



Working at a Small-to-Medium Business or ISP

CCNA Discovery
Learning Guide



Allan Reid • Jim Lorenz

Cisco | Networking Academy
Mind Wide Open

Working at a Small-to-Medium Business or ISP

CCNA Discovery Learning Guide

Allan Reid
Jim Lorenz

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Working at a Small-to-Medium Business or ISP CCNA Discovery Learning Guide

Allan Reid and Jim Lorenz

Copyright© 2008 Cisco Systems, Inc.

Published by:

Cisco Press

800 East 96th Street

Indianapolis, IN 46240 USA

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

Printed in the United States of America

First Printing April 2008

Library of Congress Cataloging-in-Publication Data

Reid, Allan.

Working at a small-to-medium business or ISP : CCNA discovery learning guide / Allan Reid, Jim Lorenz.

p. cm.

Includes index.

ISBN 978-1-58713-210-0 (pbk. w/cd)

1. Computer networks—Textbooks. 2. Computer networks—Management—Textbooks. 3. Local area networks (Computer networks)—Textbooks. 4. Business enterprises—Computer networks—Textbooks. 5. Internet service providers—Textbooks. I.

Lorenz, Jim. II. Title.

TK5105.5.R4464 2008

004.6—dc22

2008015723

ISBN-13: 978-1-58713-210-0

ISBN-10: 1-58713-210-9

Publisher

Paul Boger

Associate Publisher

Dave Dusthimer

Cisco Representative

Anthony Wolfenden

Cisco Press Program Manager

Jeff Brady

Executive Editor

Mary Beth Ray

Managing Editor

Patrick Kanouse

Development Editor

Dayna Isley

Senior Project Editor

Tonya Simpson

Copy Editor

Gayle Johnson

Technical Editors

Bernadette O'Brien, Elaine Horn,
William Shurbert, Glenn Wright

Editorial Assistant

Vanessa Evans

Book Designer

Louisa Adair

Composition

Louisa Adair

Indexer

Tim Wright

Proofreader

Molly Proue

This book is part of the Cisco Networking Academy® series from Cisco Press. The products in this series support and complement the Cisco Networking Academy curriculum. If you are using this book outside the Networking Academy, then you are not preparing with a Cisco trained and authorized Networking Academy provider.

For more information on the Cisco Networking Academy or to locate a Networking Academy, please visit www.cisco.com/edu.



Warning and Disclaimer

This book is designed to provide information about the *Working at a Small-to-Medium Business or ISP CCNA Discovery* course. Every effort has been made to make this book as complete and 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 corpsales@pearsontechgroup.com.

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

Feedback Information

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

Reader feedback is a natural continuation of this process. If you have any comments about 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 be sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

About the Authors

Allan Reid is the curriculum lead and a CCNA/CCNP instructor at the Centennial College CATC in Toronto, Canada. He is a professor in the Information and Communications Engineering Technology department and is 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 developing and implementing numerous certificate, diploma, and degree programs in networking. Allan also is a curriculum developer for the Cisco Networking Academy. Outside his academic responsibilities, he has been active in the computer and networking fields for more than 25 years. Currently he is 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, he 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. He 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.

About the Technical Reviewers

Bernadette O'Brien has been teaching in the Cisco Networking Academy in Schenectady, New York since 1998. Schenectady High School is a Regional Academy for CCNA and is a CATC for Sponsored Curriculum, which Bernadette coordinates. Bernadette received her BS degree from SUNY Buffalo and her MS degree in curriculum and instruction from SUNY Albany. She is also CCNA and CCAI certified. Bernadette and her husband and two children live in a Victorian village very near the Adirondack Mountains in upstate New York. They enjoy rehabbing their 120-year-old Victorian house, skiing, and hiking.

Elaine Horn, CCAI, has been teaching in the Cisco Networking Academy since 1998 at TRECA (<http://www.treca.org>) in Marion, Ohio. TRECA is a CATC for CCNA, a regional academy for Sponsored and Emerging Technologies Curriculum, and a local academy for CCNA. She is currently teaching and supporting academies in Ohio, Kentucky, and Michigan. Elaine received her BS degree in education and an MA in mathematics education from The Ohio State University. She has also coordinated the Skills Ohio Internetworking Competition and worked with Cisco Press as a technical editor for Academy-related materials.

Bill Shurbert is a professor of information technology at New Hampshire Technical Institute in Concord, New Hampshire. He holds a bachelor's degree in technical management from Southern New Hampshire University. He enjoys teaching the Cisco CCNA, Wireless, and IT Essentials classes. In his off time, you can find Bill and Joanne, his wife of more than 25 years, sailing the waters of Lake Winnepesaukee.

Glenn Wright, CCNA, CCAI, is the codirector of the Cisco Academy Training Center (CATC) in Fort Worth, Texas. He has a bachelor's degree in business education from the University of North Texas and 22 years of experience in computer education. He has been involved in many aspects of the Cisco Networking Academy since 1999. He serves the Academy as an instructor and supports the Regional Academies in Texas, Louisiana, Oklahoma, Arkansas, North Carolina, South Carolina, Virginia, and Tennessee. Glenn has also worked with the Academy Quality Assurance Team, reviewing and editing Academy curriculum and assessment. He has developed and edited Packet Tracer activities for the *Discovery* curriculum. He has also worked with Cisco Press as a technical editor for Academy-related materials.

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*

Acknowledgments

We want to thank Mary Beth Ray, Dayna Isley, and Drew Cupp with Cisco Press for their help and guidance in putting this book together. We also want to thank the technical editors, Bernadette O'Brien, Elaine Horn, Bill Shurbert, and Glenn Wright. Their attention to detail and suggestions made a significant contribution to the accuracy and clarity of the content.

We would also like 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

Introduction xxxii

Part I: Concepts

Chapter 1	The Internet and Its Uses	1
Chapter 2	Help Desk	19
Chapter 3	Planning a Network Upgrade	49
Chapter 4	Planning the Addressing Structure	73
Chapter 5	Configuring Network Devices	109
Chapter 6	Routing	173
Chapter 7	ISP Services	205
Chapter 8	ISP Responsibility	241
Chapter 9	Troubleshooting	285
Chapter 10	Putting It All Together	353

Part II: Labs

Chapter 1	Lab: The Internet and Its Uses	357
Chapter 2	Lab: Help Desk	367
Chapter 3	Lab: Planning a Network Upgrade	369
Chapter 4	Lab: Planning the Addressing Structure	373
Chapter 5	Lab: Configuring Network Devices	383
Chapter 6	Lab: Routing	487
Chapter 7	Lab: ISP Services	505
Chapter 8	Lab: ISP Responsibility	521
Chapter 9	Lab: Troubleshooting	589
Chapter 10	Capstone Project: Putting It All Together	679
Appendix A	Check Your Understanding and Challenge Questions Answer Key	693
Appendix B	Router Boot and Password Recovery Labs	709
Appendix C	Lab Equipment Interfaces and Initial Configuration Restoration	721
	Glossary	725
	Index	739

Contents

Introduction xxxii

Part I: Concepts

Chapter 1	The Internet and Its Uses	1
	Objectives	1
	Key Terms	1
	What Is the Internet?	2
	The Internet and Standards	2
	<i>E-Commerce</i>	2
	<i>Communications</i>	2
	<i>Collaboration and Training</i>	3
	ISPs and ISP Services	4
	Internet Service Providers	4
	Delivering Internet Services to End Users	5
	<i>Dialup Access</i>	5
	<i>DSL</i>	5
	<i>Cable Modem</i>	6
	<i>Satellite</i>	6
	<i>Dedicated Bandwidth Options</i>	6
	<i>Point of Presence</i>	7
	Internet Hierarchy	7
	<i>Tier 1 ISPs</i>	9
	<i>Tier 2 ISPs</i>	9
	<i>Tier 3 ISPs</i>	9
	Identifying the Structure of the Internet	9
	ISP Connectivity	12
	ISP Requirements	12
	Roles and Responsibilities Within an ISP	14
	Summary	15
	Activities and Labs	16
	Check Your Understanding	16
	Challenge Questions and Activities	18
Chapter 2	Help Desk	19
	Objectives	19
	Key Terms	19
	Help Desk Technicians	20
	ISP Help Desk Organization	20
	Roles of ISP Technicians	21
	Interacting with Customers	22
	OSI Model	24
	Using the OSI Model	24
	OSI Model Protocols and Technologies	27

- Step 1: Upper Layers Create the Data* 27
- Step 2: Layer 4 Packages the Data for End-to-End Transport* 27
- Step 3: Layer 3 Adds the Network IP Address Information* 28
- Step 4: Layer 2 Adds the Data Link Layer Header and Trailer* 28
- Step 5: Layer 1 Converts the Data into Bits for Transmission* 28

- Troubleshooting Using the OSI Model 29
 - Bottom-Up Approach* 30
 - Top-Down Approach* 30
 - Divide-and-Conquer Approach* 31
 - Help Desk Troubleshooting Example* 31

ISP Troubleshooting 34

- Help Desk Troubleshooting Scenarios 34
 - E-mail Issues* 35
 - Host Configuration Issues* 35
 - Customer Connectivity Issues* 36
- Creating and Using Help Desk Records 37
- Customer Site Procedures 40

Summary 42

Activities and Labs 42

Check Your Understanding 43

Challenge Questions and Activities 47

Chapter 3 Planning a Network Upgrade 49

Objectives 49

Key Terms 49

Common Issues 50

- Site Survey 50
- Physical and Logical Topologies 52
 - Star Topologies* 54
 - Mesh Topologies* 54
- Network Requirements Documentation 55

Planning the Network Upgrade 55

- Network Upgrades 56
 - Phase 1: Requirements Gathering* 56
 - Phase 2: Selection and Design* 56
 - Phase 3: Implementation* 56
 - Phase 4: Operation* 56
 - Phase 5: Review and Evaluation* 57
- Physical Environment 57
- Cabling Considerations 58
- Structured Cable 60

Purchasing and Maintaining Equipment 61

- Purchasing Equipment 61
- Selecting Network Devices 63

	Selecting LAN Devices	63
	<i>Speed and Types of Ports/Interfaces</i>	63
	<i>Expandability</i>	64
	<i>Manageability</i>	64
	<i>Cost</i>	64
	Selecting Internetworking Devices	64
	<i>Connectivity</i>	65
	<i>Features</i>	65
	<i>Cost</i>	65
	Network Equipment Upgrades	66
	Reliability and Availability	67
	IP Addressing Plan	68
	Summary	69
	Activities and Labs	69
	Check Your Understanding	70
	Challenge Questions and Activities	72
Chapter 4	Planning the Addressing Structure	73
	Objectives	73
	Key Terms	73
	IP Addressing in the LAN	74
	Review of IP Addresses	74
	<i>Hierarchical Addressing</i>	75
	<i>Classful Addressing</i>	75
	<i>Subnetting Concepts</i>	77
	<i>Classless Interdomain Routing (CIDR)</i>	79
	Subnetting a Network	82
	<i>Network Expansion Requirements</i>	82
	<i>Proposed Solution</i>	83
	Classful Subnetting	85
	Custom Subnet Masks	86
	Communicating Between Subnets	90
	IPv6	92
	NAT and PAT	93
	Basic Network Address Translation (NAT)	93
	IP NAT Terms	95
	Static and Dynamic NAT	97
	Port-Based Network Address Translation	99
	IP NAT Issues	102
	Summary	103
	Activities and Labs	103
	Check Your Understanding	104
	Challenge Questions and Activities	107

Chapter 5	Configuring Network Devices	109
	Objectives	109
	Key Terms	109
	Initial ISR Configuration	110
	Physical Setup of the ISR	112
	Bootup Process	114
	<i>Startup Configuration File</i>	114
	<i>Running Configuration File</i>	115
	In-Band and Out-of-Band Router Configuration	117
	<i>Out-of-Band Management</i>	117
	<i>In-Band Management</i>	117
	Cisco IOS Programs	118
	Configuring an ISR with SDM	120
	SDM Express	121
	<i>Basic Configuration</i>	121
	<i>LAN IP Address</i>	122
	<i>DHCP</i>	123
	Configuring a Serial WAN Connection	124
	Cisco SDM and SDM Express	126
	Configuring Dynamic NAT Using Cisco SDM	127
	Configuring a Router Using IOS CLI	128
	Command-Line Interface and Modes	128
	Using the Cisco IOS CLI	129
	Using show Commands	132
	Basic Configuration	137
	Configuring an Interface	139
	Configuring a Default Route	141
	Configuring DHCP Services	141
	<i>Step 1: Create the DHCP Address Pool</i>	142
	<i>Step 2: Specify the Network or Subnet</i>	142
	<i>Step 3: Exclude IP Addresses</i>	142
	<i>Step 4: Specify the Domain Name</i>	142
	<i>Step 5: Specify the DNS Server IP Address</i>	142
	<i>Step 6: Set the Default Gateway</i>	143
	<i>Step 7: Set the Lease Duration</i>	143
	<i>Step 8: Verify the Configuration</i>	143
	Configuring Static NAT Using Cisco IOS CLI	144
	Backing Up a Cisco Router Configuration to a TFTP Server	146
	Connecting the CPE to the ISP	148
	Installing the CPE	148
	Customer Connections over a WAN	151
	<i>Point-to-Point</i>	151
	<i>Circuit-Switched</i>	152
	<i>Packet-Switched</i>	152

Choosing a WAN Connection	153
Configuring WAN Connections	154
Initial Cisco 2960 Switch Configuration	155
Standalone Switches	156
Power Up the Cisco 2960 Switch	159
Connecting the LAN Switch to the Router	161
CDP	164
Summary	167
Activities and Labs	168
Check Your Understanding	169
Challenge Questions and Activities	172

Chapter 6

Routing	173
Objectives	173
Key Terms	173
Enabling Routing Protocols	174
Routing Basics	174
<i>Directly Connected Routes</i>	178
<i>Dynamically Updated Routes (Dynamic Routes)</i>	178
<i>Default Route</i>	178
<i>Static Routes</i>	178
Routing Protocols	179
Common Interior Routing Protocols	182
<i>RIP</i>	183
<i>EIGRP</i>	184
<i>Link-State Protocols: OSPF</i>	185
Routing Within an Organization	187
Configure and Verify RIP	190
Exterior Routing Protocols	193
Autonomous Systems	193
Routing Between Autonomous Systems	195
Routing Across the Internet	196
Exterior Routing Protocols and the ISP	197
Configure and Verify BGP	199
Summary	201
Activities and Labs	201
Check Your Understanding	202

Chapter 7

ISP Services	205
Objectives	205
Key Terms	205
Introducing ISP Services	206
ISP Services	206

Reliability and Availability 207

Reliability 207

Availability 208

Protocols That Support ISP Services 208

Review of TCP/IP Protocols 208

Application Layer Protocols 210

Transport Layer Protocols 211

TCP and UDP 212

TCP 212

UDP 212

Differences Between TCP and UDP 214

Supporting Multiple Services 215

Domain Name Service 218

TCP/IP Hosts File 218

DNS 219

Resource Records and Domain Namespace 220

Domain Name Servers 220

Resolvers 220

DNS Name Resolution 221

Forward Lookup Zones 224

Reverse Lookup Zones 224

Primary Zones 225

Secondary Zones 225

Provisioning DNS Servers 225

Using ISP DNS Servers 225

Using Local DNS Servers 226

Services and Protocols 226

Supporting HTTP and HTTPS 227

Supporting FTP 229

Protocol Interpreter (PI) 229

Data Transfer Process (DTP) 229

Supporting SMTP, POP3, and IMAP 230

Simple Mail Transfer Protocol (SMTP) 231

Post Office Protocol Version 3 (POP3) 233

Internet Message Access Protocol (IMAP4) 234

Summary 236

Activities and Labs 236

Check Your Understanding 237

Challenge Questions and Activities 239

Chapter 8 ISP Responsibility 241

Objectives 241

Key Terms 241

ISP Security Considerations 242

ISP Security	242
<i>Password Security</i>	243
<i>Extraneous Services</i>	243
<i>Patch Management</i>	244
<i>Application Security</i>	244
<i>User Rights</i>	244
<i>Security Scanning</i>	244
Best Practices for Security	245
Data Encryption	247
<i>Web Servers</i>	248
<i>E-mail Servers</i>	248
<i>Telnet Servers</i>	248
<i>FTP Servers</i>	249
<i>File Servers</i>	249
Security Tools	249
Denial-of-Service Attacks	249
<i>DoS</i>	249
<i>DDoS</i>	249
<i>DRDoS</i>	250
Access Lists and Port Filtering	250
<i>Port Filtering</i>	250
<i>Access Lists</i>	251
Firewalls	251
IDS and IPS	253
<i>IDS</i>	254
<i>IPS</i>	255
Wireless Security	256
<i>Changing Default Settings</i>	257
<i>Enabling Authentication</i>	257
<i>MAC Address Filtering</i>	257
<i>WEP</i>	257
<i>WPA</i>	258
<i>WPA2</i>	258
Host Security	258
<i>Known Attacks</i>	259
<i>Exploitable Services</i>	260
<i>Worms and Viruses</i>	260
<i>Back Doors and Trojans</i>	260
Monitoring and Managing the ISP	261
Service-Level Agreements	261
Monitoring Network Link Performance	262
Device Management Using In-Band Tools	264
<i>Telnet</i>	264
<i>Secure Shell (SSH)</i>	264
Using SNMP and Syslog	265
<i>SNMP</i>	265
<i>Syslog</i>	267
Backups and Disaster Recovery	268
Causes of Data Loss	268
<i>Hardware Failure</i>	268

