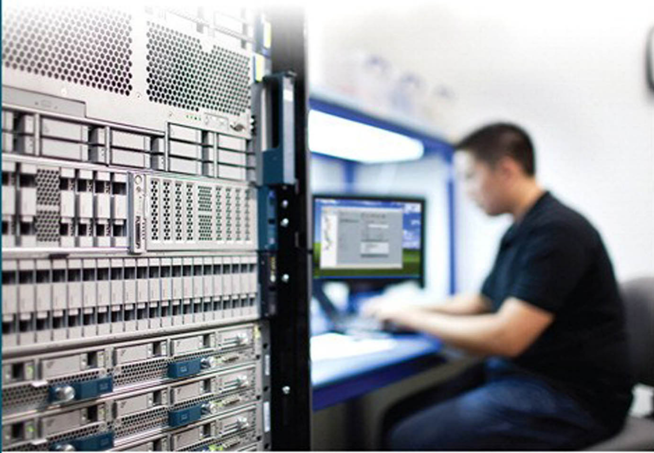
Troubleshooting and Maintaining Cisco IP Networks (TSHOOT)

Foundation Learning Guide



ciscopress.com

Amir Ranjbar

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Troubleshooting and Maintaining Cisco IP Networks (TSHOOT) Foundation Learning Guide

Amir Ranjbar,
CCIE No. 8669

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Troubleshooting and Maintaining Cisco IP Networks (TSHOOT) Foundation Learning Guide

Amir Ranjbar

Copyright © 2015 Pearson Education, 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, 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 December 2014

Library of Congress Control Number: 2014955936

ISBN-13: 978-1-58720-455-5

ISBN-10: 1-58720-455-X

Warning and Disclaimer

This book is designed to provide information about the Troubleshooting and Maintaining Cisco IP Networks (TSHOOT) course, which is an element of the CCNP Routing and Switching certification curriculum. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Trademark Acknowledgments

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

Special Sales

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

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

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

Feedback Information

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

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

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Business Operation Manager,
Cisco Press: Jan Cornelssen

Acquisitions Editor: Mary Beth Ray

Managing Editor: Sandra Schroeder

Development Editor: Ellie Bru

Senior Project Editor: Tonya Simpson

Copy Editor: Keith Cline

Technical Editor: Ted Kim

Team Coordinator: Vanessa Evans

Cover Designer: Mark Shirar

Composition: Trina Wurst

Indexer: Lisa Stumpf

Proofreader: Debbie Williams

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.**

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0812R)

About the Author

Amir Ranjbar, CCIE No. 8669, is a Certified Cisco Systems Instructor and a senior network consultant. Operating under his own corporation, AMIRACAN Inc., Amir offers his training services to Global Knowledge Network, his consulting expertise to a variety of clients (mainly Internet service providers), and his technical writing skills to Cisco Press (Pearson Education, Inc.). Born in Tehran, Iran, Amir immigrated to Canada in 1983 at the age of 16 and completed his Master's degree in knowledge-based systems (a branch in artificial intelligence [AI]) in 1991. He has been involved in training, consulting, and technical writing for the greater part of his career. Amir Ranjbar can be contacted through his email address aranjbar@amiracan.com.

About the Technical Reviewer

Ted Kim, CCIE No. 22769 (Routing and Switching and Service Provider), has 10 years of experience in the IT industry, with a focus on data center technologies during the past several years. He has experience with designing, implementing, and troubleshooting large enterprise environments. Ted's networking career began at Johns Hopkins as a network engineer, and he has been with Cisco since 2013 as a network consulting engineer.

Dedication

I dedicate this book to my father, Mr. Kavos Ranjbar, whom I lost on January 2, 2013. I wish we could all be so loving, helpful, and generous, yet humble, peaceful, and gentle, just like my dad.

Acknowledgments

This book is the result of work done by many individuals. I would like to offer my sincere gratitude to all of them, whether we worked together directly or otherwise. Mary Beth Ray, Ellie Bru, Tonya Simpson, Keith Cline, Vanessa Evans, Mark Shirar, Trina Wurst, and Lisa Stumpf, please accept my most sincere gratitude for the time and effort you put into this project. I wish I could attend the next Pearson Education social gathering and thank you all in person! Ted Kim, thank you for your technical review and feedback; I hope to meet you someday and thank you in person, too.

Contents at a Glance

Introduction xxi

Chapter 1: Troubleshooting Methods 1

Chapter 2: Structured Troubleshooting 15

Chapter 3: Network Maintenance Tasks and Best Practices 29

Chapter 4: Basic Switching and Routing Process and Effective IOS Troubleshooting Commands 61

Chapter 5: Using Specialized Maintenance and Troubleshooting Tools 99

Chapter 6: Troubleshooting Case Study: SECHNIK Networking 117

Chapter 7: Troubleshooting Case Study: TINC Garbage Disposal 173

Chapter 8: Troubleshooting Case Study: PILE Forensic Accounting 257

Chapter 9: Troubleshooting Case Study: Bank of POLONA 333

Chapter 10: Troubleshooting Case Study: RADULKO Transport 397

Appendix A: Answers to Review Questions 451

Index 453

Contents

Introduction xxi

Chapter 1 Troubleshooting Methods 1

Troubleshooting Principles 1

Structured Troubleshooting Approaches 4

The Top-Down Troubleshooting Approach 6

The Bottom-Up Troubleshooting Approach 7

The Divide-and-Conquer Troubleshooting Approach 8

The Follow-the-Path Troubleshooting Approach 9

The Compare-Configurations Troubleshooting Approach 10

The Swap-Components Troubleshooting Approach 11

Troubleshooting Example Using Six Different Approaches 12

Summary 13

Review Questions 14

Chapter 2 Structured Troubleshooting 15

Troubleshooting Method and Procedure 16

Defining the Problem 17

Gathering Information 18

Analyzing the Information 20

Eliminating Potential Causes 21

Proposing a Hypothesis (Likely Cause of the Problem) 21

Testing and Verifying Validity of the Proposed Hypothesis 23

Solving the Problem and Documenting the Work 24

Troubleshooting Example Based on the Structured Method and Procedures 25

Summary 26

Review Questions 27

Chapter 3 Network Maintenance Tasks and Best Practices 29

Structured Network Maintenance 29

Network Maintenance Processes and Procedures 31

Common Maintenance Tasks 32

Network Maintenance Planning 33

Scheduling Maintenance 33

Formalizing Change-Control Procedures 34

Establishing Network Documentation Procedures 34

Establishing Effective Communication 35

Defining Templates/Procedures/Conventions (Standardization) 36

Planning for Disaster Recovery 36

Network Maintenance Services and Tools 37

Network Time Services 39

Logging Services 40

Performing Backup and Restore 42

Integrating Troubleshooting into the Network Maintenance Process 47

Network Documentation and Baseline 48

Communication 50

Change Control 53

Summary 54

Review Questions 57

Chapter 4 Basic Switching and Routing Process and Effective IOS Troubleshooting Commands 61

Basic Layer 2 Switching Process 61

Ethernet Frame Forwarding (Layer 2 Data Plane) 62

Layer 2 Switching Verification 67

Basic Layer 3 Routing Process 69

IP Packet Forwarding (Layer 3 Data Plane) 70

Using IOS Commands to Verify IP Packet Forwarding 73

Selective Information Gathering Using IOS show Commands, debug Commands, Ping, and Telnet 76

Filtering and Redirecting show Command's Output 76

Testing Network Connectivity Using Ping and Telnet 81

Collecting Real-Time Information Using Cisco IOS debug Commands 85

Diagnosing Hardware Issues Using Cisco IOS Commands 86

Checking CPU Utilization 87

Checking Memory Utilization 88

Checking Interfaces 89

Summary 92

Review Questions 94

Chapter 5 Using Specialized Maintenance and Troubleshooting Tools 99

Categories of Troubleshooting Tools 100

Traffic-Capturing Features and Tools 101

SPAN 102

RSPAN 103

Information Gathering with SNMP 105

Information Gathering with NetFlow 107

Network Event Notification 109

Summary 113

Review Questions 114

Chapter 6 Troubleshooting Case Study: SECHNIK Networking 117

SECHNIK Networking Trouble Ticket 1 118

Troubleshooting PC1’s Connectivity Problem 118

Gathering Information 119

Analyzing Information, Eliminating Causes, and Gathering Further Information 119

Proposing Hypotheses 121

Testing the Hypotheses and Solving the Problem 121

Troubleshooting Ethernet Trunks 122

Troubleshooting PC2’s Connectivity Problem 123

Gathering Information 124

Proposing a Hypothesis, Testing the Hypothesis, and Solving the Problem 126

Troubleshooting NAT 127

Troubleshooting PC3’s Connectivity Problem 128

Gathering Information 129

Eliminating Possibilities, Proposing a Hypothesis, and Testing the Hypothesis 129

Troubleshooting Network Device Interfaces 130

Troubleshooting PC4’s IPv6 Connectivity Problem 131

Gathering Information 131

Eliminating Possibilities, Proposing a Hypothesis, and Testing the Hypothesis 132

Troubleshooting IPv6 Address Assignment on Clients 133

SECHNIK Networking Trouble Ticket 2 134

Troubleshooting PC1’s Internet Connectivity Problem 134

Gathering Information 135

Proposing a Hypothesis, Testing the Hypothesis, and Solving the Problem 137

Troubleshooting Network Layer Connectivity 138

Troubleshooting PC2’s SSH Connectivity Problem 141

Verifying and Defining the Problem 141

Gathering Information 142

Proposing a Hypothesis and Testing the Hypothesis 143

TCP Three-Way Handshake 145

Troubleshooting PC4's DHCP Address Problem 146

Verifying and Defining the Problem 146

Gathering Information 147

Proposing a Hypothesis, Testing a Hypothesis, and Solving the Problem 148

Troubleshooting Error-Disabled Ports 151

SECHNIK Networking Trouble Ticket 3 152

Troubleshooting PC1 and PC2's Internet Connectivity Issues 153

Verifying and Defining the Problem 153

Gathering Information 153

Proposing a Hypothesis and Testing the Hypothesis 157

Solving the Problem 159

Troubleshooting DHCP 160

The passive-interface Command 161

Troubleshooting PC3's Internet Connectivity Issues 162

Verifying and Defining the Problem 162

Gathering Information 162

Proposing a Hypothesis and Testing the Hypothesis 164

Solving the Problem 165

IPv6 Review 166

Summary 166

Review Questions 169

Chapter 7 Troubleshooting Case Study: TINC Garbage Disposal 173

TINC Garbage Disposal Trouble Ticket 1 174

Troubleshooting Lack of Backup Internet Connectivity Through GW2 174

Information Gathering 176

Analyzing Information, Eliminating Possibilities, and Proposing a Hypothesis 178

Proposing a Hypothesis, Testing the Hypothesis, and Solving the Problem 178

Troubleshooting BGP Neighbor Relationships 181

Troubleshooting PC1's Connectivity Problem 182

Gathering Information 182

Analyzing Information and Gathering Further Information 183

Proposing a Hypothesis, Testing the Hypothesis, and Solving the Problem 184

Troubleshooting Port Security 186

Troubleshooting PC2's Connectivity Problem 187

Gathering Information 188

Eliminating Possibilities, Proposing a Hypothesis, and Testing the Hypothesis 190

