicast addresses, 71, 180–181
multiple masks meet requirements, 418–421
multiple subnet sizes, 348–349
multiple-choice questions, strategies for solving, 279
multiplexing, 141–143
multivendor interoperability, 41

N
NAC (Network Admission Control), 163
names of TCP/IP messages, 36–37
NAT (Network Address Translation), 351-352, 613, 617
native 6500 switches, 208
network layer, 40, 104
addressing, 109–110
encapsulation, 108
interaction with data link layer, 107
routing protocols, 105–106, 110, 124–126
utilities, 127
ARP, 128–129
DHCP, 129–131
DNS, 128
ping, 131
networks, 5, 18. See also IP (Internet Protocol)
access layers, 33–34
broadcast addresses, 115
classes, 369–370
diagrams, clouds, 7
terminology, 34–37
SOHO networks, 7
TCP/IP
application layers, 24–26
history of, 21–23
Internet layers, 29–32
network access layers, 33–34
overview of, 23–24
terminology, 34–37
transport layers, 26–28
NFS (Network File System), 151
no masks meet requirements, 416–417
nonoverlapping
channels, effect on available bandwidth, 319
DSSS, 315
notation
converting subnet masks, 388–391
DDN, 31, 384–386
numbers
DDN, 31
deriving, 373–375
number of hosts per network, 373

O
objects, 158
octets, 112, 442
masks, converting, 388
interesting, 444–445, 464
subnets. See subnets
OFDM (Orthogonal Frequency Division Multiplexing), 316
one mask meets requirements, 417–418
one-size-subnet-fits-all philosophy, 346
Open System Interconnection. See OSI
operating system. See OS
ordered data transfer, 150–151
OS (operating system), 17, 507
OSI (Open System Interconnection), 17, 22
benefits of, 41
comparing to TCP/IP, 37–38
capsulation, 42
functions, 39–41
network layer, 104–105
  addressing, 109–110
interaction with data link layer, 107
routing, 105–106, 110
reversing layers, 38–39
utilities, 127–131
OUI (organizationally unique identifier), 70
output of show ip route command,
interpreting, 542
outside interfaces, 617

P
packets, 42
acknowledgements, 27
Frame Relay, 93–94
scaling benefits, 92–93
switching, 92, 609
VCs, 95–96
PAR (Positive Acknowledgment and Retransmission), 148
parts
creating, 402
networks, 371–372
subnets, 401
passwords
configuring, 250–251
encryption, configuring, 248–249
protecting switch console access, 214–216
recovery, configuring, 242–244
PAT (Port Address Translation), 613, 617
configuring on Internet access router, 634
path selection, 104
PCM (pulse code modulation), 88, 598
PDUs (protocol data units), 42
permanent virtual circuits. See PVCs
phishing attacks, 164
physical connectivity of point-to-point WANs, 84
pin positions, 59
ping command, 131, 524–526, 561
pinouts, 61–64
planning IPv4 subnets, 360–363
Point-to-Point Protocol. See PPP
point-to-point WANs
cabling, 84–86
demarc, 84
devices, legal ownership of, 84
HDLC, configuring, 624–627
Layer 1, 80
Layer 2
  HDLC, 89–90
  PPP, 91
link speeds, 88
physical connectivity, 84
PPP, configuring, 627–628
subnets, 343
ports
LED modes, switching between, 210
numbers, 143
security, configuring, 259–262
postal service and IP (Internet Protocol), 29–30
PPP (Point-to-Point Protocol), 34, 91, 627–628
practice labs, 87, 653
predictability in interesting octets, 444–445
prefixes, 397, 432
  address, 371–372
  masks, 387–391
  parts, 401
  sizing, 400
preparing for exams, 647
  Cisco CCNA Prep Center, 650
  IP addressing questions, 560
  multiple-choice questions, solving, 279
  recommended study plan, 652–655
  scenarios, 651
  sim questions, solving, 277
  simlet questions, solving, 278–279
  subnetting questions, 558–560, 650–651
presentation layer (OSI model), 39
primary functions of TCP
  connection establishment and termination, 148–149
  data segmentation, 150–151
  error recovery, 146–147
  flow control, 147
  multiplexing using TCP port numbers, 141–143
  ordered data transfer, 150–151
private IP networks, 350–353
problem isolation, 280
  at specific OSI layers, 281–282
processes
  binary, shortcuts for, 440–441
  exactly 8 subnet bits, 469
  less than 8 subnet bits, 464–468
  more than 8 subnet bits, 469–472
  subnet masks, 421–422
protocol data units (PDUs), 42
Protocol Type field (HDLC), 90
protocols
  HTTP, 25–26
  IP, 29
  addresses, 31
    postal service and, 29–30
    routing, 32–33
  PPP, 34
  status, verifying on interfaces, 495–496
  TCP, 27–28
  TCP/IP, See TCP/IP
  UDP, 27

