Warning and Disclaimer

This book is designed to provide information about the Introducing Routing and Switching in the Enterprise CCNA Discovery course. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: U.S. Corporate and Government Sales 1-800-382-3419 corp_sales@pearsontechgroup.com

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

Feedback Information

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

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

We greatly appreciate your assistance.
About the Authors

Allan Reid is the curriculum lead and a CCNA/CCNP instructor at the Centennial College CATC in Toronto, Canada. Allan is a professor in the Information and Communications Engineering Technology department and an instructor and program supervisor for the School of Continuing Education at Centennial College. He has developed and taught networking courses for both private and public organizations and has been instrumental in the development and implementation of numerous certificate, diploma, and degree programs in networking. Allan is also a curriculum developer for the Cisco Networking Academy. Outside of his academic responsibilities, he has been active in the computer and networking fields for more than 25 years and is currently a principal in a company specializing in the design, management, and security of network solutions for small and medium-sized companies. Allan authored the first edition of WAN Technologies CCNA 4 Companion Guide (Cisco Press, ISBN: 1-58713-172-2) and Using a Networker’s Journal, which is a supplement to A Networker’s Journal (Cisco Press, ISBN: 1-58713-158-7). Most recently, Allan coauthored the CCNA Discovery online academy courses Networking for Home and Small Businesses and Introducing Routing and Switching in the Enterprise, with Jim Lorenz.

Jim Lorenz is an instructor and curriculum developer for the Cisco Networking Academy. Jim has coauthored several Cisco Press titles, including Fundamentals of UNIX Companion Guide, Second Edition (ISBN 1-58713-140-4), Fundamentals of UNIX Lab Companion, Second Edition (ISBN 1-58713-139-0), and the third editions of the CCNA Lab Companions. He has more than 20 years of experience in information systems, ranging from programming and database administration to network design and project management. Jim has developed and taught computer and networking courses for numerous public and private institutions. As the Cisco Academy Manager at Chandler-Gilbert Community College in Arizona, he was instrumental in starting the Information Technology Institute (ITI) and developed a number of certificates and degree programs. Most recently, Jim coauthored the CCNA Discovery online academy courses Networking for Home and Small Businesses and Introducing Routing and Switching in the Enterprise, with Allan Reid.

Cheryl Schmidt is a professor of network engineering technology at Florida Community College in Jacksonville, Florida, where she has worked for the past 19 years (13 years as a faculty member). Before joining the classroom full time, Cheryl worked in the computer/networking industry, having begun her career in electronics/computers in the U.S. Navy. Cheryl has been active in the Cisco Academy, through which she has taught CCNA, CCNP, wireless, and security classes and has been instrumental in the development and implementation of a converged networking program including VoIP and QoS classes.
About the Technical Reviewers

Tony Chen, CCNP and CCAI, manages Cisco Networking Academy for the College of DuPage in Glen Ellyn, Illinois, and teaches CCNA and CCNP classes at the college. As a manager for a regional academy, he also trains and supports local Cisco networking academies. He also manages the computer network for the Ball Foundation. The Ball Foundation’s motto is to discover and develop human potential. Tony Chen has an understanding wife, Joanne, and one wonderful daughter, Kylie.

Tom Knott is the technology and communications specialist for the Kenan Institute for Engineering, Technology & Science at North Carolina State University. In that capacity, he works as tech support, manages websites, writes program content, and serves as staff photographer. Mr. Knott was a public school teacher for the previous 17 years, the last 10 teaching Cisco Academy courses at Southeast Raleigh High School, a magnet high school. He is also an author for Cisco Press and has worked on numerous curriculum projects for the Cisco Networking Academy.

Fred Lance teaches CCNA, CCNP, and security classes at NHTI in Concord, New Hampshire. After 15 years working in the networking field, he joined the IT faculty of NHTI in 1999 to implement the Cisco Networking Academy for the college. He received both his CCNA and CCNP certifications after moving into the teaching field. He resides in Andover, New Hampshire, with his wife Brenda and their three daughters, Abigail, Becca, and Emily. He has been a volunteer firefighter in Andover for 18 years and enjoys building and painting in his spare time.

Tara Skibar, CCNP, was introduced to networking in 1994 when she enlisted in the Air Force. After serving for four years as a network technician, she became an instructor. Tara has worked with major telecom companies in the United States and Europe. She has worked for the Cisco Networking Academy since 2003 as a subject matter expert for the CCNP assessment development team and for the CCNP certification exams. Most recently, Tara was the assessment lead for the newly modified CCNA curriculum and traveled with a group of development folks to Manila, Philippines, for the small market trial. Tara has a bachelor of science degree in information technology and is working toward a master’s degree in information systems.

Marlon Vernon currently teaches the CCNA and CCNP networking courses. He has been teaching for 23 years in the fields of electronics engineering and computer networking technologies both at the high school and college levels. He has served on the Cisco Advisory Council for the global networking academies for the past four years.

Michael Duane Taylor is department head of computer information sciences at the Raleigh Campus of ECPI College of Technology. He has more than seven years of experience teaching introductory networking and CCNA-level curriculum and was awarded the Instructor of the Year Award. Previously, Michael was a lab supervisor with Global Knowledge, working with router hardware configuration and repair. He holds a bachelor’s degree in business administration from the University of North Carolina at Chapel Hill and a master of science degree in industrial technology/computer network management from East Carolina University. His certifications include CCNA, CCNP-router, and MCSE.
Dedications

This book is dedicated to my children: Andrew, Philip, Amanda, Christopher, and Shaun. You are my inspiration, and you make it all worthwhile. Thank you for your patience and support.

—Allan Reid

To the three most important people in my life: my wife, Mary, and my daughters, Jessica and Natasha. Thanks for your patience and support.

—Jim Lorenz

In addition to my thankfulness for the production team and my family (my husband, Karl, and my daughters, Raina and Kara), I would like to thank my students and coworkers for their continued support in my projects, classes, and ideas. It truly takes a team to have success.

—Cheryl Schmidt
Acknowledgments

From Allan, Jim, and Cheryl:

We want to thank Mary Beth Ray and Dayna Isley with Cisco Press for their help and guidance in putting this book together. We also want to thank the technical editors: Tony Chen, Tom Knott, Fred Lance, Tara Skibar, Mike Taylor, and Marlon Vernon. Their attention to detail and suggestions made a significant contribution to the accuracy and clarity of the content.

We also want to acknowledge the entire CCNA Discovery development team from Cisco Systems for their hard work and dedication to making CCNA Discovery a reality.
Contents at a Glance

Part I: Concepts

Chapter 1 Networking in the Enterprise  3
Chapter 2 Exploring the Enterprise Network Infrastructure  21
Chapter 3 Switching in an Enterprise Network  65
Chapter 4 Addressing in an Enterprise Network  109
Chapter 5 Routing with a Distance Vector Protocol  157
Chapter 6 Routing with a Link-State Protocol  207
Chapter 7 Implementing Enterprise WAN Links  245
Chapter 8 Filtering Traffic Using Access Control Lists  279
Chapter 9 Troubleshooting an Enterprise Network  327
Chapter 10 Putting It All Together  383

Appendix A Check Your Understanding and Challenge Questions
   Answer Key  385
   Glossary  407
   Index  427

Part II: Labs

Chapter 1 Labs: Networking in the Enterprise  503
Chapter 2 Labs: Exploring the Enterprise Network Infrastructure  519
Chapter 3 Labs: Switching in an Enterprise Network  531
Chapter 4 Labs: Addressing in an Enterprise Network  601
Chapter 5 Labs: Routing with a Distance Vector Protocol  655
Chapter 6 Labs: Routing with a Link-State Protocol  673
Chapter 7 Labs: Implementing Enterprise WAN Links  735
Chapter 8 Labs: Filtering Traffic Using Access Control Lists  751
Chapter 9 Labs: Troubleshooting an Enterprise Network  797
Chapter 10 Capstone Project: Putting It All Together  851

Appendix B Lab Equipment Interfaces and Initial Configuration Restoration  873
Contents

Introduction xxix

Part I: Concepts

Chapter 1 Networking in the Enterprise 3
Objectives 3
Key Terms 3
Describing the Enterprise Network 4
Supporting the Business Enterprise 5
Traffic Flow in the Enterprise Network 5
  Enterprise Campus 8
  Enterprise Edge 8
  Service Provider Edge 10
Enterprise LANs and WANs 10
Intranets and Extranets 12
Identifying Enterprise Applications 12
  Traffic Flow Patterns 12
  Applications and Traffic on an Enterprise Network 13
  Network Traffic Prioritization 14
    Data Traffic 14
    Voice and Video Traffic 14
Supporting Remote Workers 15
  Teleworking 15
  Virtual Private Networks 16
Summary 18
Activities and Labs 18
Check Your Understanding 19
Challenge Questions and Activities 20

Chapter 2 Exploring the Enterprise Network Infrastructure 21
Objectives 21
Key Terms 21
Describing the Current Network 22
  Enterprise Network Documentation 22
    Business Continuity Plan 24
    Business Security Plan 25
    Network Maintenance Plan 25
    Service-Level Agreement 25
  Network Operations Center (NOC) 26
  Telecommunication Room Design and Considerations 29
Supporting the Enterprise Edge 31
  Service Delivery at the Point of Presence 31
  Security Considerations at the Enterprise Edge 32
  Connecting the Enterprise Network to External Services 33
Reviewing Routing and Switching 34
  Router Hardware 35
    Out-of-Band Management 37
    In-Band Management 38
  Basic Router CLI show Commands 38
Chapter 3  Switching in an Enterprise Network  65

Objectives  65

Key Terms  65

Describing Enterprise-Level Switching  67
  Switching and Network Segmentation  67
  Multilayer Switching  68
    Layer 2  69
    Layer 3  69
  Types of Switching  69
    Store-and-Forward  70
    Cut-Through Switching  70
  Switch Security  70

Preventing Switching Loops  71
  Redundancy in a Switched Network  72
    Multiple Frame Transmissions  74
    MAC Database Instability  75
  Spanning Tree Protocol (STP)  75
    Blocking  77
    Listening  77
    Learning  77
    Forwarding  77
    Disabled  77
  Root Bridges  78
  Spanning Tree in a Hierarchical Network  79
    PortFast  80
    UplinkFast  80
    BackboneFast  81
    STP Diagnostic show Commands  81
  Rapid Spanning Tree Protocol (RSTP)  85

Configuring VLANs  85
  Virtual LAN  85
    Static VLANs  86
    Dynamic VLANs  87
  Configuring a Virtual LAN  87
  Identifying VLANs  91

Trunking and Inter-VLAN Routing  92
  Trunk Ports  92
    Access Port  93
    Trunk Port  93
  Extending VLANs Across Switches  94
  Inter-VLAN Switching  95

Maintaining VLANs on an Enterprise LAN  97
  VLAN Trunking Protocol (VTP)  97
    VTP Modes  98
    VTP Revision Numbers  98
    VTP Message Types  99
Chapter 7 Implementing Enterprise WAN Links 245
Objectives 245
Key Terms 245
Connecting the Enterprise WAN 247
WAN Devices and Technology 247
WAN Standards 250
Accessing the WAN 251
  TDM 252
  STDM 253
Packet and Circuit Switching 254
  Dedicated Leased Line 254
  Circuit Switching 254
  Packet Switching 255
  Cell Switching 255
  Switched Virtual Circuit 256
  Permanent Virtual Circuit 256
Last-Mile and Long-Range WAN Technologies 257
Comparing Common WAN Encapsulations 258
Ethernet and WAN Encapsulations 258
  HDLC and PPP 260
    HDLC 260
    PPP 260
Configuring PPP 263
  PPP Authentication 266
    Password Authentication Protocol 266
    Challenge Handshake Authentication Protocol 267
Configuring PAP and CHAP 268
Using Frame Relay 271
Overview of Frame Relay 271
Frame Relay Functionality 272
  Inverse ARP 272
    Local Management Interface 273
Summary 275
Activities and Labs 275
Check Your Understanding 276
Challenge Questions and Activities 277
Chapter 8 Filtering Traffic Using Access Control Lists 279
Objectives 279
Key Terms 279
Using Access Control Lists 280
Traffic Filtering 280
Access Control Lists 281
Types and Usage of ACLs 283
  Standard ACLs 284
  Extended ACLs 284
  Named ACLs 284
ACL Processing 284
Using a Wildcard Mask 287
  ACL Wildcard Mask Purpose and Structure 287
  Analyzing the Effects of the Wildcard Mask 289
Configuring Access Control Lists 292
   Placing Standard and Extended ACLs 292
   Step 1: Determine Traffic-Filtering Requirements 292
   Step 2: Decide Type of ACL to Suit Requirements 292
   Step 3: Determine Router and Interface for ACL 294
   Step 4: Determine Direction to Filter Traffic 294
   Basic ACL Configuration Process 295
   Configuring Numbered Standard ACLs 297
   Configuring Numbered Extended ACLs 299
   Configuring Named ACLs 302
   Configure Router vty Access 304

Permitting and Denying Specific Types of Traffic 306
   Configuring ACLs for Application and Port Filtering 306
   Configuring ACLs to Support Established Traffic 308
   Effects of NAT and PAT on ACL Placement 309
   Analyzing Network ACLs and Placement 311
   Configuring ACLs with Inter-VLAN Routing 313

ACL Logging and Best Practices 314
   Using Logging to Verify ACL Functionality 314
   Analyzing Router Logs 317
   ACL Best Practices 318

Summary 319
Activities and Labs 320
Check Your Understanding 321
Challenge Questions and Activities 325

Chapter 9 Troubleshooting an Enterprise Network 327
Objectives 327
Key Terms 327
Understanding the Impact of Network Failure 328
   Enterprise Network Requirements 328
   Monitoring and Proactive Maintenance 330
      Network Monitoring 330
      Proactive Maintenance 332
   Troubleshooting and the Failure Domain 332
   Troubleshooting Process 334

Troubleshooting Switching and Connectivity Issues 336
   Troubleshooting Basic Switching 336
   Troubleshooting VLAN Configuration Issues 340
      Access or Trunk Port 343
      Native and Management VLANs 343
   Troubleshooting VTP 343

Troubleshooting Routing Issues 345
   RIP Issues 345
   EIGRP Issues 351
   OSPF Issues 358
   Route Redistribution Issues 361

Troubleshooting WAN Configurations 366
   Troubleshooting WAN Connectivity 367
   Troubleshooting WAN Authentication 372
Part II: Labs

Chapter 1 Labs: Networking in the Enterprise 503
Lab 1-1: Capturing and Analyzing Network Traffic (1.2.2) 504
Task 1: Connect the Routers and Configure 505
Task 2: Connect the Host to the Switch and Configure 505
Task 3: Verify Connectivity Using Ping 505
Task 4: Launch Wireshark 506
   Setting Wireshark to Capture Packets in Promiscuous Mode 508
   Setting Wireshark for Network Name Resolution 508
Task 5: Ping PDU Capture 510
Task 6: Examine the Packet List Pane 511
Task 7: Examine the Packet Details Pane 511
Task 8: Perform an FTP PDU Capture 513
Task 9: Examine the Packet List Pane 514
Task 10: Examine Packet Details and Packet Byte Panes 514
Task 11: Perform an HTTP PDU Capture 515
Task 12: Examine the Packet List Pane 515
Task 13: Examine the Packet Details and Bytes Panes 515
Task 14: Analyze the Capture 515
Task 15: Reflection 517

Chapter 2 Labs: Exploring the Enterprise Network Infrastructure 519
Lab 2-1: Configuring Basic Routing and Switching (2.3.5) 520
Task 1: Connect PC1 to the Switch 521
Task 2: Perform an Initial Configuration on the Switch 521
Task 3: Configure the Switch Management Interface on VLAN 1 522
Task 4: Verify Configuration of the Switch 522
Task 5: Perform Basic Configuration of Router R1 522
Task 6: Configure Interfaces and Static Routing on Router R1 524
Task 7: Connect PC2 to Router R2 524
Task 8: Perform Basic Configuration of Router R2 524
Task 9: Connect the Internetwork 525
Task 10: Verify and Test the Configurations 525
Task 11: Remove Static Route and Configure a Routing Protocol on Router R1 526
Task 12: Remove Static Route and Configure a Routing Protocol on Router R2 526
Task 13: Verify and Test the Configurations 527
Task 14: Use the Switch Management Interface 528
Task 15: Reflection 530

Chapter 3 Labs: Switching in an Enterprise Network 531
Lab 3-1: Applying Basic Switch Security (3.1.4) 532
Task 1: Connect PC1 to the Switch 533
Task 2: Connect PC2 to the Switch 533
Task 3: Configure PC3 But Do Not Connect 533
Task 4: Perform an Initial Configuration on the Switch 533
Task 5: Configure the Switch Management Interface on VLAN 1 534
Task 6: Verify the Management LANs Settings 534
Task 7: Disable the Switch from Being an HTTP Server 535
Task 8: Verify Connectivity 535
Task 9: Record the Host MAC Addresses 535
Task 10: Determine What MAC Addresses the Switch Has Learned 536
Task 11: View the show mac-address-table Options  536
Task 12: Configure a Static MAC Address  536
Task 13: Verify the Results  536
Task 14: List Port Security Options  537
Task 15: Limit the Number of Hosts per Port  538
Task 16: Configure the Port to Shut Down if a Security Violation Occurs  538
Task 17: Show Port 0/4 Configuration Information  539
Task 18: Reactivate the Port  540
Task 19: Disable Unused Ports  540
Task 20: Reflection  540

Lab 3-2: Building a Switched Network with Redundant Links (3.2.3)  541
Task 1: Cable the Network  542
Task 2: Configure the Switches  542
Task 3: Configure the Hosts  542
Task 4: Verify Connectivity  543
Task 5: Examine Switch Hardware Information  543
Task 6: Examine the Spanning-Tree Tables on Each Switch  544
Task 7: Reassign the Root Bridge  545
Task 8: Look at the Spanning-Tree Table  546
Task 9: Verify the Running Configuration File on the Root Bridge  547
Task 10: Reflection  547

Lab 3-3: Verifying STP with show Commands (3.2.4)  548
Task 1: Cable the Network  549
Task 2: Configure the Switches  549
Task 3: Configure the Hosts  549
Task 4: Verify Connectivity  549
Task 5: Examine Switch Hardware Information  550
Task 6: Determine the Roles of Ports Participating in the Spanning Tree on Each Switch  550
Task 7: Create a Change in the Network Topology  551
Task 8: Examine the Spanning Tree on Each Switch  552
Task 9: Reflection  554

Lab 3-4: Configuring, Verifying, and Troubleshooting VLANs (3.3.2)  555
Task 1: Connect the Equipment  556
Task 2: Perform Basic Configuration on the Router  556
Task 3: Configure the Switch  556
Task 4: Verify Connectivity and Default VLAN Configuration  556
Task 5: Configure VLANs on S1  557
Task 6: Verify VLAN Segmentation  559
Task 7: Change and Delete VLAN Configurations  560
Task 8: Reflection  562

Lab 3-5: Creating VLANs and Assigning Ports (3.4.1)  563
Task 1: Connect the Equipment  564
Task 2: Perform Basic PC Configuration  564
Task 3: Configure Switch 1  564
Task 4: Verify Connectivity  566
Task 5: Reflection  566

Lab 3-6: Configuring a Trunk Port to Connect Switches (3.4.2)  567
Task 1: Connect the Equipment  568
Task 2: Perform Basic Configuration of Switch 1 and Switch 2  568
Task 3: Configure the Host PCs   568
Task 4: Verify Default VLAN Configuration and Connectivity  568
Task 5: Create and Verify VLAN Configuration  570
Task 6: Configure and Verify Trunking  571
Task 7: Observing the Default Trunking Behavior of Switches  573
Task 8: Reflection  573

Lab 3-7: Part A: Configuring Inter-VLAN Routing (3.4.3)  574
Task 1: Connect the Equipment  575
Task 2: Perform Basic Configurations on the Router  575
Task 3: Configure Router Fast Ethernet Connections for Each Network  576
Task 4: Configure Switch1  576
Task 5: Configure Switch2  576
Task 6: Configure Switch3  576
Task 7: Configure Host 1  576
Task 8: Configure Host 2  576
Task 9: Configure Host 3  577
Task 10: Configure the Server  577
Task 11: Verify Connectivity  577
Task 12: Reflection  579

Lab 3-7: Part B: Configuring Inter-VLAN Routing (3.4.3)  580
Task 1: Connect the Equipment  581
Task 2: Perform Basic Configurations on the Router  581
Task 3: Perform Basic Configurations on the Router  581
Task 4: Configure Switch1  582
Task 5: Configure VLAN Trunking on Switch1  583
Task 6: Configure VTP on Switch1  584
Task 7: Configure Switch2  585
Task 8: Configure VLAN Trunking on Switch2  585
Task 9: Configure VTP on Switch2  585
Task 10: Verify Connectivity  586
Task 11: Reflection  587