Solving the Problem 191

Troubleshooting VLANs 192

TINC Garbage Disposal Trouble Ticket 2 193

Troubleshooting GW1's OSPF Neighbor Relation Problem with Router R1 194

Verifying the Problem 194

Gathering Information 194

Analyzing Information, Eliminating Possibilities, and Proposing a Hypothesis 199

Testing the Hypothesis and Solving the Problem 199

Troubleshooting OSPF Adjacency 201

Troubleshooting Secure Shell Version 2 Access to Router R2 from PC4 202

Verifying the Problem 202

Gathering Information 203

Proposing a Hypothesis and Testing the Hypothesis 204

Solving the Problem 205

Troubleshooting SSH and Telnet 206

Troubleshooting Duplicate Address Problem Discovered Through R1 and R2's Log Messages 207

Verifying the Problem 207

Gathering Information 207

Analyzing the Information and Proposing a Hypothesis 210

Testing the Hypothesis and Solving the Problem 210

Troubleshooting HSRP 211

TINC Garbage Disposal Trouble Ticket 3 212

Troubleshooting Sporadic Internet Connectivity Problem Experienced by Users of PC1 and PC2 212

Verifying and Defining the Problem 213

Gathering Information 213

Analyzing Information and Proposing a Hypothesis 215

Testing the Hypothesis and Solving the Problem 217

Troubleshooting Erroneous Routing Information 218

Troubleshooting Multiple Masters within a VRRP 220

Verifying and Defining the Problem 220

Gathering Information 221

Analyzing the Information and Proposing a Hypothesis 222

Testing the Hypothesis, and Solving the Problem 222

Troubleshooting VRRP 224

Troubleshooting EtherChannel Between ASW4 and ASW3 224

Verifying the Problem 224

Defining the Problem 225

Gathering Information 225

Proposing a Hypothesis and Testing the Hypothesis 227

Solving the Problem 228

Troubleshooting EtherChannel 229

TINC Garbage Disposal Trouble Ticket 4 231

Troubleshooting Inconsistent and Sporadic Internet Connectivity Problem Experienced By Users of PC1 and PC2 231

Verifying and Defining the Problem 232

Gathering Information 233

Analyzing Information and Proposing a Hypothesis 235

Testing the Hypotheses 235

Solving the Problem 239

Troubleshooting FHRPs 241

Troubleshooting Sporadic Loss of Connectivity on PC4 242

Verifying the Problem and Making a Troubleshooting Plan 242

Gathering Information 242

Analyzing the Information and Gathering Further Information 244

Proposing a Hypothesis and Testing the Hypothesis 245

Solving the Problem 246

The Cisco IOS DHCP Snooping Feature 248

Cisco Technical Assistance Center 248

Troubleshooting SSH Connection from PC4 to Router GW2 249

Verifying the Problem and Making a Troubleshooting Plan 249

Gathering Information 250

Proposing a Hypothesis and Testing the Hypothesis 251

Solving the Problem 252

Summary 252

Review Questions 255

Chapter 8 Troubleshooting Case Study: PILE Forensic Accounting 257

PILE Forensic Accounting Trouble Ticket 1 258

Troubleshooting PILE's Branch Connectivity to HQ and the Internet 258

Verifying and Defining the Problem 258

Gathering Information 260

Analyzing Information 264

Proposing a Hypothesis and Testing the Hypothesis 264

Solving the Problem 265

Troubleshooting EIGRP Adjacency 266

Troubleshooting PILE's Secondary Internet Connection Through ISP2 267

Verifying and Defining the Problem 267

Gathering Information 268

Analyzing Information and Proposing a Hypothesis 270

Testing the Hypothesis 271

Solving the Problem 273

PILE Forensic Accounting Trouble Ticket 2 274

Troubleshooting Telnet Problem: From PC3 to BR 274

Gathering Information 275

Troubleshooting PILE Network's Internet Access Problem 275

Verifying and Defining the Problem 276

Gathering Information 276

Analyzing Information, Eliminating Causes, and Gathering Further Information 278

Proposing and Testing a Hypothesis 280

Solving the Problem 281

Troubleshooting BGP 281

Troubleshooting PILE Network's NTP Problem 282

Verifying the Problem 283

Gathering Information 283

Analyzing the Gathered Information and Gathering Further Information 284

Proposing a Hypothesis and Testing the Hypothesis 285

Solving the Problem 286

Troubleshooting NTP 286

PILE Forensic Accounting Trouble Ticket 3 287

Troubleshooting PC3's Lack of Internet Connectivity After the Disaster Recovery 287

Verifying the Problem 288

Gathering Information (First Run) 288

Analyzing Information, Proposing, and Testing the First Hypothesis 289

Proposing and Testing the Second Hypothesis 290

Gathering Further Information (Second Run) 292

Proposing and Testing the Third Hypothesis 293

Solving the Problem 294

Disaster Recovery Best Practices 294

Troubleshooting Inter-VLAN Routing 296

Troubleshooting PC4's Problem Accessing Cisco.com 297

Verify the Problem and Select an Approach 297

Gather Information and Analyze the Information 298

Proposing and Testing a Hypothesis 299

Solve the Problem 299

Troubleshooting DNS 300

Remote Device Management Notes 301

PILE Forensic Accounting Trouble Ticket 4 302

Troubleshooting Branch Site Internet Connectivity Problem After EIGRP Reconfiguration 302

Verifying the Problem 302

Gathering Information 303

Gathering Further Information and Analyzing Information 303

Proposing a Hypothesis and Testing the Hypothesis 305

Solving the Problem 307

The EIGRP Stub Configuration 308

The New EIGRP Named Configuration 309

Troubleshooting Management Access to ASW2 310

Verifying the Problem 310

Gathering Information 310

Proposing a Hypothesis and Testing the Hypothesis 311

Solving the Problem 312

Providing a Default Route on Layer 2 And Multilayer Devices 313

PILE Forensic Accounting Trouble Ticket 5 313

Troubleshooting the Redundant Internet Access Path Through the New HQ0 Edge Router 314

Verifying and Defining the Problem 314

Gathering Information 315

Proposing a Hypothesis and Testing the Hypothesis 318

Solving the Problem 319

Troubleshooting BGP Route Selection 321

Troubleshooting Unauthorized Telnet Access 322

Verifying the Problem 322

Gathering Information 322

Gathering Further Information and Analysis Information 323

Proposing a Hypothesis and Testing the Hypothesis 324

Solving the Problem 325

Securing the Management Plane 325

Summary 326

Review Questions 329

Chapter 9 Troubleshooting Case Study: Bank of POLONA 333

Bank of POLONA Trouble Ticket 1 334

Troubleshooting PC3's Lack of Connectivity to SRV2 335

Verifying the Problem 335

Gathering Information 336

Analyzing Information and Proposing a Hypothesis, and Testing the Hypothesis 338

Solving the Problem 339

Troubleshooting Redistribution 339

Troubleshooting VRRP with Interface Tracking 340

Verifying the Problem 340

Gathering Information 341

Analyzing the Information 342

Proposing and Testing a Hypothesis 342

Solving the Problem 343

FHRP Tracking Options 344

Troubleshooting IP SLA Test Not Starting 345

Verifying the Problem 345

Gathering Information 346

Proposing and Testing a Hypothesis 347

Solving the Problem 348

Troubleshooting IP SLA 349

Bank of POLONA Trouble Ticket 2 349

Troubleshooting Summarization Problem on BR3 350

Verifying the Problem 350

Gathering Information 350

Analyzing Information 351

Proposing and Testing a Hypothesis 351

Solving the Problem 352

Troubleshooting EIGRP Summarization 353

Troubleshooting PC0's IPv6 Internet Connectivity 353

Verifying the Problem 353

Gathering Information 354

Analyzing Information 356

Proposing and Testing a Hypothesis 356

Solving the Problem 357

Troubleshooting RIPng 357

Troubleshooting Branch 3's IPv6 Internet Connectivity 358

Verifying the Problem 358

Gathering Information 359

Analyzing Information 361

Proposing and Testing a Hypothesis 361

Solving the Problem 362

Troubleshooting Access Control Lists 362

Bank of POLONA Trouble Ticket 3 364

Troubleshooting Branch 1's IP Connectivity to the Headquarters 364

Verifying the Problem 364

Gathering Information 365

Proposing and Testing a Hypothesis 366

Gathering Further Information 367

Proposing and Testing Another Hypothesis 367

Solving the Problem 368

Troubleshooting GRE Tunnels 368

Troubleshooting Branch 3's Route Summarization 369

Verifying the Problem and Choosing an Approach 369

Gathering Information 370

Analyzing the Information and Proposing a Hypothesis 373

Testing the Hypothesis and Solving the Problem 373

OSPF Summarization Tips and Commands 374

Troubleshooting AAA Authentication on the Branch 1 Router 375

Verifying the Problem and Choosing an Approach 375

Gathering Information 375

Proposing a Hypothesis 376

Testing the Hypothesis and Solving the Problem 376

Troubleshooting AAA 377

Bank of POLONA Trouble Ticket 4 378

Troubleshooting PC0's Connectivity to IPv6 Internet 378

Verifying the Problem and Choosing an Approach 378

Gathering Information 379

Analyzing the Information and Proposing and Testing a Hypothesis 381

Gathering Further Information 382

Analyzing Information and Proposing and Testing Another Hypothesis 383

Solving the Problem 384

Troubleshooting OSPF for IPv6 385

Troubleshooting the Dysfunctional Totally Stubby Branch Areas 386

Verifying the Problem and Choosing an Approach 386

Gathering Information 387

Analyzing Information 389

Proposing and Testing a Hypothesis 389

Solving the Problem 390

OSPF Stub Areas 391

Summary 391

Review Questions 394

Chapter 10 Troubleshooting Case Study: RADULKO Transport 397

RADULKO Transport Trouble Ticket 1 398

Mitigating Unauthorized Switches Added by Employees 398

Gathering Information 399

Analyzing Information 400

Proposing a Hypothesis and Solving the Problem 400

Troubleshooting Spanning Tree Protocol 401

Troubleshooting Policy-Based Routing 403

Verifying and Defining the Problem 404

Gathering Information 404

Analyzing the Information 405

Proposing and Testing a Hypothesis 405

Solving the Problem 406

Troubleshooting PBR 407

Troubleshooting Neighbor Discovery 407

Verifying and Defining the Problem 408

Gathering Information 408

Proposing and Testing a Hypothesis 409

Solving the Problem 409

Troubleshooting CDP and LLDP 410

RADULKO Transport Trouble Ticket 2 411

Troubleshooting VLANs and PCs Connectivity Problems 411

Verifying the Problem 412

Gathering Information 412

Analyzing the Information 413

Proposing and Testing a Hypothesis 413

Solving the Problem 414

Troubleshooting VTP 415

Troubleshooting Branch Router's IPv6 Problems 416

Verifying the Problem 416

Gathering Information 417

Proposing and Testing a Hypothesis 418

Solving the Problem 418

Troubleshooting EIGRP for IPv6 419

Troubleshooting MP-BGP Session Problem 420

Verifying the Problem 420

Gathering Information 420

Analyzing the Information and Proposing a Hypothesis 421

Solving the Problem 422

Troubleshooting MP-BGP 423

RADULKO Transport Trouble Ticket 3 424

Troubleshooting PC1's Problem Accessing the SRV Server at the Distribution Center 424