PSTN (Public Switched Telephone Network), 596
PTT (public telephone and telegraph)
  companies, 82
public classful IP networks, 15
public IP networks, 16
PVCs (permanent virtual circuits), 334, 608

Q–R
QoS (quality of service), 152–153
  TCP/IP application requirements, 154–155
  VoIP requirements, 154
ranges of usable addresses, 434
reassembly, 609
recalling commands, 217–218, 252
recommended study plan, 652–655
reconnaissance attacks, 161
referencing OSI layers, 38–39
registered public IP networks, 350
reliability, 146
reloading Cisco switches, 226
repeaters, 56
replicating subnet blocks, 471
Requests for Comments. See RFCs
requirements
  bits, selecting, 414–416
  masks, selecting to meet, 414–421
  multiple masks meet, 418–421
  no masks meet, 416–417
  one mask meets, 417–418
  of TCP/IP applications for QoS, 154–155
  of VoIP for QoS, 154
reserved IP addresses, avoiding, 557–558
resident subnets, 430–432, 446–448
resume command, 572
resuming suspended telnet sessions, 572
reusing private networks, 352
RFCs (Requests for Comments), 23
  1918, 353
  TCP/IP, 374
RIP (Routing Information Protocol), hop count, 535
RIP-2 (Routing Information Protocol version 2)
  administrative distance, 543–544
  configuring, 538–540
  verifying configuration, 540–548
  XE, 532
RJ-45 connectors, 59–64
RJ-48 connectors, 85
rogue APs, 326
ROMMON operating system, 507
route summarization, 536
routed protocols, 111

routers
clock speed, defining, 88
internal CSU/DSU, 85
synchronous serial interfaces, 84

routering, 105
across network, 106
CIDR, 387
classful, 403
IP, 32–33
tables. See routing tables

routing protocols, 110, 124–126
administrative distance, 543–544
balanced hybrid, 534
classful, 536
classless, 536
convergence, 537
exterior, 533
interior, 533, 537
link-state, 534
metrics, 534
RIP-2, 532
configuring, 538–540
verifying configuration, 540–548
route summarization, 536

routing tables
connected routes, 521, 524
default routes, 528–530
matching routes, locating, 565–567
static routes, 524–526