Challenge Lab 3-8: VTP Modes  588
Task 1: Connect the Equipment  589
Task 2: Perform Basic Configurations on the Router  589
Task 3: Configure VLAN Trunking on the Router  589
Task 4: Configure the S1 Switch  590
Task 5: Configure the S2 Switch  593
Task 6: Configure VLAN 19 on the VTP Server, S1  596
Task 7: Verify Switch 2 VLANs  596
Task 8: Configure Switches for VTP Transparent Mode  596
Task 9: Configure New VLANs  598
Task 10: Connect Hosts and Verify Connectivity  598
Task 11: Reflection  599

Chapter 4  Labs: Addressing in an Enterprise Network  601
Lab 4-1: Designing and Applying an IP Addressing Scheme (4.2.3)  602
Task 1: Cable the Network  603
Task 2: Configure the Router  603
Task 3: Configure the Switches  603
Task 4: Configure the Hosts  603
Task 5: Verify Connectivity 603
Task 6: Reflection 604

**Challenge Lab 4-2: Calculating a Network IP Addressing Scheme** 605
Task 1: Determine Management VLAN Requirements 605
Task 2: Determine VLAN 24 Requirements 606
Task 3: Determine VLAN 18 Requirements 607
Task 4: Determine VLAN 49 Requirements 607
Task 5: Reflection 608

**Lab 4-3: Calculating a VLSM Addressing Scheme (4.2.5)** 609
Task 1: Examine the Network Requirements 609
Task 2: Design an IP Addressing Scheme to Fit the Network Requirements 610
Task 3: Assign Subnets to the WAN Links Between Routers 611
Task 4: Assign IP Configurations to Router Interfaces 611
Task 5: Assign IP Configurations to Workstations 612
Task 6: Reflection 612

**Challenge Lab 4-4: Calculating VLSM Network IP Addressing Schemes** 614
Task 1: Determine Scenario 1 IP Addressing Using VLSM 614
Task 2: Determine Scenario 2 IP Addressing Using VLSM 617
Task 3: Determine Scenario 3 IP Addressing Using VLSM 619
Task 4: Reflection 621

**Lab 4-5: Calculating Summarized Routes (4.3.3)** 623
Task 1: Summarization for RouterC 624
Task 2: Summarization for RouterB 624
Task 3: Summarization for RouterA 624

**Challenge Lab 4-6: Route Summarization Practice** 625
Task 1: Scenario 1 Summarization 625
Task 2: Scenario 2 Summarization 626
Task 3: Scenario 3 Summarization 627
Task 4: Scenario 4 Summarization 629
Task 5: Reflection 630

**Lab 4-7: Configuring a LAN with Discontiguous Subnets (4.3.4)** 631
Task 1: Connect the Equipment 632
Task 2: Perform Basic Configurations on the Main Router 633
Task 3: Configure the Other Routers 633
Task 4: Configure the Hosts with the Proper IP Address, Subnet Mask, and Default Gateway 633
Task 5: Verify That the Network Is Functioning 633
Task 6: Examine the Routing Tables 634
Task 7: Identify and Attempt to Correct the Problem 634
Task 8: Verify That the Problem Has Been Corrected 635
Task 9: Reflection 636

**Lab 4-8: Configuring and Verifying Static and Dynamic NAT (4.4.3)** 637
Task 1: Connect the Equipment 638
Task 2: Perform Basic Configurations on the ISP Router 638
Task 3: Configure the Gateway Router 639
Task 4: Configure Switch1 639
Task 5: Configure the Hosts with the Proper IP Address, Subnet Mask, and Default Gateway 639
Task 6: Verify That the Network Is Functioning 639
Task 7: Create a Static Route 639
Task 8: Create a Default Route 640
Task 9: Define the Pool of Usable Public IP Addresses 640
Task 10: Define an Access List That Will Match the Inside Private IP Addresses 640
Task 11: Define the NAT Translation from the Inside List to the Outside Pool 640
Task 12: Specify the NAT Interfaces 641
Task 13: Configure Static Mapping 641
Task 14: Test the Configuration 641
Task 15: Verify NAT Statistics 642
Task 16: Reflection 642

Lab 4-9: Configuring and Verifying Dynamic NAT (4.4.3) 643
Task 1: Connect the Equipment 644
Task 2: Perform Basic Configurations on the ISP Router 644
Task 3: Configure the Gateway Router 644
Task 4: Configure Switch1 645
Task 5: Configure the Hosts with the Proper IP Address, Subnet Mask, and Default Gateway 645
Task 6: Verify That the Network Is Functioning 645
Task 7: Create a Static Route 645
Task 8: Create a Default Route 646
Task 9: Define the Pool of Usable Public IP Addresses 646
Task 10: Define an Access List That Will Match the Inside Private IP Addresses 646
Task 11: Define the NAT Translation from the Inside List to the Outside Pool 646
Task 12: Specify the NAT Interfaces 647
Task 13: Test the Configuration 647
Task 14: Verify NAT Statistics 648
Task 15: Reflection 648

Lab 4-10: Configuring and Verifying PAT (4.4.4) 649
Task 1: Connect the Equipment 650
Task 2: Perform Basic Configurations on the ISP Router 650
Task 3: Configure the Gateway Router 650
Task 4: Configure Switch1 650
Task 5: Configure the Hosts with the Proper IP Address, Subnet Mask, and Default Gateway 650
Task 6: Verify That the Network Is Functioning 651
Task 7: Create a Default Route 651
Task 8: Define the Pool of Usable Public IP Addresses 651
Task 9: Define an Access List That Will Match the Inside Private IP Addresses 651
Task 10: Define the NAT Translation from the Inside List to the Outside Pool 652
Task 11: Specify the Interfaces 652
Task 12: Generate Traffic from the Gateway to the ISP 652
Task 13: Verify That NAT/PAT Is Working 652
Task 14: Adjust the Gateway Configuration to Use an Alternate PAT Approach 653
Task 15: Reflection 653

Chapter 5 Labs: Routing with a Distance Vector Protocol 655
Lab 5-1: Designing and Creating a Redundant Network (5.1.2) 656
Task 1: Determine the Minimum Number of Links to Meet the Requirements 656
Task 2: Implement the Design 657
Task 3: Verify the Design 657
Task 4: Reflection 657
Lab 5-2: Configuring RIPv2 with VLSM and Default Route Propagation (5.2.3) 659
Task 1: Connect PC1 to the Equipment 660
Task 2: Perform Basic Configurations on the Routers 661
Task 3: Perform Basic Configurations on the Switches 661
Task 4: Configure the Hosts with the Proper IP Address, Subnet Mask, and Default Gateway 661
Task 5: Configure RIPv2 Routing 661
Task 6: Configure and Redistribute a Default Route for Internet Access 662
Task 7: Verify the Routing Configuration 662
Task 8: Verify Connectivity 663
Task 9: Reflection 663

Lab 5-3: Implementing EIGRP (5.4.1) 664
Task 1: Connect the Equipment 665
Task 2: Perform Basic Configurations on the Routers 665
Task 3: Configure EIGRP Routing with Default Commands 666
Task 4: Configure MD5 Authentication 666
Task 5: Reflection 667

Lab 5-4: EIGRP Configuring Automatic and Manual Route Summarization and Discontiguous Subnets (5.4.2) 668
Task 1: Connect the Equipment 669
Task 2: Perform Basic Configurations on the Routers 670
Task 3: Configure EIGRP Routing with Default Commands 670
Task 4: Verify the Routing Configuration 670
Task 5: Remove Automatic Summarization 671
Task 6: Verify the Routing Configuration 671
Task 7: Configure Manual Summarization 672
Task 8: Reflection 672

Chapter 6 Labs: Routing with a Link-State Protocol 673
Lab 6-1: Configuring and Verifying Single-Area OSPF (6.2.1) 674
Task 1: Connect the Equipment 675
Task 2: Perform Basic Configuration on R1 675
Task 3: Perform Basic Configuration on R2 675
Task 4: Perform Basic Configuration on S1 676
Task 5: Configure the Hosts with the Proper IP Address, Subnet Mask, and Default Gateway 676
Task 6: Verify That the Network Is Functioning 676
Task 7: Configure OSPF Routing on R1 677
Task 8: Configure OSPF Routing on R2 678
Task 9: Test Network Connectivity 679
Task 10: Reflection 679

Lab 6-2: Configuring OSPF Authentication (6.2.2) 680
Task 1: Connect the Equipment 681
Task 2: Perform Basic Configuration on Routers 681
Task 3: Configure and Verify OSPF on the Routers 681
Task 4: Configure and Verify OSPF Authentication 682
Task 5: Reflection 684

Lab 6-3: Controlling a DR/BDR Election (6.2.3.2) 685
Task 1: Connect the Equipment 686
Task 2: Perform Basic Configuration on the Routers 686
Lab 6-4: Configuring OSPF Parameters (6.2.3.5) 693
Task 1: Connect the Equipment 694
Task 2: Perform Basic Configuration on the Routers 694
Task 3: Configure Single-Area OSPF Routing on the Routers 694
Task 4: Verify Current OSPF Operation 694
Task 5: Configure Serial Interface Bandwidth Settings 697
Task 6: Use OSPF Cost to Determine Route Selection 698
Task 7: Reflection 699

Lab 6-5 Part A: Configuring and Verifying Point-to-Point OSPF (6.2.4) 700
Task 1: Connect the Equipment 702
Task 2: Perform Basic Configurations on the Routers 702
Task 3: Configure the Router Interfaces 702
Task 4: Verify IP Addressing and Interfaces 702
Task 5: Configure Ethernet Interfaces of PC1, PC2, and PC3 702
Task 6: Configure OSPF on R1 702
Task 7: Configure OSPF on R2 703
Task 8: Configure OSPF on R3 703
Task 9: Configure OSPF Router IDs 704
Task 10: Verify OSPF Operation 708
Task 11: Examine OSPF Routes in the Routing Tables 709
Task 12: Configure OSPF Cost 710
Task 13: Reflection 713

Lab 6-5 Part B: Configuring and Verifying Multiaccess OSPF (6.2.4) 714
Task 1: Connect the Equipment 715
Task 2: Perform Basic Configurations on the Routers 715
Task 3: Configure and Activate Ethernet and Loopback Addresses 715
Task 4: Verify IP Addressing and Interfaces 715
Task 5: Configure OSPF on the DR Router 716
Task 6: Configure OSPF on the BDR Router 717
Task 7: Configure OSPF on the DRother Router 718
Task 8: Use the ip ospf priority interface Command to Determine the DR and BDR 719
Task 9: Reflection 721

Lab 6-6: Configuring and Propagating an OSPF Default Route (6.3.1) 722
Task 1: Connect the Equipment 723
Task 2: Perform Basic Configurations on the Routers 723
Task 3: Configure the ISP Router 724
Task 4: Configure the Area 0 OSPF Routers 724
Task 5: Configure Hosts with Proper IP Address, Subnet Mask, and Default Gateway 725
Task 6: Verify Connectivity 725
Task 7: Configure OSPF Routing on Both Area 0 Routers 725
Task 8: Test Network Connectivity 725
Task 9: Observe OSPF Traffic 726
Task 10: Create a Default Route to the ISP 726
Task 11: Verify the Default Static Route 726
Chapter 8  Labs: Filtering Traffic Using Access Control Lists  751

Lab 8-1: Configuring and Verifying Standard ACLs (8.3.3)  752

Task 1: Connect the Equipment  753
Task 2: Perform Basic Configuration on R1  753
Task 3: Perform Basic Configuration on R2  753
Task 4: Perform Basic Configuration on S1  753
Task 5: Configure the Host with an IP Address, Subnet Mask, and Default Gateway  753
Task 6: Configure RIP and Verify End-to-End Connectivity in the Network  754
Task 7: Configure and Test a Standard ACL  754
Task 8: Test the ACL  755
Task 9: Reflection  757

Lab 8-2: Planning, Configuring, and Verifying Extended ACLs (8.3.4)  758

Task 1: Connect the Equipment  759
Task 2: Perform Basic Configuration on R1  759
Task 3: Perform Basic Configuration on R2  759
Task 4: Perform Basic Configuration on S1  760
Task 5: Configure the Hosts with an IP Address, Subnet Mask, and Default Gateway  760
Task 6: Configure RIP and Verify End-to-End Connectivity in the Network  760
Task 7: Configure Extended ACLs to Control Traffic  760
Task 8: Test the ACL  762
Task 9: Configure and Test the ACL for the Next Requirement  762
Task 10: Reflection  763

Lab 8-3: Configuring and Verifying Extended Named ACLs (8.3.5)  764

Task 1: Connect the Equipment  765
Task 2: Perform Basic Configuration on R1  765
Task 3: Perform Basic Configuration on R2  765
Task 4: Perform Basic Configuration on S1  765
Task 5: Configure the Hosts with an IP Address, Subnet Mask, and Default Gateway  766
Task 6: Verify That the Network Is Functioning  766
Task 7: Configure Static and Default Routing on the Routers  767
Task 8: Configure and Test a Simple Named Standard ACL  767
Task 9: Create and Test a Named Extended ACL  768
Task 10: Edit a Named Standard ACL  768
Task 11: Reflection  769

Lab 8-4: Configuring and Verifying VTY Restrictions (8.3.6)  770

Task 1: Connect the Equipment  771
Task 2: Perform Basic Configuration on R1  771
Task 3: Perform Basic Configuration on R2  771
Task 4: Perform Basic Configuration on S1 and S2  772
Task 5: Configure the Hosts with an IP Address, Subnet Mask, and Default Gateway  772
Task 6: Configure Dynamic Routing on the Routers  772
Task 7: Verify Connectivity  772
Task 8: Configure and Test an ACL That Will Limit Telnet Access  773
Task 9: Create VTY Restrictions for R2  773
Task 10: Reflection  773

Lab 8-5: Configuring an ACL with NAT (8.4.3)  774

Task 1: Connect the Equipment  775
Task 2: Perform Basic Configuration on R1  775
Task 3: Perform Basic Configuration on R2 775
Task 4: Perform Basic Configuration on S1 776
Task 5: Configure the Hosts with an IP Address, Subnet Mask, and Default Gateway 776
Task 6: Configure Static and Default Routes on the Routers 776
Task 7: Verify That the Network Is Functioning 776
Task 8: Configure NAT and PAT on R1 776
Task 9: Test and Verify the Configuration 777
Task 10: Configure and Apply an ACL Designed to Filter Traffic from One Host 777
Task 11: Test the Effects of the ACL on Network Traffic 777
Task 12: Move the ACL and Retest 778
Task 13: Reflection 778

Lab 8-6: Configuring and Verifying ACLs to Filter Inter-VLAN Traffic (8.4.5) 779
Task 1: Connect the Equipment 781
Task 2: Perform Basic Configuration on R1 781
Task 3: Configure R1 to Support Inter-VLAN Traffic 781
Task 4: Perform Basic Configuration on S1 782
Task 5: Create, Name, and Assign Ports to Three VLANs on S1 782
Task 6: Create the Trunk on S1 783
Task 7: Configure the Hosts 783
Task 8: Verify That the Network Is Functioning 783
Task 9: Configure, Apply, and Test an Extended ACL to Filter Inter-VLAN Traffic 784
Task 10: Reflection 784

Lab 8-7: Configuring ACLs and Verifying with Console Logging (8.5.1) 785
Task 1: Connect the Equipment 786
Task 2: Perform Basic Configuration on R1 787
Task 3: Perform Basic Configuration on R2 787
Task 4: Perform Basic Configuration on S1 787
Task 5: Configure the Hosts with the Proper IP Address, Subnet Mask, and Default Gateway 787
Task 6: Configure and Apply ACLs 787
Task 7: Reflection 790

Lab 8-8: Configuring ACLs and Recording Activity to a Syslog Server (8.5.2) 791
Task 1: Connect the Equipment 792
Task 2: Perform Basic Configuration on R1 793
Task 3: Perform Basic Configuration on R2 793
Task 4: Perform Basic Configuration on S1 793
Task 5: Configure the Hosts with the Proper IP Address, Subnet Mask, and Default Gateway 793
Task 6: Configure and Apply ACLs 793
Task 7: Configure the Syslog Service on H2 794
Task 8: Configure the Router to Properly Use the Syslog Service 795
Task 9: Reflection 796

Chapter 9  Labs: Troubleshooting an Enterprise Network 797
Lab 9-1: Troubleshooting RIPv2 Routing Issues (9.3.1) 798
Task 1: Connect the Equipment 799
Task 2: Load the Preconfigurations for R1 and R2 799
Task 3: Configure the Hosts with an IP Address, Subnet Mask, and Default Gateway 800
Task 4: Check Connectivity Between Hosts H1 and H2 800
Task 5: Show the Routing Table for Each Router 801
Task 6: Verify That Routing Updates Are Being Sent 801
Task 7: Show the Routing Tables for Each Router 802
Task 8: Show the RIP Routing Table Entries for Each Router 802
Task 9: Test Network Connectivity 803
Task 10: Reflection 803

Lab 9-2: Troubleshooting OSPF Routing Issues (9.3.3) 804
Task 1: Connect the Equipment and Configure the Hosts 806
Task 2: Load the Preconfiguration on R1 806
Task 3: Load the Preconfiguration on R2 806
Task 4: Load the Preconfiguration on R3 806
Task 5: Troubleshoot Router R1 Issues 806
R1 Troubleshooting Review 809
Task 6: Troubleshoot Router R3 Issues 809
Task 7: Troubleshoot Router R2 Issues: Part A 811
Task 8: Troubleshoot Router R2 Issues: Part B 814
Task 9: Reflection 816

Lab 9-3: Troubleshooting Default Route Redistribution with EIGRP (9.3.4) 818
Task 1: Connect the Equipment 819
Task 2: Load the Preconfigurations for R1, R2, and ISP 819
Task 3: Configure the Hosts with an IP Address, Subnet Mask, and Default Gateway 820
Task 4: Check Connectivity Between Hosts H1 and H2 821
Task 5: Show the Routing Tables for Each Router 821
Task 6: Verify That Routing Updates Are Being Sent 822
Task 7: Show Routing Tables for Each Router 822
Task 8: Show EIGRP Topology Table Entries for Each Router 823
Task 9: Show EIGRP Traffic Entries for R1 823
Task 10: Test Network Connectivity 824
Task 11: Reflection 824

Lab 9-4: Troubleshooting OSPF Default Route Redistribution (9.3.4) 825
Task 1: Connect the Equipment 826
Task 2: Perform Basic Configuration on R1 826
Task 3: Perform Basic Configuration on the GW Router 826
Task 4: Perform Basic Configuration on the ISP 827
Task 5: Configure the Hosts with an IP Address, Subnet Mask, and Default Gateway 827
Task 6: Configure Default Routing 827
Task 7: Troubleshooting Default Routing 829
Task 8: Reflection 833

Lab 9-5: Troubleshooting WAN and PPP Connectivity (9.4.2) 834
Task 1: Connect the Equipment 835
Task 2: Load the Preconfiguration on R1 835
Task 3: Load the Preconfiguration on R2 835
Task 4: Troubleshoot R1 835
Task 5: Show the Details of Serial Interface 0/0/0 on R2 836
Task 6: Turn on PPP Debugging 837
Task 7: Show the Details of the Configuration on R2 837
Task 8: Verify That the Serial Connection Is Functioning 837
Task 9: Reflection 838
Lab 9-6: Troubleshooting ACL Configuration and Placement (9.5.2)  839
Task 1: Connect the Equipment 841
Task 2: Load the Preconfiguration on ISP 841
Task 3: Load the Preconfiguration on HQ 842
Task 4: Configure Hosts H1 and H2 842
Task 5: Configure the Web Server Host H3 842
Task 6: Troubleshoot the HQ Router and Access List 101 842
Task 7: Troubleshoot the HQ Router and Access List 102 844
Task 8: Troubleshoot the HQ Router and Access List 111 846
Task 9: Troubleshoot the HQ Router and Access List 112 847
Task 10: Troubleshoot the HQ Router and Access List 121 849
Task 11: Reflection 850

Chapter 10 Capstone Project: Putting It All Together  851
Part A: Review the Work Order and Develop the VLSM Subnet Scheme  853
Task 1: Review the Customer Work Order and Proposed Network 853
ABC-XYZ-ISP Inc. 854
Official Work Order 854
Task 2: Develop the Network Addressing Scheme 855
Task 3: Determine the IP Addresses to Use for Device Interfaces 859
Part B: Physically Construct the Network and Perform Basic Device Configuration  860
Task 1: Build the Network and Connect the Cables 860
Task 2: Configure the HQ Router 860
Task 3: Configure the Remote Office 2 Router R2 861
Task 4: Configure the Remote Office 2 Switch S1 861
Task 5: Configure the Remote Office 2 Switch S2 862
Task 6: Configure the Remote Office 2 Switch S3 863
Task 7: Configure the Host IP Addresses 864
Task 8: Verify the Device Configurations and Basic Connectivity 864
Part C: Routing, ACLs, and Switch Security Configuration  865
Task 1: Configure Routing for HQ and R2 865
Task 2: Configure NAT Overload (PAT) on HQ 866
Task 3: Configure Switch Port Security 867
Task 4: Verify the Overall Network Connectivity Before Applying ACLs 869
Task 5: Configure ACL Security on HQ and R2 869

Appendix B Lab Equipment Interfaces and Initial Configuration Restoration  873
Router Interface Summary 873
Erasing and Reloading the Router 874
Erasing and Reloading the Switch 874
SDM Router Basic IOS Configuration 876
**Icons Used in This Book**

- Multilayer Switch
- Modem
- Bridge
- Hub
- Mainframe
- Workstation
- Workgroup Switch
- ISDN Switch
- Handheld
- Network Cloud
- Printer
- Laptop
- File Server
- Router
- Firewall
- Gateway
- IP Phone
- Integrated Router
- Wireless Access Point
- Route/Switch Processor
- Wireless Bridge
- Wireless Media
- LAN Media
- WAN Media

**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).

- **Italics** indicate arguments for which you supply actual values.