- User Error* 269
- Theft* 269
- Malicious Activity* 269
- Operating System Failure* 269
- Backup Media 269
 - Tape Media* 270
 - Optical Media* 270
 - Hard Disk Media* 270
 - Solid-State Media* 271
- Methods of File Backup 271
 - Normal (Full)* 271
 - Differential* 272
 - Incremental* 273
- Backup System Maintenance 273
 - Swap Media* 273
 - Review Backup Logs* 274
 - Perform Trial Restores* 274
 - Perform Drive Maintenance* 274
- Backing Up and Restoring Cisco IOS Image Files 275
 - Using TFTP to Update the IOS Image* 275
 - Using ROMmon to Recover the IOS Image* 276
- Best Practices for Disaster Recovery 277

Summary 280

Activities and Labs 281

Check Your Understanding 282

Chapter 9 Troubleshooting 285

Objectives 285

Troubleshooting Methodologies and Tools 286

The OSI Model and Troubleshooting 286

Troubleshooting Methodologies 289

Top-Down 289

Bottom-Up 289

Divide-and-Conquer 289

Troubleshooting Tools 290

Network Topologies 290

Software Troubleshooting Tools 291

Hardware Troubleshooting Tools 293

Troubleshooting Layer 1 and Layer 2 Issues 295

Layer 1 and 2 Problems 295

Troubleshooting Device Hardware and Boot Errors 298

Troubleshooting Cable and Device Port Errors 301

Excessive Noise 302

Excessive Collisions 303

Excessive Runt Frames 303

Late Collisions 303

Troubleshooting LAN Connectivity Issues	304
Troubleshooting WAN Connectivity Issues	305
<i>Serial x Is Down, Line Protocol Is Down (DTE)</i>	307
<i>Serial x Is Up, Line Protocol Is Down (DTE)</i>	307
<i>Serial x Is Up, Line Protocol Is Down (DCE)</i>	308
<i>Serial x Is Up, Line Protocol Is Up (Looped)</i>	308
<i>Serial x Is Up, Line Protocol Is Down (Disabled)</i>	308
<i>Serial x Is Administratively Down, Line Protocol Is Down</i>	309
Troubleshooting Layer 3 IP Addressing Issues	309
Review of Layer 3 Functionality and IP Addressing	310
IP Design and Configuration Issues	314
IP Address Planning and Allocation Issues	317
DHCP and NAT Issues	318
Troubleshooting Layer 3 Routing Issues	323
Layer 3 Routing Issues	323
<i>Connected Route Problems</i>	324
<i>Static and Default Route Problems</i>	324
<i>Dynamic Route Problems</i>	324
Dynamic Routing Errors	325
Troubleshooting Layer 4 and Upper Layer Issues	331
Layer 4 Traffic Filtering Errors	331
Troubleshooting Upper-Layer Problems	332
<i>Step 1: Ping the Default Gateway</i>	333
<i>Step 2: Verify End-to-End Connectivity</i>	333
<i>Step 3: Verify Routing Configuration</i>	334
<i>Step 4: Verify NAT Operation</i>	334
<i>Step 5: Verify Firewall Filtering Rules</i>	334
Using Telnet to Check Upper-Layer Connectivity	335
Preparing for Cisco Certification	336
Knowledge, Skills, and Abilities	336
Networking Knowledge, Skills, and Abilities	338
Making the Commitment	341
Creating a Plan	341
Practicing Test Taking	342
<i>Visit the Testing Center</i>	343
<i>Format of the Examination</i>	343
Summary	345
Activities and Labs	347
Check Your Understanding	348
Chapter 10 Putting It All Together	353
Summary Activity	353
Activities and Labs	353

Part II: Labs

- Chapter 1 Lab: The Internet and Its Uses 357**
- Lab 1-1: Mapping ISP Connectivity Using traceroute (1.2.3) 357**
- Objectives 357
 - Background/Preparation 357
 - Task 1: Run the tracert Utility from a Host Computer 358
 - Task 2: Interpret tracert Outputs to Determine ISP Connectivity 359
 - Task 3: Map the Connectivity of Your ISP 361
 - Routes Traced Worksheet 363
- Chapter 2 Lab: Help Desk 367**
- Chapter 3 Lab: Planning a Network Upgrade 369**
- Lab 3-1: Evaluating a Cabling Upgrade Plan (3.2.4) 369**
- Objectives 369
 - Background/Preparation 369
 - Task 1: Examine the Existing Floor Plan 369
 - Task 2: Evaluate the Plan for the New Floor Space 370
 - Task 3: Examine the Floor Space and Wiring Plan 370
 - Task 4: Reflection 371
- Chapter 4 Lab: Planning the Addressing Structure 373**
- Lab 4-1: Subnetting a Network (4.1.5) 373**
- Objective 373
 - Background/Preparation 373
 - Task 1: Analyze the Network 375
 - Task 2: Calculate the Custom Subnet Mask 375
 - Task 3: Specify the Host IP Addresses 375
 - Task 4: Consider Other Subnetting Options 376
 - Task 5: Reflection 377
- Lab 4-2: Determining PAT Translations (4.2.4) 378**
- Objectives 378
 - Background/Preparation 378
 - Task 1: Determine the IP Address of the Computer 379
 - Task 2: Determine the IP Addresses of the Gateway Router or ISR 379
 - Task 3: Display Baseline netstat Results 379
 - Task 4: Display Active Network Connections 380
 - Task 5: Determine Translated Addresses 380
 - Task 6: Reflection 381
- Chapter 5 Lab: Configuring Network Devices 383**
- Lab 5-1: Powering Up an Integrated Services Router (5.1.3) 383**
- Objectives 383
 - Background/Preparation 383

Part 1: Initial Router Setup and Startup	384
<i>Task 1: Position the Router and Connect the Ground Wire (Optional)</i>	384
<i>Task 2: Install the Compact Flash Memory Card (Optional)</i>	385
<i>Task 3: Connect the PC and Configure the Terminal Emulation Program</i>	385
<i>Task 4: Power Up the ISR</i>	386
<i>Task 5: Troubleshoot a Nonworking Router</i>	387
Part 2: Displaying Router Information Using show Commands	387
<i>Task 1: Display the Router Running Configuration</i>	387
<i>Task 2: Display the Router Startup Configuration</i>	389
<i>Task 3: Save the Running-Config to the Startup-Config</i>	389
<i>Task 4: Display the Router System Information Using the show version Command</i>	390
<i>Task 5: Reflection</i>	392
Lab 5-2: Configuring an ISR with SDM Express (5.2.3)	393
Objectives	393
Background/Preparation	393
Task 1: Configure the PC to Connect to the Router, and Then Launch Cisco SDM	394
Task 2: Perform Initial Basic Configuration	396
Task 3: Configure the LAN IP Address	397
Task 4: Deselect the DHCP Server	398
Task 5: Configure the WAN Interface	398
Task 6: Enable the Firewall and Security Settings	401
Task 7: Review and Complete the Configuration	402
Task 8: Reflection	403
Lab 5-3: Configuring Dynamic NAT with SDM (5.2.4)	405
Objective	405
Background/Preparation	405
Task 1: Establish a Connection from the PC to the Router	406
Task 2: Configure SDM to Show Cisco IOS CLI Commands	407
Task 3: Launch the Basic NAT Wizard	407
Task 4: Select the WAN Interface for NAT	408
Task 5: Reflection	411
Lab 5-4: Configuring Basic Router Settings with the Cisco IOS CLI (5.3.5)	412
Objectives	412
Background/Preparation	412
Task 1: Configure Host IP Settings	413
Task 2: Log In to Each Router, and Configure a Hostname and Password	414
Task 3: Show the Router Running Configuration	415
Task 4: Configure the Serial Interface on R1	416
Task 5: Display Information About the Serial Interface on R1	417
Task 6: Configure the Serial Interface on R2	418
Task 7: Display Information About the Serial Interface on R2	418
Task 8: Verify That the Serial Connection Is Functioning	419

- Task 9: Configure the FastEthernet Interface on R1 420
- Task 10: Display Information About the FastEthernet Interface on R1 420
- Task 11: Configure the FastEthernet Interface on R2 421
- Task 12: Display Information About the FastEthernet Interface on R2 422
- Task 13: Save the Configuration on Both Routers 423
- Task 14: Check Both Router Configurations 423
- Task 15: Verify That the FastEthernet Connection to Each Router Is Functioning 423
- Task 16: Test Connectivity (Optional Challenge) 424

Lab 5-5: Configuring DHCP with SDM and the Cisco IOS CLI (5.3.7) 425

- Objectives 425
- Background/Preparation 425
- Task 1: Configure Basic Router Settings Using IOS, and Configure PAT Using SDM 426
- Task 2: Configure and Verify DHCP Using IOS 432
- Task 3: Reflection 435

Lab 5-6: Configuring PAT with SDM and Static NAT Using Cisco IOS (5.3.8) 436

- Objectives 436
- Background/Preparation 436
- Task 1: Configure Basic Router Settings Using IOS, and Configure PAT Using SDM 437
- Task 2: Configure and Verify Static NAT Using IOS 444
- Task 3: Reflection 446

Lab 5-7: Managing Router Configuration Files Using HyperTerminal (5.3.9a) 447

- Objectives 447
- Background/Preparation 447
- Task 1: Configure Host IP Settings 448
- Task 2: Log In to Router R1, and Configure the Basic Settings 449
- Task 3: Display the R1 Router Configuration 449
- Task 4: Save the Configuration on R1 450
- Task 5: Start Capturing the Running Configuration File 450
- Task 6: Stop Capturing the Configuration File 450
- Task 7: Clean Up the Captured Configuration File 450
- Task 8: Erase the Current Startup Configuration, and Restart the Router 454
- Task 9: Reconfigure the R1 Router from the Saved Text File 455
- Task 10: Modify the R1 Text File, and Use It to Configure the R2 Router 455
- Task 11: Verify That the Network Is Functioning 456

Lab 5-8: Managing Router Configuration Files Using TFTP (5.3.9b) 457

- Objectives 457
- Background/Preparation 457
- Task 1: Build the Network and Verify Connectivity 458
- Task 2: Use TFTP to Save a Cisco IOS Configuration 459
- Task 3: Use TFTP to Restore a Cisco IOS Configuration 464
- Task 4: Reflection 465

Lab 5-9: Planning a WAN Upgrade (5.4.3) 466

- Objective 466
- Background/Preparation 466
- Task 1: Identify the Business Requirements for the WAN Upgrade 466
- Task 2: List Available WAN Options for the Business 467
- Task 3: Identify the Best WAN Connection Option for the Business 467
- Task 4: Group Discussion 467
- WAN Upgrade Proposal 468

Lab 5-10: Powering Up a Switch (5.5.2) 470

- Objectives 470
- Background/Preparation 470
- Task 1: Position and Ground the Switch (Optional) 470
- Task 2: Connect the Computer to the Switch 470
- Task 3: Configure the PC Terminal Emulation Program 471
- Task 4: Power Up the Switch 471
- Task 5: Troubleshoot a Nonworking Switch 473
- Task 6: Reflection 473

Lab 5-11: Configuring the Cisco 2960 Switch (5.5.4) 474

- Objectives 474
- Background/Preparation 474
- Task 1: Connect the Hosts to the Switch, and Configure Them 475
- Task 2: Connect the Router to the Switch, and Configure the Router 475
- Task 3: Perform an Initial Configuration on the Switch 476
- Task 4: Configure the Management Interface on VLAN 1 476
- Task 5: Verify Configuration of the Switch 477
- Task 6: Verify Connectivity Using ping and Telnet 478
- Task 7: Determine Which MAC Addresses the Switch Has Learned 480
- Task 8: Configure Basic Port Security 481
- Task 9: Connect a Different PC to the Secure Switch Port 483
- Alternative Task 9: Change the MAC Address of H2 (Optional) 484
- Task 10: Reactivate the Port 485
- Task 11: Set Speed and Duplex Options for a Port 485
- Task 12: Exit the Switch 486
- Task 13: Reflection 486

Chapter 6 Lab: Routing 487

Lab 6-1: Creating a Network Diagram from Routing Tables (6.1.2) 487

Objectives 487

Background/Preparation 487

Task 1: Examine the Routing Table Entries for Router R1 487

Task 2: Examine the Routing Table Entries for Router R2 488

Task 3: Document Router Interfaces and IP Addresses 489

Task 4: Create a Network Topology Diagram 489

Task 5: Reflection 490

Lab 6-2: Configuring and Verifying RIP (6.1.5) 491

Objective 491

Background/Preparation 491

Task 1: Build the Network and Configure the Routers 492

Task 2: Configure the Hosts with the Proper IP Address, Subnet Mask, and Default Gateway 492

Task 3: Check the Routing Table Entries 492

Task 4: Test End-to-end Connectivity 493

Task 5: Configure the Routing Protocol of the Routers 493

Task 6: Show the Routing Tables for Each Router 494

Task 7: Test End-to-end Connectivity 495

Task 8: Use debug to Observe RIP Communications 496

Task 9: Reflection 497

Lab 6-3: Configuring BGP with Default Routing (6.2.4) 498

Objectives 498

Background/Preparation 498

Task 1: Configure Basic Information on Each Router 499

Task 2: Configure the Default and Static Routes 500

Task 3: Configure BGP on Both ISP Routers 500

Task 4: View the Routing Tables 501

Task 5: Verify Connectivity 503

Task 6: View BGP Information on the ISP Routers 503

Task 7: Reflection 503

Chapter 7 Lab: ISP Services 505

Lab 7-1: Editing the HOSTS File in Windows (7.3.1) 505

Objective 505

Background/Preparation 505

Task 1: Locate the HOSTS File in Windows 505

Task 2: Edit the HOSTS File 506

Task 3: Test the New Name Mapping 507

Task 4: Reflection 507

Lab 7-2: Examining Cached DNS Information on a Windows DNS Server (7.3.3) 508

Objective 508

- Background/Preparation 508
- Task 1: Use the Windows Server DNS Administrative Tool 508
- Task 2: Perform a DNS Lookup 510
- Task 3: Examine the Cached DNS Entries 510
- Task 4: Reflection 511

Lab 7-3: Creating Primary and Secondary Forward Lookup Zones (7.3.3) 512

- Objective 512
- Background/Preparation 512
- Task 1: Create a Primary Forward Lookup Zone on Windows 512
- Task 2: Add a Host Record to the Primary Forward Lookup Zone 515
- Task 3: Create a Secondary Forward Lookup Zone 517
- Task 4: Reflection 519

Chapter 8 Labs: ISP Responsibility 521

Lab 8-1: Securing Local Data and Transmitted Data (8.1.3) 521

- Objectives 521
- Background/Preparation 521
- Part 1: Securing Local Data 521
 - Task 1: Secure Bob's Files Folder 521*
 - Task 2: Test Joe's Access to Bob's Files 525*
- Part 2: Identifying a Secure Communication Channel When Transmitting Data over the Internet 525
 - Task 1: Identify a Secure Web Page 526*
 - Task 2: Examine Secure Access to an Untrusted Source Warning 528*

Lab 8-2: Planning for Access Control Lists and Port Filters (8.2.1) 529

- Objective 529
- Background/Preparation 529
- Task 1: Restrict Client A to One Subnet 529
- Task 2: Restrict Client B Access to Server A, But Allow Access to Server B and the Internet 530
- Task 3: Allow Only Client A to Access the Routers Using Only SSH 530

Lab 8-3: Researching Anti-X Software Products (8.2.5) 532

- Objective 532
- Background/Preparation 532
- Task 1: Identify Three Products 532
- Task 2: Compare Pricing 532