Verifying and Defining the Problem 424

Gathering Information 425

Analyzing Information 428

Proposing and Testing a Hypothesis 428

Solving the Problem 429

Troubleshooting the OSPFv3 Address Families Feature 429

Troubleshooting OSPFv3 Authentication 430

Verifying the Problem 430

Gathering Information 431

Analyzing Information 432

Proposing and Testing a Hypothesis 432

Solving the Problem 433

RADULKO Transport Trouble Ticket 4 433

Troubleshooting Undesired External OSPF Routes in DST's Routing Table 434

Verifying and Defining the Problem 434

Gathering Information 435

Analyzing Information 436

Proposing and Testing a Hypothesis 437

Solving the Problem 439

Troubleshooting PCs IPv6 Internet Access 440

Verifying the Problem 440

Gathering Information 440

Analyzing Information 442

Proposing and Testing a Hypothesis 443

Solving the Problem 444

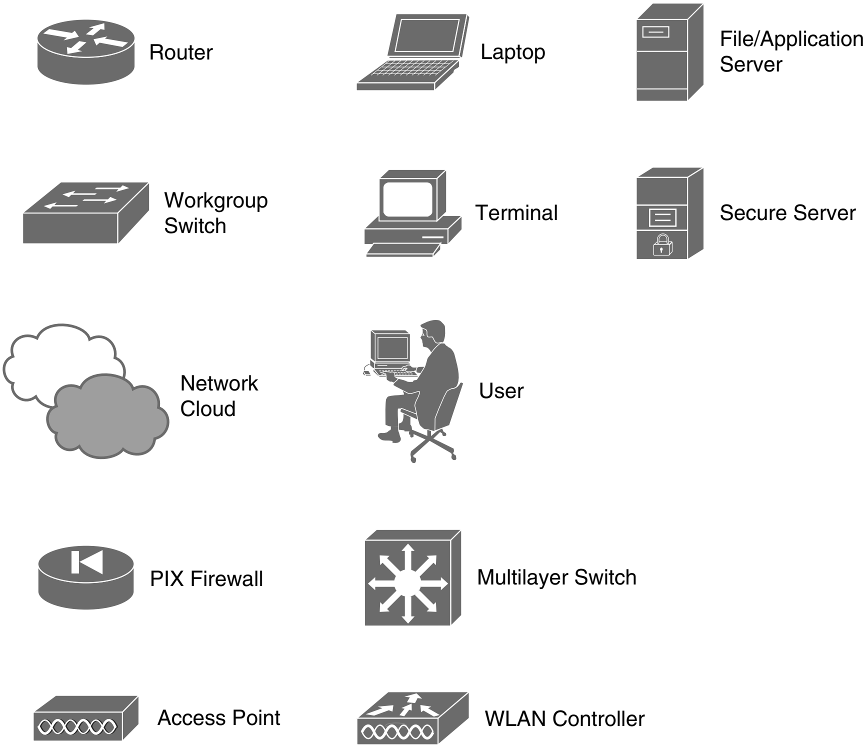
Summary 444

Review Questions 448

Appendix A Answers to Review Questions 451

Index 453

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

Introduction

This book is based on the Cisco Systems TSHOOT course, which was recently introduced as part of the CCNP curriculum. It provides troubleshooting and maintenance information and examples that relate to Cisco routing and switching. It is assumed that readers know and understand as much Cisco routing and switching background as covered in the Cisco ROUTE and SWITCH courses. The book is enough to prepare you for the TSHOOT exam, too.

Teaching troubleshooting is not an easy task. This book introduces you to many troubleshooting methodologies and identifies the benefits of different techniques. Technical routing and switching topics are briefly reviewed, but the emphasis is on troubleshooting commands, and most important, this book presents many troubleshooting examples. Chapter review questions will help you evaluate how well you absorbed material within each chapter. The questions are also an excellent supplement for exam preparation.

Who Should Read This Book?

Those individuals who want to learn about modern troubleshooting methodologies and techniques and want to see several relevant examples will find this book very useful. This book is most suitable for those who have some prior routing and switching knowledge but would like to learn more or otherwise enhance their troubleshooting skill set. Readers who want to pass the Cisco TSHOOT exam can find all the content they need to successfully do so in this book. The Cisco Networking Academy CCNP TSHOOT course students will use this book as their official textbook.

Cisco Certifications and Exams

Cisco offers four levels of routing and switching certification, each with an increasing level of proficiency: Entry, Associate, Professional, and Expert. These are commonly known by their acronyms CCENT (Cisco Certified Entry Networking Technician), CCNA (Cisco Certified Network Associate), CCNP (Cisco Certified Network Professional), and CCIE (Cisco Certified Internetworking Expert). There are others, too, but this book focuses on the certifications for enterprise networks.

For the CCNP certification, you must pass exams on a series of CCNP topics, including the SWITCH, ROUTE, and TSHOOT exams. For most exams, Cisco does not publish the scores needed for passing. You need to take the exam to find that out for yourself.

To see the most current requirements for the CCNP certification, go to Cisco.com and click **Training and Events**. There you can find out other exam details such as exam topics and how to register for an exam.

The strategy you use to prepare for the TSHOOT exam might differ slightly from strategies used by other readers, mainly based on the skills, knowledge, and experience you have already obtained. For instance, if you have attended the TSHOOT course, you might take a different approach than someone who learned troubleshooting through on-the-job training. Regardless of the strategy you use or the background you have, this book is designed to help you get to the point where you can pass the exam with the least amount of time required.

How This Book Is Organized

Although this book can be read cover to cover, it is designed to be flexible and allow you to easily move between chapters to cover only the material for which you might need additional remediation. The chapters can be covered in any order, although some chapters are related to and build upon each other. If you do intend to read them all, the order in the book is an excellent sequence to follow.

Each core chapter covers a subset of the topics on the CCNP TSHOOT exam. The chapters cover the following topics:

- Chapter 1 introduces the troubleshooting principles and discusses the most common troubleshooting approaches.
- Chapter 2 defines structured troubleshooting and analyzes all the subprocesses of structured troubleshooting.
- Chapter 3 introduces structured network maintenance and discusses network maintenance processes and procedures. Network maintenance services and tools, along with how you can integrate troubleshooting into the network maintenance process, are also presented in this chapter.
- Chapter 4 reviews the Layer 2 switching and Layer 3 routing processes and shows how to do selective information gathering using the IOS **show** command, **debug** command, ping, and Telnet.
- Chapter 5 discusses troubleshooting tools: traffic-capturing features and tools, information gathering with SNMP, information gathering with NetFlow, and network event notification with EEM.
- Chapters 6 through 10 are all troubleshooting cases. Each chapter is about a different network with many different problems. Each problem is dealt with in the form of a real-life trouble ticket, and it is fixed following the structured troubleshooting methodology using the appropriate approach. All stages of troubleshooting, including fact gathering, are presented with output from Cisco IOS routers and switches. The network diagrams for Chapters 6 through 10 appear at the beginning and end of each chapter. For easier reference, a PDF of these network diagrams is available to download and print out or read on your e-device. Go to ciscopress.com/title/9781587204555 and click on the Downloads tab.

There is also an appendix that has answers to the review questions found at the end of each chapter.

Chapter 1

Troubleshooting Methods

This chapter covers the following topics:

- Troubleshooting principles
- Common troubleshooting approaches
- Troubleshooting example using six different approaches

Most modern enterprises depend heavily on the smooth operation of their network infrastructure. Network downtime usually translates to loss of productivity, revenue, and reputation. Network troubleshooting is therefore one of the essential responsibilities of the network support group. The more efficiently and effectively the network support personnel diagnose and resolve problems, the lower impact and damages will be to business. In complex environments, troubleshooting can be a daunting task, and the recommended way to diagnose and resolve problems quickly and effectively is by following a structured approach. Structured network troubleshooting requires well-defined and documented troubleshooting procedures.

This chapter defines troubleshooting and troubleshooting principles. Next, six different troubleshooting approaches are described. The third section of this chapter presents a troubleshooting example based on each of the six troubleshooting approaches.

Troubleshooting Principles

Troubleshooting is the process that leads to the diagnosis and, if possible, resolution of a problem. Troubleshooting is usually triggered when a person reports a problem. In modern and sophisticated environments that deploy proactive network monitoring tools and techniques, a failure/problem may be discovered and even fixed/resolved before end users notice or business applications get affected by it.

Some people say that a problem does not exist until it is noticed, perceived as a problem, and reported as a problem. This implies that you need to differentiate between a problem, as experienced by the user, and the actual cause of that problem. The time a problem is reported is not necessarily the same time at which the event causing the problem happened. Also, the reporting user generally equates the problem to the symptoms, whereas the troubleshooter often equates the problem to the root cause. For example, if the Internet connection fails on Saturday in a small company, it is usually not a problem, but you can be sure that it will turn into a problem on Monday morning if it is not fixed before then. Although this distinction between symptoms and cause of a problem might seem philosophical, you need to be aware of the potential communication issues that might arise from it.

Generally, reporting of a problem triggers the troubleshooting process. Troubleshooting starts by defining the problem. The second step is diagnosing the problem, during which information is gathered, the problem definition is refined, and possible causes for the problem are proposed. Eventually, this process should lead to a hypothesis for the root cause of the problem. At this time, possible solutions need to be proposed and evaluated. Next, the best solution is selected and implemented. Figure 1-1 illustrates the main elements of a structured troubleshooting approach and the transition possibilities from one step to the next.

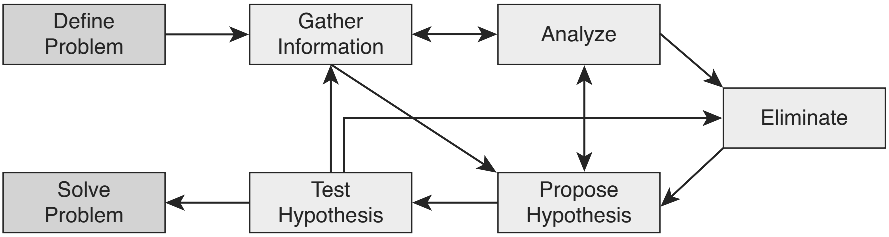


Figure 1-1 *Flow Chart of a Structured Troubleshooting Approach*

Note It is noteworthy, however, that the solution to a network problem cannot always be readily implemented and an interim workaround might have to be proposed. The difference between a solution and a workaround is that a solution resolves the root cause of the problem, whereas a workaround only alleviates the symptoms of the problem.

Although problem reporting and resolution are definitely essential elements of the troubleshooting process, most of the time is spent in the diagnostic phase. One might even believe that diagnosis is all troubleshooting is about. Nevertheless, within the context of network maintenance, problem reporting and resolution are indeed essential parts of troubleshooting. Diagnosis is the process of identifying the nature and cause of a problem. The main elements of this process are as follows:

- **Gathering information:** Gathering information happens after the problem has been reported by the user (or anyone). This might include interviewing all parties (user) involved, plus any other means to gather relevant information. Usually, the problem report does not contain enough information to formulate a good hypothesis without first gathering more information. Information and symptoms can be gathered directly, by observing processes, or indirectly, by executing tests.