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

- Square brackets [ ] indicate optional elements.

- Braces { } indicate a required choice.

- Braces within brackets [{ }] indicate a required choice within an optional element.
Introduction

Cisco Networking Academy is a comprehensive e-learning program that delivers information technology skills to students around the world. The Cisco CCNA Discovery curriculum consists of four courses that provide a comprehensive overview of networking, from fundamentals to advanced applications and services. The curriculum emphasizes real-world practical application, while providing opportunities for you to gain the skills and hands-on experience needed to design, install, operate, and maintain networks in small to medium-sized businesses and in enterprise and Internet service provider environments. The Introducing Routing and Switching in the Enterprise course is the third course in the curriculum.

Introducing Routing and Switching in the Enterprise, CCNA Discovery Learning Guide is the official supplemental textbook for the third course in v4.x of the CCNA Discovery online curriculum of the Networking Academy. As a textbook, this book provides a ready reference to explain the same networking concepts, technologies, protocols, and devices as the online curriculum. In addition, it contains all the interactive activities, Packet Tracer activities, and hands-on labs from the online curriculum and bonus labs.

This book emphasizes key topics, terms, and activities and provides many alternative explanations and examples as compared with the course. You can use the online curriculum as directed by your instructor and then also use this Learning Guide’s study tools to help solidify your understanding of all the topics. In addition, the book includes the following:

- Expanded coverage of CCNA exam material
- Additional key Glossary terms
- Bonus labs
- Additional Check Your Understanding and Challenge questions and activities
- Interactive activities and Packet Tracer activities on the CD-ROM

Goal of This Book

First and foremost, by providing a fresh, complementary perspective of the online content, this book helps you learn all the required materials of the third course in the Networking Academy CCNA Discovery curriculum. As a secondary goal, individuals who do not always have Internet access can use this text as a mobile replacement for the online curriculum. In those cases, you can read the appropriate sections of this book, as directed by your instructor, and learn the topics that appear in the online curriculum. Another secondary goal of this book is to serve as your offline study material to help prepare you for the CCNA exams.

Audience for This Book

This book’s main audience is anyone taking the third CCNA Discovery course of the Networking Academy curriculum. Many Networking Academies use this textbook as a required tool in the course, whereas other Networking Academies recommend the learning guides as an additional source of study and practice materials.
Book Features

The educational features of this book focus on supporting topic coverage, readability, and practice of the course material to facilitate your full understanding of the course material.

Topic Coverage

The following features give you a thorough overview of the topics covered in each chapter so that you can make constructive use of your study time:

- **Objectives**: Listed at the beginning of each chapter, the objectives reference the core concepts covered in the chapter. The objectives match the objectives stated in the corresponding chapters of the online curriculum; however, the question format in the Learning Guide encourages you to think about finding the answers as you read the chapter.

- **“How-to” feature**: When this book covers a set of steps that you need to perform for certain tasks, the text lists the steps as a how-to list. When you are studying, the icon helps you easily refer to this feature as you skim through the book.

- **Notes, tips, cautions, and warnings**: These short sidebars point out interesting facts, timesaving methods, and important safety issues.

- **Chapter summaries**: At the end of each chapter is a summary of the chapter’s key concepts. It provides a synopsis of the chapter and serves as a study aid.

Readability

The authors have compiled, edited, and in some cases rewritten the material so that it has a more conversational tone that follows a consistent and accessible reading level. In addition, the following features have been updated to assist your understanding of the networking vocabulary:

- **Key terms**: Each chapter begins with a list of key terms, along with a page-number reference from inside the chapter. The terms are listed in the order in which they are explained in the chapter. This handy reference allows you to find a term, flip to the page where the term appears, and see the term used in context. The Glossary defines all the key terms.

- **Glossary**: This book contains an all-new Glossary with more than 300 computer and networking terms.

Practice

Practice makes perfect. This new *Learning Guide* offers you ample opportunities to put what you learn to practice. You will find the following features valuable and effective in reinforcing the instruction that you receive:

- **Check Your Understanding questions and answer key**: Updated review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions that you see in the online course. Appendix A, “Check Your Understanding and Challenge Questions Answer Key,” provides an answer key to all the questions and includes an explanation of each answer.

- **(New) Challenge questions and activities**: Additional, and more challenging, review questions and activities are presented at the end of chapters. These questions are purposefully designed to be similar to the more complex styles of questions you might see on the CCNA exam. This section might also include activities to help prepare you for the exams. Appendix A provides the answers.
Packet Tracer activities: Interspersed throughout the chapters, you'll find many activities to work with the Cisco Packet Tracer tool. Packet Tracer enables you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available on this book’s CD-ROM; Packet Tracer software, however, is available through the Academy Connection website. Ask your instructor for access to Packet Tracer.

Interactive activities: These activities provide an interactive learning experience to reinforce the material presented in the chapter.

Labs: Part II of this book contains all the hands-on labs from the curriculum plus additional labs for further practice. Part I includes references to the hands-on labs, as denoted by the lab icon, and Part II of the book contains each lab in full. You may perform each lab when it is referenced in the chapter or wait until you have completed the entire chapter.

A Word About Packet Tracer Software and Activities
Packet Tracer is a self-paced, visual, interactive teaching and learning tool developed by Cisco. Lab activities are an important part of networking education. However, lab equipment can be a scarce resource. Packet Tracer provides a visual simulation of equipment and network processes to offset the challenge of limited equipment. Students can spend as much time as they like completing standard lab exercises through Packet Tracer, and have the option to work from home. Although Packet Tracer is not a substitute for real equipment, it allows students to practice using a command-line interface. This “e-doing” capability is a fundamental component of learning how to configure routers and switches from the command line.

Packet Tracer v4.x is available only to Cisco Networking Academies through the Academy Connection website. Ask your instructor for access to Packet Tracer.

A Word About the Discovery Server CD
The CCNA Discovery series of courses is designed to provide a hands-on learning approach to networking. Many of the CCNA Discovery labs are based on Internet services. Because it is not always possible to allow students access to these services on a live network, the Discovery Server has been developed to provide them.

The Discovery Server CD is a bootable CD that transforms a regular PC into a Linux server running several preconfigured services for use with Discovery labs. Your instructor can download the CD files, burn a CD, and show you how to use the server. Hands-on labs that use the Discovery Server are identified within the labs themselves.

Once booted, the server provides many services to clients, including the following:

- Domain Name Services
- Web services
- FTP
- TFTP
- Telnet
SSH
DHCP
Streaming video

How This Book Is Organized
This book covers the major topics in the same sequence as the online curriculum for the CCNA Discovery Introducing Routing and Switching in the Enterprise course. The online curriculum has ten chapters for this course, so this book has ten chapters, with the same names and numbers as the online course chapters.

To make it easier to use this book as a companion to the course, the major topic headings in each chapter match, with just a few exceptions, the major sections of the online course chapters. However, the Learning Guide presents many topics in slightly different order inside each major heading. In addition, the book occasionally uses different examples than the course. As a result, students get more detailed explanations, a second set of examples, and different sequences of individual topics, all to aid the learning process. This new design, based on research into the needs of the Networking Academies, helps typical students lock in their understanding of all the course topics.

Chapters and Topics
Part I of this book has ten chapters, as follows:

- **Chapter 1, “Networking in the Enterprise,”** describes the goals of the enterprise network and compares enterprise LANs, WANs, intranets, and extranets. Types of enterprise applications are identified, including traffic flow patterns and prioritization. This chapter also focuses on the needs of teleworkers and the use of virtual private networks to support them.

- **Chapter 2, “Exploring the Enterprise Network Infrastructure,”** describes the network operations center (NOC), telecommunications rooms, and network documentation used in the enterprise. Requirements for supporting the enterprise edge are introduced, including external service delivery and security considerations. This chapter also provides a good review of switch and router hardware. It reinforces the basic commands necessary to configure switches and routers and verify their operation.

- **Chapter 3, “Switching in an Enterprise Network,”** focuses on the characteristics of switches and issues associated with supporting them in an enterprise environment. These include redundancy and Spanning Tree Protocol (STP). You learn to configure VLANs, trunking, and multi-switch inter-VLAN routing. The chapter also covers the VLAN Trunking Protocol (VTP), support for IP telephony, and wireless and VLAN implementation best practices.

- **Chapter 4, “Addressing in an Enterprise Network,”** compares flat and hierarchical network design with a focus on the structure and advantages of hierarchical IP addressing. This chapter provides a review of subnet masks and basic subnetting and introduces variable-length subnet masks (VLSM) and their benefits. It provides instruction on how to implement VLSM addressing in hierarchical network design. The use and importance of classless routing, classless inter-domain routing (CIDR), and route summarization are explained, along with subnetting best practices. This chapter also provides a review of private IP addressing, Network Address Translation (NAT), and Port Address Translation (PAT), with examples of implementation.
Chapter 5, “Routing with a Distance Vector Protocol,” describes common network topologies and provides a review of static and dynamic routing and default routes. The chapter also provides a review of distance vector routing protocols. The advantages and disadvantages of using Routing Information Protocol (RIP) and Enhanced Interior Gateway Routing Protocol (EIGRP) are discussed. Instructions are provided for the configuration and implementation of the RIPv2 and EIGRP dynamic routing protocols.

Chapter 6, “Routing with a Link-State Protocol,” focuses on link-state routing protocols, specifically the Open Shortest Path First (OSPF) Protocol. OSPF characteristics are described, as are advantages and issues involved with implementing OSPF. Instructions are provided for configuring single-area OSPF. In addition, issues associated with using multiple routing protocols in a network are addressed.

Chapter 7, “Implementing Enterprise WAN Links,” focuses on devices and technology options for connecting the enterprise WAN. Packet- and circuit-switching technologies are compared, as are last-mile and long-range technologies. WAN encapsulations, such as High-Level Data Link Control (HDLC) and PPP, are described. You learn how to configure PPP on a WAN link, including authentication. The chapter also provides an overview of the popular Frame Relay WAN technology.

Chapter 8, “Filtering Traffic Using Access Control Lists,” emphasizes the importance of using access control lists (ACL) in network security and traffic flow control. This chapter describes the various types of Cisco IOS ACLs and how they are configured, including the use of the wildcard mask. Standard, extended, and named ACLs are compared, with suggestions for when to use them and placement in specific scenarios. Details are provided on how to create, edit, and apply various ACLs. Filtering traffic based on specific fields in the IP packet is covered. The use of ACLs with NAT and PAT and inter-VLAN routing is discussed. In addition, ACL logging (and the use of syslog servers) is introduced.

Chapter 9, “Troubleshooting an Enterprise Network,” emphasizes the impact of network failure on an organization and the concept of a failure domain. This chapter describes network monitoring tools and techniques and reviews the troubleshooting process. This chapter identifies common problems associated with switching and connectivity, routing, WAN configurations and ACLs, and ways to troubleshoot these problems.

Chapter 10, “Putting It All Together,” In this summary activity, you use what you have learned about the enterprise network infrastructure, switching technologies, hierarchical IP addressing, routing protocols, WAN technologies, and ACLs to build and configure a multi-switch, multirouter simulated enterprise network.

Part I: Concepts also includes the following:

- Appendix A, “Check Your Understanding and Challenge Questions Answer Key,” provides the answers to the Check Your Understanding questions that you find at the end of each chapter. It also includes answers for the Challenge questions and activities that conclude most chapters.

- The Glossary provides a compiled list of all the key terms that appear throughout this book, plus additional computer and networking terms.

Part II of this book includes the labs that correspond to each chapter. Part II also includes the following:

- Appendix B, “Lab Equipment Interfaces and Initial Configuration Restoration,” provides a table listing the proper interface designations for various routers. Procedures are included for erasing and restoring routers and switches to clear previous configurations. In addition, the steps necessary to restore an SDM router are provided.
About the CD-ROM

The CD-ROM included with this book provides many useful tools and information to support your education:

- **Packet Tracer Activity files**: These are files to work through the Packet Tracer activities referenced throughout the book, as indicated by the Packet Tracer activity icon.

- **Interactive activities**: The CD-ROM contains the interactive activities referenced throughout the book.

- **Taking Notes**: This section includes a TXT file of the chapter objectives to serve as a general outline of the key topics of which you need to take note. The practice of taking clear, consistent notes is an important skill for not only learning and studying the material, but for on-the-job success, too. Also included in this section is “A Guide to Using a Networker’s Journal” PDF booklet providing important insight into the value of the practice of using a journal, how to organize a professional journal, and some best practices on what, and what not, to take note of in your journal.

- **IT Career Information**: This section includes a student guide to applying the toolkit approach to your career development. Learn more about entering the world of information technology as a career by reading two informational chapters excerpted from *The IT Career Builder's Toolkit*: “Communication Skills” and “Technical Skills.”

- **Lifelong Learning in Networking**: As you embark on a technology career, you will notice that it is ever changing and evolving. This career path provides new and exciting opportunities to learn new technologies and their applications. Cisco Press is one of the key resources to plug into on your quest for knowledge. This section of the CD-ROM provides an orientation to the information available to you and tips on how to tap into these resources for lifelong learning.
# PART 1

## Concepts

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Networking in the Enterprise</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Exploring the Enterprise Network Infrastructure</td>
<td>21</td>
</tr>
<tr>
<td>3</td>
<td>Switching in an Enterprise Network</td>
<td>65</td>
</tr>
<tr>
<td>4</td>
<td>Addressing in an Enterprise Network</td>
<td>109</td>
</tr>
<tr>
<td>5</td>
<td>Routing with a Distance Vector Protocol</td>
<td>157</td>
</tr>
<tr>
<td>6</td>
<td>Routing with a Link-State Protocol</td>
<td>207</td>
</tr>
<tr>
<td>7</td>
<td>Implementing Enterprise WAN Links</td>
<td>245</td>
</tr>
<tr>
<td>8</td>
<td>Filtering Traffic Using Access Control Lists</td>
<td>279</td>
</tr>
<tr>
<td>9</td>
<td>Troubleshooting an Enterprise Network</td>
<td>327</td>
</tr>
<tr>
<td>10</td>
<td>Putting It All Together</td>
<td>383</td>
</tr>
<tr>
<td>A</td>
<td>Check Your Understanding and Challenge Questions Answer Key</td>
<td>385</td>
</tr>
<tr>
<td></td>
<td>Glossary</td>
<td>407</td>
</tr>
<tr>
<td></td>
<td>Index</td>
<td>427</td>
</tr>
</tbody>
</table>
This page intentionally left blank
CHAPTER 2

Exploring the Enterprise Network Infrastructure

Objectives

Upon completion of this chapter, you should be able to answer the following questions:

- What are the main types of network documentation and how are they interpreted?
- What equipment is found in the enterprise Network Operations Center?
- What is the point of presence for service delivery and how is service delivered?
- What are network security considerations and what equipment is used at the enterprise edge?
- What are some characteristics of router and switch hardware?
- What are the most common and useful router and switch CLI configuration and verification commands?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

- physical topology page 22
- logical topology page 22
- control plane page 22
- redlined page 24
- as-built page 24
- business continuity plan (BCP) page 24
- business security plan (BSP) page 25
- network maintenance plan (NMP) page 25
- service-level agreement (SLA) page 25
- Network Operations Center (NOC) page 26
- data center page 26
- server farm page 26
- load balancing page 26
- network attached storage (NAS) page 27
- storage-area network (SAN) page 27
- rack units (RU) page 27
- Structured cabling page 28
- electromagnetic interference (EMI) page 28
- telecommunications room page 29
- intermediate distribution facility (IDF) page 29
- access point (AP) page 29
- main distribution facility (MDF) page 29
- extended star page 29
- Power over Ethernet (PoE) page 31
- point of presence (POP) page 31
- service provider (SP) page 32
- (T1/E1) page 33
- punchdown block page 33
- channel service unit/data service unit (CSU/DSU) page 33
- customer premise equipment (CPE) page 34
- form factors page 36
- out-of-band page 37
- in-band page 37
- Port density page 49
Enterprise networks contain hundreds of sites and support thousands of users worldwide. A well-managed network allows users to work reliably. Network documentation is crucial for maintaining the required 99.999 percent uptime. All Internet traffic flows through the enterprise edge, making security considerations necessary. Routers and switches provide connectivity, security, and redundancy while controlling broadcasts and failure domains.

Describing the Current Network

The following sections describe network documentation required to support the enterprise and equipment found in the Network Operations Center as well as telecommunications room design considerations.

Enterprise Network Documentation

One of the first tasks for a new network technician is to become familiar with the current network structure. Enterprise networks can have thousands of hosts and hundreds of networking devices, all of which are interconnected by copper, fiber-optic, and wireless technologies. End-user workstations, servers, and networking devices, such as switches and routers, must all be documented. Various types of documentation show different aspects of the network.

Network infrastructure diagrams, or topology diagrams, keep track of the location, function, and status of devices. Topology diagrams represent either the physical or logical network.

A physical topology map uses icons to document the location of hosts, networking devices, and media. It is important to maintain and update physical topology maps to aid future installation and troubleshooting efforts.

A logical topology map groups hosts by network usage, regardless of physical location. Host names, addresses, group information, and applications can be recorded on the logical topology map. Connections between multiple sites might be shown but do not represent actual physical locations.

Enterprise network diagrams can also include control plane information. Control plane information describes failure domains and defines the interfaces where different network technologies intersect. Figure 2-1 shows a physical topology and Figure 2-2 shows the corresponding logical topology.
Figure 2-1  Physical Network Topology
It is crucial that network documentation remain current and accurate. Network documentation is usually accurate at the installation of a network. As the network grows or changes, however, you need to update the documentation.

Network topology maps are frequently based on original floor plans. The current floor plans might have changed since the construction of the building. Blueprints can be marked up, or redlined, to show the changes. The modified diagram is known as an as-built. An as-built diagram documents how a network was actually constructed, which can differ from the original plans. Always ensure that the current documentation reflects the as-built floor plan and all network topology changes.

Network diagrams are commonly created using graphical drawing software. In addition to being a drawing tool, many network diagramming tools are linked to a database. This feature allows the network support staff to develop detailed documentation by recording information about hosts and networking devices, including manufacturer, model number, purchase date, warranty period, and more. Clicking a device in the diagram opens an entry form with device data listed.

In addition to network diagrams, several other important types of documentation are used in the enterprise network, including a business continuity plan, a business security plan, a network maintenance plan, and a service-level agreement.

Business Continuity Plan

The business continuity plan (BCP) identifies the steps to be taken to continue business operation in the event of a natural or man-made disaster. The BCP helps to ensure business operations by defining procedures that must take place when a disaster strikes. IT support can include:

- Off-site storage of backup data
- Alternate IT processing centers
- Redundant communication links
Business Security Plan

The business security plan (BSP) prevents unauthorized access to organizational resources and assets by defining security policies. The BSP includes physical, system, and organizational control measures. The overall security plan must include an IT portion that describes how an organization protects its network and information assets. The IT security plan can contain policies related to

- User authentication
- Permissible software
- Remote access
- Intrusion monitoring
- Incident handling

Network Maintenance Plan

The network maintenance plan (NMP) minimizes downtime by defining hardware and software maintenance procedures. The NMP ensures business continuity by keeping the network up and running efficiently. Network maintenance must be scheduled during specific time periods, usually nights and weekends, to minimize the impact on business operations. The maintenance plan can contain

- Maintenance time periods
- Scheduled downtime
- Staff on-call responsibilities
- Equipment and software to be maintained (OS, IOS, services)
- Network performance monitoring

Service-Level Agreement

A service-level agreement (SLA) ensures service parameters by defining required service provider level of performance. The SLA is a contractual agreement between the customer and a service provider or ISP, specifying items such as network availability and service response time. An SLA can include

- Connection speeds/bandwidth
- Network uptime
- Network performance monitoring
- Problem resolution response time
- On-call responsibilities

Network documentation should be kept in a centrally located area that is available by all who need access to it. Although it is common to store network documentation on network servers in digital form, hard copy versions should also be kept in filing cabinets in the event the network or server is down. Digital and hard copy versions should also be kept in a secure off-site location in the event of a disaster.
Interactive Activity 2-1: Matching Network Information to Documentation Type (2.1.1)

In this activity, you identify the network documentation where the information would most likely be found. Use file d3ia-2114 on the CD-ROM that accompanies this book to perform this interactive activity.