Lab 8-4: Interpreting a Service-Level Agreement (8.3.1) 533

- Objectives 533
- Background/Preparation 533
- Task 1: Review Typical Customer Needs 533
- Task 2: Analyze a Sample SLA and Identify Its Key Components 534
 - I. General Terms of the Service-Level Agreement 536*
 - II. Warranty and Liability 536*

<i>III. Services Provided to [Client]</i>	536
<i>IV. System Availability</i>	537
<i>V. System Monitoring</i>	537
<i>VI. System Notifications</i>	537
<i>VII. Change Management Process</i>	537
<i>VIII. Penalties for Service Outages</i>	540
<i>IX. ISP Facilities Policies</i>	540
<i>X. Billing</i>	540
<i>XI. Signatures</i>	540
<i>Appendix 1: Services and Pricing</i>	540
<i>Appendix 2: System Requests Contact Lists</i>	541

Lab 8-5: Conducting a Network Capture with Wireshark (8.3.2) 542

Objectives	542
Background/Preparation	542
Task 1: Install and Launch Wireshark	542
Task 2: Select an Interface to Use for Capturing Packets (Optional)	543
Task 3: Start a Network Capture	543
Task 4: Analyze Web Traffic Information (Optional)	543
Task 5: Filter a Network Capture	544
Task 6: Reflection	545

Lab 8-6: Managing Remote Network Devices with Telnet (8.3.3a) 546

Objectives	546
Background/Preparation	546
Task 1: Build the Network and Verify Connectivity	547
Task 2: Establish a Telnet Session from a Host Computer	548
Task 3: Perform Basic Telnet Operations Between Two Routers	549
Task 4: Perform Telnet Operations Between Multiple Routers	552
Task 5: Experiment with Multiple Linked Telnet Sessions	553
Task 6: Reflection	554

Lab 8-7: Configuring a Remote Router Using SSH (8.3.3b) 555

Objectives	555
Background/Preparation	555
Task 1: Configure the ISR to Accept SSH Connections Using SDM	557
Task 2: Configure SSH on a Non-SDM Router (Optional)	559
Task 3: Configure the SSH Client, and Connect the PC to the ISR	560
Task 4: Check the Configuration of the Cisco 1841 ISR	562
Task 5: Log Out of the Cisco 1841 ISR	562
Task 6: Reflection	562

Lab 8-8: Planning a Backup Solution (8.4.2) 563

Objective	563
Background/Preparation	563
Task 1: Choose the Media and Backup Hardware	563
Task 2: Design a Backup Plan and Procedure	564

Lab 8-9: Managing Cisco IOS Images with TFTP (8.4.3a) 565

Objectives 565

Background/Preparation 565

Task 1: Build the Network and Verify Connectivity 566

Task 2: Collect Information About the Router Memory and IOS Image 567

Task 3: Use TFTP to Save the Cisco IOS Image 569

Task 4: Use TFTP to Update a Cisco IOS Image 573

Task 5: Reflection 574

Lab 8-10: Managing Cisco IOS Images with ROMmon and TFTP (8.4.3b) 575

Objectives 575

Background/Preparation 575

Task 1: Build the Network and Verify Connectivity 576

Task 2: Collect Information About the Router Memory and IOS Image 577

Task 3: Use TFTP to Save the Current Cisco IOS Image 578

Task 4: Consider IOS Restoration Options 582

Task 5: Working in ROMmon Mode 582

Task 6: Use ROMmon and tftpdnld to Restore an IOS Image (Optional) 585

Task 7: Reflection 588

Chapter 9 Lab: Troubleshooting 589**Lab 9-1: Organizing CCENT Objectives by OSI Layer (9.1.1) 589**

Objectives 589

Background/Preparation 589

Task 1: Access the CCENT Exam Web Page 589

Task 2: Review the OSI Model Layers 592

Task 3: Reflection 596

Lab 9-2: Using Wireshark to Observe the TCP Three-Way Handshake (9.1.3) 597

Objectives 597

Background/Preparation 597

Task 1: Prepare Wireshark to Capture Packets 597

Task 2: Generate and Analyze Captured Packets 598

Task 3: Reflection 603

Lab 9-3: Identifying Cabling and Media Errors (9.2.3) 604

Objectives 604

Background/Preparation 604

Task 1: Review Ethernet Device Cabling 605

Task 2: Build the Network and Configure Devices 606

Task 3: Verify Cabling and Interface Link LEDs 606

Task 4: Verify Interface Status and Connectivity 607

Task 5: Observe the Effects of Using Different Cable 610

Task 7: Reflection 614

Lab 9-4: Troubleshooting LAN Connectivity (9.2.4) 615

Objectives 615

Background/Preparation 615

Task 1: Build the Network and Configure Devices 616

Task 2: Verify Cabling, Interface LEDs, and Link Speed 617

Task 3: Verify Switch Interface Information 618

Task 4: Change Duplex Settings 619

Task 5: Change Speed Settings 620

Task 6: Set Both Duplex and Speed Settings 621

Task 7: Check Settings and Characteristics of Neighboring Devices and Interfaces 622

Task 8: Change Router Duplex Settings 623

Task 9: Reflection 623

Lab 9-5: Troubleshooting WAN Connectivity (9.2.5) 624

Objectives 624

Background/Preparation 624

Task 1: Build the Network and Configure Devices 625

Task 2: Verify Cabling and Interface LEDs 625

Task 3: Verify Router Interface Status and Connectivity 626

Task 4: Change the Clock Rate 628

Task 5: Remove the Serial Cable and Observe the Effects 630

Task 6: Change the Encapsulation Type 632

Task 7: Reflection 636

Lab 9-6: Designing an IP Subnetting Scheme for Growth (9.3.3) 637

Objectives 637

Background/Preparation 637

Task 1: Analyze the Network Topology for Subnetting Requirements 637

Task 2: Develop the Subnet Scheme 638

Task 3: Document Network Device and Host Interfaces 639

Task 4: Reflection 640

Lab 9-7: Correcting RIPv2 Routing Problems (9.4.2) 641

Objectives 641

Background/Preparation 641

Task 1: Build the Network and Configure Devices 643

Task 2: Load Routers with the Supplied Scripts 643

Task 3: Troubleshoot the BRANCH1 Router 646

Task 4: Troubleshoot HQ 650

Task 5: Troubleshoot BRANCH2 651

Task 6: Remove Auto-Summary 654

Task 7: Reflection 655

Task 8: Documentation 655

Lab 9-8: Using Telnet and SSH to Access Networking Devices (9.5.3) 656

Objectives 656

Background/Preparation	656
Part 1. Working with Telnet to Verify Device Configurations and Connectivity	658
<i>Task 1: Build the Network and Verify Network Layer Connectivity</i>	658
<i>Task 2: Establish a Telnet Session from a Host Computer</i>	659
<i>Task 3: Perform Basic Telnet Operations Between the Routers</i>	660
<i>Task 4: Perform Telnet Operations Between Multiple Routers</i>	661
<i>Task 5: Remove the vty Password from R3</i>	662
Part 2. Working with SSH to Verify Device Configurations and Connectivity	663
<i>Task 1: Configure SSH on Router R2</i>	664
<i>Task 2: Log In to R2 Using the R1 CLI SSH Client</i>	666
<i>Task 3: Reflection</i>	667
Lab 9-9: Identifying Necessary Knowledge, Skills, and Abilities (9.6.2)	668
Objectives	668
Background/Preparation	668
Task 1: Review the Definitions for KSAs	668
Task 2: Review an Existing Lab	669
Task 3: Identify the Knowledge, Skills, and Abilities Required for the Lab	670
Lab 9-10: Exploring the CCNA Prep Center (9.6.5)	671
Objectives	671
Background/Preparation	671
Task 1: Identify the Tools and Resources Available	671
Task 2: Explore the Cisco CCNA Prep Center Website	672
Task 3: Explore the Exam Study Area and Take Practice Exams	675
Task 4: Reflection	676
Chapter 10 Capstone Project: Putting It All Together	679
Objectives	679
Background/Preparation	679
Part A: Review the Existing Network and Customer Work Order	681
Part B: Develop the Subnet Scheme	682
Task 1: Determine the Number of Hosts and Subnets	682
Task 2: Calculate the Custom Subnet Mask	682
Task 3: Identify Subnet and Host IP Addresses	682
Part C: Document Network Device Interfaces and Physical Topology	683
Task 1: Document the Cisco 1841 Router Interfaces and Host IP Addresses	683
Task 2: Document the Linksys Interfaces and Host IP Addresses	684
Task 3: Diagram the Upgraded Network	684

Part D: Configure Devices, and Verify Default Settings	685
Task 1: Verify the Default Settings for the Cisco 1841 Customer Router	685
Task 2: Configure the Cisco 1841 Customer Router	685
Task 3: Verify Default Settings for the Linksys, and Set the SSID	687
Task 4: Verify Default Settings for the Cisco 2960 Switch	687
Task 5: Verify That Host PCs Are DHCP Clients	687
Part E: Connect Network Devices, and Verify Connectivity	688
Task 1: Connect the Network Devices	688
Task 2: Verify Device Configurations and Network Connectivity	689
Part F: Configure Port Security for the Switch	690
Task 1: Display the MAC Address Table Entry for the Port to Which the Wired Host Is Connected	690
Task 2: Clear the Dynamically Learned MAC Address Entry	691
Task 3: Shut Down the Port, Configure It as an Access Port, and Then Issue the Port Security Commands	691
Task 4: Ping from the Wired Host to the AnyCompanyX Router Default Gateway	691
Task 5: Display the Port Security Using the show port-security interface Command	692
Task 6: Remove the Wired Host Cable from the Switch Port and Connect the Cable from Another PC	692
Task 7: Reconnect the Original Host to Its Port and Restore the Port	692

Appendix A **Check Your Understanding and Challenge Questions Answer Key** **693**

Chapter 1	693
Check Your Understanding	693
Challenge Questions and Activities	694
Chapter 2	694
Check Your Understanding	694
Challenge Questions and Activities	696
Chapter 3	696
Check Your Understanding	696
Challenge Questions and Activities	697
Chapter 4	698
Check Your Understanding	698
Challenge Questions and Activities	700
Chapter 5	701
Check Your Understanding	701
Challenge Questions and Activities	702
Chapter 6	702
Check Your Understanding	702

Chapter 7 704

Check Your Understanding 704

Challenge Questions and Activities 705

Chapter 8 705

Check Your Understanding 705

Chapter 9 707

Check Your Understanding 707

Appendix B Router Boot and Password Recovery Labs 709**Lab B-1: Using the boot system Command 710**

Task 1: Log in to the Router 710

Task 2: Enter Privileged EXEC Mode 710

Task 3: Save the Existing running-config to the startup-config 711

Task 4: Configure the Router and View the Running Configuration File 711

Task 5: Show Information About the Backup Configuration File 711

Task 6: Display the IOS Version and Other Important Information 711

Task 7: Create the Statements to Perform the Following Functions 712

Task 8: Show Information About the Flash Memory Device 712

Task 9: Specify a Fallback Boot Sequence 713

Lab B-2: Troubleshooting Configuration Register Boot Problems 714

Task 1: Log in to the Router 714

Task 2: Configure the Router Name and Configuration Register Setting 715

Task 3: Save the Existing running-config to the startup-config 715

Task 4: Restart the Router 715

Task 5: View the Running Configuration File 715

Task 6: Reload the Saved Configuration 715

Task 7: Display the IOS Version and Other Important Information 716

Task 8: Change the Configuration Register to Load the Startup Configuration File from NVRAM, Save, and Reload the Router 716

Task 9: Verify the Configuration Register Setting and Log Out of the Router 716

Lab B-3: Password Recovery Procedures 717

Task 1: Attempt to Log in to the Router 718

Task 2: Document the Current Configuration Register Setting 718

Task 3: Enter ROM Monitor Mode 718

Task 4: Examine the ROM Monitor Mode Help 718

Task 5: Change the Configuration Register Setting to Boot Without Loading the Configuration File 719

Task 6: Restart the Router 719

Task 7: Enter Privileged EXEC Mode and Change the Password 719

Task 8: Verify the New Password and Configuration 719

Appendix C	Lab Equipment Interfaces and Initial Configuration Restoration	721
	Router Interface Summary	721
	Erasing and Reloading the Router	722
	Erasing and Reloading the Switch	722
	SDM Router Basic IOS Configuration	724
	Glossary	725
	Index	739

Icons Used in This Book



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 the user enters (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

The Cisco 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, as well as enterprise and Internet service provider environments. The *Working at a Small-to-Medium Business or ISP* course is the second course in the curriculum.

This book is the official supplemental textbook for the second course in v4.1 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 as well as bonus activities.

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 book's study tools to help solidify your understanding of all the topics. In addition, this book includes the following:

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

Goals of This Book

First and foremost, by providing a fresh, complementary perspective on the online content, this book helps you learn all the required materials of the second 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 CCENT and CCNA exams.

Audience for This Book

This book's main audience is anyone taking the second *CCNA Discovery* course of the Networking Academy curriculum. Many Networking Academies use this textbook as a required tool in the course. Other Networking Academies recommend the *Learning Guides* as an additional source of study and practice materials.

Book Features

This book’s educational features 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. 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, this icon helps you easily find this feature as you skim through the book.
- **Notes, tips, cautions, and warnings:** These are short sidebars that point out interesting facts, time-saving 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 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 it 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 260 computer and networking terms.

Practice

Practice makes perfect. This new *Learning Guide* offers you ample opportunities to put what you learn into practice. You will find the following features valuable and effective in reinforcing the instruction 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 answers for all the questions and explains each answer.
- **(New) Challenge questions and activities:** Additional—and more challenging—review questions and activities are presented at the end of the 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
Activity

- **Packet Tracer activities:** Interspersed throughout the chapters you'll find many activities to perform with the Cisco Packet Tracer tool. Packet Tracer allows you to create a network, 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; the 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:** 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 you see its reference in the chapter, or you can wait until you have completed the chapter.

A Word About the 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. You can spend as much time as you like completing standard lab exercises using Packet Tracer, and you have the option to work from home. Although Packet Tracer is not a substitute for real equipment, it allows you 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 to access 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 *CCNA Discovery* labs. Your instructor can download the CD files, burn a CD, and show you how to use the server. Hands-on labs that make use of the Discovery server are identified within the labs themselves.

After it is booted, the server provides many services to clients:

- Domain Name System
- 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 Working at a Small-to-Medium Business or ISP* course. The online curriculum has nine chapters for this course, so this book has 10 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 a slightly different order under each major heading. Additionally, the book occasionally uses different examples than the course. As a result, you 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 10 chapters:

- **Chapter 1, “The Internet and Its Uses,”** discusses the Internet—how it is evolving and how businesses and individuals make use of it. The importance of the ISP and standards in the continuing growth of the Internet is emphasized. This chapter focuses on the Internet infrastructure, including POPs, IXPs, and the types of devices ISPs use to provide services.
- **Chapter 2, “Help Desk,”** introduces the help desk and the various roles of help desk and installation technicians. It also describes the levels of support provided by these personnel. This chapter reviews the seven layers of the OSI model as they relate to help desk support and their use in troubleshooting network issues. Common tools and diagnostic procedures used by help desk technicians are examined, as well as on-site procedures used to resolve issues.
- **Chapter 3, “Planning a Network Upgrade,”** emphasizes the importance of proper planning when performing a network upgrade, including the use of a site survey, and it describes the steps involved in performing one. An overview of structured cabling is provided, along with the factors you must consider when upgrading LAN and internetworking devices.
- **Chapter 4, “Planning the Addressing Structure,”** describes how IP addressing is implemented in the LAN and compares classful and classless networks and subnets. This chapter explains the process for subnetting a network to allow for efficient use of available IP addresses. In addition, it describes how Network Address Translation (NAT) and Port Address Translation (PAT) are used in modern-day networks.
- **Chapter 5, “Configuring Network Devices,”** introduces the ISR and the methods available for configuring an ISR using both in-band and out-of-band techniques. This chapter introduces SDM and IOS commands and discusses how each is used to configure a Cisco device. The purpose and relationship of the device startup configuration and the running configuration are explained. In addition, Cisco Discovery Protocol (CDP) is introduced. Finally, the types of WAN connections available are discussed and compared in terms of cost and speed.