- **Analyzing information:** After the gathered information has been analyzed, the troubleshooter compares the symptoms against his knowledge of the system, processes, and baselines to separate normal behavior from abnormal behavior.
- **Eliminating possible causes:** By comparing the observed behavior against expected behavior, some of the possible problem causes are eliminated.
- **Formulating/proposing a hypothesis:** After gathering and analyzing information and eliminating the possible causes, one or more potential problem causes remain. The probability of each of these causes will have to be assessed and the most likely cause proposed as the hypothetical cause of the problem.
- **Testing the hypothesis:** The hypothesis must be tested to confirm or deny that it is the actual cause of the problem. The simplest way to do this is by proposing a solution based on this hypothesis, implementing that solution, and verifying whether this solved the problem. If this method is impossible or disruptive, the hypothesis can be strengthened or invalidated by gathering and analyzing more information.

All troubleshooting methods include the elements of gathering and analyzing information, eliminating possible causes, and formulating and testing hypotheses. Each of these steps has its merits and requires some time and effort; how and when one moves from one step to the next is a key factor in the success level of a troubleshooting exercise. In a scenario where you are troubleshooting a complex problem, you might go back and forth between different stages of troubleshooting: Gather some information, analyze the information, eliminate some of the possibilities, gather more information, analyze again, formulate a hypothesis, test it, reject it, eliminate some more possibilities, gather more information, and so on.

If you do not take a structured approach to troubleshooting and do troubleshooting in an ad hoc fashion, you might eventually find the solution; however, the process in general will be very inefficient. Another drawback of ad hoc troubleshooting is that handing the job over to someone else is very hard to do; the progress results are mainly lost. This can happen even if the troubleshooter wants to resume his own task after he has stopped for a while, perhaps to take care of another matter. A structured approach to troubleshooting, regardless of the exact method adopted, yields more predictable results in the long run. It also makes it easier to pick up where you left off or hand the job over to someone else without losing any effort or results.

A troubleshooting approach that is commonly deployed both by inexperienced and experienced troubleshooters is called shoot-from-the-hip. After a very short period of gathering information, taking this approach, the troubleshooter quickly makes a change to see if it solves the problem. Even though it may seem like random troubleshooting on the surface, it is not. The reason is that the guiding principle for this method is prior and usually vast knowledge of common symptoms and their corresponding causes, or simply extensive relevant experience in a particular environment or application. This technique might be quite effective for the experienced troubleshooter most times, but it usually does not yield the same results for the inexperienced troubleshooter. Figure 1-2 shows how the "shoot-from-the-hip" approach goes about solving a problem, spending almost no effort in analyzing the gathered information and eliminating possibilities.

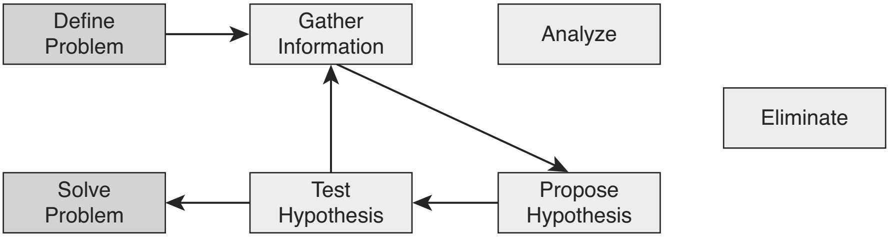


Figure 1-2 *Shoot-from-the-Hip*

Assume that a user reports a LAN performance problem and in 90 percent of the past cases with similar symptoms, the problem has been caused by duplex mismatch between users' workstations (PC or laptop) and the corresponding access switch port. The solution has been to configure the switch port for 100-Mbps full duplex. Therefore, it sounds reasonable to quickly verify the duplex setting of the switch port to which the user connects and change it to 100-Mbps full duplex to see whether that fixes the problem. When it works, this method can be very effective because it takes very little time. Unfortunately, the downside of this method is that if it does not work, you have not come any closer to a possible solution, you have wasted some time (both yours and users'), and you might possibly have caused a bit of frustration. Experienced troubleshooters use this method to great effect. The key factor in using this method effectively is knowing when to stop and switch to a more methodical (structured) approach.

Structured Troubleshooting Approaches

Troubleshooting is not an exact science, and a particular problem can be diagnosed and sometimes even solved in many different ways. However, when you perform structured troubleshooting, you make continuous progress, and usually solve the problem faster than it would take using an ad hoc approach. There are many different structured troubleshooting approaches. For some problems, one method might work better, whereas for others, another method might be more suitable. Therefore, it is beneficial for the troubleshooter to be familiar with a variety of structured approaches and select the best method or combination of methods to solve a particular problem.

A structured troubleshooting method is used as a guideline through a troubleshooting process. The key to all structured troubleshooting methods is systematic elimination of hypothetical causes and narrowing down on the possible causes. By systematically eliminating possible problem causes, you can reduce the scope of the problem until you manage to isolate and solve the problem. If at some point you decide to seek help or hand the task over to someone else, your findings can be of help to that person and your efforts are not wasted. Commonly used troubleshooting approaches include the following:

- **The top-down approach:** Using this approach, you work from the Open Systems Interconnection (OSI) model's application layer down to the physical layer. The OSI seven-layer networking model and TCP/IP four-layer model are shown side by side in Figure 1-3 for your reference.

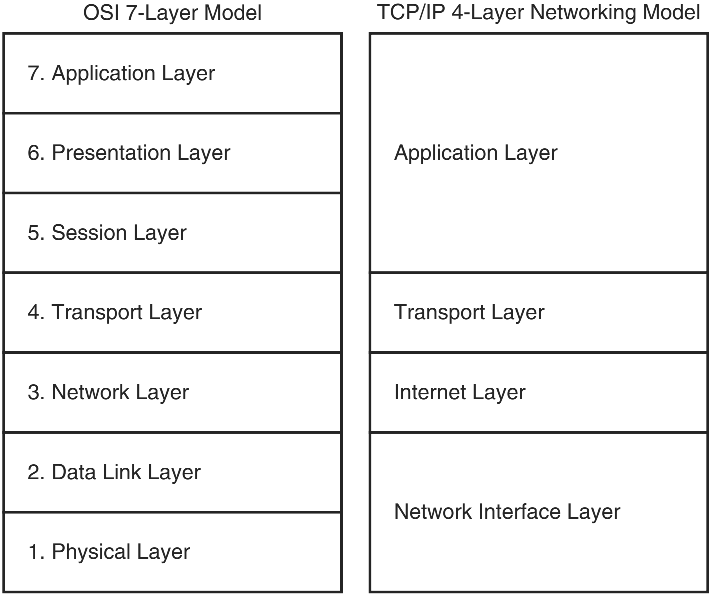


Figure 1-3 *The OSI and TCP/IP Networking Models*

- **The bottom-up approach:** This approach starts from the OSI model's physical layer and moves up toward the application layer.
- **The divide-and-conquer approach:** Using this approach, you start in the middle of the OSI model's stack (usually the network layer), and then, based on your findings, you move up or down the OSI stack.
- **The follow-the-path approach:** This approach is based on the path that packets take through the network from source to destination.
- **The spot-the-differences approach:** As the name implies, this approach compares network devices or processes that are operating correctly to devices or processes that are not operating as expected and gathers clues by spotting significant differences. In case the problem occurred after a change on a single device was implemented, the spot-the differences approach can pinpoint the problem cause by focusing on the difference between the device configurations, before and after the problem was reported.
- **The move-the-problem approach:** The strategy of this troubleshooting approach is to physically move components and observe whether the problem moves with the moved components.

The sections that follow describe each of these methods in more detail.

The Top-Down Troubleshooting Approach

The top-down troubleshooting method uses the OSI model as a guiding principle. One of the most important characteristics of the OSI model is that each layer depends on the underlying layers for its operation. This implies that if you find a layer to be operational, you can safely assume that all underlying layers are fully operational as well.

Let's assume that you are researching a problem of a user that cannot browse a particular website and you find that you can establish a TCP connection on port 80 from this host to the server and get a response from the server (see Figure 1-4). In this situation, it is reasonable to conclude that the transport layer and all layers below must be fully functional between the client and the server and that this is most likely a client or server problem (most likely at application, presentation, or session layer) and not a network problem. Be aware that in this example it is reasonable to conclude that Layers 1 through 4 must be fully operational, but it does not definitively prove this. For instance, nonfragmented packets might be routed correctly, whereas fragmented packets are dropped. The TCP connection to port 80 might not uncover such a problem.

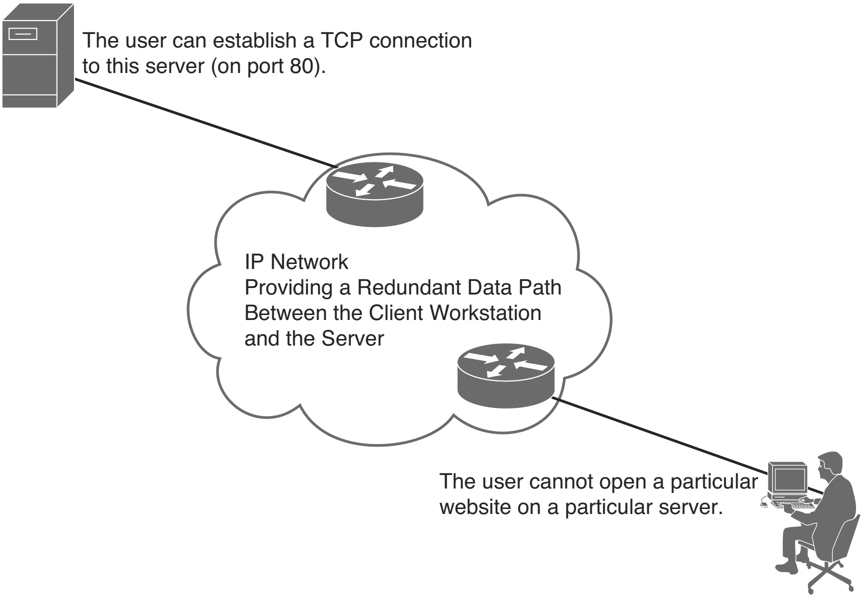

The user can establish a TCP connection to this server (on port 80).
IP Network
Providing a Redundant Data Path
Between the Client Workstation
and the Server
The user cannot open a particular website on a particular server.

Figure 1-4 *Application Layer Failure*

Essentially, the goal of the top-down approach is to find the highest OSI layer that is still working. All devices and processes that work on that layer or layers below are then eliminated from the scope of the troubleshooting. It might be clear that this approach is most effective if the problem is on one of the higher OSI layers. It is also one of the most straightforward troubleshooting approaches, because problems reported by users are typically defined as application layer problems, so starting the troubleshooting process at that layer is a natural thing to do. A drawback or impediment to this approach is that you need to have access to the client's application layer software to initiate the troubleshooting process, and if the software is only installed on a small number of machines, your troubleshooting options might be limited.

The Bottom-Up Troubleshooting Approach

The bottom-up troubleshooting approach also uses the OSI model as its guiding principle with the physical layer (bottom layer of the OSI seven-layer network model) as the starting point. In this approach, you work your way layer by layer up toward the application layer and verify that relevant network elements are operating correctly. You try to eliminate more and more potential problem causes so that you can narrow down the scope of the potential problems.