Network Operations Center (NOC)

Most enterprise networks have a Network Operations Center (NOC) that allows central management and monitoring of all network resources. The NOC is sometimes referred to as a data center.

Employees in a typical enterprise NOC provide support for both local and remote locations, often managing both local- and wide-area networking issues. Larger NOCs can be multiroom areas of a building where network equipment and support staff are concentrated. Figure 2-3 shows a large NOC surrounded by the types of features and equipment found there.

Figure 2-3  Network Operations Center Components and Features

The NOC usually has

- Raised floors to allow cabling and power to run under the floor to the equipment
- High-performance UPS systems and air conditioning equipment to provide a safe operating environment for equipment
- Fire suppression systems integrated into the ceiling
- Network monitoring stations, servers, backup systems, and data storage
- Access layer switches and distribution layer routers, if it serves as a main distribution facility (MDF) for the building or campus where it is located

In addition to providing network support and management, many NOCs also provide centralized resources such as servers and data storage. Servers in the NOC are usually clustered together, creating a server farm. The server farm is frequently considered as a single resource but, in fact, provides two functions: backup and load balancing. If one server fails or becomes overloaded, another server takes over.
The servers in the farm can be rack-mounted and interconnected by very high-speed switches (Gigabit Ethernet or higher). They can also be blade servers mounted in a chassis and connected by a high-speed backplane within the chassis. Figure 2-4 shows a group of rack-mounted servers.

**Figure 2-4  Rack-Mounted Server Farm**

Another important aspect of the enterprise NOC is high-speed, high-capacity data storage. This data storage, or network attached storage (NAS), groups large numbers of disk drives that are directly attached to the network and can be used by any server. An NAS device is typically attached to an Ethernet network and is assigned its own IP address. Figure 2-5 shows an example of multiple rack-mounted NAS drives.

**Figure 2-5  Network Attached Storage (NAS)**

A more sophisticated version of NAS is a storage-area network (SAN). A SAN is a high-speed network that interconnects different types of data storage devices over a LAN or WAN.

Equipment in the enterprise NOC is usually mounted in racks. In large NOCs, racks are usually floor-to-ceiling mounted and can be attached to each other. When mounting equipment in a rack, ensure that there is adequate ventilation and access from front and back. Equipment must also be attached to a known good ground.

The most common rack width is 19 inches (48.26 cm). Most equipment is designed to fit this width. The vertical space that the equipment occupies is measured in rack units (RU). A unit equals 1.75 inches (4.4 cm). For example, a 2RU chassis is 3.5 inches (8.9 cm) high. The lower the RU number the less space a device needs; therefore, more devices can fit into the rack. Figure 2-6 shows multiple servers and disk drives in a rack configuration. Each server occupies one RU and the drives typically take two or more RUs.
Another consideration is equipment with many connections, like switches. They might need to be positioned near patch panels and close to where the cabling is gathered into cable trays.

In an enterprise NOC, thousands of cables can enter and exit the facility. *Structured cabling* creates an organized cabling system that is easily understood by installers, network administrators, and any other technicians who work with cables.

Cable management serves many purposes. First, it presents a neat and organized system that aids in isolating cabling problems. Second, best cabling practices protect the cables from physical damage and *electromagnetic interference (EMI)*, which greatly reduces the number of problems experienced.

To assist in troubleshooting

- All cables should be labeled at both ends, using a standard convention that indicates source and destination.
- All cable runs should be documented on the physical network topology diagram.
- All cable runs, both copper and fiber, should be tested end to end by sending a signal down the cable and measuring loss.

Cabling standards specify a maximum distance for all cable types and network technologies. For example, the IEEE specifies that, for Fast Ethernet over unshielded twisted-pair (UTP), the cable run from switch to host cannot be greater than 100 meters (approximately 328 ft.). If the cable run is greater than the recommended length, problems could occur with data communications, especially if the terminations at the ends of the cable are poorly completed.

Documentation of the cable plan and testing are critical to network operations. Figure 2-7 shows cabling routed efficiently to the back of a patch panel. Cable bends are minimized, and each cable is clearly labeled for its destination.
Telecommunication Room Design and Considerations

The NOC is the heart of the enterprise. In practice, however, most users connect to a switch in a telecommunications room, which is some distance from the NOC. The telecommunications room is also referred to as a wiring closet or intermediate distribution facility (IDF). It contains the access layer networking devices and ideally maintains environmental conditions similar to the NOC, such as air conditioning and UPS. IDFs typically contain

- Fast Ethernet switches
- Gigabit link to MDF
- Wireless access points

Users working with wired technology connect to the network through Ethernet switches or hubs. Users working with wireless technology connect through an access point (AP). Access layer devices such as switches and APs are a potential vulnerability in network security. Physical and remote access to this equipment should be limited to authorized personnel. Network personnel can also implement port security and other measures on switches, as well as various wireless security measures on APs.

Securing the telecommunications room has become even more important because of the increasing occurrence of identity theft. New privacy legislation results in severe penalties if confidential data from a network falls into the wrong hands. Modern networking devices offer capabilities to help prevent these attacks and protect data and user integrity.

Many IDFs connect to a main distribution facility (MDF) using an extended star design. The MDF is usually located in the NOC or centrally located within the building.

MDFs are typically larger than IDFs. They house high-speed switches, routers, and server farms. The central MDF switches can have enterprise servers and disk drives connected using gigabit copper links. MDFs typically contain

- Point of presence (POP)
- Routers
- Gigabit switches
IDFs contain lower-speed switches, APs, and hubs. The switches in the IDFs typically have large numbers of Fast Ethernet ports for users to connect at the access layer.

The switches in the IDF usually connect to the switches in the MDF with Gigabit interfaces. This arrangement creates backbone connections, or uplinks. These backbone links, also called vertical cabling, can be copper or fiber-optic. Copper Gigabit or Fast Ethernet links are limited to a maximum of 100 meters and should use CAT5e or CAT6 UTP cable. Fiber-optic links can run much greater distances. Fiber-optic links commonly interconnect buildings, and because they do not conduct electricity, they are immune to lightning strikes, EMI, RFI, and differential grounds. Figure 2-8 illustrates a multi-building Ethernet network design with one MDF in Building A and IDFs in Buildings A, B, and C. The vertical or backbone cabling connecting the MDF and the two IDFs in Building A can be UTP or fiber depending on distance. Vertical (and horizontal) cable runs longer than 100 meters (approx. 328 ft.) should be fiber-optic.

Figure 2-8  MDFs and IDFs Connect Multiple Buildings and Users

The vertical cabling between the buildings should always be fiber-optic, regardless of distance, to account for the electrical differential between buildings. Inter-building cabling can also be exposed to weather and lightning strikes, which fiber-optic can withstand more easily without damaging equipment connected to it.

In addition to providing basic network access connectivity, it is becoming more common to provide power to end-user devices directly from the Ethernet switches in the telecommunications room. These devices include IP phones, access points, and surveillance cameras.
These devices are powered using the IEEE 802.3af standard, *Power over Ethernet (PoE)*. PoE provides power to a device over the same twisted-pair cable that carries data. This allows an IP phone, for example, to be located on a desk without the need for a separate power cord or a power outlet. To support PoE devices such as the IP phone, the connecting switch must have PoE capability.

PoE can also be provided by power injectors or PoE patch panels for those switches that do not support PoE. Panduit and other suppliers produce PoE patch panels that allow non-PoE-capable switches to participate in PoE environments. Legacy switches connect into the PoE patch panel, which then connects to the PoE-capable device. Figure 2-9 illustrate devices that can be powered by a PoE-capable switch. This allows the devices to be placed without regard to the location of power outlets.

**Figure 2-9 End Devices Receive Power from a PoE Switch**

Interactive Activity 2-2: Placing MDFs, IDFs, and Cabling (2.1.3)

In this activity, you place the MDFs and IDFs in an appropriate location in the campus diagram and identify appropriate cables to connect them. Use file d3ia-213 on the CD-ROM that accompanies this book to perform this interactive activity.

Supporting the Enterprise Edge

The enterprise edge is the entry and exit point to the network for external users and services. The following sections describe how external services are delivered as well as security considerations at the edge.

Service Delivery at the Point of Presence

At the outer edge of the enterprise network is the *point of presence (POP)*, which provides an entry point for services to the enterprise network. Externally provided services coming in through the POP include Internet access, wide-area connections, and telephone services (public switched telephone network [PSTN]).
The POP contains a point of demarcation, or the demarc. The demarc provides a boundary that designates responsibility for equipment maintenance and troubleshooting between the service provider (SP) and customer. Equipment from the service provider up to the point of demarcation is the responsibility of the provider; anything past the demarc point is the responsibility of the customer.

In an enterprise, the POP provides links to outside services and sites. The POP can provide a direct link to one or more ISPs, which allows internal users the required access to the Internet. The remote sites of an enterprise are also interconnected through the POPs. The service provider establishes the wide-area links between these remote sites.

The location of the POP and the point of demarcation vary in different countries. While they are often located within the MDF of the customer, they can also be located at the SP.

Figure 2-10 shows an example of a school district with a hub-and-spoke, or star, design. The school district main office is the center of the star or hub and has the primary connections to the Internet and the PSTN. Each of the schools A, B, C, and D connect back to the district office for phone and Internet access to the outside world. The district office and each of the schools have their own POP to make the necessary WAN connections. Each school is connected to the district office with a T1 circuit with a bandwidth of 1.544 Mbps. Because all the schools share the main Internet connection at the district office, the connection to the ISP is a T3 circuit with approximately 45 Mbps bandwidth. This is a scalable design, where additional schools with T1s can connect back to the district office. This design can be applied to businesses and other organizations with multiple remote locations that connect to a central site. If additional remote sites are added to the network, the bandwidth of the Internet and PSTN connections at the central site can be upgraded to higher-speed links, if necessary.

![Figure 2-10 POPs at Each Location Connect Schools to the District Office and External Services](image)

**Security Considerations at the Enterprise Edge**

Large enterprises usually consist of multiple sites that interconnect. Multiple locations can have edge connections at each site connecting the enterprise to other individuals and organizations.

The edge is the point of entry for outside attacks and is a point of vulnerability. Attacks at the edge can affect thousands of users. For example, denial of service (DoS) attacks prevent access to resources for legitimate users inside or outside the network, affecting productivity for the entire enterprise.
All traffic into or out of the organization goes through the edge. Edge devices must be configured to defend against attacks and provide filtering based on website, IP address, traffic pattern, application, and protocol.

An organization can deploy a firewall and security appliances with an intrusion detection system (IDS) and intrusion prevention system (IPS) at the edge to protect the network. They can also set up a demilitarized zone (DMZ), an area isolated by firewalls, where web and FTP servers can be placed for external users to access.

External network administrators require access for internal maintenance and software installation. Virtual Private Networks (VPN), access control lists (ACL), user IDs, and passwords provide that access. VPNs also allow remote workers access to internal resources. Figure 2-11 depicts a network with the headquarters (HQ) as the edge, with security protection tools deployed to protect the internal network.

**Figure 2-11  Security Defense Tools at the Enterprise Edge**

![Security Defense Tools at the Enterprise Edge](image)

**Connecting the Enterprise Network to External Services**

The network connection services commonly purchased by an enterprise include leased lines (T1/E1), Frame Relay, and ATM. Physical cabling brings these services to the enterprise using copper wires, as in the case of T1/E1, or fiber-optic cable for higher-speed services.

The POP must contain certain pieces of equipment to obtain whichever WAN service is required. For example, to obtain T1/E1 service, the customer might require a punchdown block to terminate the T1/E1 circuit, as well as a channel service unit/data service unit (CSU/DSU) to provide the proper
electrical interface and signaling for the service provider. This equipment can be owned and main- 
tained by the service provider or can be owned and maintained by the customer. Regardless of owners- 
ship, all equipment located within the POP at the customer site is referred to as customer premise 
equipment (CPE). The CSU/DSU can be an external standalone device connected to the edge router 
with a cable or it can be integrated into the router.

Figure 2-12 shows an example of the equipment in the proper sequence required to bring a T1 circuit 
from a service provider to a customer and finally to the end user. The T1 can be provided by an SP or 
an ISP and can provide access to the Internet directly or to another site to form a WAN.

**Interactive Activity 2-3: Specifying Components to Bring Service to the Internal Network**

In this activity, you specify the components, in order, needed to connect a service from the edge to the 
internal network. Use file d3ia-223 on the CD-ROM that accompanies this book to perform this inter-
active activity.

**Reviewing Routing and Switching**

The following sections provide a review of router and switch hardware characteristics. They also 
serve as a review of router and switch commands most commonly used to display information about 
and configure these devices.
Router Hardware

One important device in the distribution layer of an enterprise network is a router. Without the routing process, packets could not leave the local network.

The router provides access to other private networks as well as to the Internet. All hosts on a local network specify the IP address of the local router interface in their IP configuration. This router interface is the default gateway.

Routers play a critical role in networking by interconnecting multiple sites within an enterprise network, providing redundant paths, and connecting ISPs on the Internet. Routers can also act as a translator between different media types and protocols. For example, a router can re-encapsulate packets from an Ethernet to a serial encapsulation.

Routers use the network portion of the destination IP address to route packets to the proper destination. They select an alternate path if a link goes down or traffic is congested. Routers also serve the following other beneficial functions:

- **Provide broadcast containment:** Routers in the distribution layer limit broadcasts to the local network where they need to be heard. Although broadcasts are necessary, too many hosts connected on the same local network generate excessive broadcast traffic and slow the network.

- **Connect remote locations:** Routers in the distribution layer interconnect local networks at various locations of an organization that are geographically separated.

- **Group users logically by application or department:** Routers in the distribution layer logically group users, such as departments within a company, who have common needs or for access to resources.

- **Provide enhanced security (using Network Address Translation [NAT] and ACLs):** Routers in the distribution layer separate and protect certain groups of computers where confidential information resides. Routers also hide the addresses of internal computers from the outside world to help prevent attacks and control who gets into or out of the local network.

With the enterprise and the ISP, the ability to route efficiently and recover from network link failures is critical to delivering packets to their destination. Figure 2-13 depicts each of the main functions the routers can perform.
Routers come in many shapes and sizes called *form factors*, as shown in Figure 2-14, and can support a few users or thousands of users, depending on the size and needs of the organization. Network administrators in an enterprise environment should be able to support a variety of routers and switches, from a small desktop to a rack-mounted or blade model.
Routers can also be categorized as fixed configuration or modular. With the fixed configuration, the desired router interfaces are built in. Modular routers come with multiple slots that allow a network administrator to change the interfaces on the router. As an example, a Cisco 1841 router comes with two Fast Ethernet RJ-45 interfaces built in and two slots that can accommodate many different network interface modules.

Routers come with a variety of different interfaces, such as Fast and Gigabit Ethernet, serial, and fiber-optic. Router interfaces use the controller/interface or controller/slot/interface conventions. For example, using the controller/interface convention, the first Fast Ethernet interface on a router is numbered as Fa0/0 (controller 0 and interface 0). The second is Fa0/1. The first serial interface on a router using controller/slot/interface is S0/0/0. Figure 2-15 shows the back of an 1841 ISR router with a serial interface card and an integrated 4-port Fast Ethernet switch.

Two methods exist for connecting a PC to a network device for configuration and monitoring tasks: *out-of-band* and *in-band* management.

**Out-of-Band Management**

Out-of-band management is used for initial configuration or when a network connection is not unavailable. If there is a problem with access to a network device through the network, it might be
necessary to use out-of-band management. For example, a WAN serial interface on a remote router might have been misconfigured so that normal network access is not possible. If the AUX port is properly configured for remote access and a dialup modem is connected, it might be possible to dial in to the modem using out-of-band management and reconfigure the router to correct the problem. Configuration using out-of-band management requires

- Direct connection to the device console port or a direct or remote connection (through dialup) to the AUX port
- Terminal emulation client

In-Band Management

In-band management is used to monitor and make configuration changes to a network device over a network connection. With in-band, the connection shares network bandwidth with other hosts on the network. Configuration using in-band management requires

- At least one network interface on the device to be connected and operational
- Valid IP configuration on interfaces involved (for an IP-based network)
- Telnet, Secure Shell (SSH), or HTTP to access a Cisco device (these protocols are primarily IP based)

Figure 2-16 shows two forms of out-of-band and two forms of in-band management.

**Figure 2-16 Out-of-Band and In-Band Management Methods**

![Out-of-Band Router Configuration](image1)

![In-Band Router Configuration](image2)

**Basic Router CLI show Commands**

This section includes some of the most commonly used Cisco IOS commands to display and verify the operational status of the router and related network functionality. These commands are divided into several categories, as shown in Table 2-1.

Table 2-1 lists these commands with common options used and the minimum abbreviation allowable, along with a description of their function and key information displayed.
<table>
<thead>
<tr>
<th>Table 2-1</th>
<th>Common Router show Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full Command</strong></td>
<td><strong>Abbreviation</strong></td>
</tr>
<tr>
<td><strong>General Use</strong></td>
<td></td>
</tr>
<tr>
<td>show running-config</td>
<td>sh run</td>
</tr>
<tr>
<td>show startup-config</td>
<td>sh star</td>
</tr>
<tr>
<td>show version</td>
<td>sh ve</td>
</tr>
<tr>
<td><strong>Routing Related</strong></td>
<td></td>
</tr>
<tr>
<td>show ip protocols</td>
<td>sh ip pro</td>
</tr>
<tr>
<td>show ip route</td>
<td>sh ip ro</td>
</tr>
<tr>
<td><strong>Interface Related</strong></td>
<td></td>
</tr>
<tr>
<td>show interfaces (type #)</td>
<td>sh int f0/0</td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>sh ip int br</td>
</tr>
<tr>
<td>show protocols</td>
<td>sh prot</td>
</tr>
<tr>
<td><strong>Connectivity Related</strong></td>
<td></td>
</tr>
<tr>
<td>show cdp neighbors (detail)</td>
<td>sh cdp ne</td>
</tr>
<tr>
<td>show sessions</td>
<td>sh ses</td>
</tr>
<tr>
<td>show ssh</td>
<td>sh ssh</td>
</tr>
<tr>
<td>ping (ip / hostname)</td>
<td>p</td>
</tr>
<tr>
<td>traceroute (ip / hostname)</td>
<td>tr</td>
</tr>
</tbody>
</table>
Figure 2-17 shows two networks (192.168.1.0/24 and 192.168.3.0/24) interconnected with a WAN link (network 192.168.2.0/24).

**Figure 2-17 Multi-router and Multi-switch Network**

![](image_url)

The following examples display the `show` command output for the R1 model 1841 router in the Figure 2-17 network topology. Example 2-1 shows the `show running-config` output for R1.

**Example 2-1 R1 show running-config Command Output**

```
R1# show running-config

<output omitted>
Building configuration...
Current configuration : 1063 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
enable secret 5 $1$i6w9$dvdpVM6zV10E6tSyLdkR5/
no ip domain lookup
!
interface FastEthernet0/0
description LAN 192.168.1.0 default gateway
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
description WAN link to R2
ip address 192.168.2.1 255.255.255.0
encapsulation ppp
clock rate 64000
no fair-queue
```
Example 2-2 presents the `show version` output for R1.