- **Chapter 6, “Routing,”** describes the purpose and function of dynamic routing and compares the characteristics of different types of routes. The main interior gateway protocols and their key features are introduced, as is the configuration process for RIPv2 dynamic routing, using Cisco IOS. In addition, exterior gateway routing protocols, such as BGP, are introduced, as are the steps required to configure BGP.
- **Chapter 7, “ISP Services,”** builds on network services introduced in the first *CCNA Discovery* course. It describes them in greater detail as they relate to those provided by an ISP. It describes the most common application layer protocols, such as HTTP, FTP, SMTP, IMAP, and POP3, as well as secure versions where they exist. This chapter also compares the UDP and TCP protocols and the types of traffic for which they are best suited. It also provides additional information on the Domain Name System (DNS) and how it functions.
- **Chapter 8, “ISP Responsibility,”** describes ISP security policies and procedures and the tools used in implementing security at the ISP. This chapter describes the monitoring and managing of the ISP, as well as the responsibilities of the ISP with regard to maintenance and recovery.
- **Chapter 9, “Troubleshooting,”** provides a review of Chapters 1 through 8, with a focus on identifying and correcting network problems using the OSI model as a basis. This chapter also provides guidance in preparing for the CCENT certification exam.
- In **Chapter 10, “Putting It All Together,”** you use what you have learned about computer hardware and software, wired and wireless networking components, protocols and applications, and techniques for securing a network to plan and implement a technical solution for a small business.

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

This book 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.
- **Appendix B, “Router Boot and Password Recovery Labs,”** provides several additional labs to help you learn how to control the router bootup process and troubleshoot configuration register boot problems. Password recovery procedures are also included.
- **Appendix C, “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.
- The **glossary** provides a compiled list of all the key terms that appear throughout this book, plus additional computer and networking terms.

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 files allow you 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.



- **CCENT Study Guides:** Referenced throughout Chapter 9, “Troubleshooting,” the six Study Guides and one Preparation Guide provide you with a method to prepare to obtain your CCENT certification by organizing your review of the topics covered on the ICND1 exam.
- **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 not only for learning and studying the material but also for on-the-job success. Also included in this section is “A Guide to Using a Networker’s Journal.” It’s a PDF booklet providing important insights into the value of using a professional journal, how to organize a journal, and some best practices for 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*: “Defining Yourself: Aptitudes and Desires” and “Making Yourself Indispensable.”
- **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 gives you tips on how to tap into these resources for lifelong learning.

This page intentionally left blank

Concepts

- Chapter 1** **The Internet and Its Uses** page 1
- Chapter 2** **Help Desk** page 19
- Chapter 3** **Planning a Network Upgrade** page 49
- Chapter 4** **Planning the Addressing Structure** page 73
- Chapter 5** **Configuring Network Devices** page 109
- Chapter 6** **Routing** page 173
- Chapter 7** **ISP Services** page 205
- Chapter 8** **ISP Responsibility** page 241
- Chapter 9** **Troubleshooting** page 285
- Chapter 10** **Putting It All Together** page 353

This page intentionally left blank

Planning a Network Upgrade

Objectives

After completing this chapter, you should be able to answer the following questions:

- Why is proper planning necessary when you perform a network upgrade?
- What is a site survey, and why is it necessary?
- What steps are involved in performing a site survey?
- What is structured cabling?
- What factors must you consider when upgrading LAN and internetworking devices?

Key Terms

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

site survey 50

SWOT 55

failure domain 64

Cisco IOS 65

Integrated Services Router (ISR) 65

Fault tolerance 68

As businesses grow and evolve, they may outgrow their existing network and require a network upgrade. To help ensure a smooth transition, a careful look at both the current network and the new network requirements is necessary. This will help determine what new equipment and configurations are necessary to ensure that the new network fully supports both the current and future needs of the company or organization.

Part II of this book includes the corresponding labs for this chapter.

Common Issues

When a small company grows rapidly, the original network that supported the company often cannot keep pace with the expansion. Employees at the company may not realize how important it is to properly plan for network upgrades. In many cases, the business may just add various network hardware devices, of varying quality, from different manufacturers, and different network connection technologies, to connect new users. Often this causes a degradation in the quality of the network as each new user or device is added. If this continues, at some point the network is unable to properly support the types and level of network traffic that the users generate. Only when the network starts to fail do most small businesses look for help to redesign the network. An ISP or managed service provider may be called in to provide advice and to install and maintain the network upgrade.

Before a network upgrade can be properly designed, an onsite technician is dispatched to perform a site survey to document the existing network structure. It is also necessary to investigate and document the physical layout of the premises to determine where new equipment can be installed.

Site Survey

A *site survey* can give the network designer a substantial amount of information and create a proper starting point for the project. It shows what is already on site and indicates what is needed. A sales representative may accompany the technician to the site to interview the customer as well. A proper site survey gathers as much information as possible about the current business and its projected growth. This information is gathered from different people in an attempt to accurately forecast the current and future network requirements. Table 3-1 lists the information sought in a site survey.

Table 3-1 Site Survey Information

Category	Information Sought
Number of users and types of equipment	How many network users, printers, and servers will the network support? To determine the number of network users the network must support, be sure to consider how many users will be added over the next 12 months, and how many network printers and network servers the network has to accommodate.
Projected growth	What is the expected growth in the company or organization? Will the company be hiring new employees who must be provided with access to network resources? Will a new branch office be opened that will require connectivity? A network is a long-term investment. Planning for future growth now can save a great deal of time, money, and frustration in the future.

Category	Information Sought
Current Internet connectivity	How does your business connect to the Internet? Does the ISP provide the equipment, or do you own it? Often with a high-speed Internet connection such as DSL or cable, the service provider owns the equipment needed to connect to the Internet (for example, a DSL router or cable modem). If the connectivity is upgraded, the equipment that provides the connectivity may also need to be upgraded or replaced.
Application requirements	What applications does the network need to support? Do you require services for applications such as IP telephony or videoconferencing? It is important to identify the needs of particular applications, especially voice and video. These applications may require additional network device configuration and new ISP services to support the necessary quality.
Existing network infrastructure and physical layout	How many networking devices are installed in your network? What functions do they perform? Understanding the existing number and types of networking equipment that are currently installed is critical to being able to plan for the upgrade. It is also necessary to document any configurations that are loaded on the existing devices.
New services required	Will any new services be required either now or in the future? Will the company be implementing VoIP or videoconferencing technology? Many services require special equipment or configurations to optimize their performance. Equipment and configurations must take into account the possibility of new services to protect the investment and optimize performance.
Security and privacy considerations	Do you currently have a firewall in place to protect your network? When a private network connects to the Internet, it opens physical links to more than 50,000 unknown networks and all their unknown users. Although this connectivity offers exciting opportunities for information sharing, it also creates threats to information not meant for sharing. Integrated Services Routers (ISR) incorporate firewall features along with other functionality.
Wireless requirements	Would you like a wired, wireless, or wired plus wireless local-area network (LAN)? How big is the area that the wireless LAN (WLAN) must cover? It is possible to connect computers, printers, and other devices to the network using a traditional wired network (10/100 switched Ethernet), a wireless-only network (802.11x), or a combination of wired and wireless networking. Each wireless access point that connects the wireless desktop and wireless laptop computers to the network has a given range. To estimate the number of access points that are required, you must know the required coverage area and the physical characteristics of the location that the wireless network must cover.

continues

Table 3-1 Site Survey Information *continued*

Category	Information Sought
Reliability and uptime expectations	What is the real cost of downtime in the company or organization? How long an outage can the company tolerate before suffering serious financial or customer losses? Maintaining nearly 100% uptime requires complete redundancy in all equipment and services and is extremely expensive to implement. Networks must be designed to reflect the real need for uptime and system reliability. This level can be determined only through intensive investigation and discussions with all the business stakeholders.
Budget constraints	What is the budget for the network installation or upgrade? System performance, reliability, and scalability are all expensive to achieve. The project budget normally is the deciding factor as to what can and cannot be done. A complete cost-benefit analysis must be completed to determine which features and services are the most critical and which could be put off to a later date.

It is a good idea to obtain a floor plan if possible. If a floor plan is not available, you can draw a diagram indicating the size and locations of all rooms. An inventory of existing network hardware and software is also useful to provide a baseline of requirements.

You should be prepared for anything when doing the site survey. Networks do not always meet local electrical, building, or safety codes or adhere to standards. Sometimes networks grow haphazardly over time and end up being a mixture of technologies and protocols. When doing a site survey, be careful not to offend the customer by expressing an opinion about the quality of the existing installed network.

When the technician visits the customer premises, he or she should do a thorough overview of the network and computer setup. There may be some obvious issues, such as unlabeled cables, poor physical security for network devices, lack of emergency power, or lack of an uninterruptible power supply (UPS) for critical devices. These conditions should be noted on the technician's report, as well as the other requirements gathered from the survey and the customer interview. These deficiencies in the current network should be addressed in the proposal for a network upgrade.

When the site survey is complete, it is important that the technician review the results with the customer to ensure that nothing is missed and that the report has no errors. A summary of the questions asked and the information gathered can greatly simplify the review process. If the information is accurate, the report provides an excellent basis for the new network design.

Physical and Logical Topologies

Both the physical and logical topologies of the existing network need to be documented. A technician gathers the information during the site survey to create both a physical and logical topology map of the network. A physical topology, as shown in Figure 3-1, is the actual physical location of cables, computers, and other peripherals. A logical topology, as shown in Figure 3-2, documents the path that data takes through a network and the location where network functions, such as routing, occur.

Figure 3-1 Physical Topology

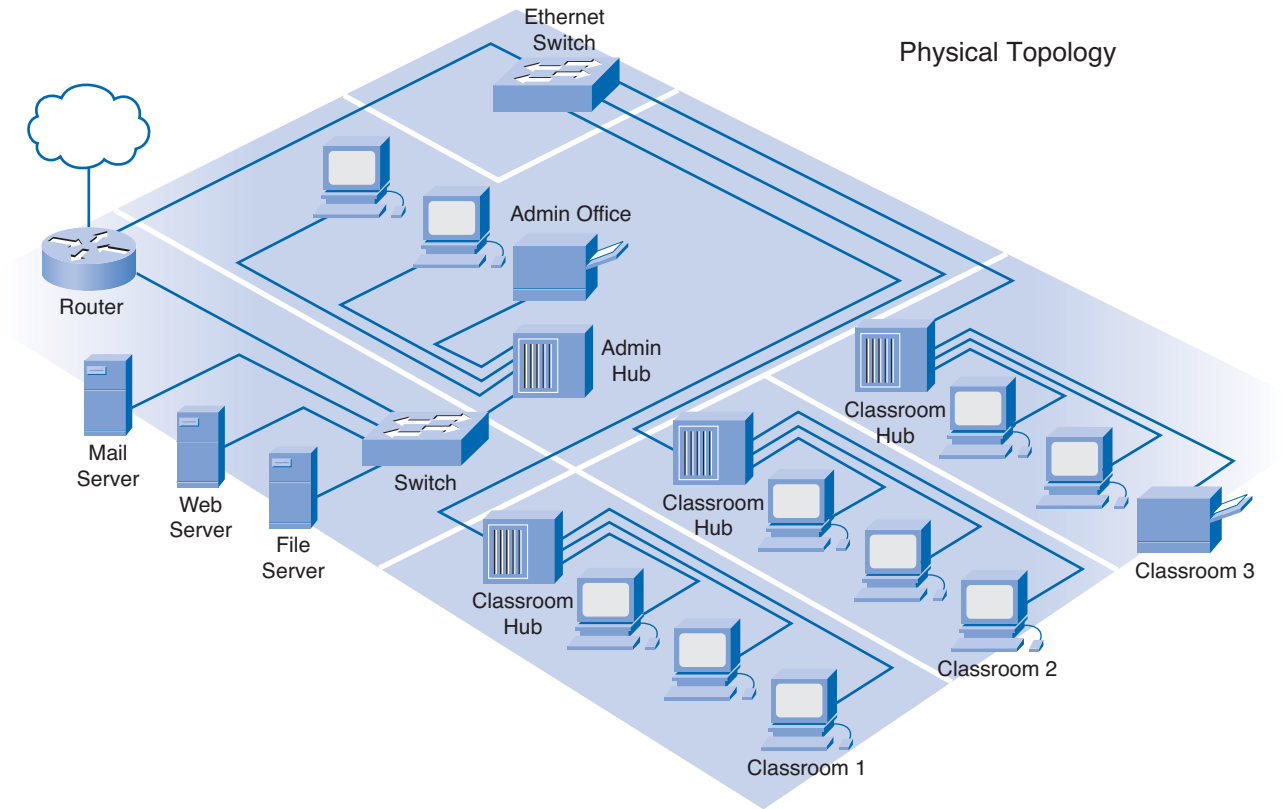
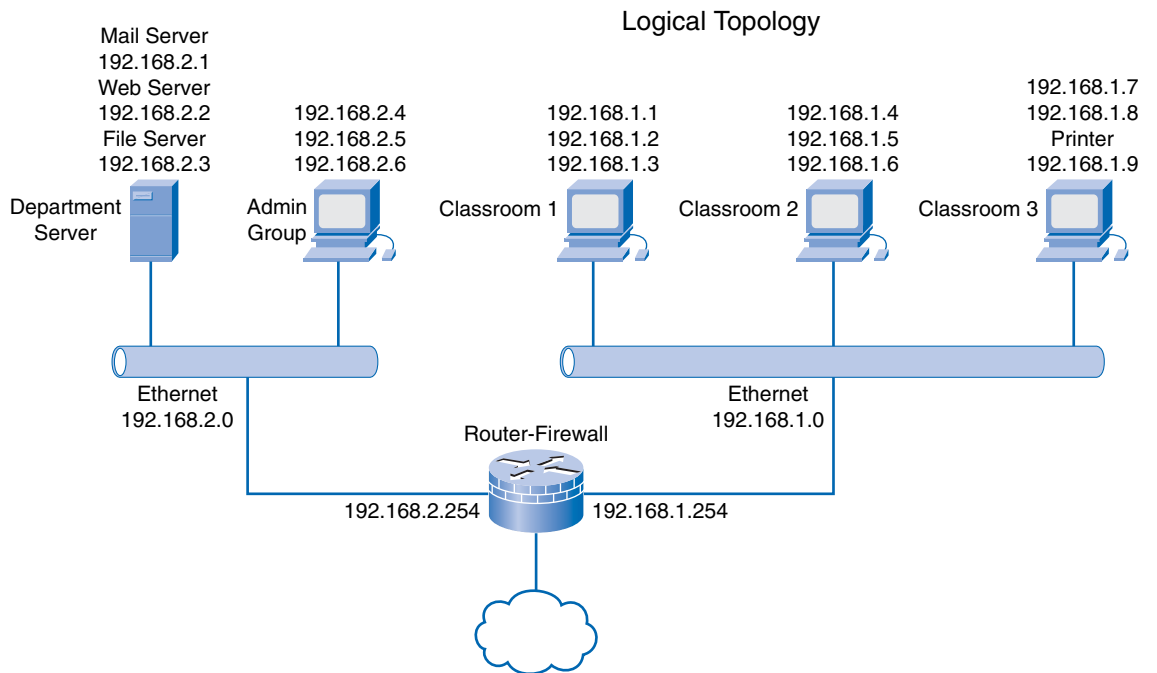


Figure 3-2 Logical Topology

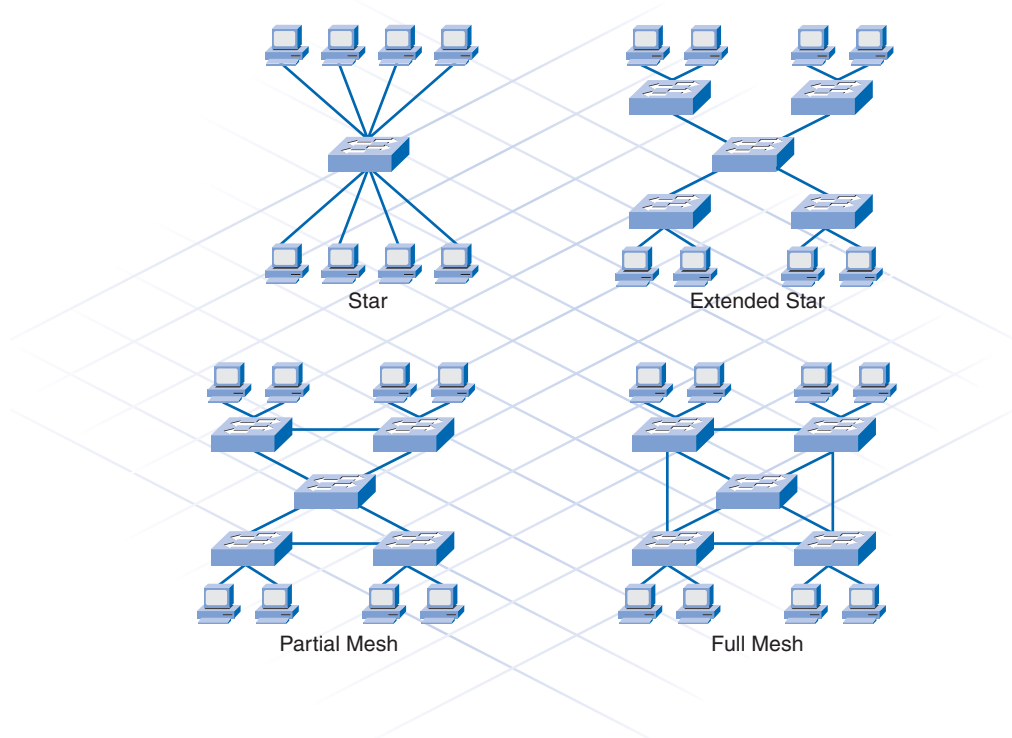


In a wired network, the physical topology map consists of the wiring closet, as well as the wiring to the individual end-user stations. In a wireless network, the physical topology consists of the wiring closet and any access points that may be installed. Because there are no wires, the physical topology contains the wireless signal coverage area.