Let's assume that you are researching a problem of a user that cannot browse a particular website and while you are verifying the problem, you find that the user's workstation is not even able to obtain an IP address through the DHCP process (see Figure 1-5). In this situation it is reasonable to suspect lower layers of the OSI model and take a bottom-up troubleshooting approach.

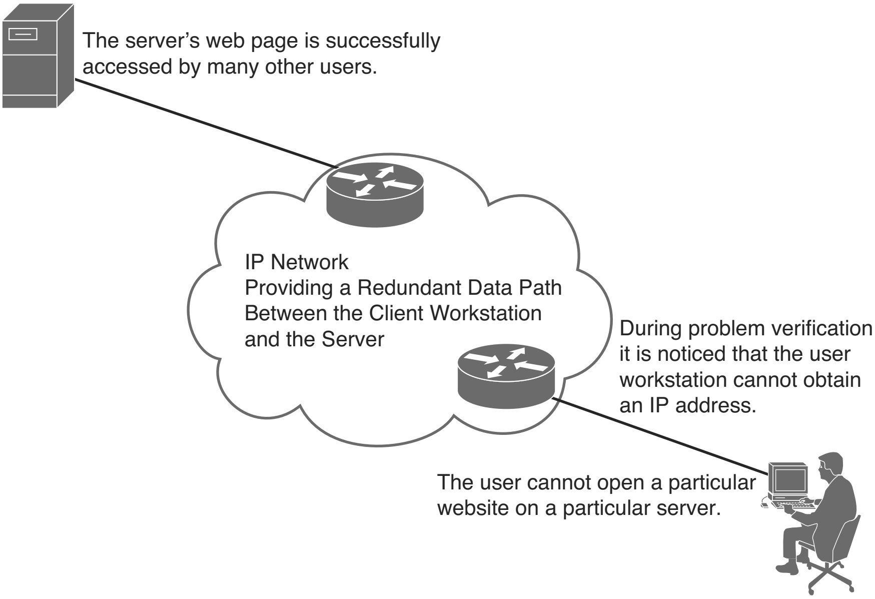

The server's web page is successfully accessed by many other users.
IP Network
Providing a Redundant Data Path
Between the Client Workstation
and the Server
During problem verification it is noticed that the user workstation cannot obtain an IP address.
The user cannot open a particular website on a particular server.

Figure 1-5 *Failure at Lower OSI Layers*

A benefit of the bottom-up approach is that all the initial troubleshooting takes place on the network, so access to clients, servers, or applications is not necessary until a very late stage in the troubleshooting process. In certain environments, especially those where many old and outdated devices and technologies are still in use, many network problems are hardware related. The bottom-up approach is very effective under those circumstances. A disadvantage of this method is that, in large networks, it can be a time-consuming process because a lot of effort will be spent on gathering and analyzing data and you always start from the bottom layer. The best bottom-up approach is to first reduce the scope of the problem using a different strategy and then switch to the bottom-up approach for clearly bounded parts of the network topology.

The Divide-and-Conquer Troubleshooting Approach

The divide-and-conquer troubleshooting approach strikes a balance between the top-down and bottom-up troubleshooting approaches. If it is not clear which of the top-down or bottom-up approaches will be more effective for a particular problem, an alternative is to start in the middle (usually from the network layer) and perform some tests such as ping and trace. Ping is an excellent connectivity testing tool. If the test is successful, you can assume that all lower layers are functional, and so you can start a bottom-up troubleshooting starting from the network layer. However, if the test fails, you can start a top-down troubleshooting starting from the network layer.

Let's assume that you are researching a problem of a user who cannot browse a particular website and that while you are verifying the problem you find that the user's workstation can successfully ping the server's IP address (see Figure 1-6). In this situation, it is reasonable to assume that the physical, data link, and network layers of the OSI model are in good working condition, and so you examine the upper layers, starting from the transport layer in a bottom-up approach.

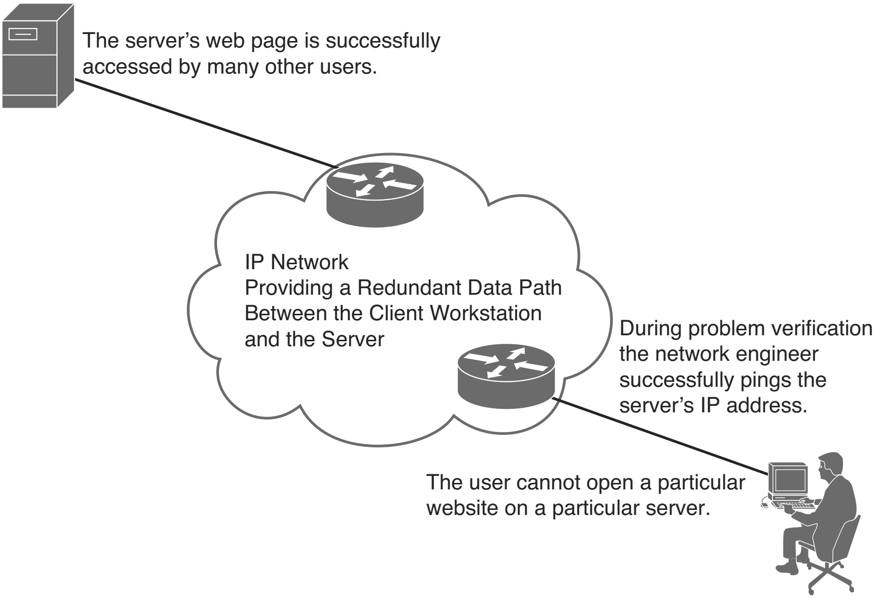

The server's web page is successfully accessed by many other users.
IP Network
Providing a Redundant Data Path
Between the Client Workstation
and the Server
During problem verification the network engineer successfully pings the server's IP address.
The user cannot open a particular website on a particular server.

Figure 1-6 *Successful Ping Shifts the Focus to Upper OSI Layers (Divide-and-Conquer Approach)*

Whether the result of the initial test is positive or negative, the divide-and-conquer approach usually results in a faster elimination of potential problems than what you would achieve by implementing a full top-down or bottom-up approach. Therefore, the divide-and-conquer method is considered highly effective and possibly the most popular troubleshooting approach.

The Follow-the-Path Troubleshooting Approach

The follow-the-path approach is one of the most basic troubleshooting techniques, and it usually complements one of the other troubleshooting methods such as the top-down or the bottom-up approach. The follow-the-path approach first discovers the actual traffic path all the way from source to destination. Next, the scope of troubleshooting is reduced to just the links and devices that are actually in the forwarding path. The principle of this approach is to eliminate the links and devices that are irrelevant to the troubleshooting task at hand.

Let's assume that you are researching a problem of a user who cannot browse a particular website and that while you are verifying the problem you find that a trace (tracert) from the user's PC command prompt to the server's IP address succeeds only as far as the first hop, which is the L3 Switch v (Layer 3 or Multilayer Switch v) in Figure 1-7. Based on your understanding of the network link bandwidths and the routing protocol used on this network, you mark the links on the best path between the user workstation and the server on the diagram with numbers 1 through 7, as shown in Figure 1-7.

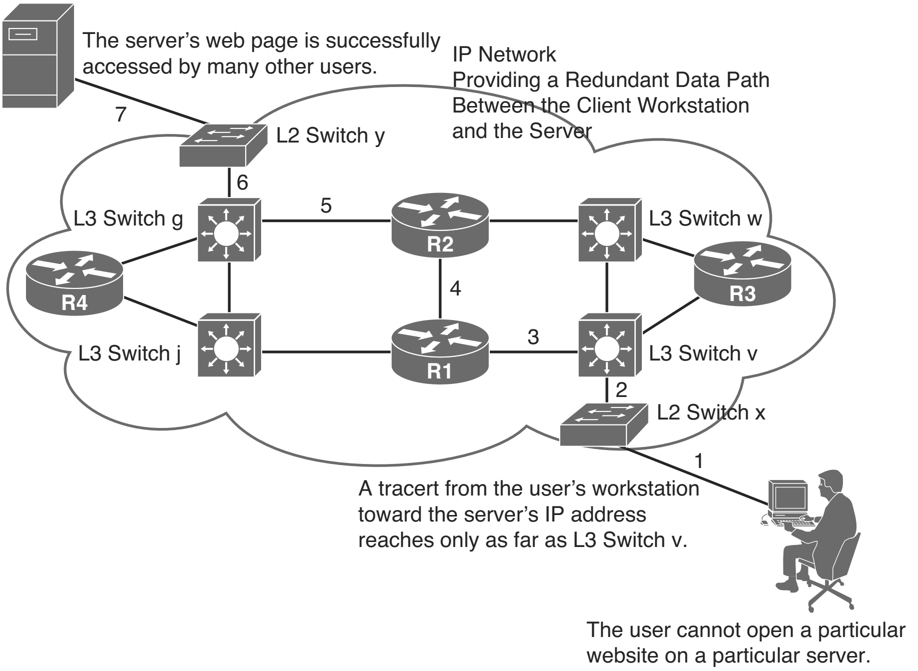

The server's web page is successfully accessed by many other users.
IP Network
Providing a Redundant Data Path
Between the Client Workstation
and the Server
7
L2 Switch y
6
L3 Switch g
5
R2
L3 Switch w
R3
R4
4
L3 Switch j
R1
3
L3 Switch v
2
L2 Switch x
1
A tracert from the user's workstation toward the server's IP address reaches only as far as L3 Switch v.
The user cannot open a particular website on a particular server.

Figure 1-7 *The Follow-the-Path Approach Shifts the Focus to Link 3 and Beyond Toward the Server*

In this situation it is reasonable to shift your troubleshooting approach to the L3 Switch v and the segments beyond, toward the server along the best path. The follow-the-path approach can quickly lead you to the problem area. You can then try and pinpoint the problem to a device, and ultimately to a particular physical or logical component that is either broken, misconfigured, or has a bug.

The Compare-Configurations Troubleshooting Approach

Another common troubleshooting approach is called the compare-configurations approach, also referred to as the spotting-the-differences approach. By comparing configurations, software versions, hardware, or other device properties between working and nonworking situations and spotting significant differences between them, this approach attempts to resolve the problem by changing the nonoperational elements to be consistent with the working ones. The weakness of this method is that it might lead to a working situation, without clearly revealing the root cause of the problem. In some cases, you are not sure whether you have implemented a solution or a workaround.

Example 1-1 shows two routing tables; one belongs to Branch2's edge router, experiencing problems, and the other belongs to Branch1's edge router, with no problems. If you compare the content of these routing tables, as per the compare-configurations (spotting-the-differences) approach, a natural deduction is that the branch with problems is missing a static entry. The static entry can be added to see whether it solves the problem.

Example 1-1 *Spot-the-Differences: One Malfunctioning and One Working Router*

```
------------- Branch1 is in good working order ----------
Branch1# show ip route
<...output omitted...>
10.0.0.0/24 is subnetted, 1 subnets
C   10.132.125.0 is directly connected, FastEthernet4
C   192.168.36.0/24 is directly connected, BVI1
S*  0.0.0.0/0 [254/0] via 10.132.125.1
------------- Branch2 has connectivity problems ----------
Branch2# show ip route
<...output omitted...>
10.0.0.0/24 is subnetted, 1 subnets
C 10.132.126.0 is directly connected, FastEthernet4
C 192.168.37.0/24 is directly connected, BVI1
```

The compare-configurations approach (spotting-the-differences) is not a complete approach; it is, however, a good technique to use undertaking other approaches. One benefit of this approach is that it can easily be used by less-experienced troubleshooting staff to at least shed more light on the case. When you have an up-to-date and accessible set of baseline configurations, diagrams, and so on, spotting the difference between the current configuration and the baseline might help you solve the problem faster than any other approach.