**Example 2-2  R1 show version Command Output**

```
R1# show version
<output omitted>
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(10b),
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
R1 uptime is 43 minutes
System returned to ROM by reload at 22:05:12 UTC Sat Jan 5 2008
System image file is "flash:c1841-advipservicesk9-mz.124-10b.bin"

Cisco 1841 (revision 6.0) with 174080K/22528K bytes of memory.
Processor board ID FTX1111W0QF
6 FastEthernet interfaces
2 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
62720K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```
Example 2-3 presents the **show ip protocols** output for R1.

**Example 2-3 R1 show ip protocols Command Output**

```plaintext
R1# show ip protocols

Routing Protocol is "rip"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Sending updates every 30 seconds, next due in 20 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Redistributing: rip
Default version control: send version 2, receive version 2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Send</th>
<th>Recv</th>
<th>Triggered RIP</th>
<th>Key-chain</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet0/0</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial0/0/0</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  192.168.1.0
  192.168.2.0

Routing Information Sources:

<table>
<thead>
<tr>
<th>Gateway</th>
<th>Distance</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.2.2</td>
<td>120</td>
<td>00:00:20</td>
</tr>
</tbody>
</table>

Distance: (default is 120)
```

Example 2-4 presents the **show ip route** output for R1.

**Example 2-4 R1 show ip route Command Output**

```plaintext
R1# show ip route

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

Gateway of last resort is not set
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:24, Serial0/0/0
```

Example 2-5 presents the **show interfaces** output for R1.
Example 2-5 R1 show interfaces Command Output

R1# show interfaces

< Some output omitted >

FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.5325.256e (bia 001b.5325.256e)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
   reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:17, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  196 packets input, 31850 bytes
    Received 181 broadcasts, 0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog
    0 input packets with dribble condition detected
  392 packets output, 35239 bytes, 0 underruns
    0 output errors, 0 collisions, 3 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out

FastEthernet0/1 is administratively down, line protocol is down

Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
   reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Listen, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:02, output 00:00:03, output hang never
  Last clearing of "show interface" counters 00:51:52
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  401 packets input, 27437 bytes, 0 no buffer
    Received 293 broadcasts, 0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  389 packets output, 26940 bytes, 0 underruns
Example 2-6 presents the **show ip interfaces brief** output for R1.

**Example 2-6 R1 show ip interfaces brief Command Output**

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK? Method Status</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>FastEthernet0/0</td>
<td>192.168.1.1</td>
<td>YES manual up</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>FastEthernet0/1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Serial0/0/0</td>
<td>192.168.2.1</td>
<td>YES manual up</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Serial0/0/1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Vlan1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>up</td>
<td>down</td>
</tr>
</tbody>
</table>

Example 2-7 presents the **show protocols** output for R1.

**Example 2-7 R1 show protocols Command Output**

```
R1# show protocols

Global values:
   Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
   Internet address is 192.168.1.1/24
FastEthernet0/1 is administratively down, line protocol is down
FastEthernet0/1/0 is up, line protocol is down
FastEthernet0/1/1 is up, line protocol is down
FastEthernet0/1/2 is up, line protocol is down
FastEthernet0/1/3 is up, line protocol is down
Serial0/0/0 is up, line protocol is up
   Internet address is 192.168.2.1/24
Serial0/0/1 is administratively down, line protocol is down
Vlan1 is up, line protocol is down
```

Example 2-8 presents the **show cdp neighbors** output for R1.
Example 2-8 R1 show cdp neighbors Command Output

```
R1# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Infrerce     Holdtime Capability Platform  Port ID
R2               Ser 0/0/0          137       R S I      1841      Ser 0/0/0
S1               Fas 0/0            175         S I       WS-C2960- Fas 0/1
```

Example 2-9 presents the `show cdp neighbors detail` output for R1.

Example 2-9 R1 show cdp neighbors detail Command Output

```
R1# show cdp neighbors detail

-------------------------
Device ID: R2
Entry address(es):
   IP address: 192.168.2.2
Platform: Cisco 1841, Capabilities: Router Switch IGMP
Interface: Serial0/0/0, Port ID (outgoing port): Serial0/0/0
Holdtime : 164 sec
Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(10b),
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team
advertisement version: 2
VTP Management Domain: ''
-------------------------
Device ID: S1
Entry address(es):
   IP address: 192.168.1.5
Platform: cisco WS-C2960-24TT-L, Capabilities: Switch IGMP
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/1
Holdtime : 139 sec
Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)SEE3, RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 22-Feb-07 13:57 by myl
advertisement version: 2
Protocol Hello: OUI=0x00000C, Protocol ID=0x0112; payload len=27, value=00000000
0FFFFFFF010221FF000000000000001D46350C80FF0000
VTP Management Domain: ''
Native VLAN: 1
Duplex: full
```
Interactive Activity 2-4: Matching the Command to the Information Needed (2.3.2)

In this activity, you identify the command that can provide the information indicated. Use file d3ia-232 on the CD-ROM that accompanies this book to perform this interactive activity.

Basic Router Configuration Using CLI

A basic router configuration includes the host name for identification, passwords for security, and assignment of IP addresses to interfaces for connectivity. Verify and save configuration changes using the `copy running-config startup-config` command. To clear the router configuration, use the `erase startup-config` command and then the `reload` command. Table 2-2 shows common IOS commands used to configure routers. Also listed are the abbreviation, the purpose of the command, and the required mode to execute the command.

Table 2-2 Common Router Configuration Commands

<table>
<thead>
<tr>
<th>Full Command / Example</th>
<th>Abbreviation</th>
<th>Purpose / Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td><code>en</code></td>
<td>Changes from user EXEC mode (&gt;) to privileged EXEC mode (#)</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td><code>conf t</code></td>
<td>Changes from privileged EXEC mode to global configuration mode</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td><code>cop r s</code></td>
<td>Copies the running configuration from RAM to the startup configuration file in NVRAM</td>
</tr>
<tr>
<td><code>erase startup-config</code></td>
<td><code>era sta</code></td>
<td>Deletes the startup configuration file (startup-config)</td>
</tr>
<tr>
<td><code>reload</code></td>
<td><code>rel</code></td>
<td>Performs a software reboot</td>
</tr>
<tr>
<td><strong>Global Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>hostname R1</code></td>
<td><code>ho</code></td>
<td>Sets the device host name to R1</td>
</tr>
<tr>
<td><code>banner motd #XYZ#</code></td>
<td><code>ban m</code></td>
<td>Sets the banner message of the day, which is displayed at login, to XYZ</td>
</tr>
<tr>
<td><code>enable secret itsasecret</code></td>
<td><code>ena s</code></td>
<td>Sets the privileged mode encrypted password to itsasecret</td>
</tr>
<tr>
<td><strong>Line Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>line con 0</code></td>
<td><code>lin c</code></td>
<td>Enters line config mode for console port 0</td>
</tr>
<tr>
<td><code>line aux 0</code></td>
<td><code>lin a</code></td>
<td>Enters line config mode for auxiliary port 0</td>
</tr>
<tr>
<td><code>line vty 0 4</code></td>
<td><code>lin v</code></td>
<td>Enters line config mode for VTY lines 0 through 4</td>
</tr>
<tr>
<td><code>login</code></td>
<td><code>login</code></td>
<td>Allows login to a line in line config mode</td>
</tr>
<tr>
<td><code>password</code></td>
<td><code>pas</code></td>
<td>Sets line login password in line config mode</td>
</tr>
<tr>
<td>Full Command / Example</td>
<td>Abbreviation</td>
<td>Purpose / Mode</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>Interface Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface S0/0/0</td>
<td>int</td>
<td>Enters interface config mode for interface Serial 0/0/0 (specifies the interface as type/number)</td>
</tr>
<tr>
<td>description XYZ</td>
<td>des</td>
<td>Specifies a description for the interface as XYZ (in interface config mode)</td>
</tr>
<tr>
<td>ip address 192.168.1.1</td>
<td>ip add</td>
<td>Specifies an IP address and subnet mask for the interface (in interface config mode)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>no shutdown</td>
<td>no sh</td>
<td>Brings up the interface (in interface config mode). Use shutdown to disable the interface.</td>
</tr>
<tr>
<td>clock rate 64000</td>
<td>clo r</td>
<td>Sets the clock rate for a serial interface, with a DCE cable connected, to 64000 (in interface config mode)</td>
</tr>
<tr>
<td>encapsulation ppp</td>
<td>enc</td>
<td>Specifies the encapsulation for the interface as ppp (in interface config mode)</td>
</tr>
<tr>
<td><strong>Routing Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>router rip</td>
<td>router</td>
<td>Enters router config mode for the RIP routing protocol</td>
</tr>
<tr>
<td>network 172.16.0.0</td>
<td>net</td>
<td>Specifies network 172.16.0.0 to be advertised by RIP (in RIP router config mode)</td>
</tr>
<tr>
<td>ip route 172.16.0.0</td>
<td>ip route</td>
<td>Specifies a static route to network 172.16.0.0 through exit interface Serial 0/0/0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>255.255.0.0 S0/0/0</td>
</tr>
<tr>
<td>ip route 0.0.0.0 0.0.0.0</td>
<td>ip route</td>
<td>Specifies a static default route through next-hop IP address 192.168.2.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192.168.2.2</td>
</tr>
</tbody>
</table>

Example 2-10 shows the configuration commands used to configure the R1 router in Figure 2-18. Refer to Example 2-1 to see the results of the commands as displayed with the show running-config command. The resulting running configuration frequently has a number of commands inserted automatically by the IOS that were not entered during the configuration process.

**Example 2-10  Router R1 Basic Configuration Commands**

```
Router> enable
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname R1
R1(config)# banner motd %Unauthorized Access Prohibited%
R1(config)# enable secret class
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# line aux 0
R1(config-line)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
```
It is common to copy the running configuration of a device, such as the R1 router, and paste it into a text editor file for backup or use it as a starting point for modification. The text file can then be edited as necessary so that it can be used to reconfigure the router or configure another router.

**Note**

After a device has been configured, it is critical to copy the running configuration to the startup configuration using the `copy run start` command. Otherwise, changes will be lost if the router is restarted using the `reload` command or if it loses power.

---

**Basic Router Configuration Using CLI (2.3.3)**

In this activity, you practice basic router configuration and verification commands. Use file d3-233.pka on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

---

**Switch Hardware**

Although all three layers of the hierarchical design model contain switches and routers, the access layer generally has more switches. The main function of switches is to connect hosts such as end-user workstations, servers, IP phones, web cameras, access points, and routers. This means that there are many more switches in an organization than routers.

As shown in Figure 2-18, switches come in many form factors:

- Small standalone models sit on a desk or mount on a wall.
- Integrated routers include a switch built into the chassis that is rack mounted.
- High-end switches mount into a rack and are often a chassis-and-blade design to allow more blades to be added as the number of users increases.
High-end enterprise and service provider switches support ports of varying speeds, from 100 MB to 10 GB.

An enterprise switch in an MDF connects other switches from IDF directors using Gigabit fiber or copper cable. An IDF switch typically needs both RJ-45 Fast Ethernet ports for device connectivity and at least one Gigabit Ethernet port (copper or fiber) to uplink to the MDF switch. Some high-end switches have modular ports that can be changed if needed. For example, it might be necessary to switch from multimode fiber to single-mode fiber, which would require a different port.

Like routers, switch ports are also designated using the controller/port or controller/slot/port convention. For example, using the controller/port convention, the first Fast Ethernet port on a switch is numbered as Fa0/1 (controller 0 and port 1). The second is Fa0/2. The first port on a switch that uses controller/slot/port is Fa0/0/1. Gigabit ports are designated as Gi0/1, Gi0/2, and so on.

**Port density** on a switch is an important factor. In an enterprise environment where hundreds or thousands of users need switch connections, a switch with a 1RU height and 48 ports has a higher port density than a 1RU 24-port switch. Figure 2-19 shows a Cisco Catalyst 4948 switch with 48 access ports capable of operating at 10 Mbps (regular Ethernet), 100 Mbps (Fast Ethernet), or 1000 Mbps (Gigabit Ethernet). In addition, it has two built-in 10-Gbps UTP ports and two modular ports that can accept various fiber-optic Ethernet interfaces, including 10-Gbps multimode or single-mode.
Basic Switch CLI Commands

Switches make use of common IOS commands for configuration, to check for connectivity and to display current switch status. These commands can be divided into several categories, as shown in Table 2-2.

Table 2-3 lists these commands with common options used and the minimum abbreviation allowable, along with a description of their function and key information displayed.

### Table 2-3  Common Switch show Commands

<table>
<thead>
<tr>
<th>Full Command</th>
<th>Abbreviation</th>
<th>Purpose / Information Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Use</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>show running-config</td>
<td>sh run</td>
<td>Displays current config running in RAM. Includes host name, passwords, interface IP addresses (if present), port numbers, and characteristics (duplex/speed).</td>
</tr>
<tr>
<td>show startup-config</td>
<td>sh star</td>
<td>Displays backup config in NVRAM. Can be different if running config has not been copied to backup.</td>
</tr>
<tr>
<td>show version</td>
<td>sh ve</td>
<td>Displays IOS version, ROM version, switch uptime, system image file name, boot method, number and type of interfaces installed, and amount of RAM, NVRAM, and flash. Also shows the Configuration register.</td>
</tr>
<tr>
<td><strong>Interface / Port Related</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>show interfaces</td>
<td>sh int f0/l</td>
<td>Displays one or all interfaces with line (protocol) status, bandwidth, delay, reliability, encapsulation, duplex, and I/O statistics.</td>
</tr>
<tr>
<td>(type and number)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show ip interface brief</td>
<td>sh ip int br</td>
<td>Displays all interfaces with IP address with interface status (up/down/admin down) and line protocol status (up/down).</td>
</tr>
</tbody>
</table>
### Full Command | Abbreviation | Purpose / Information Displayed
--- | --- | ---
**Interface / Port Related**
show port-security | sh por | Displays any ports where security has been activated, along with max address allowed, current count, security violation count, and action to take (normally shut-down).
show mac-address-table | sh mac-a | Displays all MAC addresses the switch has learned, how learned (dynamic/static), the port number, and VLAN the port is in.

**Connectivity Related**
show cdp neighbors (detail) | sh cdp ne | Displays information on directly connected devices, including device ID (host name), local interface where device is connected, capability (R=router, S=switch), platform (e.g., WS-2950-2), and port ID of remote device. The detail option provides the IP address of the other device as well as the IOS version.
show sessions | sh ses | Displays Telnet sessions (VTY) with remote hosts. Displays session number, host name, and address.
show ssh | sh ssh | Displays SSH server connections with remote hosts.
ping (ip / hostname) | p | Sends five ICMP echo requests to an IP address or host name (if DNS is available) and displays the min/max and avg time to respond.
traceroute (ip / hostname) | tr | Sends echo request with varying TTL. Lists routers (hops) in path and time to respond.

The same in-band and out-of-band management techniques that apply to routers also apply to switch configuration.

The following examples display show command output for the S1 model 2960 switch in the Figure 2-18 network topology. This switch has 24 10/100 Ethernet UTP ports and two Gigabit ports. Port Fa0/3 has a host attached and port security has been set. If the mac-address sticky option is used with the switchport port-security command, the running configuration is automatically updated when the MAC address of the host attached to that port is learned.

Example 2-11 presents the show running-config output for S1.

**Example 2-11  S1 show running-config Command Output**

```
S1# show running-config
< output omitted >
Building configuration...
Current configuration : 1373 bytes
!
version 12.2
```
Example 2-12 presents the `show version` command output for S1.
Example 2-12  S1 show version Command Output

S1# show version

< output omitted >
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)SEE3, RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 22-Feb-07 13:57 by myl
Image text-base: 0x00003000, data-base: 0x00AA3380

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)SEE1, RELEASE SOFTWARE (fc1)

S1 uptime is 55 minutes
System returned to ROM by power-on

cisco WS-C2960-24TT-L (PowerPC405) processor (revision D0) with 61440K/4088K bytes of memory.
Processor board ID FOC1129X56L
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address : 00:1D:46:35:0C:80
Motherboard assembly number : 73-10390-04
Power supply part number : 341-0097-02
Motherboard serial number : FOC11285HJ7
Power supply serial number : AZ511280656
Model revision number : D0
Motherboard revision number : A0
Model number : WS-C2960-24TT-L
System serial number : FOC1129X56L
Top Assembly Part Number : 800-27221-03
Top Assembly Revision Number : A0
Version ID : V03
CLEI Code Number : COM3L00BRB
Hardware Board Revision Number : 0x01

<table>
<thead>
<tr>
<th>Switch</th>
<th>Ports</th>
<th>Model</th>
<th>SW Version</th>
<th>SW Image</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>WS-C2960-24TT-L</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* 1 26  WS-C2960-24TT-L  12.2(25)SEE3  C2960-LANBASE-M

Configuration register is 0xF

Example 2-13 presents the **show interfaces** command output for S1.
Example 2-13  S1 show interfaces Command Output

S1# show interfaces

< output omitted >
Vlan1 is up, line protocol is up
Hardware is EtherSVI, address is 001d.4635.0cc0 (bia 001d.4635.0cc0)
Internet address is 192.168.1.5/24
MTU 1500 bytes, BW 10000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:09, output 00:47:51, output hang never
Last clearing of 'show interface' counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
216 packets input, 23957 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicast)
0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
25 packets output, 5161 bytes, 0 underruns
0 output errors, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
FastEthernet0/1 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 001d.4635.0c81 (bia 001d.4635.0c81)
MTU 1500 bytes, BW 10000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is 10/100BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:28, output 00:00:00, output hang never
Last clearing of 'show interface' counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
564 packets input, 57713 bytes, 0 no buffer
Received 197 broadcasts (0 multicast)
0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 195 multicast, 0 pause input
0 input packets with dribble condition detected
2515 packets output, 195411 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out
< output omitted >
Example 2-14 presents the `show ip interface brief` command output for S1.

**Example 2-14  S1 show ip interface brief Command Output**

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK? Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan1</td>
<td>192.168.1.5</td>
<td>YES manual</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/2</td>
<td>unassigned</td>
<td>YES unset</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/3</td>
<td>unassigned</td>
<td>YES unset</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/22</td>
<td>unassigned</td>
<td>YES unset</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/23</td>
<td>unassigned</td>
<td>YES unset</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/24</td>
<td>unassigned</td>
<td>YES unset</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>GigabitEthernet0/1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>GigabitEthernet0/2</td>
<td>unassigned</td>
<td>YES unset</td>
<td>down</td>
<td></td>
</tr>
</tbody>
</table>

Example 2-15 presents the `show mac-address-table` output for S1.

**Example 2-15  S1 show mac-address-table Command Output**

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>0100.0ccc.cccc</td>
<td>STATIC</td>
<td>CPU</td>
</tr>
<tr>
<td>All</td>
<td>0180.c200.0010</td>
<td>STATIC</td>
<td>CPU</td>
</tr>
<tr>
<td>All</td>
<td>ffff.ffff.ffff</td>
<td>STATIC</td>
<td>CPU</td>
</tr>
<tr>
<td>1</td>
<td>000b.db04.a5cd</td>
<td>DYNAMIC</td>
<td>Fa0/3</td>
</tr>
<tr>
<td>1</td>
<td>001b.5325.256e</td>
<td>DYNAMIC</td>
<td>Fa0/1</td>
</tr>
</tbody>
</table>

Example 2-16 presents the `show port-security` output for S1.

**Example 2-16  S1 show port-security Command Output**

<table>
<thead>
<tr>
<th>Secure Port</th>
<th>MaxSecureAddr (Count)</th>
<th>CurrentAddr (Count)</th>
<th>SecurityViolation (Count)</th>
<th>Security Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fa0/9</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>Shutdown</td>
</tr>
</tbody>
</table>

Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8320
Example 2-17 presents the `show cdp neighbors` output for S1.

**Example 2-17   S1 show cdp neighbors Command Output**

```
S1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID         Local Intrfce        Holdtme    Capability    Platform   Port ID
R1                  Fas 0/1             122           R S I     1841       Fas0/0
```

A basic switch configuration includes the host name for identification, passwords for security, and assignment of IP addresses for connectivity. In-band access requires the switch to have an IP address.

Verify and save the switch configuration using the `copy running-config startup-config` command. To clear the switch configuration, use the `erase startup-config` command and then the `reload` command. You might also need to erase any VLAN information using the `delete flash:vlan.dat` command. Table 2-4 shows common IOS commands used to configure switches. Also listed is a short abbreviation, the purpose of the command, and the required mode to execute the command.

**Table 2-4    Common Switch Configuration Commands**

<table>
<thead>
<tr>
<th>Full Command / Example</th>
<th>Abbreviation</th>
<th>Purpose / Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>en</td>
<td>Changes from user EXEC mode (&gt;) to privileged EXEC mode (#)</td>
</tr>
<tr>
<td>configure terminal</td>
<td>conf t</td>
<td>Changes from privileged EXEC mode to global configuration mode</td>
</tr>
<tr>
<td>copy running-config</td>
<td>cop r s</td>
<td>Copies the running configuration from RAM to the startup configuration file in NVRAM</td>
</tr>
<tr>
<td>startup-config</td>
<td></td>
<td></td>
</tr>
<tr>
<td>erase startup-config</td>
<td>era sta</td>
<td>Deletes the startup configuration file (startup-config)</td>
</tr>
<tr>
<td>delete vlan.dat</td>
<td>del</td>
<td>Removes the VLAN configuration from the switch</td>
</tr>
<tr>
<td>reload</td>
<td>rel</td>
<td>Performs a software reboot</td>
</tr>
<tr>
<td>Global Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>hostname S1</td>
<td>ho</td>
<td>Sets the device host name to S1</td>
</tr>
<tr>
<td>banner motd #XYZ#</td>
<td>Ban m</td>
<td>Sets the banner message of the day, which is displayed at login, to XYZ</td>
</tr>
<tr>
<td>enable secret itsasecret</td>
<td>Ena s</td>
<td>Sets the privileged mode encrypted password to itsasecret</td>
</tr>
<tr>
<td>ip default gateway</td>
<td>ip def ga</td>
<td>Specifies the router gateway the switch will use (in global config mode)</td>
</tr>
<tr>
<td>Full Command / Example</td>
<td>Abbreviation</td>
<td>Purpose / Mode</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>Line Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>line con 0</td>
<td>Lin c</td>
<td>Enters line config mode for console port 0</td>
</tr>
<tr>
<td>line vty 0 4</td>
<td>Lin v</td>
<td>Enters line config mode for VTY lines 0 through 4</td>
</tr>
<tr>
<td>login</td>
<td>login</td>
<td>Allows login to a line in line config mode</td>
</tr>
<tr>
<td>password</td>
<td>Pas</td>
<td>Sets line login password in line config mode</td>
</tr>
<tr>
<td><strong>Interface Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface vlan 1</td>
<td>Int</td>
<td>Enters interface config mode for logical interface management VLAN 1 (default native VLAN)</td>
</tr>
<tr>
<td>ip address 192.168.1.1</td>
<td>ip add</td>
<td>Specifies an IP address and subnet mask for the interface (in VLAN interface config mode)</td>
</tr>
<tr>
<td>255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface f0/1</td>
<td>Int</td>
<td>Enters interface config mode for physical port Fast Ethernet 0/1</td>
</tr>
<tr>
<td>speed 100</td>
<td>Spe</td>
<td>Sets the speed of the interface at 100 Mbps (in interface config mode)</td>
</tr>
<tr>
<td>duplex full</td>
<td>Du</td>
<td>Sets the duplex mode of the interface to full (in interface config mode)</td>
</tr>
<tr>
<td>switchport mode access</td>
<td>switch m a</td>
<td>Sets the switch port to access mode unconditionally (in interface config mode)</td>
</tr>
<tr>
<td>switchport port-security</td>
<td>switch po</td>
<td>Sets basic default port security on a port (in interface config mode)</td>
</tr>
</tbody>
</table>

Example 2-18 shows the configuration commands used to configure the S1 switch in Figure 2-18. Refer to Example 2-11 to see the results of the commands as displayed with the show running-config command. As with the router configuration, the resulting running configuration frequently has a number of commands inserted automatically by the IOS that were not entered during the configuration process.

**Example 2-18 Switch S1 Basic Configuration Commands**