The logical topology generally is the same for both a wired and wireless network. It includes the naming and Layer 3 addressing of end stations, router gateways, and other network devices, regardless of the physical location. It indicates the location of routing, network address translation, and firewall filtering.

Developing a logical topology requires understanding of the relationship between the devices and the network, regardless of the physical cabling layout. Several topological arrangements are possible. Examples include star, extended star, partial mesh, and full mesh topologies, as shown in Figure 3-3.

Figure 3-3 Common Topologies



Star Topologies

In a star topology, each device is connected via a single connection to a central point, which is typically a switch or a wireless access point. The advantage of a star topology is that if a single connecting device fails, only that device is affected. However, if the central device, such as the switch, fails, then all connecting devices lose connectivity.

An extended star is created when the central device in one star is connected to a central device of another star, such as when multiple switches are interconnected, or daisy-chained together.

Mesh Topologies

Most core layers in a network are wired in either a full mesh or a partial mesh topology. In a full mesh topology, every device has a connection to every other device. Although full mesh topologies provide the benefit of a fully redundant network, they can be difficult to wire and manage and are more costly.

A partial mesh topology is used for larger installations. In a partial mesh topology, each device is connected to at least two other devices. This arrangement creates sufficient redundancy, without the complexity of a full mesh.

Implementing redundant links through partial or full mesh topologies ensures that network devices can find alternative paths to send data in the event of a failure.

Network Requirements Documentation

Along with creating the topology maps for the existing network, it is necessary to obtain additional information about the hosts and networking devices that are currently installed in the network. Record this information on a brief inventory sheet. In addition to currently installed equipment, document any planned growth that the company anticipates in the near future. This information helps the network designer determine what new equipment is required and the best way to structure the network to support the anticipated growth.

The inventory sheet of all the devices installed on the network includes the following:

- Device name
- Date of purchase
- Warranty information
- Location
- Brand and model
- Operating system
- Logical addressing information
- Connection information
- Security information

Packet Tracer
□ **Activity**

Creating Network Diagrams (3.1.3)

In this activity, you create a logical diagram and inventory list for a network. Use file d2-313 on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Planning the Network Upgrade

Extensive planning should go into a network upgrade. As with any project, a need is first identified, and then a plan outlines the upgrade process from beginning to end. A good project plan helps identify any strengths, weaknesses, opportunities, and threats. This is called a *SWOT* analysis. The plan should clearly define the tasks and the order in which tasks are completed.

Some common examples of good planning include

- Sports teams following game plans
- Builders following blueprints
- Ceremonies or meetings following agendas

Network Upgrades

A network that is a patchwork of devices strung together using a mixture of technologies and protocols usually indicates poor or no initial planning. These types of networks are susceptible to downtime and are extremely difficult to maintain and troubleshoot. Unfortunately, this type of network is often encountered as small businesses experience rapid, unexpected growth. Even larger organizations often experience unplanned growth in their networks when they acquire or merge with other organizations. Organizations that experience a controlled rate of growth can properly plan their network to avoid problems and give their users an acceptable level of service.

The planning of a network upgrade begins after the initial site survey and report are complete. It consists of five distinct phases:

- Phase 1: Requirements gathering
- Phase 2: Selection and design
- Phase 3: Implementation
- Phase 4: Operation
- Phase 5: Review and evaluation

The next sections describe each phase in greater detail.

Phase 1: Requirements Gathering

After all the information has been gathered from the customer and the site visit, the design team at the ISP analyzes the information to determine network requirements and then generates an analysis report. If insufficient information is available to properly determine the best network upgrade path to follow, this team may request additional information.

Phase 2: Selection and Design

When the analysis report is complete, devices and cabling are selected. The design team creates multiple designs and shares them with other members on the project. This allows team members to view the LAN from a documentation perspective and evaluate trade-offs in performance and cost. It is during this step that any weaknesses of the design can be identified and addressed. Also during this phase, prototypes are created and tested. A successful prototype is a good indicator of how the new network will operate.

Phase 3: Implementation

If the first two steps are done correctly, the implementation phase may be performed without incident. If tasks were overlooked in the earlier phases, they must be corrected during implementation. A good implementation schedule must allow time for unexpected events and also schedules events to keep disruption of the customer's business to a minimum. Staying in constant communication with the customer during the installation is critical to the project's success.

Phase 4: Operation

When the network implementation phase is complete, the network moves into a production environment. In this environment, the network is considered live and performs all the tasks it has been designed to accomplish. If all steps up to this point have been properly completed, very few unexpected incidents should occur when the network moves into the operation phase.

Phase 5: Review and Evaluation

After the network is operational, the design and implementation must be reviewed and evaluated against the original design objectives. This is usually done by members of the design team with assistance from the network staff. This evaluation includes costs, performance, and appropriateness for the environment. For this process, the following items are recommended:

- Compare the user experience with the goals in the documentation, and evaluate whether the design is right for the job.
- Compare the projected designs and costs with the actual deployment. This ensures that future projects will benefit from the lessons learned on this project.
- Monitor the operation, and record changes. This ensures that the system is always fully documented and accountable.

It is important that, at each phase, careful planning and review occur to ensure that the project goes smoothly and the installation is successful. Onsite technicians are often included in all phases of the upgrade, including planning. This allows them to gain a better understanding of the expectations and limitations of the network upgrade and to give the end users a much-improved level of service.



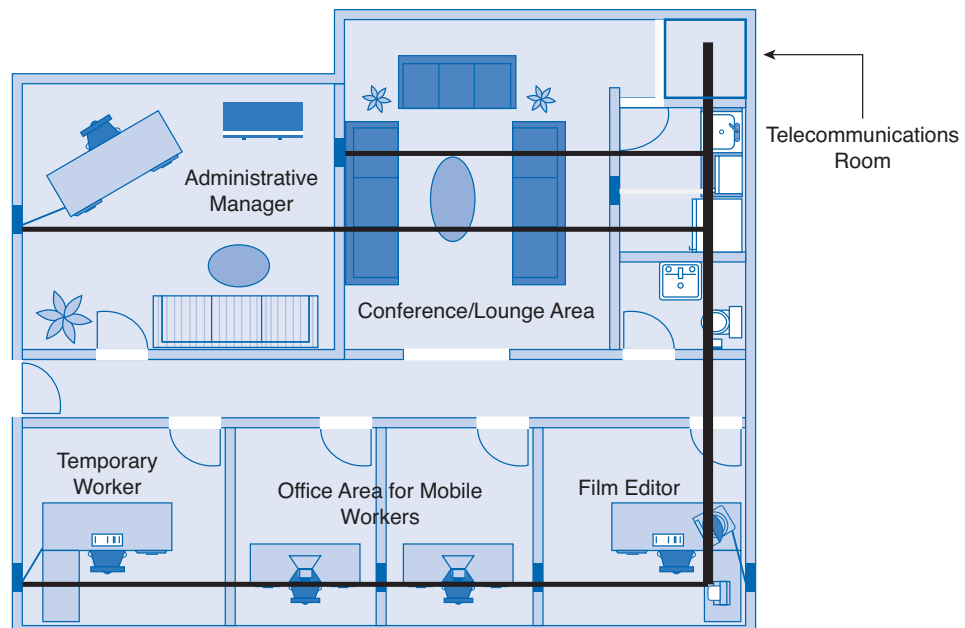
Activity 3-1: Network Planning Phases (3.2.1)

In this activity, you determine at which phase of the network planning process certain events occur. Use file d2ia-321 on the CD-ROM that accompanies this book to perform this interactive activity.

Physical Environment

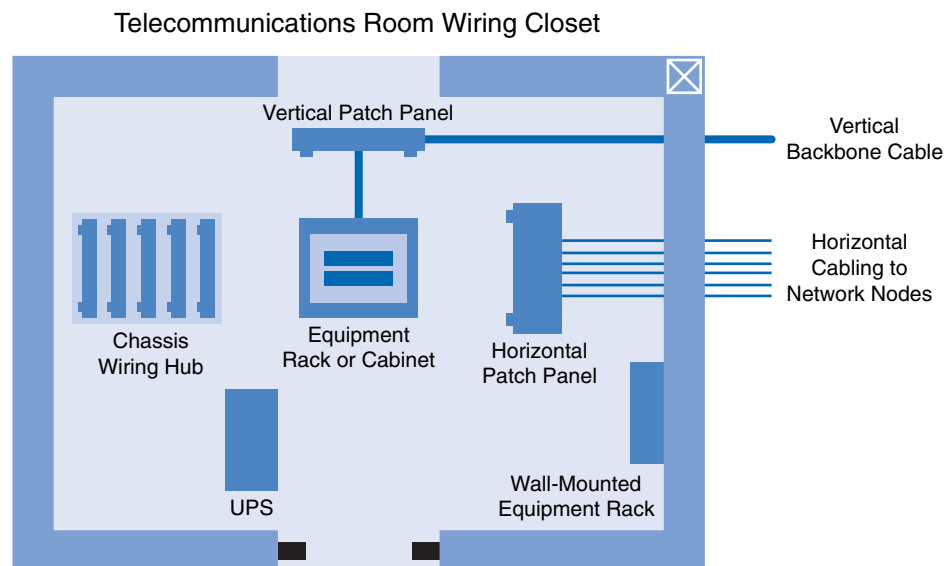
Before selecting equipment and determining the design of the new network, the network designer must examine the existing network facilities and cabling. This is part of the initial site survey. The facilities include the physical environment, the telecommunication room, and the existing network wiring. A telecommunications room or wiring closet in a small, single-floor network is usually called the main distribution facility (MDF). Figure 3-4 shows a small office environment with a single MDF.

Figure 3-4 Main Distribution Facility



The MDF typically contains many of the network devices, such as switches or hubs, routers, access points, and so on. It is where all the network cable is concentrated in a single point. Many times, the MDF also contains the ISP's point of presence (POP), where the network connects to the Internet through a telecommunications service provider. Figure 3-5 shows the layout of a typical MDF. If additional wiring closets are required, these are called intermediate distribution facilities (IDF). IDFs typically are smaller than the MDF and connect to the MDF with backbone cabling.

Figure 3-5 Typical MDF Layout



Tip

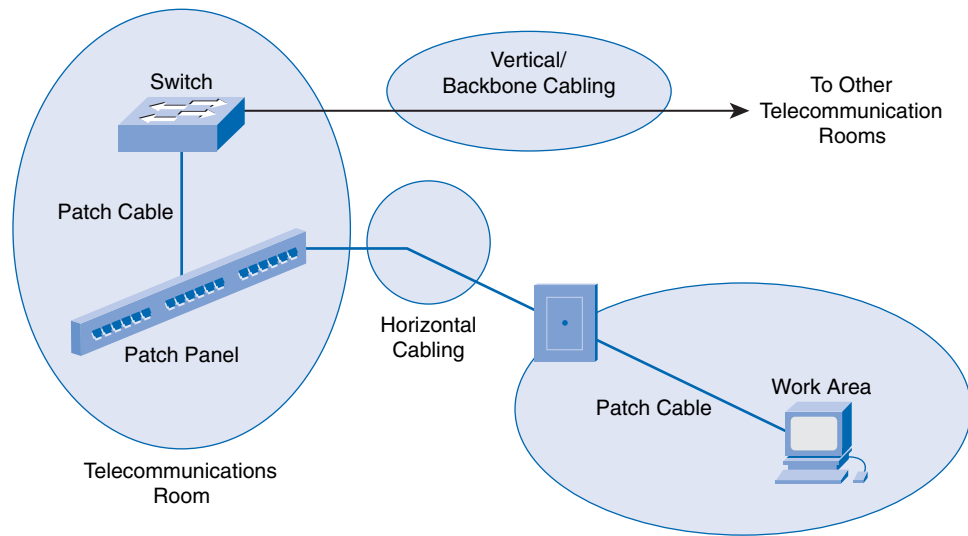
ISO standards refer to MDFs and IDFs using different terminology. MDFs and IDFs are sometimes called wiring closets. Because normally one MDF distributes telecommunication services to all areas of the building, MDFs are also called *building distributors*. Most environments have one or more IDFs on each floor of a building, so the ISO calls IDFs *floor distributors*.

Many small businesses have no telecommunications room or closet. Network equipment may be located on a desk or other furniture, and wires could be just lying on the floor. This arrangement should be avoided. Network equipment must always be secure to protect data. Loose or improperly installed cables are prone to damage and also present a tripping hazard to employees. As a network grows, it is important to consider the telecommunications room as critical to the network's security and reliability.

Cabling Considerations

When the existing cabling is not up to specification for the new equipment, you must plan for and install new cable. The condition of the existing cabling can quickly be determined by a physical inspection of the network during the site visit. This inspection should reveal the type of cable installed as well as any issues, such as improper termination, that could degrade network performance. When planning the installation of network cabling, you must consider different physical areas, as shown in Figure 3-6:

- User work areas
- Telecommunications rooms
- Backbone area (vertical backbone cabling)
- Distribution area (horizontal cabling)

Figure 3-6 Cabling Areas

You have many different types of network cables to choose from; some are more common than others. Each type of cable is best suited to specific applications and environments. The most common type of LAN cable is unshielded twisted-pair (UTP). This cable is easy to install, is fairly inexpensive, and has a high bandwidth capability. For long backbone runs or runs between buildings, fiber-optic cable normally is installed. Coaxial cable is not typically used in LANs, but it is widely used in cable modem provider networks. Table 3-2 describes some of the more common types of network cables.

Table 3-2 Common Network Cables

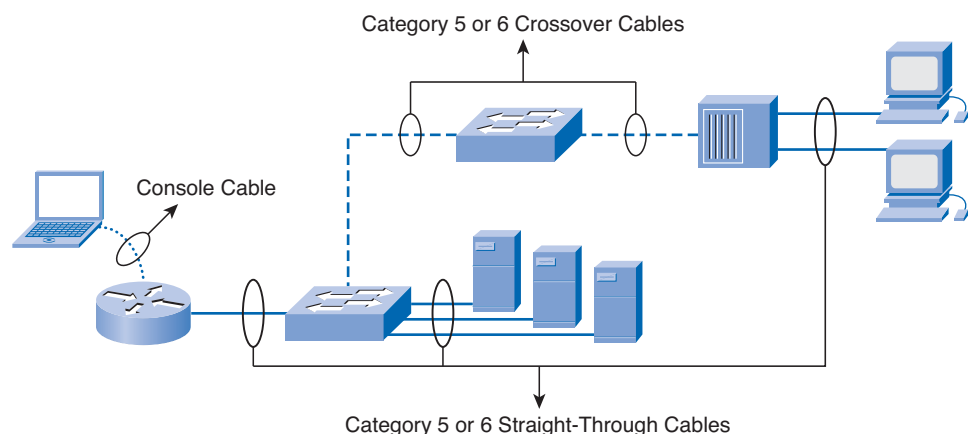
Cable Type	Characteristics
Shielded twisted-pair (STP)	Usually Category 5, 5e, or 6 cable that has a foil shielding to protect from outside electromagnetic interference (EMI). The distance limitation is approximately 328 feet (100 meters).
Unshielded twisted-pair (UTP)	Usually Category 5, 5e, or 6 cable. It does not provide extra shielding from EMI, but it is inexpensive. Cable runs should avoid electrically noisy areas. The distance limitation is approximately 328 feet (100 meters).
Coaxial	Has a solid copper core with several protective layers, including polyvinyl chloride (PVC), braided wire shielding, and a plastic covering. The distance limitation of several miles (kilometers) depends on the purpose of the connection.
Fiber-optic cable	A medium that is not susceptible to EMI and that can transmit data faster and farther than copper. Depending on the type of fiber optics, distance limitations can be several miles (kilometers).