The Swap-Components Troubleshooting Approach

Also called move-the-problem, the swap-components approach is a very elementary troubleshooting technique that you can use for problem isolation: You physically swap components and observe whether the problem stays in place, moves with the component, or disappears entirely. Figure 1-8 shows two PCs and three laptops connected to a LAN switch, among which laptop B has connectivity problems. Assuming that hardware failure is suspected, you must discover whether the problem is on the switch, the cable, or the laptop. One approach is to start gathering data by checking the settings on the laptop with problems, examining the settings on the switch, comparing the settings of all the laptops, and the switch ports, and so on. However, you might not have the required administrative passwords for the PCs, laptops, and the switch. The only data that you can gather is the status of the link LEDs on the switch and the laptops and PCs. What you can do is obviously limited. A common way to at least isolate the problem (if it is not solved outright) is cable or port swapping. Swap the cable between a working device and laptop B (the one that is having problems). Move the laptop from one port to another using a cable that you know for sure is good. Based on these simple moves, you can isolate whether the problem is cable, switch, or laptop related.

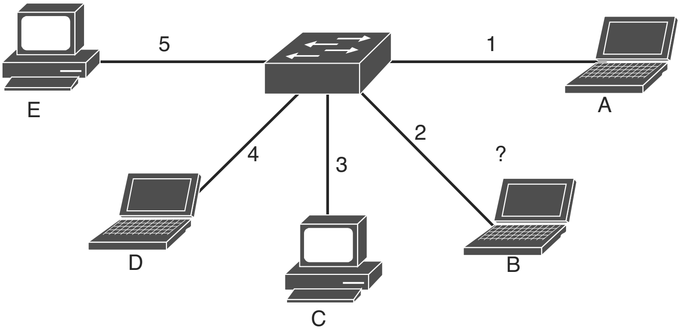


Figure 1-8 *Swap-the-Component: Laptop B Is Having Network Problems*

Just by executing simple tests in a methodical way, the swap-components approach enables you to isolate the problem even if the information that you can gather is minimal. Even if you do not solve the problem, you have scoped it to a single element, and you can now focus further troubleshooting on that element. Note that in the previous example if you determine that the problem is cable related, it is unnecessary to obtain the administrative password for the switch, PCs, and laptops. The drawbacks of this method are that you are isolating the problem to only a limited set of physical elements and not gaining any real insight into what is happening, because you are gathering only very limited indirect information. This method assumes that the problem is with a single component. If the problem lies within multiple devices, you might not be able to isolate the problem correctly.

Troubleshooting Example Using Six Different Approaches

An external financial consultant has come in to help your company's controller with an accounting problem. He needs access to the finance server. An account has been created for him on the server, and the client software has been installed on the consultant's laptop. You happen to walk past the controller's office and are called in and told that the consultant can't connect to the finance server. You are a network support engineer and have access to all network devices, but not to the servers. Think about how you would handle this problem, what your troubleshooting plan would be, and which method or combination of methods you would use.

What possible approaches can you take for this troubleshooting task? This case lends itself to many different approaches, but some specific characteristics can help you decide an appropriate approach:

- You have access to the network devices, but not to the server. This implies that you will likely be able to handle Layer 1–4 problems by yourself; however, for Layer 5–7, you will probably have to escalate to a different person.
- You have access to the client device, so it is possible to start your troubleshooting from it.
- The controller has the same software and access rights on his machine, so it is possible to compare between the two devices.

What are the benefits and drawbacks of each possible troubleshooting approach for this case?

- **Top-down:** You have the opportunity to start testing at the application layer. It is good troubleshooting practice to confirm the reported problem, so starting from the application layer is an obvious choice. The only possible drawback is that you will not discover simple problems, such as the cable being plugged in to a wrong outlet, until later in the process.
- **Bottom-up:** A full bottom-up check of the whole network is not a very useful approach because it will take too much time and at this point, there is no reason to assume that the network beyond the first access switch would be causing the issue. You could consider starting with a bottom-up approach for the first stretch of the network, from the consultant's laptop to the access switch, to uncover potential cabling problems.
- **Divide-and-conquer:** This is a viable approach. You can ping from the consultant's laptop to the finance server. If that succeeds, the problem is most likely at upper layers. For example, a firewall or access control list could be the culprit. If the ping fails, assuming that ping is not blocked in the network, it is safe to assume that the problem is at network or lower layers and you are responsible for fixing it. The advantage of this method is that you can quickly decide on the scope of the problem and whether escalation is necessary.

- **Follow-the-path:** Similar to the bottom-up approach, a full follow-the-path approach is not efficient under the circumstances, but tracing the cabling to the first switch can be a good start if it turns out that the link LED is off on the consultant's PC. This method might come into play after other techniques have been used to narrow the scope of the problem.
- **Compare-configurations:** You have access to both the controller's PC and the consultant's laptop; therefore, compare-configurations is a possible strategy. However, because these machines are not under the control of a single IT department, you might find many differences, and it might therefore be hard to spot the significant and relevant differences. The compare-configurations approach might prove useful later, after it has been determined that the problem is likely to be on the client.
- **Swap-components:** Using this approach alone is not likely to be enough to solve the problem, but if following any of the other methods indicates a potential hardware issue between the consultant's PC and the access switch, this method might come into play. However, merely as a first step, you could consider swapping the cable and the jack connected to the consultant's laptop and the controller's PC, in turn, to see whether the problem is cable, PC, or switch related.

Many combinations of these different methods could be considered here. The most promising methods are top-down or divide-and-conquer. You will possibly switch to follow-the-path or compare-configurations approach after the scope of the problem has been properly reduced. As an initial step in any approach, the swap-components method could be used to quickly separate client-related issues from network-related issues. The bottom-up approach could be used as the first step to verify the first stretch of cabling.

Summary

The fundamental elements of a troubleshooting process are as follows:

- Defining the problem
- Gathering information
- Analyzing information
- Eliminating possible causes
- Formulating a hypothesis
- Testing the hypothesis
- Solving the problem

Some commonly used troubleshooting approaches are as follows:

- Top-down
- Bottom-up

- Divide-and-conquer
- Follow-the-path
- Compare-configurations
- Swap-components

Review Questions

1. Which *three* of the following processes are subprocesses or phases of a troubleshooting process?

a. Solve the problem
b. Eliminate
c. Compile
d. Report the problem
e. Define the problem

2. Which *three* of the following approaches are valid troubleshooting methods?

a. Swap-components
b. Ad Hoc
c. Compare-configurations
d. Follow-the-path
e. Hierarchical

3. Which *three* of the following troubleshooting approaches use the OSI reference model as a guiding principle?

a. Top-down
b. Bottom-up
c. Divide-and-conquer
d. Compare-configurations
e. Swap-components

4. Which of the following troubleshooting methods would be most effective when the problem is with the Ethernet cable connecting a workstation to the wall RJ-45 jack?

a. Top-down
b. Divide-and-conquer
c. Compare-configurations
d. Swap-components
e. Follow-the-path

Index

Symbols

! (exclamation point), 84

& (packet lifetime exceeded), 84

. (period), 84

| (pipe), 78

? (unknown packet type), 84

A

AAA, troubleshooting, 377-378

AAA authentication, 375-378

ABR (OSPF Area Border Router), 372

access ports, 400

access switches, 290

ACL (access control lists), 361
- troubleshooting, 362-364

addressing schemes, documentation, 48

analyzing information, 3, 20-21

append, 79-80

approaches to troubleshooting, 4-5
- bottom-up approach, 5, 7-8, 12
- compare-configurations approach, 10, 13
- divide-and-conquer approach, 5, 8-9, 12
- follow-the-path approach, 5, 9-10, 13
- move-the-problem approach, 5
- spot-the-differences approach, 5
- swap-components approach, 11, 13
- top-down approach, 4, 6-7, 12

ASW2, management access to ASW2, 310-313

authentication
- AAA authentication, 375-378
- OSPFv3 authentication, RADULKO Transport, 430-433

B

BA (Bridge Assurance), 403

backup servers, 39

backups, 32
- performing, 42-47

Bank of POLONA, 333-334
- trouble ticket 1, 334

IP SLA test not starting, 345-349

lack of connectivity to SRV2, 335-340

VRRP with interface tracking, 340-345

trouble ticket 2, 349-350

IP connectivity to headquarters, 364-369

IPv6 connectivity problems, 353-364

summarization problems, 350-353

trouble ticket 3, 364

AAA authentication, 375-378

route summarization, 369-374

trouble ticket 4, 378

dysfunctional stubby branch areas, 386-391

troubleshooting PC0's connectivity to IPv6 Internet, 378-386

baselines, network maintenance processes, 48-50

begin keyword, 78

best practices, disaster recovery, 294-296

BGP

redistribution, 340

troubleshooting, 281-282

BGP neighbor relationships, 272-273, 278

troubleshooting, 181-182

BGP neighbor status, 269

BGP route selection, troubleshooting, 321-322

bottom-up approach, 5, 7-8, 12

BPDU Guard, 152

BPDUFilter, 402-403

BR (branch router), 274

branch connectivity to HQ and the Internet, PILE Forensic Accounting, 258-267

branch router's IPv6 problems, RADULKO Transport, 416-420

branch site Internet connectivity problems after EIGRP reconfiguration, 302-309

Bridge Assurance (BA), 403

brief, 345

C

cables, labeling, 48

capacity planning, 33

caret (^) character, 79

case studies

Bank of POLONA. *See* Bank of POLONA

PILE Forensic Accounting. *See* PILE Forensic Accounting

RADULKO Transport. *See* RADULKO Transport

SECHNIK Networking. *See* SECHNIK Networking

TINC Garbage Disposal. *See* TINC Garbage Disposal

categories of troubleshooting tools, 100-101

CDP (Cisco Discovery Protocol), 410-411

CEF (Cisco Express Forwarding), 73, 75, 139

switching methods, 141

CEF FIB table, displaying content, 140

change control, network maintenance processes, 53

change-control procedures, formalizing, 34

Cisco Discovery Protocol (CDP), 410-411

Cisco Express Forwarding (CEF), 73, 75

Cisco IOS DHCP snooping feature, 248

Cisco Technical Assistance Center, 248-249

Cisco.com, problems accessing, 297-302

clear bgp ipv6 unicast *, 423

CLI (command-line interface), 301

collecting real-time information, debug commands, 85-86

collectors, exporting NetFlow information to, 107-108

command-line device management, 38

commands

- clear bgp ipv6 unicast *, 423
- configure replace, 46
- configure replace *url* time *seconds*, 301
- debug bgp ipv6 unicast updates, 423
- debug cdp, 411
- debug eigrp packets hello, 85
- debug glbp [packets | events | terse | error | all], 241
- debug interface *interface-slot/number*, 85
- debug ip bgp, 182
- debug ip bgp events, 85
- debug ip bgp updates, 85, 282
- debug ip eigrp packets, 267
- debug ip icmp, 85
- debug ip ospf adjacency, 85
- debug ip ospf events, 85
- debug ip packet, 85-86
- debug ipv6 eigrp, 420
- debug ipv6 rip, 358
- debug lldp, 411
- debug ospfv3 events, 430
- debug spanning-tree bpdu receive, 85
- debug tunnel, 369
- debug vrrp all, 224
- debug vrrp authentication, 224
- debug vrrp error, 224
- debug vrrp events, 224
- debug vrrp packets, 224
- debug vrrp state, 224
- distribute-list access-list, 281
- distribute-list prefix-list, 282
- eigrp stub, 306
- eigrp stub connected, 308
- eigrp stub receive-only, 308
- eigrp stub redistribute, 308
- eigrp stub static, 308
- eigrp stub summary, 308
- filter-list *as-path-ACL-number*, 282
- ip config/all, 296
- ip default-gateway *ip-address*, 313
- ip default-network *network-number*, 313
- ip helper-address, 159
- ip route 0.0.0.0.0.0.0.0 {*ip-address* | *interface-type interface-number* [*ip-address*]}, 313
- passive-interface, 161-162
- passive-interface default, 161
- passive-interface *interface* command, 161
- reload in [*hh*:]*mm* [*text*], 301
- route-map *route-map-name*, 282
- running-config, 305