```
Switch> enable
Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# hostname S1
S1(config)# banner motd %Unauthorized Access Prohibited%
S1(config)# enable secret class
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# line vty 0 4
S1(config-line)# password cisco
```
Basic Switch Configuration Using CLI (2.3.5)

In this activity, you configure a switch in a switching environment. Use file d3-235.pka on the CD-ROM that accompanies this book to perform this interactive activity using Packet Tracer.

Lab 2-1: Configuring Basic Routing and Switching (2.3.5)

In this lab, you will connect and configure a multirouter network. Refer to the hands-on lab in Part II of this Learning Guide. You can perform this lab now or wait until the end of the chapter.
Summary


The enterprise NOC manages and monitors all network resources. End users connect to the network through access layer switches and wireless APs in the IDF, and PoE provides power to devices over the same UTP cable that carries data.

The enterprise edge provides Internet access and service for users inside the organization. Edge devices provide security against attacks.

The POP at the edge provides a direct link to an SP or ISP and connects remote sites. The POP contains a demarc line of responsibility between the service provider and customer. Services are brought to the enterprise POP by copper wires or fiber-optic cable.

Distribution layer routers move packets between locations and the Internet and can control broadcasts. Routers and switches use in-band and out-of-band management.

Activities and Labs

This summary outlines the activities and labs you can perform to help reinforce important concepts described in this chapter. You can find the activity and Packet Tracer files on the CD-ROM accompanying this book. The complete hands-on labs appear in Part II.

Interactive Activities on the CD-ROM:

Interactive Activity 2-1: Matching Network Information to Documentation Type (2.1.1)
Interactive Activity 2-2: Placing MDFs, IDFs, and Cabling (2.1.3)
Interactive Activity 2-3: Specifying Components to Bring Service to the Internal Network (2.2.3)
Interactive Activity 2-4: Matching the Command to the Information Needed (2.3.2)

Packet Tracer Activities on the CD-ROM:

Basic Router Configuration Using CLI (2.3.3)
Basic Switch Configuration Using CLI (2.3.5)

Hands-on Labs in Part II of this book:

Lab 2-1: Configuring Basic Routing and Switching (2.3.5)
Check Your Understanding

Complete all the review questions listed here to check your understanding of the topics and concepts in this chapter. Appendix A, “Check Your Understanding and Challenge Questions Answer Key,” lists the answers.

1. Draw a line from each term on the left to its correct description on the right. (Not all terms are used.)

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POP</td>
<td>Maliciously prevents access to network resources by legitimate users</td>
</tr>
<tr>
<td>VPN</td>
<td>Boundary that designates responsibility for equipment maintenance and troubleshooting</td>
</tr>
<tr>
<td>DoS</td>
<td>Physical link to outside networks at the enterprise edge</td>
</tr>
<tr>
<td>CPE</td>
<td>An area of the network accessible to external users and protected by firewalls</td>
</tr>
<tr>
<td>DM</td>
<td>A telecommunications room to which IDFs connect</td>
</tr>
<tr>
<td>Demarc</td>
<td>A method of providing electrical power to Ethernet end devices</td>
</tr>
<tr>
<td></td>
<td>Allows remote workers to access the internal network securely</td>
</tr>
<tr>
<td></td>
<td>Equipment located at the customer facility</td>
</tr>
</tbody>
</table>

2. What information can you find by using the `show mac-address-table` command on a Cisco Catalyst switch?

A. The MAC address of the console interface on the Catalyst switch
B. The MAC addresses of the hosts connected to the switch ports
C. The IP addresses of directly connected network devices
D. The mapping between MAC address and IP address for network hosts

3. While troubleshooting a network problem, the network administrator issues the `show version` command on a router. What information can be found using this command?

A. The amount of NVRAM, DRAM, and flash memory installed on the router
B. The bandwidth, encapsulation, and I/O statistics on the interfaces
C. Differences between the backup configuration and the current running configuration
D. The version of the routing protocols running on the router

4. After gathering a thorough list of network applications, the traffic generated by these applications, and the priority of this traffic, a network engineer wants to integrate this information into a single document for analysis. How can this be accomplished?

A. Create a physical topology map of the network and annotate it with the network application data.
B. Create a logical topology map of the network and annotate it with the network application data.
C. Create a blueprint of the facility, including network cabling and telecommunications rooms, and annotate it with the network applications data.
D. Take a photograph of the facility, and annotate it with the network application data.
5. One evening a network administrator attempted to access a recently deployed website and received a “Page not found” error. The next day the administrator checked the web server logs and noticed that during the same hour that the site failed to load, there were hundreds of requests for the website home page. All the requests originated from the same IP address. Given this information, what might the network administrator conclude?

A. It is normal web-surfing activity.
B. It is likely that someone attempted a DoS attack.
C. The link to the website does not have enough capacity and needs to be increased.
D. The web server was turned off and was not able to service requests.

6. What type of media typically connects an MDF switch to an IDF switch in another building with an Ethernet network?

A. Fiber-optic
B. Coaxial cable
C. Unshielded twisted-pair
D. Shielded twisted-pair

7. Which of the following devices can receive power over the same twisted-pair Ethernet cable that carries data? (Choose three.)

A. Wireless access points
B. Monitors
C. Web cameras
D. IP phones
E. Network switches
F. Laptops

8. Indicate which type of hardware each characteristic describes by marking with an R (router) or S (switch).

A. Defines broadcast domains
B. Connects IP phones and access points to the network
C. Enhances security with ACLs
D. Interconnects networks
E. Appears more commonly at the access layer
F. Connects hosts to the network
G. First Fast Ethernet interface designation is Fa0/0
H. First Fast Ethernet interface designation is Fa0/1

9. Which of the following protocols are normally used to access a Cisco router for in-band management? (Choose two.)

A. ARP
B. SSH
C. FTP
D. SMTP
E. Telnet
10. A network analyst is documenting the existing network at ABC-XYZ Corporation. The analyst decides to start at the core router to identify and document the Cisco network devices attached to the core. Which command executed on the core router provides the required information?

A. show version
B. show ip route
C. show tech-support
D. show running-config
E. show cdp neighbors detail

11. A network administrator suspects that there is a problem with the configuration of the RIP routing protocol. She investigates the interfaces and finds that all interfaces are up/up. Which of the following commands could help to identify the problem? (Choose two.)

A. show cdp neighbors
B. show ip route
C. show sessions
D. show ip protocols
E. show version

12. As a network technician, you are troubleshooting a router configuration. You want to get a concise display of the status of the router interfaces. You also want to verify the IP address of each interface and the subnet mask in slash format (/XX). Which command would you use?

A. show protocols
B. show ip route
C. show running-config
D. show ip protocols
E. show ip interfaces brief

13. What is the correct sequence of devices and connections for providing a T1 service to an organization’s end user? Number each term in the proper sequence.

A. DMZ router
B. T1 circuit line
C. Internal switch
D. CSU/DSU
E. DMZ switch
F. Punchdown block
G. Internal router
H. Service provider
I. End-user PC
14. Which of the following is not a type of network protection device or technique to help security?
   A. DoS
   B. Firewall
   C. ACL
   D. IDS
   E. IPS
   F. DMZ
   G. VPN

**Challenge Questions and Activities**

These questions require a deeper application of the concepts covered in this chapter. You can find the answers in Appendix A.

1. Routers R1 and R2 are connected by a serial link. As a network administrator, you entered the following commands to configure the Serial 0/0/0 interface on Router R1. From Router R1 you are unable to ping the R2 S0/0/0 interface. What interface-related issues could be causing the problem, and what commands would you use on which routers to help isolate the problem?

   ```
   R1(config-if)# interface Serial0/0/0
   R1(config-if)# description WAN link to R2
   R1(config-if)# ip address 192.168.2.1 255.255.255.0
   R1(config-if)# encapsulation ppp
   R1(config-if)# clock rate 64000
   R1(config-if)# no shutdown
   ```

2. ISP or WAN Link Investigation Interview Activity (optional)

   In this activity, you will talk with your instructor or a network administrator at the institution where you work or other organization. Use the following form to ask a few questions to learn more about the organization’s ISP service or service provider being used for a WAN connection.

   Organization: _______________________________________________
   Person’s name: _______________________________________________
   Position/title: _______________________________________________  
   ISP or service provider name: _________________________________
   Internet or WAN: ______________________________________________
   Connection type/speed (DSL, cable, T1/E1, fractional T1, Frame Relay, and so on): _________________________________
   CPE device (CSU/DSU, cable modem, DSL modem, and so on): ______
   If CSU/DSU, location of device (standalone or integrated into router): _______________________________
   Location of POP: _____________________________________________
   Is there a DMZ? _____________________________________________
   Is there an SLA? _____________________________________________
This page intentionally left blank
NUMBERS
2-way state (OSPF protocol neighbor adjacencies), 212
802.1Q frame-tagging standard, 91-92

A
ABR (Area Border Routers), 217
access layer (hierarchical design model), enterprise networks, 6
access ports, 77, 93, 343
access-class command, configuring ACL router VTY access, 305
acknowledgment packets, EIGRP, 185
ACL (Access Control Lists), 281
analyzing, 311
best practices, 318
configuring, 295-297
   statement syntax, 296
   troubleshooting, 375-376
debugging, 375
deleting, 296-297
deny any statements, 288-291, 318
deny statements, 284, 297, 302
echo-reply statements, 308
enterprise edge security, 33
established traffic support, 308
extended ACL, 284
   configuring, 292-293, 299-301
   ping responses, 308
   port filtering, 306-307
   statement creation, 300-301
functions of, 311, 313
implicit deny statements, 284
inbound ACL
   configuring, 294
   placement, 286
inter-VLAN routing, configuring via, 313
latency, 286
logging, 314-315
   analyzing router logs, 317
   security levels, 316
   syslog messages, 316-317
   troubleshooting, 375
match-tracking, 315
NAC, configuring, 308
NACL, 284
   configuring, 302-304
   deleting statements, 303
   inserting new lines in, 304
NAT, 309-310
outbound ACL
   configuring, 294
   placement, 286
PAT, 309
permit statements, 284, 297, 302
problems with, 283
processing, 284-286
remark statements, 297
router VTY access, configuring, 304-305
routers, 285-286
standard ACL, 284
   configuring, 292, 297-299
   Dynamic NAT configuration, 145
troubleshooting, 374-376
unreachable statements, 308
wildcard masks
   converting subnet masks to, 290-291
   filtering specific hosts, 289-290
   packet-matching, 288
   statement creation, 288
   structure of, 287
active topologies, 85
AD (Administrative Distance), 163
   comparison table, 180
   multiple routing protocols, 233-236
AD (Advertised Distance) metrics, EIGRP, 188
adaptive cut through switching, 70
adjacencies
   EIGRP neighbors, 184-185
   OSPF protocol neighbors, 212-213
   viewing, 190
advertisement requests (VTP), 99
aggregation (routes). See summarization (routes)
aging time, 67
analog data connections, 251
AP (Access Points), 29
Area 0 (OSPF networks), 216
areas (OSPF protocol), 208
   ABR, 217
   Area 0, 216
   ID, 218
as-built diagrams, 24
ASBR (Autonomous System Boundary Routers), 217, 228-229
ASIC (Application-Specific Integrated Circuits), 69
asymmetric switching, 68
ATM (Asynchronous Transfer Mode), 255
authentication
   LCP, 262
   MD5, RIP, 175
   OSPF protocol, 221
   PPP, 270
      CHAP, 267-269
      PAP, 266-269
   WAN
      debugging, 373
      troubleshooting, 372
authentication phase (PPP), 262
authentication servers, CHAP, 268
auto-cost reference-bandwidth command, OSPF protocol
bandwidth modification, 224
autonomous systems
   ASBR, 217, 228-229
   OSPF, 217
availability, redundancy in switched networks, 72

B
BackboneFast, 81
backups
   redundant backup sites, 330
   server farms, 26
bandwidth
   metrics, EIGRP, 186
   OSPF protocol modifications, 223
   reference bandwidth, OSPF protocol, 224
   STDM, 253
   TDM, 252
   time slices, 252
bandwidth command
   EIGRP, 190
   OSPF protocol bandwidth modification, 223
baselines (network monitoring), 330
Be (committed burst), 273
BCP (Business Continuity Plans), 24, 330, 333
BDR (Backup Designated Routers)
   DROthers, 213-214
   Full state (OSPF protocol neighbor adjacencies), 213
   OSPF protocol
      interaction with, 213-215
      selecting in, 222
      router ID, 213-214, 222
Be (excess bursts), 273
BECN (Backward Explicit Congestion Notification), Frame
   Relay encapsulation, 274
BID (Bridge IDs), 78
blocked ports, 79
blocking state (switches), 77
blueprints, redlined, 24

border routers
   default routes, 169
   static routing, 164
bounded updates, EIGRP, 181
BPDU (Bridge Protocol Data Units), 76-77
bridge priority command, 79
broadcast domains, 67, 110
broadcast multiaccess network, OSPF protocol, 215
broadcast storms, 72-73
BSP (Business Security Plans), 25
business enterprises. See enterprises

C

cabling
   documentation, 28
   EMI (Electromagnetic Interference), 28
   structured cabling, 28
   T1/E1 lines, 33
   troubleshooting, 28
   vertical cabling, 30
calculators (subnet), 127
callbacks (PPP), 262
CAM (Content Addressable Memory), aging time, 67
carrier waves, analog data connections, 251
cell switching, 255. See also packet switching
challenge messages (CHAP), 267
CHAP (Challenge Handshake Authentication Protocol),
   267-269
child routes, EIGRP route summarization, 193
CIDR (Classless Interdomain Routing)
   contiguous networks, 136-137
   prefix lengths, 131
   route summarization, 133-135
CIR (Committed Information Rates), 273
circuit switching, WAN, 254
classful boundaries
   contiguous networks, 170
   RIP, 170
classful routing, 122, 129-130
   classless routing versus, 132
   updates to, 131
classless routing, 122
   CIDR, 131-135
classful routing versus, 132
   contiguous networks, 136-137
   EGP, 131
   IGP, 131
   prefix lengths, 131
   router updates, 132
clear access-list counters command, 375
clear ip ospf process command, OSPF protocol router selec-
tion, 222
clear ip route command, troubleshooting RIP, 349
clear mac-address-table dynamic command, 337

CLI (Command-Line Interface)

routers
  configuration commands list, 46-47
  R1 router configuration commands, 47-48
show commands (routers)
  list of, 38-39
  show cdp neighbors command, 44-45
  show cdp neighbors detail command, 45-46
  show interfaces command, 42-44
  show ip interfaces brief command, 44
  show ip protocols command, 42
  show ip route command, 42
  show protocol command, 44
  show running-config command, 40-41
  show version command, 41

show commands (switches)
  show cdp neighbors command, 56
  show interfaces command, 53-54
  show ip interface brief command, 55
  show mac-address-table command, 55
  show port-security command, 55
  show running-config command, 51-52
  show version command, 52-53

switches
  configuration commands list, 50-51, 56-57
  S1 switch configuration commands, 57-58

client mode (VTP), 98

clocking signals, 248

CO (Central Office), 248

collision domains, 67

committed burst (Bc), 273

committed time (Tc), 273

composite metrics
  EIGRP, 180, 186
  K values, 166

compression (data)
  LCP, 262
  predictor compression, 263
  stacker compression, 263

configuring
  ACL, 295, 375-376
    established traffic support, 308
    extended ACL, 292-293, 306-307
    extended standard ACL, 299-301
    inbound traffic, 294
    NAC, 308
    NACL, 302-304
    numbered standard ACL, 297-299
    outbound traffic, 294
  ping responses, 308
  router VTY access, 304-305
  standard ACL, 292
  statement syntax, 296
  CHAP, 268-269
  default routes, 169
  Dynamic NAT, 145
  EIGRP, 189
    key creation, 191
    MD5 authentication, 192
    wildcard masks, 190
  global interfaces, RIP, 173
  NAC, ACL, 308
  OSPF protocol
    authentication, 221
    default route configurations, 229-231
    E2 routes, 229
    route summarization, 231-232
    single-area configurations, 218-220
  PAP, 268-269
  PAT, 147
  PPP, 263
  RIP, 173-175

routers
  CLI configuration commands list, 46-47
  copying running configurations, 48
  R1 router configuration commands, 47-48
  Static NAT, 144
  static routes, 166-167

switches
  CLI configuration commands list, 50-51, 56-57
  S1 switch configuration commands, 57-58
  trunk ports, switch configurations, 96
  VTP, 99-102

congestion
  Frame Relay circuits, 274
  reducing, 72

contiguous networks, classful boundaries, 170

continuity plans, 24, 330, 333

control plane information (network infrastructure diagrams), 22

convergence (routers), OSPF protocol, 211

converting subnet masks to wildcard masks, 290-291

coordinated universal time (UTC), 318

copy run start command, 48

core layer (hierarchical design model), enterprise networks, 6-7

core routers, summary static routes, 167

cost metrics, OSPF protocol, 209-210, 224

counts to infinity, 176

CPE (Customer Premise Equipment), 34
CSU/DSU (Channel Service Units/Data Service Units), 33, 248
cut-through switching, 70

data center. See NOC (Network Operations Center)
data compression
LCP, 262
predictor compression, 263
stacker compression, 263
data link layer
encapsulation, 259-270
standards, 251
data storage
NAS (Network Attached Storage), 27
SAN (storage-area networks), 27
data traffic, network traffic prioritization, 14
DCE (Data Communications Equipment), 248
DE (Discard Eligible) frames, 273
dead intervals (hello packets), 213
debug eigrp fsm command, 200
debug eigrp packet command, 199, 356
debug ip eigrp command, 356-357
debug ip ospf events command, 360
debug ip ospf packet command, 360-361
debug ip packet command, 375
debug ip rip command, 177-178, 349
debug ppp authentication command, 373
debug ppp negotiation command, 265-266, 370-371
debug ppp packet command, 371-372
debug serial interface command, 265
debugging
ACL, 375
EIGRP, 356-357
OSPF protocol, 360-361
PPP, 269
RIP, 171, 349
WAN
authentication, 373
connectivity, 370-372
default routes
configuring, 169
gateways of last resort, 169
quad zero routes, 168
default-information originate command, troubleshooting
route redistribution, 361
delay metrics, EIGRP, 187
delays, 14
deleting
ACL, 296-297
NACL statements, 303
VLAN, 91
demarc (demarcation points)
POP, 32
WAN, 248
dense wavelength division multiplexing (DWDM), 258
deny add statements, ACL logging, 318
deny any statements, ACL, 288-291
deny ip any log command, 375
deny statements, 284, 297, 302
designated ports, 79
diagrams (topology)
as-built diagrams, 24
control plane information, 22
creating, 24
logical topology maps, 22
modifying, 24
physical topology maps, 22
updating, 24
Diffusing Update Algorithm (DUAL)
acknowledgment packets, 185
EIGRP, 180
hello intervals, 184
query packets, 185
reply packets, 185
update packets, 185