Several organizations provide LAN cabling specifications. The Telecommunications Industry Association (TIA) and the Electronic Industries Association (EIA) worked together to provide the TIA/EIA cable specifications for LANs. Two of the most common TIA/EIA cable specifications are the 568-A and 568-B standards. Both of these standards typically use the same Category 5 or 6 cable, but with a different termination color code.

Three different types of UTP cables are commonly encountered in the network environment:

- Straight-through cables have the same pinout on both ends. They normally are used to connect dissimilar devices, such as a switch and a computer or a switch and a router.
- Crossover cables have the transmit pins on one end connected to the receive pins on the other end. This type of cable is used to connect like devices, such as two computers, two switches, or two routers. Crossover cables can also be used to connect a computer directly to a router interface.
- A console cable or a rollover cable has the pinouts on each end reversed. Normally it is used to connect the serial port of a computer to the console port of a router or switch to perform the initial configuration. Figure 3-7 shows typical uses of these cables.

Figure 3-7 Typical Uses of Cables



Another type of cable that is common in networks is a serial cable. A serial cable typically is used to connect the router to an Internet connection. This Internet connection may be to the phone company, the cable company, or a private ISP.

Structured Cable

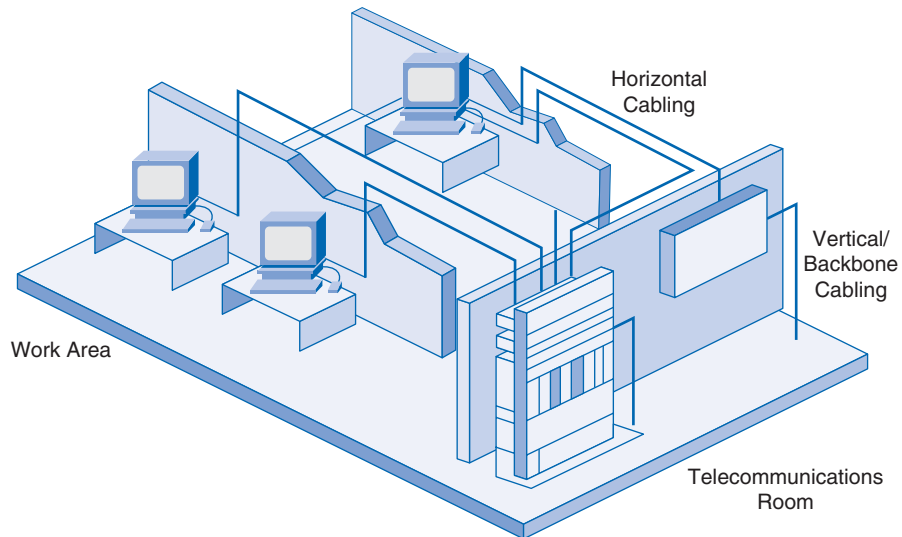
When designing a structured cabling project, the first step is to obtain an accurate floor plan. The floor plan allows the technician to identify possible wiring closet locations, cable runs, and which electrical areas to avoid.

After the technician has identified and confirmed the locations of network devices, it is time to draw the network on the floor plan. Some of the more important items to document include the following:

- **Patch cable:** A short cable from the computer to the wall plate in the user work area.
- **Horizontal cable:** A cable from the wall plate to the IDF in the distribution area.
- **Vertical cable:** A cable from the IDF to the MDF in the organization's backbone area.
- **Backbone cable:** The part of a network that handles the major traffic.
- **Location of wiring closet:** An area to concentrate the end-user cable to the hub or switch.
- **Cable management system:** A series of trays and straps used to guide and protect cable runs.
- **Cable labeling system:** A proper labeling system or scheme that identifies cables.
- **Electrical considerations:** The premises should have adequate outlets to support the electrical requirements of the network equipment.

Figure 3-8 shows a telecommunications room and work area with both horizontal and vertical cabling.

Figure 3-8 Horizontal and Vertical Cabling



Lab 3-1: Evaluating a Cabling Upgrade Plan (3.2.4)

In this lab, you propose a cable upgrade plan to accommodate extra floor space acquired by a company. Refer to the hands-on lab in Part II of this book. You may perform this lab now or wait until the end of the chapter.

Purchasing and Maintaining Equipment

As the ISP team plans the network upgrade, issues arise related to purchasing new equipment, as well as maintaining new and existing equipment. Generally you have two options for the new equipment: managed service or in-house solutions. With a managed service solution, the equipment is obtained from the ISP through a lease or some other agreement. The ISP is responsible for updating and maintaining the equipment. With an in-house solution, the customer purchases the equipment and is responsible for updates, warranties, and maintaining the equipment.

Purchasing Equipment

When you purchase equipment, cost is always a major factor. A cost analysis of the purchase options must be conducted to provide a sound basis for the final purchase decision. Normally the customer conducts the cost analysis, but this may be done in conjunction with the ISP. Many other factors should be considered in addition to cost. Table 3-3 describes some of the factors you must consider when you're trying to decide if a managed or in-house solution is more appropriate.

Table 3-3 Managed Service or In-house Solution

	In-House	Managed Service
Considerations	Requires many decisions: Type of equipment Equipment location IT organization staffing Network design Maintenance requirements	Initial evaluation and choice of service provider Requirements definition Ongoing evaluation of service provider
Costs	Equipment purchasing or leasing IT organization staffing Training costs Multiple vendor costs and building Hardware repairs and upgrades Software release upgrades Telephone line changes Redundancy and reliability requirements	Single, predictable, monthly recurring bill Minimal up-front costs
Control and responsibility	You have most of the control and responsibility for managing and maintaining your network system	Delegate the level of network management to a qualified service provider based on your needs Keep your core business processes in-house Maintain control of the work flow in your organization Set service-level agreements (SLA) with a service provider
Reliability	You are responsible for keeping your network system available to employees, customers, and partners at all times	Service provider can guarantee availability up to 99.999% A 24-hour help desk is available for remote-access users Service provider management is transparent to the end users
End-user experience	Users are unaware of whether the network is managed by the company or an external partner	Users are unaware of whether the network is managed by the company or an external partner

If the customer chooses the managed service, the SLA outlines the lease costs as well as other service costs. If the equipment is purchased outright, the customer should be aware of cost, warranty coverage, compatibility with existing equipment, and update and maintenance issues, all of which have an associated cost. This cost must be analyzed to determine the cost-effectiveness of any planned solution.

Selecting Network Devices

After the customer requirements have been analyzed, the design staff recommends the appropriate network devices to connect and support the new network functionality. Modern networks use a variety of devices for connectivity. Each device has certain capabilities to control the flow of data across a network. A general rule is that the higher the device is in the OSI model, the more intelligent it is. This means that a higher-level device can better analyze the data traffic and forward it based on information not available at lower layers. For example, a Layer 1 hub can only forward data out all ports, a Layer 2 switch can filter the data and only send it out the port connected to the destination based on MAC address, and a Layer 3 router can decide which traffic to forward or block based on the logical address.

As switches and routers evolve, the distinction between them becomes blurred. One simple distinction remains: LAN switches provide connectivity within an organization's LAN, whereas routers are needed to interconnect local networks or to form a wide-area network (WAN) environment.

In addition to switches and routers, other connectivity options are available for LANs. Wireless access points allow computers and other devices, such as handheld Internet Protocol (IP) phones, to wirelessly connect to the network or share broadband connectivity. Firewalls guard against network threats and provide application security, network control and containment, and secure connectivity technologies. ISRs combine the functionality of switches, routers, access points, and firewalls in the same networking device.

Selecting LAN Devices

Although both a hub and a switch can provide connectivity at the access layer of a network, switches should be chosen for connecting devices to a LAN. Switches generally are more expensive than hubs, but the enhanced performance makes them cost-effective. A hub generally is chosen as a networking device within a very small LAN, within a LAN that requires low throughput requirements, or when finances are limited. A hub may also be installed in a network when all network traffic is to be monitored. Hubs forward all traffic out all ports, whereas switches microsegment the network. Connecting a network-monitoring device to a hub allows the monitoring device to see all network traffic on that segment. Some switches do provide the ability to monitor all network traffic through a special port, but this is not a universal feature.

When selecting a switch for a particular LAN, network designers need to consider a number of factors, including the following:

- Speed and types of ports/interfaces
- Expandability
- Manageability
- Cost

Speed and Types of Ports/Interfaces

Choosing Layer 2 devices that can accommodate increased speeds allows the network to evolve without your having to replace the central devices. It is a good idea to purchase the fastest ports available within the budgeted funds. A bit of extra money spent now can save a great deal of time and expense later, when it is time to upgrade the network again.

The same can be stated about the number and types of network ports. Network designers must carefully consider how many UTP and fiber ports are needed. It is important to estimate how many additional ports will be required to support network expansion in the future.

Expandability

Networking devices come in both fixed and modular physical configurations. Fixed configurations have a specific number and type of ports or interfaces and cannot be expanded. Modular devices have expansion slots that provide the flexibility to add new modules as requirements evolve. Most modular devices come with a basic number of fixed ports as well as expansion slots.

A typical use of an expansion slot is to add fiber-optic modules to a device that was originally configured with a number of fixed UTP ports. Modular switches can be a cost-effective approach to scaling LANs.

Manageability

A managed switch provides control over individual ports or over the switch as a whole. Typical controls include the ability to monitor operation and change the settings for a device. A managed device can be monitored for performance and security and typically provides enhancements to the monitoring and security features. For example, with a managed switch, ports can be turned on or off as required to control access. In addition, administrators can control which computers or devices are allowed to connect to a port.

Cost

The cost of a switch is determined by its capacity and features. The switch capacity includes the number and types of ports available and the overall throughput. Other factors that impact the cost are the switch's network management capabilities, embedded security technologies, and optional advanced switching technologies.

Using a simple cost-per-port calculation, it may appear initially that the best option is to deploy one large switch at a central location. However, this apparent cost savings may be offset by the expense from the longer cable lengths required to connect every device on the LAN to one central switch. Compare this option with the cost of deploying a number of smaller switches connected by a few long cables to a central switch.

Deploying a number of smaller devices instead of a single large device also has the benefit of reducing the size of the *failure domain*. A failure domain is the area of the network affected when a piece of networking equipment malfunctions or fails.

Packet Tracer
Activity

Exploring Different LAN Switch Options (3.3.3)

In this activity, you determine which types of interfaces are required to connect a new company switch to a router, Linksys wireless router, and hosts. Use file d2-333 on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Selecting Internetworking Devices

After the LAN switches have been selected, it is time to determine which router is appropriate for the customer. A router is a Layer 3 device. It performs all tasks of devices in lower layers and selects the best route to the destination network based on Layer 3 information. Routers are the primary devices used to interconnect networks. Each port on a router connects to a different network and routes packets between the networks. Routers can break up broadcast domains and collision domains.

You must consider a number of factors when selecting a router. It is necessary to match the router's characteristics to the network's requirements. Factors for choosing a router include

- The type of connectivity required
- Features available
- Cost

Connectivity

Routers are used to interconnect networks that use different technologies. They can have both LAN and WAN interfaces. The router's LAN interfaces connect to the LAN medium. This medium typically is UTP cabling, but modules can be added to the router to allow the use of fiber-optic cable and other types of media. Depending on the series or model of router, there can be multiple interface types for connecting LAN and WAN cabling. It is important to anticipate an organization's future connectivity requirements and purchase a router that will serve the organization well into the future.

Features

It is necessary to match the router's characteristics to the network's requirements. After analysis, the business may need a router with specific features in addition to basic routing. Many routers provide features such as the following:

- Security
- Quality of service (QoS)
- Voice over IP (VoIP)
- Network Address Translation (NAT)
- Dynamic Host Configuration Protocol (DHCP)
- Wireless access
- Virtual private network (VPN)
- Intrusion detection

Most of these services are contained in the *Cisco IOS* that manages the router hardware and resources. Although normally these are software features, the hardware must be able to support the IOS required.

Cost

When you select internetwork devices, budget is an important consideration. Routers can be expensive. Additional modules, such as fiber optics, can increase the costs. To keep costs as low as possible, the medium used to connect to the router should be supported without the purchase of additional modules.

An *Integrated Services Router (ISR)* is a relatively new technology that combines multiple services into one device. Before the ISR, multiple devices were required to meet the needs of data, wired and wireless, voice and video, firewall, and VPN technologies. The ISR was designed with multiple services to accommodate the demands of small to medium-sized businesses and branch offices of large organizations. An ISR is designed for ease of use. It can quickly and easily enable end-to-end protection for users, applications, network endpoints, and wireless LANs. The cost of an ISR normally is less than if the individual devices are purchased separately.

Packet Tracer
Activity**Exploring Internetworking Devices (3.3.4)**

In this activity, you determine and install the correct modules in the 1841 ISR to provide network connectivity. In addition, you select the correct cables to connect various network devices to the 1841 ISR. Use file d2-334 on the CD-ROM that accompanies this book to perform this activity using Packet Tracer.

Network Equipment Upgrades

Many small networks were initially built using a low-end integrated router to connect wireless and wired users. This type of device is designed to support small networks, usually consisting of a few wired hosts and possibly four or five wireless devices. When a small business outgrows the capabilities of its existing network devices, it must upgrade to more-capable devices. The devices used in this course and book are the Cisco 1841 ISR and the Cisco 2960 switch, as shown in Figure 3-9.

Figure 3-9 Cisco 1841 ISR and 2960 Switch



Cisco 1841 ISR



Cisco 2960 Switch

The Cisco 1841 ISR is designed to be a branch office or medium-sized business router. As an entry-level multiservice router, it offers a number of different connectivity options. It is modular in design and can deliver multiple security services.

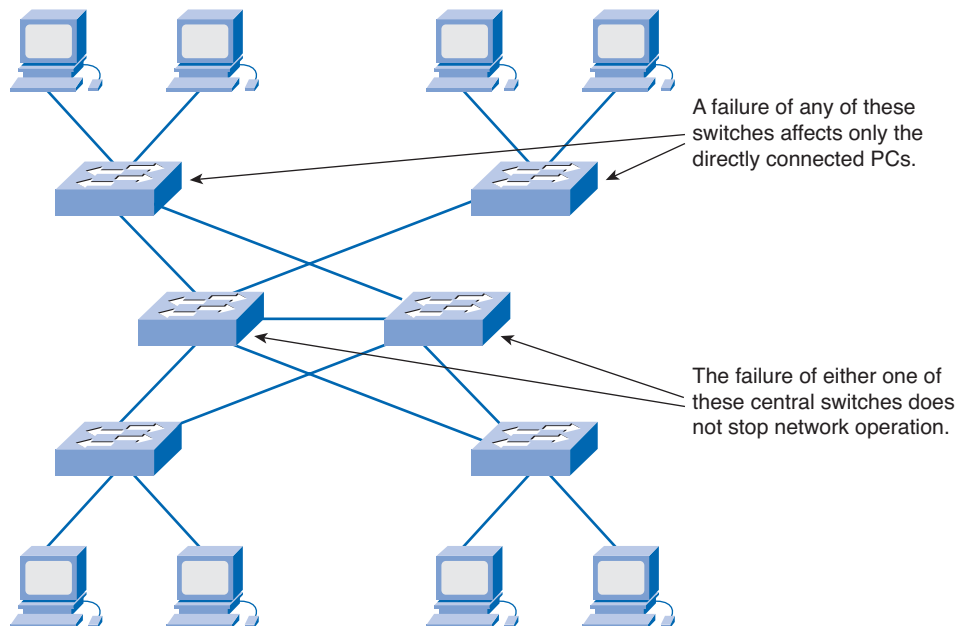
The Cisco Catalyst 2960 series Intelligent Ethernet switches are a family of fixed-configuration, standalone devices that provide Fast Ethernet and Gigabit Ethernet connectivity to the desktop. These switches can provide the high speeds and high-density switching capabilities that the smaller ISRs with integrated switching cannot. They are therefore a good option when upgrading networks built with either hubs or small ISR devices.

The Catalyst 2960 family of switches, shown in Figure 3-10, provides entry-level, enterprise-class, fixed-configuration switching that is optimized for access layer deployments. They provide both Fast Ethernet and Gigabit Ethernet to the desktop and are ideal for entry-level enterprise, mid-market, and branch-office environments. These compact switches often are deployed outside the wiring closet.