show, filtering/redirecting output, 76-80
show access-list, 363
show archive, 45
show bgp ipv6 unicast, 423
show bgp ipv6 unicast summary, 423
show cdp, 410
show cdp entry, 410
show cdp interface, 411
show cdp neighbors, 411
show cdp neighbors detail, 411
show cdp traffic, 411
show controllers, 91
show diag, 92
show eigrp address-family {ipv4 | ipv6} [*autonomous-system-number*] [multicast] accounting, 309
show eigrp address-family interfaces detail [*interface-type interface-number*], 309
show eigrp address-family topology route-type summary, 309
show eigrp plugins, 309
show etherchannel *group_number* detail, 230
show etherchannel summary, 230
show frame-relay map, 141
show glbp brief, 241
show glbp interface *type number* [brief], 241
show interfaces, 91
show interfaces switchport, 69
show interfaces trunk, 69, 296
show inventory, 92
show ip access-list, 363
show ip arp, 140
show ip bgp, 282
show ip bgp neighbors *neighbor-ip-address* [routes | advertised-routes], 282
show ip bgp summary, 182, 282
show ip cache flow, 109
show ip cef exact-route source destination, 75, 140
show ip cef *ip-address*, 74, 140
show ip cef network mask, 75, 140
show ip eigrp interfaces, 267
show ip eigrp neighbors, 267
show ip eigrp topology, 309
show ip interface brief, 296
show ip interface *interface-type interface-number*, 363
show ip nat translations, 128
show ip ospf neighbor, 215, 366
show ip protocols, 264
show ip route, 77, 311
show ip route *ip-address*, 74, 139
show ip route longer-prefixes, 77
show ip route network mask, 74, 139
show ip route network mask longer-prefixes, 74, 140
show ip route ospfv3, 430
show ip sla application, 345
show ip ssh, 204
show ipv6 access-list, 363
show ipv6 eigrp interfaces, 420
show ipv6 eigrp neighbors, 419
show ipv6 eigrp topology, 420
show ipv6 interface *interface-type interface-number*, 364
show ipv6 ospf *process-id*, 386
show ipv6 protocols, 419
show ipv6 protocols | section rip, 358
show ipv6 rip [*name*] [database], 358

show ipv6 route [rip], 358
show ipv6 route ospf, 430
show lldp, 410
show lldp entry, 410
show lldp interface, 411
show lldp neighbors, 411
show lldp neighbors detail, 411
show lldp traffic, 411
show mac-address-table, 68-69, 187
show memory, 89
show ospfv3, 430
show ospfv3 interface, 430
show ospfv3 neighbor, 430
show platform, 91
show platform forward *interface-id*, 69
show processes cpu, 76, 87
show running-config, 304
show running-config | include [*ACL-number*| *ACL-name*|], 364
show running-config | include interface|access-group, 363
show running-config | include interface|traffic-filter, 363
show running-config | include line|access-class, 363
show running-config | section interface, 430
show running-config | section router ospfv3, 430
show spanning-tree, 402
show spanning-tree mst configuration, 402
show spanning-tree summary, 402
show vlan, 69
show vlan [brief], 296
show vlan vlan-id, 296
show vrrp brief, 224
show vrrp interface, 224
summary, 352
traceroute mac, 69

common maintenance tasks, 32-33

communication
establishing network maintenance, 35
network maintenance processes, 50-53

compare-configurations approach, 10, 13

configuration archives, setting up, 45

configuration errors, 86

configure replace, 46

configure replace *url* time *seconds*, 301

configuring, SSH, 44

connection documentation, 35

connectivity problems
branch site Internet connectivity problems after EIGRP reconfiguration, 302-309
information gathering, SECHNIK Networking, 124-126
Internet connectivity problems, SECHNIK Networking, 153-162
IP connectivity to headquarters, 364-369
IP SLA test not starting, 345-349
IPv6 connectivity problems, Bank of POLONA, 353-364
lack of backup Internet connectivity through GW2, 174-182
lack of connectivity to SRV2, 335-340
OSPF neighbor relation problems with router R1, 194-202
PC0's connectivity to IPv6 Internet, 378-386

PILE Forensic Accounting, branch connectivity to HQ and the Internet, 258-267

RADULKO Transport

branch router's IPv6 problems, 416-420

IPv6 Internet access, 440-444

VLANs and PCs, 411-416

redundant Internet connectivity test, 314-322

SECHNIK Networking, 118-119, 123-128

analyzing information, eliminating causes, 119-120

information gathering, 119

Internet connectivity problems, 134-141

IPv6 connectivity problems, 131-134

PC2's connectivity problems, 123-128

PC3's connectivity problem, 128-130

proposing hypotheses, 121

proposing/testing hypothesis, 126-127

SSH (Secure Shell), 128-130

testing hypothesis, 121

troubleshooting Ethernet trunks, 122-123

troubleshooting NAT, 127-128

troubleshooting network device interfaces, 130

sporadic Internet connectivity, 212-220, 231-241

SSH (Secure Shell), 141-146

TINC Garbage Disposal

PC1's connectivity problems, 182-187

PC2's connectivity problems, 187-193

sporadic Internet connectivity, 242-249

SSH (Secure Shell), 249-252

unauthorized Telnet access, 322-326

conventions, standardizing, 36

cost-effectiveness, 31

CPU utilization, checking, 87-88

D

debug bgp ipv6 unicast updates, 423

debug cdp, 411

debug commands, 85-86

information gathering, 142-143

debug eigrp packets hello, 85

debug glbp [packets | events | terse | error | all], 241

debug interface *interface-slot/number*, 85

debug ip bgp, 182

debug ip bgp events, 85

debug ip bgp updates, 85, 282

debug ip eigrp packets, 267

debug ip icmp, 85

debug ip ospf adjacency, 85

debug ip ospf events, 85

debug ip packet, 85-86

debug ipv6 eigrp, 420

debug ipv6 rip, 358

debug lldp, 411

debug ospfv3 events, 430

debug spanning-tree bpdu receive, 85

debug tunnel, 369

debug vrrp all, 224

debug vrrp authentication, 224

debug vrrp error, 224

debug vrrp events, 224

debug vrrp packets, 224

debug vrrp state, 224

default routes

Layer 2 and multilayer devices, 313

redundant default routes, 179-180

defining problems, 17-18

design documentation, 35, 48

device configurations, documentation, 48

devices

failed devices, 32

replacing, 32

installing, 32

df-bit, ping, 82

DHCP (Dynamic Host Configuration Protocol), 288

information gathering, 154-155

troubleshooting, 160

DHCP address problems, SECHNIK Networking, 146-152

DHCP server configuration, 299

DHCP snooping, 152, 248

diagnosing hardware issues, 86-87

checking CPU utilization, 87-88

checking interfaces, 89-92

checking memory utilization, 88-89

diagnosis, 2

diagrams, network documentation, 48

disaster recovery

best practices, 294-296

lack of Internet connectivity after disaster recovery, 287-297

planning for, 36-37

displaying

CEF FIB table content, 140

IP routing tables, content, 139-140

distribute-list access-list, 281

distribute-list prefix-list, 282

divide-and-conquer approach, 5, 8-9, 12

DNS (Domain Name System), troubleshooting, 300

documentation

network documentation, 48-50

network documentation procedures, establishing, 34-35

updating, 49

documenting work, 24

network maintenance, 33

Domain Name System (DNS), troubleshooting, 300

duplicate address problems discovered through log messages, TINC Garbage Disposal, 207-212

dysfunctional stubby branch areas, Bank of POLONA, 386-391

E

EEM (Embedded Event Manager), 110-112

egress interface, 75

EIGRP

branch site Internet connectivity problems after EIGRP reconfiguration, 302-309

for IPv6, troubleshooting, 419-420

redistribution, 340

summarization, 353

EIGRP adjacency, troubleshooting, 266-267

EIGRP autonomous system configuration, 309

EIGRP Debug, 263

EIGRP named configuration, 309

eigrp stub, 306

EIGRP stub configuration, 308

eigrp stub connected, 308

eigrp stub receive-only, 308

eigrp stub redistribute, 308

eigrp stub static, 308

eigrp stub summary, 308

eliminating possible causes, 3, 21

Embedded Event Manager (EEM), 110

equipment lists, 35

erroneous routing information, troubleshooting, 218-220

Eth0/2 configuration, 184

EtherChannel

- misconfigurations, 152
- TINC Garbage Disposal, 224-231
- troubleshooting, 229-231

Ethernet frame forwarding (Layer 2 data plane), 62-67

Ethernet interface status, checking, 276

Ethernet trunks, troubleshooting, 122-123

examples, troubleshooting processes, 25-26

exclude, 78

exporting, NetFlow information, to collectors, 107-108

external route summarization, 374

external routing status, 268-269

F

failed devices, 32

- replacing, 32

fault notification, 109

FHRP (first-hop routing protocol), 344

- tracking options, 344-345
- troubleshooting, 241

FIB, 139

filter-list *as-path-ACL-number*, 282

filtering, show command output, 76-80

follow-the-path approach, 5, 9-10, 13

formalizing change-control procedures, 34

formulating hypothesis, 3

forwarding packets, 138

frame header address fields, Layer 3 routing processes, 72

FTP, performing backup with FTP, 43

G

gathering information, 2, 18-20

GOLD (Generic Online Diagnostics), 92

graphical user interface-based device management, 39

GRE tunnels, troubleshooting, 368-369

H

hardware failures, 86

HSRP, troubleshooting, 211-212

HSRP interface tracking, 344-345

hub-and-spoke topology, 308

hypothesis

- formulating/proposing, 3
- proposing, 21-22
  - *SECHNIK Networking, 121, 126-127*

testing, 3, 23-24

SECHNIK Networking, 121, 126-127

I

IGP (interior routing protocols), 161

incident-driven work, reducing, 30

include, 78

information

analyzing, 3, 20-21

gathering, 2, 18-20

information gathering, 76, 99

collecting real-time information, debug commands, 85-86

connectivity problems, SECHNIK Networking, 124-126

DHCP, 154-155

diagnosing hardware issues, 86-87

checking CPU utilization, 87-88

checking interfaces, 89-92

checking memory utilization, 88-89

IP traceroute, 135

NetFlow, 107-109

SECHNIK Networking, 119-120

connectivity problems, 119

show command, filtering/redirecting output, 76-80

SNMP (Simple Network Management Protocol), 105-107

source-specific ping, 155-156

testing network connectivity

ping, 81-84

Telnet, 84

installing devices, 32

interarea route summarization, 374

interface, 345

interface tracking, VRRP, 340-345

interfaces

checking, 89-92

labeling, 48

interior routing protocols (IGP), 161

Internet access problems, PILE Forensic Accounting, 275-282

Internet connectivity problems, SECHNIK Networking, 134-141, 153-162

IPv6 connectivity problems, 162-166

Internet reachability, checking, 277-278

inter-VLAN routing, troubleshooting, 296-297

IOS commands, IP packet forwarding (Layer 3 data plane), verifying, 73-75

IP address administration, 35

ip config/all, 296

IP connectivity to headquarters, 364-369

ip default-gateway *ip-address*, 313

ip default-network *network-number*, 313

ip flow ingress interface, 107

ip helper-address, 159

IP Input, show processes cpu, 78

IP packet forwarding (Layer 3 data plane), 70-73

verifying, 73-75

ip route, 345

ip route 0.0.0.0.0.0.0.0 {*ip-address* | *interface-type interface-number* [*ip-address*]}, 313