Dijkstra’s algorithm. See SPF algorithm
directly connected routing, 164
disabled state (switches), 77
discarding state (RSTP), 85
discontiguous networks, 136-137
distance vector protocols
EIGRP
acknowledgment packets, 185
bandwidth metrics, 186
bounded updates, 181
composite metrics, 180, 186
configuring, 189-191
delay metrics, 187
DUAL, 180
FD metrics, 188
feasible successors, 181, 188
features of, 179-180
hello packets, 181
hold times, 181
limitations of, 201
load metrics, 187
MD5 authentication, 192
MTU, 186
neighbor tables, 181
neighbors, 184-185, 190
protocol dependent modules, 186
query packets, 185
reliability metrics, 187
reply packets, 185
route summarization, 193-194
routing tables, 182-184
RTP, 186
successors, 188
topology tables, 181-182
troubleshooting, 199-200
update packets, 185
verifying, 195-198
metrics, 170
RIP
anti-looping features, 176
classful boundaries, 170
configuring, 173-175
connectivity tests, 178
debugging, 171
global interface configuration, 173
limitations of, 178-179
MD5 authentication, 175
request messages, 172
response messages, 172
send/receive versions example, 173
triggered updates, 172, 177
troubleshooting, 175-177
updates, 179
verifying, 177-178
distribution layer (hierarchical design model), enterprise networks, 6-7
DLCI (Data-Link Connection Identifiers), Frame Relay encapsulation, 272
DMZ (Demilitarized Zones), enterprise edge security, 33
documentation
BCP (Business Continuity Plans), 24, 330, 333
BSP (Business Security Plans), 25
cabling plans, 28
network infrastructure diagrams
as-built diagrams, 24
control plane information, 22
creating, 24
logical topology maps, 22
modifying, 24
physical topology maps, 22
redlined blueprints, 24
updating, 24
NMP (Network Maintenance Plans), 25
SLA (Service Level Agreements), 25
storing, 25
dot1q. See 802.1Q frame-tagging standard
DR (Designated Routers)
DROthers, 213-214
Full state (OSPF protocol neighbor adjacencies), 213
OSPF protocol
interaction with, 213-215
selecting in, 222
router ID, 213-214, 222
DS0 (Digital Signal level 0) standard, 249
DS1 (Digital Signal level 1) standard, 249
DS3 (Digital Signal level 3) standard, 250
DTE (Dat Terminal Equipment), 248
DUAL (Diffusing Update Algorithm), EIGRP, 180, 184-185
DWDM (Dense Wavelength Division Multiplexing), 258
Dynamic NAT (Network Address Translation), 143
configuring, 145
PAT, 146-147
dynamic routing
distance vector protocols
EIGRP, 179-201
metrics, 170
RIP, 170-179
link state protocols, 170
static routing versus, 164-166
dynamic VLAN, VMPS, 87
E
E2 (external type routes), 229
echo-reply statements, ACL, 308
ECNM (Enterprise Composite Network Model)
Enterprise Campus, 8
Enterprise Edge, 8
Service Provider Edge, 10
edge devices, 9
EGP (Exterior Gateway Protocols), 131
EIGRP (Enhanced Interior Gateway Routing Protocol)
acknowledgment packets, 185
bandwidth metrics, 186
bounded updates, 181
composite metrics, 180, 186
configuring, 189
key creation, 191
MD5 authentication, 192
wildcard masks, 190
debugging, 356-357
delay metrics, 187
DUAL, 180, 184-185
FD metrics, 188
feasible successors, 181, 188
features of, 179-180
hello packets, 181
hold times, 181
limitations of, 201
load metrics, 187
MD5 authentication, 192
MTU, 186
neighbors

- adjacencies, 184-185, 190
- show ip eigrp neighbors detail command, 197
- tables, 181

protocol dependent modules, 186

query packets, 185

reliability metrics, 187

reply packets, 185

route redistribution, troubleshooting, 363-364

route summarization

- child routes, 193
- disabling, 194
- manual summarization, 194
- Null0 interfaces, 193
- parent routes, 193

routing tables, 182-184

RTP, 186

successor routes, 181

successors, 188

topology tables, 181-182

troubleshooting, 199-200, 351-358

update packets, 185

verifying, 195-198

eigrp log-neighbor-changes command, viewing neighbor adjacencies, 190

EIR (Excess Information Rates), 273
e-mail, junk e-mail filtering, 280

EMI (Electromagnetic Interference), 28

encapsulation
data link layer

- HDLC, 260
- PPP, 260-263
- WAN, 259

Ethernet, WAN, 258-259

Frame Relay, 271

- BECN, 274
- CIR, 273
- congestion, 274
- DLCI, 272
- EIR, 273
- FECN, 274
- Inverse ARP, 272
- LMI, 273

layer 2, WAN, 258

eapsulation hdlc interface command, 263
eapsulation ppp interface command, 263

Enterprise Campus (ECNM), 8

Enterprise Edge

- NAT, 142
- POP, 31
- CPE, 34
- enterprise network/external service connections, 33
- links from, 32
- location of, 32
- security, 32
- SP, 32

Enterprise Edge (ECNM), 8
topologies

- full mesh topologies, 162-163
- partial mesh topologies, 162
- star topologies, 160
traffic flows, 5, 8, 10
allowed traffic, 13
capturing/analyzing traffic, 14
classifying traffic, 14
hierarchical design model, 6-7
packet sniffers, 13
patterns of, 12
prioritization, 14
WAN, 10
enterprises, examples of, 4
Ethernet
   frame-tagging
      802.1Q frame-tagging standard, 91-92
      ISL, 93
frames, 70
PoE (Power over Ethernet), 31
WAN encapsulations, 258-259
excess bursts (Be), 273
Exchange state (OSPF protocol neighbor adjacencies), 213
exit interfaces, 163, 166-167
Exstart state (OSPF protocol neighbor adjacencies), 212
extended ACL (Access Control Lists), 284
   configuring, 292-293
   numbered extended ACL, configuring, 299-301
   port filtering, 306-307
   statement creation, 300-301
extended star design connections, IDF to MDF connections, 29
extended star topologies, 160
external type routes (E2), 229
extranets, 12
failure domains, 9, 333
failures (networks)
   business continuity plans, 330, 333
   factors of, 328
   redundant backup sites, 330
fast-forward switching, 70
FD (Feasible Distance) metrics, EIGRP, 188
feasible successors, EIGRP, 181, 188
FECN (Forward Explicit Congestion Notification), Frame Relay encapsulation, 274
filtering
   junk e-mail, 280
   packets, 280
   ports, extended ACL, 306-307
filtering traffic, 280
   ACL, 281
      analyzing, 311
      best practices, 318
      configuring, 294-297, 304-305, 313, 375-376
debugging, 375
deleting, 296-297
deny any statements, 288-289, 291
deny statements, 284, 297, 302, 318
echo-reply statements, 308
established traffic support, 308
extended ACL, 284, 292-293, 299-301, 306-307
functions of, 311-313
implicit deny statements, 284
inbound placement, 286
latency, 286
logging, 314-317
match-tracking, 315
NAC, 308
NACL, 284, 302-304
NAT, 309-310
outbound placement, 286
PAT, 309
permit statements, 284, 297, 302
ping responses, 308
problems with, 283
processing, 284-286
remark statements, 297
routers, 285-286
standard ACL, 284, 292, 297-299
troubleshooting, 374-376
unreachable statements, 308
wildcard masks, 287-291
networking devices, 281
performance, effects on, 281
routers, 281
firewalls, enterprise edge security, 33
first miles, WAN connections, 248
fixed configuration routers, 37
flapping, 217
flat networks, 110
floating static routes, 168
form factors
   routers, 36
   switches, 48
forwarding state (switches), 77
fractional E1 lines, WAN connections, 252
fractional T1 lines
   OSPF protocol bandwidth modification, 223
   WAN connections, 252
fragment-free switching, 70
Frame Relay encapsulation, 271
   BECN, 274
   CIR, 273
   congestion, 274
   DLCI, 272
EIR, 273
FECN, 274
Inverse ARP, 272
LMI, 273

frame-tagging
  802.31Q frame-tagging standard, 91-92
  ISL, 93

full mesh topologies, enterprise networks, 162-163
Full state (OSPF protocol neighbor adjacencies), 213

G - H

gateways of last resort, 169
global interfaces, configuring via RIP, 173
GMT (Greenwich Mean Time), 317

HDLC (High-Level Data Link Control) encapsulation, 260
hello intervals, 184
hello packets
  adjacencies, 184-185
  EIGRP, 181
  hello intervals, 184
  hold times, 181
  OSPF protocol, 213
Hello protocol (OSPF protocol), 213
hierarchical networks, 111
  addressing schemes, 113
  IP addressing
    private addresses, 140-147
    public addresses, 140
  router functions, 115
  subnetting, 115
  best practices, 138
  calculating, 118-120
  classful routing, 129-132
  classless routing, 131-137
  process overview, 120-121
  sub-subnets, 123
  subnet masks, 117-118
  VLSM, 122-128
High-Level Data Link Control (HLC) encapsulation, 260
hijack attacks, 267
hold times, 181
holddown timer (RIP anti-looping features), 177
HTTP (Hypertext Transfer Protocol), switch security, 71
hub-and-spoke topologies, example of, 32
hubs, collision domains, 67

ID
  area ID, 218
  keys, 221
  routers
    DR/BDR selection, 213-214, 222
    viewing, 214
IDF (Intermediate Distribution Facilities)
  MDF connections, 29
  security, 29
  switches, 30, 49
  vertical cabling, 30
IDS (Intrusion Detection Systems), 9, 33
IETF (Internet Engineering Task Force), CIDR, 131
IGP (Interior Gateway Protocols), 131
implicit deny statements, 284
in band management (PC/network device configuration/monitoring), 38
inbound ACL
  placement, 286
  traffic, configuring, 294
infrastructure diagrams
  as-built diagrams, 24
  control plane information, 22
  creating, 24
  logical topology maps, 22
  modifying, 24
  physical topology maps, 22
  updating, 24
Init state (OSPF protocol neighbor adjacencies), 212
inside global addresses, 143
inside local addresses, 142
inter-VLAN routing, configuring via ACL, 313
interface addresses, OSPF protocol router selection, 222
interface priority, setting in OSPF protocol, 222
intranets, 12
Inverse ARP (Address Resolution Protocol), Frame Relay encapsulation, 272
ip access-list command, editing NACL, 303
IP addressing
  hierarchical networks, 113
  private addresses, 140-147
  subnetting, 115-137
  inside global addresses, 143
  inside local addresses, 142
ip ospf cost command, OSPF protocol, 210, 223
ip ospf message-digest-key command, OSPF routine authentication, 221
ip ospf priority number command, OSPF protocol, 214
ip route command
  configuring static routes, 166
  floating static routes, creating, 168
IP telephony, VLAN support for, 102
IPS (Intrusion Prevention Systems), 9, 33
IPsec (IP Security), 17
ISL (Inter-Switch Link), 93

J - K - L

jitters, 14
junk e-mail filtering, 280
K values (composite metrics), 186
key chain command, EIGRP key creation, 191
key-string command, EIGRP key creation, 191
keys (routers), ID, 221
LAN (Local Area Networks), VLAN, 10, 85
  creating, 87
  dynamic VLAN, 87
  management VLAN, 87
  port assignments, 88
  show commands, 88-90
  static VLAN, 86
last miles, WAN connections, 248, 257
latencies, 14, 286
layer 1 WAN standards, 250
layer 2
  encapsulation, WAN, 258
  switches, 69
  WAN standards, 250
layer 3 switches. See multilayer switching
LCP (Link Control Protocol)
  authentication, 262
  compression, 262
  PPP, 261-262
  show interfaces serial command, 263-264
learning state (switches), 77
leased lines, WAN, 254
least-cost paths (switches), 79
legacy equipment, routing, 233
legacy switches, PoE patch panel connections, 31
link costs, OSPF protocol, 224
link state protocols, 170
link-establishment phase (PPP), 262
link-state routing protocol. See also OSPF (Open Shortest Path First) protocol
  network maps, 209
  requirements for, 208
  updates, 208
listening state (switches), 77
LMI (Local Management Interface), Frame Relay encapsulation, 273
load balancing, 26, 72
load metrics, EIGRP, 187
Loading state (OSPF protocol neighbor adjacencies), 213
local loops, WAN, 248, 257
logging ACL, 314-315
  analyzing router logs, 317
  security levels, 316
  syslog messages, 316-317
  troubleshooting, 375
logical topology maps, 22
long-range communications, 258
loopback addresses, OSPF protocol router selection, 222
loopback interfaces, 214
loops
  local loops, WAN, 248, 257
  routing loops, 170
    counts to infinity, 176
    RIP anti-looping features, 176-177
  switching loops, 72
    MAC database instability, 75
    multiple frame transmissions, 74
    STP, 75
LSA (Link-State Advertisements), OSPF protocol, 211

M

MAC addresses
  aging time, 67
  CAM, 67
  layer 2 switches, 69
  redundant switched networks, instability in, 75
  troubleshooting switches, 337-338
maintenance (proactive), 332. See also troubleshooting
maintenance plans, 25
management VLAN (Virtual Local Area Networks), 87, 343
manual route summarization, EIGRP, 194
maps (network)
  OSPF protocol, 209
  SPF algorithm, 211
masks
  subnet masks
    calculating, 118-120
    classful routing, 129-131
    classless routing, 131
    converting to wildcard masks, 290-291
    directly connected routing, 164
    dynamic routing, 164
    number of hosts table, 117-118
    single-area OSPF configurations, 219
    slash notation, 117
static routing, 164
VLSM, 122-128
wildcard masks
ACL, 287-291
converting subnet masks to, 290-291
EIGRP, 190
single-area OSPF configurations, 218-220
viewing, 190
MD5 authentication
EIGRP, 192
OSPF protocol, 221
RIP, 175
MDF (Main Distribution Facilities)
components of, 29
IDF connections, 29
switches, 30, 49
vertical cabling, 30
metric weights command, changing K values, 186
metrics
AD, EIGRP, 188
bandwidth metrics, EIGRP, 186
composite metrics
EIGRP, 180, 186
K values, 186
delay metrics, EIGRP, 187
FD, EIGRP, 188
load metrics, EIGRP, 187
OSPF protocol, 209-210
reliability metrics, EIGRP, 187
routing protocols, 170
MIB (Management Information Bases), 331
microsegregation, 67
modems
clocking signals, 248
WAN connections, 251
modular routers, 37
modulated data, analog data connections, 251
monitoring networks
baselines, 330
packet sniffing tools, 331
ping command, 330-331
plans for, 332
SNMP, 331
MTU (Maximum Transmission Units), EIGRP, 186
multilayer switching, 69
multilink PPP (Point-to-Point Protocol), 262-263
multiple frame transmissions, 74
multiple routing protocols, importance of, 233-236

N
NAC (Network Access Control), ACL, 308
NACL (Named Access Control Lists), 284
configuring, 302-304
deleting statements, 303
inserting new lines in, 304
NAS (Network Attached Storage), 27
NAT (Network Address Translation), 142
ACL, 309-310
Dynamic NAT, 143
configuring, 145
PAT, 146-147
NAT Overload. See PAT
Static NAT, 142-144
native VLAN (Virtual Local Area Networks), 94, 343
NBMA (Nonbroadcast Multiaccess) networks
OSPF protocol, 215-216
point-to-multipoint environment mode, 216
simulated broadcast environment mode, 216
NCP (Network Control Protocol), PPP, 262-263
neighbor tables, 181
neighbors
adjacencies
EIGRP, 184-185
OSPF, 212-213
viewing, 190
EIGRP
adjacencies, 184-185
show ip eigrp neighbors detail command, 197
OSPF protocol, adjacencies, 212-213
network boundaries, 132
network command, single-area OSPF configurations, 218
network discovery, 164
network failures, factors of, 328
network infrastructure diagrams
as-built diagrams, 24
control plane information, 22
creating, 24
logical topology maps, 22
modifying, 24
physical topology maps, 22
updating, 24
network maps
OSPF protocol, 209
SPF algorithm, 211
network monitoring
baselines, 330
packet sniffing tools, 331
ping command, 330-331
plans for, 332
SNMP, 331
network statements, OSPF Protocol, 219

networks
  failure domains, 333
  failures
    business continuity plans, 330, 333
    factors of, 328
    redundant backup sites, 330
  redundancy, 333
  three-layer hierarchical network design model, 329

next-hops, 163
  recursive lockup, 166
  static route configuration, enterprise networks, 166-167

NMP (Network Maintenance Plans), 25
NMS (Network Management Stations), 332

no auto-summary command
  disabling EIGRP route summarization, 194
  RIP configurations, 175

no ip access-group command, deleting ACL, 297
no logging console command, ACL logging, 316
no switchport mode trunk command, 94

NOC (Network Operations Center)
  components of, 26
  NAS (Network Attached Storage), 27
  SAN (Storage-Area Networks), 27
  server farms, 26-27

Null0 interfaces, EIGRP route summarization, 193

numbered extended ACL (Access Control Lists), configuring, 299-301

numbered standard ACL (Access Control Lists), configuring, 297-299

open standard routing protocols, 208

OSPF (Open Shortest Path First) protocol. See also link-state routing protocols
  advantages of, 232
  areas, 208
    ABR, 217
    Area 0, 216
    ID, 218
  authentication, 221
  autonomous systems, ASBR, 217, 228-229
  bandwidth modification, 223-224
  broadcast multiaccess networks, 215
  convergence, 211
  debugging, 360-361
  default route configurations, 229-231
  DR/BDR
    interaction with, 213-215
    selection, 222
  E2 routes, 229
  hello packets, 213
  Hello protocol, 213
  limitations of, 232
  link costs, 224
  LSA, 211
  metrics, 209-210
  NBMA networks, 215-216
  neighbor adjacencies, 212-213
  network maps, 209
  network statements, 219
  point-to-point networks, 215
  route summarization, 217, 231-232
  router prioritization, 214
  scalability of, 208
  single-area configurations, 218-220
  topology databases, SPF trees, 211
  troubleshooting, 358-360, 365-366
  verifying operation of, 224-228

out-of-band management (PC/network device configuration/monitoring), 37-38

outages (networks)
  business continuity plans, 330, 333
  factors of, 328
  redundant backup sites, 330

outbound ACL
  placement, 286
  traffic, configuring, 294

packets
  filtering, 280
  sniffing, 13, 331
  switching. See also cell switching
    VC, 256
    WAN, 255

PAP (Password Authentication Protocol), 266-269

parent routes, EIGRP route summarization, 193

partial mesh topologies, enterprise networks, 162

passive-interface command, RIP configurations, 176

passwords
  keys (routers), 221
  shared secret passwords, CHAP, 267
  simple password authentication, OSPF protocol, 221
  switch security, 71
  VTP, 344
  VTY passwords, configuring, 305

PAT (Port Address Translation), 146-147, 309

patch panels (PoE), 31

PDM (Protocol Dependent Modules), EIGRP, 186

performance, traffic filtering effects on, 281

permit any command, ACL, 289

permit statements, 284, 297, 302

physical interface addresses, OSPF protocol router selection, 222
physical layer protocols, WAN, 249
physical link layer standards, WAN, 251
physical topologies
  full mesh topologies, enterprise networks, 162-163
  maps, 22
  partial mesh topologies, enterprise networks, 162
  star topologies, 160
pie charts (VLSM), 127
ping command
  ACL, 308
  RIP connectivity tests, 178
  troubleshooting via, 330-331
PoE (Power over Ethernet), 31
point-to-multipoint environment mode (NBMA networks), 216
point-to-point networks, OSPF protocol, 215
poisoned reverse (RIP anti-looping features), 176
POP (Point Of Presence), 31
  CPE, 34
  demarc, 32
  enterprise network/external service connections, 33
  links from, 32
  location of, 32
PortFast, 80
ports
  access ports, 77, 93
  blocked ports, 79
  designated ports, 79
  density, switches, 49
  filtering, extended ACL, 306-307
  PortFast, 80
  root ports, 79
  switch security, 71
  trunk ports, 93
    no switchport mode trunk command, 94
    switch configurations, 96
  trunking ports, 77
VLAN
  disassociating from, 91
  port assignments, 88
POTS (Plain Old Telephone Systems), 251
PPP (Point-to-Point Protocol)
  authentication, 262, 270
    CHAP, 267-269
    PAP, 266-269
  callbacks, 262
  configuring, 263
  debugging, 269
  encapsulation, 260-262
  LCP, 261-262
  link-establishment phase, 262
  multi-link PPP, 262-263
  NCP, 262-263
  NCP Negotiation phase, 262-263
  troubleshooting, 263-266
predictor compression, 263
prefix lengths, CIDR, 131
priority command, OSPF protocol router selection, 222
private addresses, NAT, 140-142
  Dynamic NAT, 143-145
  PAT, 146-147
  Static NAT, 142-144
proactive maintenance, 332. See also troubleshooting
public addresses, 140
punchdown blocks, 33
PVC (Permanent Virtual Circuits), 256
Q - R
QoS (Quality of Service), 14
quad zero routes, 168
query packets, EIGRP, 185
R1 router configuration commands, 47-48
rack-mounted server farms, 27
recursive lockup, 166
redistribute static command, troubleshooting route redistribution, 361
re lined blueprints, 24
redundancy, 333
  backup sites, 330
  switched networks
    broadcast storms, 72-73
    MAC database instability, 75
    multiple frame transmissions, 74
    STP, 75
    switching loops, 72
reliability metrics, OSPF protocol, 224
reload command, 48
reload in 30 command, testing ACL functionality, 318
remark statements, 297
remote workers
  teleworking, 15
  VPN
    IPsec, 17
    virtual tunnels, 16
replay attacks, 267
reply packets, EIGRP, 185
reported distance. See AD (Advertised Distance) metrics
request messages (RIP), 172
resource management. See NOC (Network Operations Center)