Figure 3-10 Cisco Catalyst 2960 Family of Switches

Reliability and Availability

Purchasing network devices and the installation of cabling for a network upgrade is only the beginning. Networks must be both reliable and available. Reliability is usually achieved by adding redundant components to the network, such as two routers instead of one. In this case, alternative data paths are created, so if one router experiences problems, the data can take an alternative route to arrive at the destination. For better reliability, all devices and connections should have complete redundancy. Unfortunately, this is extremely expensive in most environments. Therefore, the network design team must determine the level of redundancy to incorporate to achieve the necessary reliability. Figure 3-11 shows redundancy in a switched network.

Figure 3-11 Redundancy in a Switched Network

Availability is the amount of time the network is ready and able to deliver the necessary services. Any increase in reliability improves availability. Ensuring a higher level of availability requires not only redundancy but also equipment and software that have been engineered to provide this level of service. As an example of availability, telephone systems require “five 9s” of uptime. This means that the telephone system must be available 99.999% of the time. Telephone systems cannot be down, or unavailable, more than .001% of the time.

Fault tolerance systems typically are used to improve network reliability. Fault tolerance systems include devices such as UPSs, multiple AC power supplies, hot-swappable devices, and multiple interface cards. When one device fails, the redundant or backup system takes over to ensure minimal loss of reliability.

IP Addressing Plan

Planning for the network installation must include planning the logical addressing. Changing the Layer 3 IP addressing is a major issue when upgrading a network. If the network’s structure is changed in the upgrade, the IP address scheme and network information may need to be altered to reflect the new structure.

When developing the addressing scheme, you must consider every device that requires an IP address, now and in the future. Some devices require addresses to carry out their functionality, and others only require an IP address to allow them to be accessed and configured across the network. Hosts and network devices that require an IP address include

- User computers
- Administrator computers
- Servers
- Other end devices such as printers, IP phones, and IP cameras
- Router LAN interfaces
- Router WAN (serial) interfaces
- Standalone switches
- Wireless access points

For example, if a new router is introduced to the network, new local networks, or subnets, are created. These new subnets need to have the proper IP address and subnet mask calculated. Sometimes, this means having to assign a totally new addressing scheme to the entire network.

After all the planning and design phases are complete, the upgrade proceeds to the implementation phase, in which the actual network installation begins.

Summary

Networks often experience unexpected growth and develop in a disorganized manner. When this happens, network performance degrades slowly with each new device added. At some point, the network no longer can support the traffic being generated by the users, so a network upgrade is required.

Whether the network upgrade is forced or planned, the upgrade process must be conducted in an organized manner. The upgrade plan must consider the strengths and weaknesses of and opportunities and threats posed by the network installation.

A network upgrade has five phases:

- Requirements gathering
- Equipment selection and network design
- Implementation
- Operation
- Review and evaluation

Documentation must include the physical and logical topology of the existing network, along with a complete inventory sheet of all equipment. This includes the location and layout of any telecommunications rooms as well as existing network wiring. Customer network requirements are gathered through surveys and interviews.

Cabling has four physical areas to consider: work areas, distribution area, telecommunications room, and backbone. Structured cabling projects deal with the placement of cables, the location of wiring closets, cable management, and electrical considerations.

When new equipment is used in a network upgrade, you have two purchase options: managed service and in-house. Both of these present many advantages and have serious limitations. The choice depends on the current business strengths and weaknesses.

Cost and expandability are two of the most important considerations when upgrading network devices. Generally, a device that functions at a higher OSI layer is considered a more intelligent device.

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 Activity on the CD:

Interactive Activity 3-1: Network Planning Phases (3.2.1)



Packet Tracer Activities on the CD:

Creating Network Diagrams (3.1.3)

Exploring Different LAN Switch Options (3.3.3)

Exploring Internetworking Devices (3.3.4)

**Hands-on Lab in Part II of this book:**Lab 3-1: Evaluating a Cabling Upgrade Plan (3.2.4)

Check Your Understanding

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

1. What is the purpose of a site survey? (Select all that apply.)
 - A. To determine what network resources are currently in place.
 - B. To accurately forecast the current and future network requirements.
 - C. To repair any malfunctioning network equipment.
 - D. To ensure that all purchased networking equipment is still properly installed and functioning.
2. What should a site survey technician do if he or she finds nonstandard network installations during the survey process?
 - A. Report the condition to management to make sure that the previous contractor does not get rehired.
 - B. Inform management that they are in violation of standards and must pay you to correct the situation, or you will have to report them.
 - C. Ignore the situation, and proceed with the survey.
 - D. Report the condition to management, pointing out that this often happens when networks grow unexpectedly.
3. What should be done as a first step after the technician completes the site survey?
 - A. Use the information contained in the site survey documents to determine the customer’s network requirements.
 - B. Review the site survey with the customer to make sure that nothing has been missed and everything is accurate.
 - C. Use the information contained in the site survey documents to determine how long the planned network upgrade will take.
 - D. Ask the technician to summarize the site survey documentation, summarizing only the important facts.
4. What should be contained on a logical topology diagram? (Select all that apply.)
 - A. Location of all networking devices
 - B. Physical location of cabling runs
 - C. IP address information of all devices
 - D. Device names
 - E. Location of wiring closets

-
5. What information should you record about devices when performing a network inventory? (Select all that apply.)
- A. Device name, brand, and model
 - B. Physical location
 - C. Operating system
 - D. Logical addressing information
 - E. Connection information
 - F. Security information
6. What is the correct sequence of steps when performing a network upgrade?
- 1. Review and evaluation
 - 2. Implementation
 - 3. Operation
 - 4. Requirements gathering
 - 5. Selection and design
- A. 1, 2, 3, 4, 5
 - B. 4, 5, 1, 2, 3
 - C. 4, 5, 2, 3, 1
 - D. 4, 1, 5, 3, 2
 - E. 1, 4, 5, 2, 3
7. What is the name of the location where all network cable is concentrated in a single point?
- A. IDF
 - B. ISP
 - C. IXP
 - D. MDF
 - E. MFD
8. What type of cable typically is used to connect a workstation network interface card (NIC) to the wall outlet?
- A. STP
 - B. UTP
 - C. Coaxial
 - D. Fiber-optic
9. Which of the following direct connections normally would require a crossover cable? (Select all that apply.)
- A. A PC connected to another PC
 - B. A PC connected to a switch
 - C. A PC connected to a router
 - D. A switch connected to a router
 - E. A router connected to another router
10. What factors should you consider when selecting an internetworking device?

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. A small company is trying to decide if it should install and manage its own network solution or if it should invest in a managed solution from its local ISP. The company currently is having financial difficulties and does not have an internal IT department. What suggestion would you make, and why?
2. You have asked two new network technicians to recommend a switch for a new department within the company. The department will have 27 users and four networked printers. All devices currently connect at 100 Mbps. The first technician recommends a switch that has 48 10/100-Mbps ports. The second technician recommends a slightly more expensive switch that has 48 10/100/1000-Mbps ports and two fiber-optic uplink ports. Which technician has made the better recommendation, and why?

Symbols

^ (caret symbol), 131

A

AAA, 246
 access lists, 251
 active data connections, 230
 address translation (NAT), troubleshooting, 321-323
 administratively down interfaces, 315
 ADSL (Asymmetric Digital Subscriber Line), 6
 Anti-X software, 259
 application layer, 25
 OSI model, 286
 protocols, 210
 application security, 244
 ASN (AS number), 193
 assigning permissions, 245
 attacks, 249-250
 autonomous systems, 193-194
 reachability, 196
 routing between, 195
 availability, 67, 208

B

back doors, 260
 backing up Cisco router configuration files, 146-148
 backup solutions
 differential backups, 272
 full backups, 271
 hard disk media, 270
 incremental backups, 273
 maintenance, 273-275
 optical media, 270
 solid state media, 271
 tape media, 270
 bandwidth, 4
 banners, configuring on Cisco routers, 137
 baseline tools, 291
 Basic Configuration window (SDM Express), 121
 BGP (Border Gateway Protocol), 195, 199-200
 boot errors, troubleshooting, 298-301
 bootup process, Cisco ISR, 114
 running configuration, 115-116
 startup configuration, 114
 troubleshooting, 116
 bottom-up troubleshooting methodology, 30-34, 289
 building distributors, 58

C

cable modems, 6
 cable testers, 294
 cables, 58, 60, 301
 excessive collisions, troubleshooting, 303
 excessive noise, troubleshooting, 302
 excessive runt frames, troubleshooting, 303
 late collisions, troubleshooting, 303
 structured, 60-61
 Catalyst 2960 switches. *See* Cisco Catalyst 2960 series switches
 Catalyst switches. *See* Cisco Catalyst switches
 CCENT exam, preparing for, 336-340
 commitment, 341
 creating a plan, 341-342
 practicing test taking, 342-344
 CDP (Cisco Discovery Protocol), configuring on Cisco Catalyst switches, 164-166
 certification exams, format of, 343
 CIDR (Classless Interdomain Routing), 79-82
 circuit-switched WAN connections, 152
 Cisco Catalyst 2960 series switches, 66
 CDP, configuring, 164-166
 configuring, 156-160
 connecting to router, 161-162
 powering up, 159
 switch port security, 162-164
 Cisco Catalyst switches
 LAN connectivity, troubleshooting, 304-305
 LED lights, 157
 switch port modes, 158-159
 Cisco IOS Firewall software, 252
 Cisco IOS Software
 CLI
 Cisco ISR, configuring, 118
 commands, recalling, 131-132
 global configuration mode, 129
 help system, 129-130
 router configuration submode, 129
 routers, configuring, 128, 137-146
 banners, 137
 show commands, 132-136
 image files
 corrupt images, troubleshooting, 301
 IP Base image, 111
 recovering, 276-277
 updating, 275
 Cisco ISR (Integrated Services Router)
 bootup process, 114
 running configuration, 115-116
 startup configuration, 114
 troubleshooting, 116

- configuring, 110
 - with CLI, 118*
 - with SDM, 118-120*
 - with SDM Express, 121-124*
- in-band management, 117
- initial setup, 112-113
- out-of-band management, 117
- Cisco routers**
 - configuration files, backing up, 146-148
 - connecting to Cisco Catalyst switches, 161-162
 - WAN connections, configuring PPP, 154-155
- Cisco SDM (Security Device Manager), configuring**
 - dynamic NAT, 127**
- Class A addresses, 76**
- Class B addresses, 77**
- Class C addresses, 77**
- classful addressing, 75-77**
- classful subnetting, 85-86**
- CLI (command-line interface), 128**
 - help system, 129-130
 - commands, recalling, 131-132*
 - routers, configuring, 128
 - show commands, 132-136
 - versus SDM, 119-120
- CMTS (cable modem termination system), 13**
- collisions**
 - effect on network performance, 296
 - troubleshooting, 303
- commands**
 - copy running-config startup config, 115
 - copy tftp flash, 275
 - debug ip rip, 193, 330
 - enable password, 137
 - enable secret, 137
 - ipconfig, 93
 - ping, 9
 - recalling, 131-132
 - router bgp, 199
 - service password encryption, 138
 - show, 132-133
 - show arp, 135
 - show flash, 300
 - show history, 131-132
 - show interfaces, 134-135, 329
 - show interfaces serial, 306-307
 - show ip dhcp binding, 317
 - show ip interface, 329
 - show ip interfaces brief, 300-303
 - show ip nat translation, 322
 - show ip protocols, 192, 327
 - show ip route, 135, 175-177, 323, 330
 - show protocols, 136
 - show running-config, 328-329
 - show running-config interface, 304
 - show running-configuration, 138, 300
 - show startup-configuration, 300
 - show version, 115-116, 136, 299
 - tracert, 11-12
 - Windows, ipconfig /all, 318-320
- committing to exam preparation, 341**
- communicating between subnets, 90-91**
- community strings, 266**
- comparing**
 - CLI and SDM, 119-120
 - TCP/IP and OSI models, 211
 - UDP and TCP, 214
- configuration files**
 - backing up, 146-148
 - corrupt configuration files, troubleshooting, 301
- configuring**
 - BGP, 199-200
 - Cisco Catalyst 2960 switches, 156-160
 - CDP, 164-166*
 - router connection, 161-162*
 - switch port security, 162-164*
 - Cisco ISR, 110
 - bootup process, 114-116*
 - in-band management, 117*
 - initial setup, 112-113*
 - out-of-band management, 117*
 - with CLI, 118*
 - with SDM, 118-120*
 - with SDM Express, 121-124*
 - Cisco routers with CLI, 128, 137
 - banners, 137*
 - console port, 138-139*
 - default routes, 141*
 - DHCP services, 141-144*
 - interfaces, 139-140*
 - static NAT, 144-146*
 - dynamic NAT with Cisco SDM, 127
 - NAT, 321
 - RIP, 190-193
 - serial WAN connections
 - IP address, 125-126*
 - serial line encapsulations, 124-125*
 - static routes, 178-179
- connecting CPE over WAN**
 - connection type, selecting, 153-154
 - via circuit-switched connection, 152
 - via packet-switched connection, 152
 - via point-to-point connection, 151
- connecting to Internet, 5-7**
- connection-oriented protocols, 212**
- connectivity**
 - duplex mismatches, troubleshooting, 305
 - troubleshooting, 36, 304
 - verifying with ping command, 9
 - verifying with tracert command, 11-12
- console port, configuring on Cisco routers, 138-139**
- context-sensitive help (CLI), 130**
- convergence, 180**
- copy running-config startup-config command, 115**
- copy tftp flash command, 275**
- corrupt Cisco IOS images, troubleshooting, 301**
- CPE (customer premises equipment)**
 - connecting over WAN, 151
 - connection type, selecting, 153-154*
 - via circuit-switched connection, 152*
 - via packet-switched connection, 152*

via point-to-point connection, 151
 installing, 148-151
CSMA/CD (carrier sense multiple access/collision detect), 296
custom subnet masks, 86, 90
customer site troubleshooting procedures, 40-41

D

data encryption, 247-249
data link layer, 25
 cables, troubleshooting, 301-303
 OSI model, 287
 troubleshooting, 295-298
DCE (data circuit-terminating equipment), 139
DDoS attacks, 249
debug ip rip command, 193, 330
decapsulation, 29
default routes, 178
 configuring on Cisco routers, 141
 troubleshooting, 324
devices
 availability, 67
 inventory sheets, 55
 reliability, 67
 routers, selecting, 64-65
 switches, selecting, 63-64
 upgrading, 66
DHCP (Dynamic Host Configuration Protocol)
 configuring on Cisco routers, 141-144
 troubleshooting, 318-320
DHCP window (SDM Express), 123-124
dialup access, 5
differential backups, 272
directly connected routes, 178
 troubleshooting, 324
disabling privileged EXEC mode, 128
disaster recovery
 backup solutions
 differential backups, 272
 full backups, 271
 hard disk media, 270
 incremental backups, 273
 optical media, 270
 solid-state media, 271
 tape media, 270
 best practices, 277-279
 causes of data loss, 268-269
distance vector routing protocols, 180-182
 RIP, configuring, 190-193
divide-and-conquer troubleshooting methodology, 289
DMM (digital multimeters), 294
DMZ (demilitarized zone), 252
DNS (Domain Name System), 218-219
 domain name servers, 220
 implementing
 via ISPs, 225
 via local DNS servers, 226

 name resolution, 33, 221-224
 forward lookup zones, 224
 primary DNS zones, 225
 reverse lookup zones, 224
 secondary DNS zones, 225
 resolvers, 220-221
 resource records, 220
 top-level domains, 221
 verifying operation, 334

documenting

 help desk calls, 37-39
 network requirements, 55

domain name servers, 220

domain namespace, 220

DoS (denial-of-service) attacks, 249-250

DRDoS (distributed reflected denial-of-service) attacks, 250

DSL (Digital Subscriber Line), 5

DSLAM (DSL access multiplexer), 13

DTE (data terminal equipment), 139

DTP (Data Transfer Process) function of FTP, 229

DUAL (diffusing update algorithm), 185

duplex settings, displaying, 305

dynamic NAT, 97

 configuring with Cisco SDM, 127

dynamic routes, 178

 troubleshooting, 324-330

E

e-commerce, 2

EAP (Extensible Authentication Protocol), 257

EGPs (Exterior Gateway Protocols), 195

EIGRP (Enhanced IGRP), 184-185

e-mail, troubleshooting, 35

enable password command, 137

enable secret command, 137

encapsulation, 27, 213

encoding, 27

encryption, 247-249

end systems, 288

equipment, purchasing, 61-62

escalation, 21

evaluating network design and implementation, 57

exam

 format of, 343
 preparing for, 336-340
 commitment, 341
 creating a plan, 341-342
 practicing test taking, 342-344