rules
hosts, selecting, 342
subnet masks, 386–387

running-config, storage on
Cisco switches, 224
RxBoot operating system, 507

S
same-layer interaction, 28
sample RIP-2 configuration, 539–540
SAR (segmentation and reassembly), 609
saving Internet access router configurations, 636
scaling packet-switched WANs, 92–93
scanners, 163
scenario
preparing for ICND1 exam, 651
for troubleshooting IP routing, 573–586
SDM (Cisco Router and Security Device Manager), 628
installing, 630–631
Internet access routers
configuring, 629–639
verifying configuring, 639–641
searching, 418–421
IP addresses ranges, 434
ranges of addresses, 442
subnets
binary, 435–437
broadcast addresses, 449–451
decimal, 437–438
difficult masks, 446
exactly 8 subnet bits, 469
IDs, 459, 462–464, 472
less than 8 subnet bits, 464–468
more than 8 subnet bits, 469–472
secure-shutdown state, 262
security, 163
anti-x, 166
CLI, 241–242
VPNs, 167–168
WLANs, 326–327
IEEE 802.11i, 331
MAC address filtering, 330
SSID cloaking, 329–330
WEP, 328–330
WPA, 331
segmentation, 42, 150–151
selecting, 414–421
hosts, 342
IP networks, 353
masks, 354
number of hosts per subnet, 345–346
sizes of subnets, 347
SEQ (sequence number), 28
sequence number (SEQ), 28
serial cabling, 84
back-to-back serial connections, 87
serial interfaces, 493–495
bandwidth, configuring, 353, 497–499
clock rate, configuring, 353, 497–499
service password-encryption command, 248
services
  providers, 82
  sets, 312–313
setup mode, 227, 231, 499–502
shared Ethernet, 68
show commands, 219–220
  show cdp command, role in troubleshooting, 284, 287–288
  show dhcp server command, 637
  show interfaces status command, 289–290
  show ip arp command, 567
  show ip dhcp binding command, 640–641
  show ip interface brief command, 542
  show ip nat translations command, 641
  show ip protocols command, 544–548
  show ip route command, 542
  show mac address-table command, 546
  show running-config command, 245, 625–626
  show sessions command, 572
  show ssh command, 572
  show users command, 572
  show version command, 511–512
  show vlan brief command, 298–299
Sim questions, strategies for solving, 277
Simlet questions, strategies for solving, 278–279
simulation mode (exam engine), 655
site surveys, 325
site-to-site intranet VPNs, 167
sizing
  hosts, 400
  prefixes, 400
  subnets, 346–348
  VLSMs, 348–349
slash masks, 387
sliding window, 147
small LANs, uses for, 53
SNA (Systems Networking Architecture), 21
SNMP (Simple Network Management Protocol), 145
SNR (Signal-to-Noise Ratio), 317
sockets, 142–143
SOHO (single office, home office) networks, 7
solving
  multiple-choice questions, 279
  sim questions, 277
  simlet questions, 278–279
sources
  interference in wireless communication, 317
  MAC addresses, 183
specifications, CIDR, 387
speed settings, displaying, 290–293
SPF (Small-Form Pluggables), 60
spyware, 163
SSH (Secure Shell)
  CLI, accessing, 214
  configuring on Cisco Catalyst switches, 245–248
SSID (service set identifier), cloaking, 329–330
standardization, OSI models, 22
standards bodies, 85
  WLAN standards, 310
startup-config, storage on Cisco switches, 224
static routes, 524–526
  configuring, 529–530
  default routes, 528
stick secure MAC addresses, 261
storing configuration files, 224
STP (Spanning Tree Protocol), 185–186
straight-through cables, 62
study mode (exam engine), 655
subcommands, 221
subnets, 109, 116–120
  analyzing, 427, 451–452
  binary, 434–442
  bits, selecting, 414–416
  blocks, 470
  broadcast addresses, 433–434, 449–451, 464, 467
  calculating, 356, 401
  classful networks, 354–355
  connected routes, 524
  decimal, analyzing, 442–449
  defining, 430–434
  design, 337
  exactly 8 bits, 469
  examples, 340, 357
  four, example, 430–432
  hosts
    routing problems, troubleshooting, 564–565
    selecting, 342, 345-346
IDs, 432–433
difficult masks, 446
searching, 459, 462–464, 472–473
IPv4, 337
analyzing, 342-349
applying addressing rules, 349-360
overview of, 340-342
planning, 360-363
less than 8 bits, 464–468
masks
converting, 383, 386–391
design, 411
existing, 397, 400–405
processes, 421–422
selecting, 414–421
more than 8 bits, 469–472
one-size-subnet-fits-all philosophy, 346
practicing, 650–653
preparing for exam, 558, 560
resident, 430, 432, 446–448
reserved IP addresses, avoiding, 558
sizing, 346-348
VLSMs, 348-349
summarization, 536
suspending sessions
resuming, 572
telnet, 569–571
SWAN (Structured Wireless-Aware Network), 327
switches, 67, 179
circuits, 600
Ethernets, 68
frame forwarding logic, 180
flooding, 184–185
forwarding versus filtering, 181–183
internal switch processing, 186–187
loop avoidance, 185–186
MAC address learning process, 183–184
switching, 67
between configuration modes, 222
VLANs, 193–194
symmetric DSL, 603
SYN flags (TCP), 149
synchronization, 84-86
SYST LED, 210

T

T1 lines, 88, 92
TCP (Transmission Control Protocol), 27, 140, 145
error recovery, 27–28, 139
headers, 151
primary functions of, 139
connection establishment and termination, 148–149
data segmentation, 150–151
error recovery, 146–147
flow control, 147
multiplexing using TCP port numbers, 141–143
ordered data transfer, 150–151
segments, 150
TCP/IP (Transmission Control Protocol/Internet Protocol)
applications
DNS, 145
FTP, 145
QoS needs, 152–153
SNMP, 145
TCP, 145
well-known port numbers, 145
WWW, 145, 155–158
models, 17
application layers, 24–26
history of, 21–23
Internet layers, 29–32
network access layers, 33–34
overview of, 23–24
terminology, 34–37
transport layers, 26–28
OSI models, comparing to, 37–38
QoS, need for, 154–155
RFCs, 374
TDM (time-division multiplexing), 88
telcos, 82, 91
CO, 83
demarc, 84
local loop, 597
PSTN, 596
telnet sessions
CLI, accessing, 214
commands, 569
resuming suspended sessions, 572
suspending, 569, 571
Tera Term Pro software package, 213
terminal emulators, Tera Term Pro, 213
terminology
  encapsulation, 42
  TCP/IP, 34–37
testing network connectivity with extended
  ping command, 526–528
threats
  to Enterprise networks, 161–162
  to WLAN security, 326–327
TIA (Telecommunications Industry
  Association), 85
tools for generating network attacks, 163
trace command, 568–569
Transmission Control Protocol. See TCP
Transmission Control Protocol/Internet
  Protocol. See TCP/IP
transmit power of APs, 317
transport layers, 40, 139. See also Layer 4
troubleshooting
  CDP, 283–288
  host routing problems, 564–565
  HTTP errors, 26
  interfaces
    Layer 1 problems, 293–295
    speed/duplex issues, 290–293
    status codes, 288–290
  IP routing scenarios, 573–586
  problem isolation, 280–282
  TCP error recovery techniques, 27–28
  trunks, 64
  twisted pair, 60
  Type fields, 73–74