response messages (RIP), 172
revision numbers (VTP), 98
RIP (Routing Information Protocol)
- anti-looping features, 176
  - holdown timer, 177
  - poisoned reverse, 176
  - split horizon, 176-177
- classful boundaries, 170
- configuring, 173-175
- connectivity tests, 178
- debugging, 171, 349
- global interface configuration, 173
- limitations of, 178-179
- MD5 authentication, 175
- request messages, 172
- response messages, 172
- route redistribution, troubleshooting, 361-363
- send/receive versions example, 173
- triggered updates, 172, 177
- troubleshooting, 175-177, 345-350
- updates, 179
- verifying, 177-178

rogue switches, VLAN, 344

root bridges
- BID, 78
- BPDU, fields list, 76-77
- specifying, 79

root ports, 79

route summarization, 122
- calculating, 135
- CIDR, 133
- EIGRP
  - child routes, 193
  - disabling, 194
  - manual summarization, 194
- Null0 interfaces, 193
- parent routes, 193
- flapping, 217
- OSPF protocol, 217, 231-232
- static routing, 167

router-id configuration command, OSPF protocol router selection, 222

router-on-a-stick configurations (VLAN), 95

routers
- ABR, 217
- ACL, 285-286, 317
- ASBR, 217, 228-229
- BDR, Full state (OSPF protocol neighbor adjacencies), 213
- border routers
  - default routes, 169
  - static routing, 164
- classes of, 36
- classless routing, 132

CLI show commands
- list of, 38-39
- show cdp neighbors command output, 44-45
- show cdp neighbors detail command output, 45-46
- show interfaces command output, 42-44
- show ip interfaces brief command output, 44
- show ip protocols command output, 42
- show ip route command output, 42
- show protocol command output, 44
- show running-config command output, 40-41
- show version command output, 41

configuring
- CLI configuration commands list, 46-47
- R1 router configuration commands, 47-48

convergence, OSPF protocol, 211
core routers, summary static routes, 167
DR, Full state (OSPF protocol neighbor adjacencies), 213
enterprise networks, 165
fixed configuration routers, 37
form factors, 36
functions of, 35
hierarchical networks, 111, 115
ID
  - DR/BDR selection, 213-214, 222
  - viewing, 214
in band management, 38
interfaces of, 37
keys, 221
logs (ACL), 317
modular routers, 37
OSPF protocol neighbor adjacencies, 212-213
out-of-band management, 37-38
route summarization, 122
running configurations, copying, 48
traffic filtering, 281
triggered updates, 172, 177
VTY passwords, configuring, 305

routing
administrative distances comparison table, 180
devugging
- EIGRP, 356-357
- OSPF protocol, 360-361
- RIP, 349
directly connected routing, 164
dynamic routing
- distance vector protocols, 170-201
  - link state protocols, 170
- static routing versus, 164-166
legacy equipment, 233
link-state protocols. See also OSPF (Open Shortest Path First) protocol

- network maps, 209
- requirements for, 208
- updates, 208
- multiple routing protocols, importance of, 233-236
- open standard routing protocols, 208
- OSPF protocol. See also link-state routing protocols
  - advantages of, 232
  - areas, 208, 216-218
  - authentication, 221
  - autonomous systems, 217, 228-229
  - bandwidth modification, 223-224
  - broadcast multiaccess networks, 215
  - convergence, 211
  - default route configurations, 229-231
  - DR/BDR interaction with, 213-215
  - DR/BDR selection, 222
  - E2 routes, 229
  - hello packets, 213
  - Hello protocol, 213
  - limitations of, 232
  - link costs, 224
  - LSA, 211
  - metrics, 209-210
  - NBMA networks, 215-216
  - neighbor adjacencies, 212-213
  - network maps, 209
  - network statements, 219
  - point-to-point networks, 215
  - route summarization, 217, 231-232
  - router prioritization, 214
  - scalability of, 208
  - single-area configurations, 218-220
  - SPF trees, 211
  - verifying operation of, 224-228
- router tables, core routers, 167
- routing loops, 170
  - counts to infinity, 176
  - RIP anti-looping features, 176-177
- routing tables
  - administrative distance, 163
  - core router tables, 167
  - default routes, 168-169
  - directly connected routing, 164
  - dynamic routing, 164
  - EIGRP, 182-184
  - exit interfaces, 163
  - next hops, 163
  - static routing, 164-167
- static routing
  - border routers, 164
  - configuring, 166-167
  - default routes, 168-169
  - dynamic routing versus, 164-166
  - exit interfaces, 166-167
  - floating static routes, 168
  - next-hops, 166-167
  - recursive lockup, 166
  - route summarization, 167
- troubleshooting
  - EIGRP, 351-358, 363-364
  - OSPF protocol, 358-360, 365-366
  - RIP, 345-350, 361-363
  - route redistribution, 361-366
- RSTP (Rapid Spanning Tree Protocol), 85
- RTP (Reliable Transport Protocol), 186
- RU (Rack Units), 27
- runts (Ethernet frames), 70

S

- S1 switch configuration commands, 57-58
- SAN (Storage-Area Networks), 27
- SDH (Synchronous Digital Hierarchies), 258
- security
  - enterprise edge, 32
  - IDF (Intermediate Distribution Facilities), 29
  - junk e-mail filtering, 280
  - packet filtering, 280
  - passwords, VTP, 344
  - plans, 25
  - switches, 70-71
  - telecommunications rooms, 29
  - traffic filtering, 280-318, 374-376
  - VTP, passwords, 344
- segmented data, ATM, 255
- server farms
  - backups, 26
  - load balancing, 26
  - rack-mounted farms, 27
- server mode (VTP), 98
- Service Provider Edge (ECNM), 10
- shared secret passwords, CHAP, 267
- show access-list command
  - ACL
    - logging, 314
    - numbered standard ACL, 298
    - remark statements, 297
    - troubleshooting, 374
  - NACL, editing, 303-304
- show cdp neighbors command, 44-45, 56
show cdp neighbors detail command, 45-46
show commands
router show commands
list of, 38-39
show cdp neighbors command output, 44-45
show cdp neighbors detail command output, 45-46
show interfaces command output, 42-44
show ip interfaces brief command output, 44
show ip protocols command output, 42
show ip route command output, 42
show protocol command output, 44
show running-config command output, 40-41
show version command output, 41
STP diagnostic show commands
show spanning-tree blockedports command, 84
show spanning-tree command, 81
show spanning-tree detail command, 83
show spanning-tree interface command, 84
show spanning-tree root command, 82
show spanning-tree summary command, 82
switch show commands
how cdp neighbors command output, 56
show interfaces command output, 53-54
show ip interface brief command output, 55
show mac-address-table command output, 55
show port-security command output, 55
show running-config command output, 51-52
show version command output, 52-53
troubleshooting RIP, 345
VLAN commands
show vlan brief command, 89
show vlan command, 88-89
show vlan id command, 89-90
show vlan name command, 89-90
show controllers command
PPP, 264-265
troubleshooting WAN connectivity, 367
show interface command, 338, 372
show interfaces brief command, 370
show interfaces command
OSPF protocol, 210
output of, 42-44, 53-54
troubleshooting
RIP, 347
WAN connectivity, 368-369
show interfaces serial command, 263-264
show ip eigrp interfaces detail command, 198
show ip eigrp neighbors command, 354, 357
show ip eigrp neighbors detail command, 197
show ip eigrp topologies command, 197-198
show ip eigrp topology command, 355
show ip eigrp traffic command
EIGRP verification, 198
troubleshooting EIGRP, 355
show ip interface brief command, 55, 369
show ip interface command
troubleshooting
EIGRP, 354
RIP, 346
verifying OSPF protocol operation, 226
show ip rip database command, 177
show ip route command, 342
EIGRP verification, 196
OSPF protocol route configurations, 229-231
output of, 42
troubleshooting
EIGRP, 353-354, 357
RIP, 348-349
verifying OSPF protocol operation, 227-228
show mac-address-table command, 55, 337
show port-security command, 55
show protocol command, 44
show running-config command
ACL remark statements, 297
numbered standard ACL, configuring, 298
output of, 40-41, 51-52
RIP
troubleshooting, 346-347
verifying, 178
troubleshooting
EIGRP, 351-352
RIP, 346-347
viewing wildcard masks, 190
show spanning-tree blockedports command, 84
show spanning-tree command, 81, 339
show spanning-tree detail command, 83
show spanning-tree interface command, 84
show spanning-tree root command, 82
show spanning-tree summary command, 82
show up interface brief command, 342
show version command, 41, 52-53
show vlan brief command, 89, 341
show vlan command, 88-89, 340
show vlan id command, 89-90, 341
show vlan name command, 89-90
show vsto status command, 344
show vtp password command, 344
simple password authentication, OSPF protocol, 221
simulated broadcast environment mode (NBMA networks), 216
SLA (Service Level Agreements), 25, 329
SLARP (Serial Line Address Resolution Protocol), 369
slash notation, 117
SNMP (Simple Network Management Protocol), network monitoring, 331
SONET (Synchronous Optical Networks), 258
SP (Service Providers), 32
spanning-tree vlan VLAN-Id priority command, 79
SPF algorithm, 211, 232
SPF trees, 211
split horizon (RIP anti-looping features), 176-177
SSH (Secure Shell), switch security, 71
stacker compression, 263
stakeholders, traffic filtering requirements, 292
standard ACL (Access Control Lists), 284
configure, 292
Dynamic NAT configuration, 145
numbered standard ACL, configuring, 297-299
star topologies
enterprise networks, 160
element of, 32
extended star topologies, 160
Static NAT (Network Address Translation), 142-144
static routing
border routers, 164
configure, 166-167
default routes
configure, 169
gateways of last resort, 169
quad zero routes, 168
dynamic routing versus, 164-166
exit interfaces, 166-167
floating static routes, 168
next-hops, 166-167
recursive lockup, 166
route summarization, 167
static VLAN (Virtual Local Area Networks), 86
STDM (Statistical Time Division Multiplexing), 253
store-and-forward switching, 70
storing
data
NAS (Network Attached Storage), 27
SAN (Storage-Area Networks), 27
documentation, 25

STP (Spanning Tree Protocol)
BackboneFast, 81
blocked ports, 79
blocking state, 77
designated ports, 79
diagnostic show commands
show spanning-tree blockedports command, 84
show spanning-tree command, 81
show spanning-tree detail command, 83
show spanning-tree interface command, 84
show spanning-tree root command, 82
show spanning-tree summary command, 82
disabled state, 77
forwarding state, 77
learning state, 77
listening state, 77
PortFast, 80
recalculations, 79
root bridges
BID, 78
BDPU, 76-77
specifying, 79
root ports, 79
RSTP, 85
switching loops, preventing, 75
troubleshooting switches, 339-340
UplinkFast, 80
structured cabling, 28
stub networks, 164
sub-subnets, 123
subinterfaces, 95
subnet calculators, 127
subnet masks, 117
subnetting
best practices, 138
calculating, 118-120
classful routing protocols, 122
classless routing protocols, 122
classful routing protocols, 122
classless routing protocols, 122
classful routing, 129-131
classless routing, 131
converting to wildcard masks, 290-291
directly connected routing, 164
dynamic routing, 164
number of hosts table, 117-118
single-area OSPF configurations, 219
slash notation, 117
static routing, 164
VLSM, 123-124
addressing process overview, 126-128
benefits of, 122
classful routing protocols, 122
classless routing protocols, 122
VLSM, 123-124
classful routing, 129-130
  classless routing versus, 132
  updates to, 131
classless routing
  CIDR, 133-135
  classful routing versus, 132
discontiguous networks, 136-137
  EGP, 131
  IGP, 131
  router updates, 132
hierarchical networks, 115
  process overview, 120-121
sub-subnets, 123
subnet calculators, 127
subnet masks
  directly connected routing, 164
dynamic routing, 164
  number of hosts table, 117-118
  slash notation, 117
  static routing, 164
VLSM, 123
  addressing process overview, 126-128
  benefits of, 122
classful routing protocols, 122
classless routing protocols, 122
  requirements for, 124-126
suboptimal switching, 339
subset advertisements (VTP), 99
successor routes, EIGRP, 181
successors, EIGRP, 188
summarization (route), 132
calculating, 135
CIDR, 133
EIGRP
  child routes, 193
disabling, 194
  manual summarization, 194
  Null0 interfaces, 193
  parent routes, 193
flapping, 217
OSPF protocol, 217, 231-232
static routing, 167
summary advertisements (VTP), 99
supernetting, 133
SVC (Switched Virtual Circuits), 256
switches
  access ports, 93, 343
  adaptive cut through switching, 70
  aging time, 67
  asymmetric switching, 68
  blocking state, 77
  broadcast domains, 67, 110
  broadcast storms, 72-73
CAM, 67
classes of, 49
CLI show commands
  show cdp neighbors command output, 56
  show interfaces command output, 53-54
  show ip interface brief command output, 55
  show mac-address-table command output, 55
  show port-security command output, 55
  show running-config command output, 51-52
  show version command output, 52-53
collision domains, 67
  configuring
    CLI configuration commands list, 50-51, 56-57
    S1 switch configuration commands, 57-58
cut-through switching, 70
disabled state, 77
flat networks, 110
form factors, 48
forwarding state, 77
hierarchical networks, 112
IDF, 30, 49
interfaces of, 49
layer 2 switches, 69
learning state, 77
least-cost paths, 79
legacy switches, PoE patch panel connections, 31
listening state, 77
MDF, 30, 49
microwave connection, 67
multilayer switching, 69
port density, 49
priority, setting, 79
redundancy, 72, 75
root bridges
  BID, 78
  BPDU, 76-77
  specifying, 79
  security, 70-71
store-and-forward switching, 70
STP, troubleshooting, 339-340
suboptimal switching, troubleshooting, 339
switching loops, 72
  MAC database instability, 75
  multiple frame transmissions, 74
  STP, 75
  troubleshooting, 338-339
symmetric switching, 68
troubleshooting, 336
  access ports, 343
  MAC addresses, 337-338
  STP, 339-340
  suboptimal switching, 339
switching loops, 338-339
trunk ports, 343
VLAN, 340-344
trunk ports, 93
configuring, 96
no switchport mode trunk command, 94
troubleshooting, 343
uplink ports, 68
vertical cabling, 30
virtual circuits, 68
VLAN
extending across switches, 94
inter-VLAN switching, 95-97
troubleshooting, 340-344
VTP, configuring, 99-102
wire speed, 67
switching loops, 338-339
symmetric switching, 68
syslog messages, ACL, 316-317

T

T1 lines (fractional), OSPF protocol bandwidth modification, 223
T1/E1 cabling, 33
tabular charts (VLSM), 127
Tc (committed time), 273
TDM (Time Division Multiplexing), 252
telecommunications rooms
MDF connections, 29
security, 29
switches, 30, 49
vertical cabling, 30
telecommuting. See teleworking
teleconferencing, 15
telephony, VLAN support for, 102
teleworking, 15
Telnet, switch security, 71
three-layer hierarchical network design model, 329
time slices (bandwidth), 252
topologies
databases, OSPF protocol, 211
diagrams
as-built diagrams, 24
control plane information, 22
creating, 24
logical topology maps, 22
modifying, 24
physical topology maps, 22
updating, 24
extended star topologies, 160
full mesh topologies, 162-163
partial mesh topologies, 162
star topologies, 160
tables
EIGRP, 181-182
feasible successors, 181
successor routes, 181
traffic filtering, 280
ACL, 281
analyzing, 311
best practices, 318
configuring, 294-297, 304-305, 313, 375-376
debugging, 375
deleting, 296-297
deny any statements, 288-291, 318
deny statements, 284, 297, 302
echo-reply statements, 308
established traffic support, 308
extended ACL, 284, 292-293, 299-301, 306-307
functions of, 311-313
implicit deny statements, 284
inbound placement, 286
latency, 286
logging, 314-317
match-tracking, 315
NAC, 308
NACL, 284, 302-304
NAT, 309-310
outbound placement, 286
PAT, 309
permit statements, 284, 297, 302
ping responses, 308
problems with, 283
processing, 284, 286
remark statements, 297
routers, 285-286
standard ACL, 284, 292, 297-299
troubleshooting, 374-376
unreachable statements, 308
wildcard masks, 287-291
networking devices, 281
performance, effects on, 281
routers, 281
traffic sniffing tools, 331
transceivers, 338
transport mode (VTP), 98
triggered updates, 172, 177
troubleshooting. See also proactive maintenance
ACL, 374-376
cabling, 28
common network problems, 335-336
EIGRP, 199-200, 351-358
OSPF protocol, 358-360, 365-366
packet sniffing tools, 331
ping command, 330-331
PPP encapsulation, 263-266
RIP, 175-177
routing, 345
  EIGRP, 351-358, 363-364
  OSPF protocol, 358-360, 365-366
  RIP, 345-350, 361-363
  route distribution, 361-366
switches, 336
  access ports, 343
  MAC addresses, 337-338
  STP, 339-340
  suboptimal switching, 339
  switching loops, 338-339
  trunk ports, 343
VLAN, 340-344
techniques for, 334
WAN
  authentication, 372
  connectivity, 367-370
trunk ports, 77, 93
  no switchport mode trunk command, 94
switches
  configuring on, 96
  troubleshooting, 343

U - V
unreadable statements, ACL, 308
updates
  bounded updates, EIGRP, 181
  classful routing, 131
  link-state routing protocols, 208
  RIP, 179
  routers, classless routing, 132
  triggered updates, 172, 177
update packets, EIGRP, 185
updating network infrastructure diagrams, 24
uplink ports, 68
UplinkFast, 80
UTC (coordinated universal time), 318
VC (virtual circuits), 68, 256
verifying
  EIGRP, 195-198
  OSPF protocol, 224-228
  RIP, 177-178
vertical cabling, 30
VID (VLAN IDs), frame-tagging, 91-92
video traffic, network traffic prioritization, 14
virtual tunnels (VPN), 16
VLAN (Virtual Local Area Networks), 85
  access ports, 77, 93
  best practices, 103-104
  broadcast domains, 110
  creating, 87
  deleting, 91
  dynamic VLAN, VMPS, 87
  flat networks, 110
  IP telephony, support for, 102
  management VLAN, 87, 343
  native VLAN, 94, 343
  ports
    assignments, 88
    disassociating from, 91
  rogue switches, 344
  router-on-a-stick configurations, 95
  show commands
    show vlan brief command, 89
    show vlan command, 88-89
    show vlan id command, 89-90
    show vlan name command, 89-90
  static VLAN, 86
  subinterfaces, 95
  switches
    extending across, 94
    inter-VLAN switching, 95-97
  troubleshooting, 340-342
    access ports, 343
    management VLAN, 343
    native VLAN, 343
    trunk ports, 343
    VTP, 343-344
  trunk ports, 77, 93
    no switchport mode trunk command, 94
  switches
    configuring on, 96
    troubleshooting, 343
  VIC, frame-tagging, 91-92
VMPS, 87
VTP, 97
  advertisement requests, 99
  client mode, 98
  configuring, 99-102
  passwords, 344
  revision numbers, 98
  server mode, 98
  subset advertisements, 99
  summary advertisements, 99
  transport mode, 98
  troubleshooting, 343-344
  wireless support for, 102
VLSM (Variable Length Subnet Masks)
  addressing process overview, 126-128
  benefits of, 122
classful routing protocols, 122
classless routing protocols, 122
pie charts, 127
requirements for, 124-126
sub-subnets, 123
tabular charts, 127
VMPS (VLAN management policy servers), 87
voice traffic, network traffic prioritization, 14
VPN (Virtual Private Networks)
    enterprise edge security, 33
    IPsec, 17
    virtual tunnels, 16
VTP (VLAN Trunking Protocol), 97
    advertisement requests, 99
    client mode, 98
    configuring, 99-102
    passwords, 344
    revision numbers, 98
    server mode, 98
    subset advertisements, 99
    summary advertisements, 99
    transport mode, 98
    troubleshooting, 343-344
vtp version command, 344

W - X - Y - Z

WAN (Wide Area Networks), 10, 247
    analog data connections, 251
    cell switching, 255
    circuit switching, 254
    data link layer standards, 251
    debugging
        authentication, 373
        connectivity, 370-372
demarc, 248
DS0 standard, 249
DS1 standard, 249
DS3 standard, 250
encapsulation
    data link layer, 259
    Ethernet, 258-259
    Frame Relay, 271-274
    HDLC, 260
    layer 2, 258
    PPP, 260-263
first miles, 248
fractional E1 connections, 252
fractional T1 connections, 252
last miles, 248, 257
layer 1 standards, 250
layer 2 standards, 250
leased lines, 254
line characteristics, 250
local loops, 248, 257
long-range communications, 258
packet switching, 255
physical layer protocols, 249
physical link layer standards, 251
troubleshooting
    authentication, 372
    connectivity, 367-370
wildcard masks
        ACL, 291
            filtering specific hosts, 289-290
            packet-matching, 288
            statement creation, 288
            structure of, 287
converting subnet masks to, 290-291
EIGRP, 190
single-area OSPF configurations, 218-220
viewing, 190
wire speed, 67
wireless traffic, VLAN support for, 102
wiring closets. See telecommunications rooms