exterior routing protocols, autonomous systems, 193-196

external interfaces, 144

F-G

factual knowledge, importance of during exam preparation, 338

failure domains, 64

fault tolerance, 68

firewalls, 251, 253

five 9s, 208

Flash memory, displaying contents of, 300

floor distributors, 58

forward lookup zones, 224

frame headers, 28

FTP (File Transfer Protocol), 229

DTP function, 229

PI function, 229

full backups, 271

global configuration mode (CLI), 129

H

hard disk media, 270

hardware troubleshooting tools, 293-295

help desk technicians, 20

calls, documenting, 37, 39

connectivity issues, troubleshooting, 36

customer interaction, 22-24

customer site troubleshooting procedures, 40-41

e-mail issues, troubleshooting, 35

levels of customer support, 21

roles of, 21-22

help system, Cisco IOS CLI, 129-132

hierarchical addressing, 75, 314

HOB (high-order bits), 75

HOSTS file, 218-219

HTTP (HyperText Transfer Protocol)

proxy servers, 229

URLs, 227

HTTPS (Secure HTTP), 227-229

hubs, 288

IDF (intermediate distribution facility), 58

IDS (intrusion detection systems), 254-255

IGPs (Interior Gateway Protocols), 195

image files

corrupt images, troubleshooting, 301

IP Base image, 111

recovering, 276-277

updating, 275

IMAP4 (Internet Message Access Protocol), 234-235

implementing DNS

via ISPs, 225

via local DNS servers, 226

in-band management, 262

Cisco ISR, 117

SNMP, 265

Syslog, 267

Telnet, 264

incident management, 23

incremental backups, 273

inside global addresses, 95

inside local addresses, 95

installing CPE, 148-151

interfaces

administratively down, 315

configuring on Cisco routers, 139-140

troubleshooting, 301

interior routing protocols

EIGRP, 184-185

RIP, 183-184

configuring, 190-193

internal help desk technicians, 20

internal interfaces, 144

Internet, 2-3

internetworking devices, 111

inventory checklists, 150

inventory sheets, 55

IP addresses, 310-311

addressing scheme, developing, 68

assigning to serial WAN connection, 125-126

classful addressing, 75-77

DHCP, troubleshooting, 318-320

DNS resolution, 33

hierarchical addressing, 75, 314

IPv6, 92-93

NAT, 93-96

dynamic NAT, 97

static NAT, 98

troubleshooting, 321-323

PAT, 99-102

subnet masks, troubleshooting, 315-317

subnets, 312

overlapping, 314-315

subnetting, 77-78

CIDR, 79-82

classful, 85-86

communicating between subnets, 90-91

custom subnet masks, 86, 90

network expansion requirements, 82-85

VLSM, 81

unavailable addresses, troubleshooting, 317-318

IP Base image, 111

ipconfig /all command (Windows), 318-320

ipconfig command, 93

IPS (intrusion prevention systems), 255-256

IPv6, 92-93

ISPs, 4, 197-198

backup solutions, maintenance, 273-275

connection methods

cable modem, 6

dialup access, 5

- DSL, 5
- Metro Ethernet, 7
- satellite connection, 6
- T1/E1, 7
- T3/E3, 7
- connectivity, requirements, 13
- disaster recovery
 - backup media, 270
 - best practices, 277-279
 - data loss, causes of, 268-269
 - file backups, 271-275
 - solid-state media, 271
- help desk technicians, 20
 - calls, documenting, 37-39
 - connectivity, troubleshooting, 36
 - customer interaction, 22-24
 - customer site troubleshooting procedures, 40-41
 - e-mail, troubleshooting, 35
 - levels of customer support, 21
 - roles of, 21-22
- host security, 258-260
- in-band management
 - SNMP, 265
 - Syslog, 267
 - Telnet, 264
- IXPs, 7
- link performance, monitoring, 262
- POP, 7
- roles and responsibilities, 14
- security, 242-243
 - applications, 244
 - extraneous services, 243
 - passwords, 243
 - user rights, 244
 - wireless, 256-257
- services, 206
 - application layer protocols, 210
 - availability, 208
 - reliability, 207
 - TCP/IP protocols, 208
 - transport layer protocols, 211-217
- SLAs, 261
 - Tier 1, 9
 - Tier 2, 9
 - Tier 3, 9

ISR. *See* Cisco ISR

IXP (Internet Exchange Point), 7

J-K-L

knowledge bases, 292

LAN connectivity, 304-305

LAN IP Address window (SDM Express), 122

Layer 1, 301. *See also* physical layer
troubleshooting, 295-298

Layer 2, 301. *See also* data link layer
devices, selecting, 63-64
troubleshooting, 295-298

Layer 3, 310. *See also* network layer

- devices, selecting, 64-65
- DHCP, troubleshooting, 318-320
- IP addressing
 - overlapping subnets, troubleshooting, 314-315
 - subnet masks, troubleshooting, 315-317
 - unavailable addresses, troubleshooting, 317-318
- NAT, troubleshooting, 321-323
- routing, troubleshooting, 323-330

Layer 4, troubleshooting, 331-332

layers of OSI model, 25-26

- decapsulation, 29
- encapsulation, 27

LED indicators (Cisco routers), 157, 300

link performance, monitoring, 262

link state routing protocols, OSPF, 185, 187

local traffic, 198

logical networks, 291, 310

logical topologies, 52

lower layers, 25, 288

LSAs (link-state advertisements), 186

M

MAC address filtering, 257

malware, 242

managed services, 22

MBSA (Microsoft Baseline Security Analyzer), 244

MDF (main distribution facility), 57

media errors, troubleshooting, 302-303

Metro Ethernet, 7

monitoring ISP link performance, 262

- in-band tools, 264-267

MTBF (mean time between failure), 207

MTTR (mean time to repair), 207

multiple service support at transport layer, 215-217

N

name resolution, DNS, 221-224

- forward lookup zones, 224
- primary zones, 225
- reverse lookup zones, 224
- secondary zones, 225

NAPs (Network Access Points), 7

NAT (Network Address Translation), 93-96

- configuring, 321
- dynamic NAT, 97
- static NAT, 98
 - configuring on Cisco routers, 144-146
- troubleshooting, 321-323

Nessus Vulnerability Scanner, 244

network documentation, 291

network layer, 25

- OSI model, 287-288, 310-311
- troubleshooting, 312

network management system tools, 292

network naming systems

DNS, 218-219

domain name servers, 220

implementing via ISPs, 225

implementing via local DNS servers, 226

name resolution, 221-225

resolvers, 220-221

resource records, 220

TCP/IP HOSTS file, 218-219

network prefix, 79

network support services, 14

network topologies

logical, 291

physical, 290

network upgrades, planning, 56-57

NOC (network operations center), 14

NVRAM (non-volatile random access memory), 114

O

open authentication, 257

operating systems

patching, 244

version, displaying, 299

optical media, 270

OSI model, 24, 286

as troubleshooting tool, 25, 29-30

bottom-up approach, 30-34

top-down approach, 30

corresponding TCP/IP model layers, 286

data link layer, troubleshooting, 295-298

decapsulation, 29

encapsulation, 27

encoding, 27

layers of, 25-26

lower layers, 288

network layer, 310-311

routing, troubleshooting, 323-330

troubleshooting, 312

physical layer, troubleshooting, 295-298

transport layer, troubleshooting, 331-332

upper layers, 288

troubleshooting, 332-336

OSPF (Open Shortest Path First), 185-187

out-of-band management, 262

Cisco ISR, 117

outside global address, 95

outside local address, 95

outsourcing, 21

overlapping subnets, troubleshooting, 314-315

P

packet-switched WAN connections, 152

packet trailers, 28

passive data connections, 230

passwords, 243

PAT (Port Address Translation), 99-102

patches, 244

permissions, assigning, 245

physical environment, documenting, 57

physical layer, 25

cables, troubleshooting, 301-303

OSI model, 287-288

troubleshooting, 295-298

physical topologies, 52, 290

PI (Protocol Interpreter) function of FTP, 229

ping command, 9

planning

for exam preparation, 341-342

network upgrades, 56-57

IP addressing, 68

point-to-point WAN connections, 151

POP (point of presence), 7

POP3 (Post Office Protocol version 3), 233

port filtering, 250

portable network analyzers, 295

ports, 215

duplex settings, displaying, 305

POST (power-on self test), 114

failures, troubleshooting, 301

powering up Cisco Catalyst 2960 switches, 159

PPP encapsulation, configuring, 154-155

practicing test taking, 342-344

preparing for CCENT exam, 336-340

commitment, 341

creating a plan, 341-342

factual knowledge, importance of, 338

practicing test taking, 342-344

presentation layer, 25, 286

primary DNS zones, 225

privileged EXEC mode, 128

problem-solving procedures, 29-30

protocol analyzers, 293

protocol stack, 26

proxy servers, 229

PSKs (preshared keys), 257

purchasing equipment, 61-62

Q-R

reachability, 196

recalling commands, 131-132

recovering Cisco IOS images, 276-277

redundancy, 208

reliability, 67

of ISP services, 207

required devices for ISP connectivity, 13

resolvers, 220-221
resource records, 220
reverse lookup zones, 224
RFCs (Requests For Comments), 3
RIP (Routing Information Protocol), 183-184
 configuring, 190-193
roles within ISPs, 14, 21-22
ROMmon, recovering Cisco IOS image, 276-277
router bgp command, 199
router configuration submode (CLI), 129
routers, 128, 137
 banners, configuring, 137
 bootup, troubleshooting, 298-301
 console port, 138-139
 default routes, configuring, 141
 DHCP services, configuring, 141-144
 interfaces, configuring, 139-140
 selecting, 63-65
 static NAT, configuring, 144-146
routes, 174
 default, 178
 directly connected, 178
 troubleshooting, 324
 dynamic, 178
 troubleshooting, 324-330
 static, configuring, 178-179
 troubleshooting, 323
routing protocols, 179
 configuring, 190-193
 distance vector, 180-182
 EIGRP, 184-185
 exterior routing protocols, autonomous systems, 193-195
 link state, OSPF, 185-187
 RIP, 183-184
routing table, 186
running configuration, 115-116
runt frames, troubleshooting, 303

S

satellite Internet connection, 6
scalability, 14
scanning, 244
SDM (Cisco Router and Security Device Manager)
 Cisco ISR, configuring, 118-120
 dynamic NAT, configuring, 127
 versus CLI, 119-120
SDM Express, configuring Cisco ISR
 Basic Configuration window, 121
 DHCP window, 123-124
 LAN IP Address window, 122
SDSL (Symmetric Digital Subscriber Line), 6
secondary DNS zones, 225
security
 access lists, 251
 attacks, 249-250
 best practices, 245
 AAA, 246
 permissions, 245
 data encryption, 247-249
 firewalls, 251-253
 host security, 258-260
 IDS, 254-255
 IPS, 255-256
 port filtering, 250
 scanning, 244
 user rights, 244
 wireless, 256-257
selecting
 routers, 64-65
 switches, 63-64
 WAN connection type, 153-154
serial cables, 60
serial line encapsulations, 124-125
serial link problems
 loops, troubleshooting, 308
 troubleshooting, 307-309
serial WAN connections
 configuring, 124
 IP address, assigning, 125-126
 serial line encapsulations, 124-125
service password encryption command, 138
session layer, 25
 OSI model, 286
setting up Cisco ISR, 112-113
show arp command, 135
show commands, 132-133
show flash command, 300
show history command, 131-132
show interfaces command, 134-135, 329
show interfaces serial command, 306-307
show ip dhcp binding command, 317
show ip interface brief command, 300
show ip interface command, 329
show ip interfaces brief command, 301-303
show ip nat translation command, 322
show ip protocols command, 192, 327
show ip route command, 135, 175-177, 323, 330
show protocols command, 136
show running-config command, 328-329
show running-config interface command, 304
show running-configuration command, 300
show running-configuration command, 138
show startup-configuration command, 300
show version command, 115-116, 136, 299
sign-off phase, 150
site surveys, documenting physical environment, 57
SLAs (service-level agreements), 22, 261
SMTP (Simple Mail Transfer Protocol), 231-233
SNMP (Simple Network Management Protocol), 265
sockets, 217

software troubleshooting tools, 291-293

solid-state media, 271

SPF (shortest path first) algorithm, 186

SPI (stateful packet inspection), 252

standards, Internet, 3

startup configuration, 114

static NAT, 98

configuring on Cisco routers, 144-146

static port security, 162

static routes

configuring, 178-179

troubleshooting, 324

structured cable, 60-61

subnet masks, 175

troubleshooting, 315-317

subnetting, 77-78, 312

CIDR, 79-82

classful, 85-86

communicating between subnets, 90-91

custom subnet masks, 86, 90

network expansion requirements, 82-85

overlapping subnets, troubleshooting, 314-315

VLSM, 81

swap media, 273

switch port modes, 158-159

switch ports, 158-161

switches, selecting, 63-64

Syslog, 267

T

T1/E1 Internet connections, 7

T3/E3 Internet connections, 7

tape media, 270

TCP (Transport Control Protocol), 212

and UDP, 214

TCP/IP model, corresponding OSI model layers, 286. *See also* TCP/IP protocols

TCP/IP protocols, 208

application layer, 210

FTP, 229

DTP function, 229

PI function, 229

HOSTS file, 218-219

HTTP, 227

proxy servers, 229

URLs, 227

IMAP4, 234-235

POP3, 233

SMTP, 231-233

transport layer, 211

multiple service support, 215-217

TCP, 212

UDP, 212-214

Telnet, 264

troubleshooting upper-layer problems, 335-336

TFTP servers, backing up Cisco router configuration files, 146-148

three-way handshakes, 213

Tier 1 ISPs, 9

Tier 2 ISPs, 9

Tier 3 ISPs, 9

top-down troubleshooting methodology, 30, 289

top-level domains, 221

topological database, 186

topology maps, creating, 52-54

tracert command, 11-12

traffic, 198

trailers, 28

transit traffic, 198

transport layer, 25

OSI model, 287-288

protocols, 211

multiple service support, 215-217

TCP, 212

UDP, 212-214

troubleshooting, 331-332

traps, 266

Trojans, 260

trouble tickets, 23

troubleshooting. *See also* troubleshooting tools

boot errors, 298-301

cables, 301-303

calls, documenting, 37-39

Cisco ISR bootup process, 116

connectivity issues, 36

customer site procedures, 40-41

data link layer, 295-298

divide-and-conquer methodology, 289

e-mail issues, 35

IP addressing, unavailable addresses, 317-318

LAN connectivity, 304

duplex mismatches, 305

Layer 3

DHCP, 318-320

NAT, 321-323

network layer, 312

OSI model as framework, 29-30

bottom-up approach, 30-34

top-down approach, 30

overlapping subnets, 314-315

physical layer, 295-298

routing, 323

directly connected routes, 324

dynamic routes, 324-330

subnet masks, 315, 317

transport layer problems, 331-332

upper-layer problems, 332-335

with Telnet, 335-336

WAN connectivity, 305

serial link problems, 307-309

troubleshooting tools

baseline tools, 291

cable testers, 294

- digital multimeters, 294
- knowledge bases, 292
- logical network topologies, 291
- network documentation, 291
- network management system tools, 292
- physical network topologies, 290
- portable network analyzers, 295
- protocol analyzers, 293

TSPs (telecommunications service providers), 124

U-V

UDP (User Datagram Protocol), 212-214

unavailable IP addresses, troubleshooting, 317-318

unrecognized interface modules, troubleshooting, 301

updating Cisco IOS image, 275

upgrading network devices, 66

- cabling, 58-61

upper layers, 25

- encoding, 27

- OSI model, 288

- troubleshooting, 332-335

- with Telnet, 335-336*

URLs, 227

user EXEC mode, 128

user rights, 244

viruses, 260

VLSM (variable length subnet masking), 79-81

W-X-Y-Z

WANs

- connectivity, troubleshooting, 305

- CPE, connecting to, 151

- connection type, selecting, 153-154*

- via circuit-switched connection, 152*

- via packet-switched connection, 152*

- via point-to-point connection, 151*

- PPP encapsulation, configuring, 154-155

- serial link problems, troubleshooting, 307-309

WEP (Wired Equivalent Privacy), 257

WireShark protocol analyzer, 262, 293

WLANs (wireless LANs), security, 256-257

worldwide enterprise routing, 188-190

worms, 260

WPA (WiFi Protected Access), 258