U
UAA (universally administered addresses), 70
UDP (User Datagram Protocol), 27
  headers, 151
  multiplexing, 141
  unicast addresses, 180–181, 430
  universal resource locators (URLs), 26, 156
  unknown unicast frames, 184
  unused interfaces, securing, 265–266
  unusual network IDs, 375–376
  updates for ICND1 exams, 689–690
  upgrading images into Flash memory, 502–505
  URLs (universal resource locators), 26, 156
  usable addresses, ranges of, 434
User Datagram Protocol. See UDP
user EXEC mode, 216, 250–251
usernames, configuring, 245–248
utilities, network layer, 127
  ARP, 128–129
  DHCP, 129–131
  DNS, 128
  ping, 131
UTP (unshielded twisted pair) cabling, 51, 58–59

V
VCI (Virtual Channel Identifier) field (ATM), 608
VCs (virtual circuits), 95–96
verifying
  CDP operations, 288
  RIP-2 configuration, 540–548
  WLAN configuration, 325–326
VLANs (virtual LANs), 193–194
  configuring on Cisco Catalyst switches, 262–265
  subnets, selecting hosts, 344
VLSMs (variable length subnet masks), 348–349
VoIP (Voice over IP), 153
QoS, need for, 154
VPI (Virtual Path Identifier) field (ATM), 608
VPNs (virtual private networks), 167–168
vulnerabilities
  of Enterprise networks, 161–162
  of WLANs, 326–327

W–Z
WANs (wide area networks)
  analog modems, 599–601
  ATM, 607–609
  building for practice lab, 87
  cable Internet, 605–606
  cabling, 84–86
  circuit switching, 609
  comparing to LANs, 82
  DSL, 601–604
  Frame Relay, 344
  Internet access routers
    address assignment, 611–612
    default routes, 612–613
  leased lines, 81
Metro E, 609–610
packet switching, 92, 609
Frame Relay, 93–96
scaling benefits, 92–93
physical connectivity, 84
point-to-point, 343
demarc, 84
devices, legal ownership of, 84
HDLC, configuring, 624–627
Layer 1 operation, 80
Layer 2, 89–91
link speeds, 88
physical connectivity, 84
PPP, configuring, 627–628
switched circuits, 600
telcos, 596–598
war drivers, 326
web browsers, 155
web pages, objects, 158
web servers, 155
well-known port numbers, 143
for TCP/IP applications, 145
WEP (Wired Equivalent Privacy), 328
enhancements to, 330
windowing, 147
wireless clients, configuring, 324
wizards, SDM Ethernet wizard
DHCP, configuring on Internet
access router, 632
Summary page, 635
WLANs (wireless LANs)
ad hoc, 311
APs, 309
configuring, 323–324
rogue APs, 326
transmit power, 317
BSS, 323
collisions, 320
comparing with Ethernet LANs, 309
coverage area, 317
deploying, 321–326
encoding types, 315–316
ESS, 323
IEEE standards, 310
infrastructure mode, 311–313
interference, 317
Layer 1 operations, 313–315
Layer 2 operations, 320–321
MAC address filtering, 330
nonoverlapping channels, 319
security
IEEE 802.11i, 331
issues, 326–327
SSID cloaking, 329–330
verifying configuration, 325–326
WEP, 328–330
wireless clients, configuring, 324
WPA, 331
worms, 163
WPA (Wi-Fi Protected Access), 331
WPA-2 (Wi-Fi Protected Access version 2), 331
WWW (World Wide Web), 145, 155
DNS resolution, 156–158
HTTP, 158
URLs, 156