IP routing tables, displaying content, 139-140

IP security option (IPSO), 85

IP SLA, troubleshooting, 349

IP SLA test not starting, 345-349

IP traceroute, 135

IPSO (IP security option), 85

IPv6

- OSPF, troubleshooting, 385-386
- overview, 166

IPv6 connectivity problems

- Bank of POLONA, 353-364, 378-386
- EIGRP, 419-420
- RADULKO Transport, branch routers, 416-420
- SECHNIK Networking, 162-166
- troubleshooting, 131-134
  - *address assignments on clients, 133-134*

IPv6 Internet access, RADULKO Transport, 440-444

K

keywords

- append, 79-80
- begin, 78
- exclude, 78
- include, 78
- longer-prefixes, 77
- redirect, 79-80
- tee, 79-80

L

labeling

- cables, 48
- interfaces, 48

lack of backup Internet connectivity through GW2, 174-182

lack of connectivity to SRV2, 335-340

lack of Internet connectivity after disaster recovery, 287-297

Layer 2, default routes, 313

Layer 2 data plane (Ethernet frame forwarding), 62-67

Layer 2 switching process, 61-62

- Ethernet frame forwarding (Layer 2 data plane), 62-67
- verification, 67-69

Layer 3 data plane (IP packet forwarding), 70-73

Layer 3 routing processes, 69-70

- IP packet forwarding (Layer 3 data plane), 70-73
  - *verifying, 73-75*

Link Layer Discovery Protocol (LLDP), 410-411

link-local address, 385

LLDP (Link Layer Discovery Protocol), 410-411

local prefix advertisement, 279

log messages, duplicate addresses, 207-212

log servers, 39

logging services, 40-41

logging severity levels, 56

longer-prefixes, 77

Loop Guard, 403

M

M (could not fragment), 84

Mac address, Layer 2 switching, 68

MAC addresses, port security, 186-187

maintenance

network maintenance toolkit. *See* network maintenance toolkit

scheduling, 33-34

management access to ASW2, 310-313

management planes, securing, 325-326

maximum transmission unit (MTU), 81, 83

memory, checking utilization, 88-89

misconfigurations, EtherChannel, 152

mitigating unauthorized switches added by employees, 398-403

monitoring, networks, 32

move-the-problem approach, 5

MP-BGP, troubleshooting, 423

MP-BGP sessions, RADULKO Transport, 420-423

MSTP (Multiple Spanning Tree Protocol), 401

MTU (maximum transmission unit), 81, 83

multilayer devices, default routes, 313

multiple masters within VRRP, TINC Garbage Disposal, 220-224

Multiple Spanning Tree Protocol (MSTP), 401

N

NAT (Network Address Translation), 125

troubleshooting, 127-128

NAT Virtual Interface (NVI), 127

neighbor reachability, 269

neighbor relationships, 278

RADULKO Transport, 407-411

NetFlow, 107-109

network device interfaces, troubleshooting, 130

network diagrams, 48

network documentation, 48-50

network documentation procedures, establishing, 34-35

network drawings, 35

network event notification, 109-112

network maintenance, 29-31

incident-driven work, reducing, 30

processes and procedures, 31-32

common maintenance tasks, 32-33

planning. See *planning network maintenance*

network maintenance processes, 47-48

baselines, 48-50

change control, 53

communication, 50-53

network documentation, 48-50

network maintenance toolkit, 37-39

backup servers, 39

command-line device management, 38

graphical user interface-based device management, 39

log servers, 39

logging services, 40-41

network time services, 39-40

performing backup and restore, 42-47

timer servers, 39

network time services, 39-40

network traffic, accounting of, 50

network troubleshooting process, 16

networking monitoring, 32

NMS (SNMP network management station), 106

notifications, network event notification, 109-112

NTP (Network Time Protocol), 39-40

troubleshooting, 286-287

NTP (Network Time Protocol) problems, PILE Forensic Accounting, 282-287

NTP packet debugging, 284

NVI (NAT Virtual Interface), 127

O

OSPF

redistribution, 340

summarization, 374

OSPF adjacency, troubleshooting, 201-202

OSPF Area Border Router (ABR), 372

OSPF for IPv6, troubleshooting, 385-386

OSPF neighbor list, 365

OSPF neighbor relation problems with router R1, TINC Garbage Disposal, 194-202

OSPF stub areas, 391

OSPFv3 address families feature, 429-430

OSPFv3 authentication, RADULKO Transport, 430-433

P

packet header address fields, Layer 3 routing processes, 72

packet sniffers, 101

packets, forwarding, 138

passive-interface, 161-162

passive-interface default, 161

passive-interface *interface* command, 161

passwords, 325

patching, software, 32

PBR (policy-based routing), troubleshooting, 407

PCs, connectivity problems, RADULKO Transport, 411-416

PC1's connectivity problems, TINC Garbage Disposal, 182-187

PC1's problem accessing SRV server at the distribution center, RADULKO Transport, 424-430

PC2's connectivity problems, TINC Garbage Disposal, 187-193

performance measurement, 33

performing backup and restore, 42-47

PILE Forensic Accounting, 257-258

trouble ticket 1, 258

branch connectivity to HQ and the Internet, 258-267

troubleshooting secondary Internet connection through ISP2, 267-274

trouble ticket 2, 274

Internet access problems, 275-282

NTP problems, 282-287

Telnet problems, 274-275

trouble ticket 3, 287

lack of Internet connectivity after disaster recovery, 287-297

problems accessing Cisco.com, 297-302

trouble ticket 4, 302

branch site Internet connectivity problems after EIGRP reconfiguration, 302-309 *management access to ASW2, 310-313*

trouble ticket 5, 313-314

redundant Internet access path through the new HQ0 edge router, 314-322

unauthorized Telnet access, 322-326

ping

symbols, 84

testing network connectivity, 81-84

pipe (|), 78

planning for disaster recovery, 36-37

planning network maintenance, 33

communication, establishing, 35

defining templates/procedures/conventions, 36

disaster recovery, 36-37

establishing network documentation procedures, 34-35

formalizing change-control procedures, 34

scheduling maintenance, 33-34

point-to-point egress interfaces, 138

policy-based routing

RADULKO Transport, 403-407

troubleshooting, 407

port security, 151-152

troubleshooting, 186-187

verifying, 150-151

port-to-VLAN, 69

PortFast, 402

PortFast BPDU Guard, 402

preferred NTP servers, 285-286

prefixes local prefix advertisement, 279

principles of troubleshooting, 1-4

problem reports, 17

problems

defining, 17-18

solving, 24

problems accessing Cisco.com, 297-302

procedures, standardizing, 36

processes

Layer 2 switching process. *See* Layer 2 switching process

Layer 3 routing processes. *See* Layer 3 routing processes

network maintenance, 31-32

common maintenance tasks, 32-33

planning. See *planning network maintenance*

processes of troubleshooting, 2-3, 16-17

analyzing information, 20-21

defining problems, 17-18

eliminating possible causes, 21

examples, 25-26

gathering information, 18-20

network maintenance processes. *See* network maintenance processes

proposing, hypothesis, 21-22

solving problems and documenting work, 24

testing hypothesis, 23-24

proposing hypothesis, 3, 21-22

SECHNIK Networking, 121, 126-127

protocols

CDP (Cisco Discovery Protocol), 410-411

FHRP (first-hop routing protocol), 344

LLDP (Link Layer Discovery Protocol), 410-411

NTP (Network Time Protocol), 39-40

SNMP (Simple Network Management Protocol), 105-107, 110

syslog, 110

VLAN Trunking Protocol (VTP), 415-416

PVRST+, 401

PVST+, 401

Q

Q (source quench), 84

R

RADULKO Transport, 397

trouble ticket 1, 398

mitigating unauthorized switches added by employees, 398-403

neighbor discovery, 407-411

policy-based routing, 403-407

trouble ticket 2, 411

branch router's IPv6 problems, 416-420

MP-BGP sessions, 420-423

VLANs and PCs connectivity problems, 411-416

trouble ticket 3, 424

OSPFv3 authentication, 430-433

PC1's problem accessing SRV server at the distribution center, 424-430

trouble ticket 4, 433

IPv6 Internet access, 440-444

undesired external OSPF routes in DST's routing table, 434-439

Rapid PVST+, 401

redirect, 79-80

| redirect option, 80

redirecting, show command output, 76-80

redistribution, troubleshooting, 339-340

reducing, incident-driven work, 30

redundant default routes, 179-180

redundant Internet connectivity test, 273-274, 314-322

reload in [*hh:*]*mm* [*text*], 301

remote device management, 301-302

Remote Monitoring (RMON), 50

repeat repeat-count, 81

replacing, failed devices, 32

resolution, 345

restore, performing, 42-47

RIB (Routing Information Base), 139

RIPng, troubleshooting, 357-358

RIPv2, 161

RMON (Remote Monitoring), 50

Root Guard, 403

route summarization, 369-374

route-map *route-map-name*, 282

routing, erroneous routing information, 218-220

Routing Information Base (RIB), 139

routing tables, 138

RSPAN (Remote Switched Port Analyzer), 103-105

VLANs, 103-105

running-config, 301, 305

S

scheduling maintenance, 33-34

SECHNIK Networking, 117-118

trouble ticket 1, 118

PC1's connectivity problems, 118-123

PC2's connectivity problems, 122-123

PC3's connectivity problem, 128-130

PC4's IPv6 connectivity problems, 131-134

trouble ticket 2, 134-152

DHCP address problems, 146-152

Internet connectivity problems, 134-141

SSH connectivity problems, 141-146

trouble ticket 3, 152-166

Internet connectivity problems, 162-166

secondary Internet connections through ISP2, troubleshooting, 267-274

section option, 79

securing, management planes, 325-326

security, port security, 151-152

verifying, 150-151

servers

backup servers, 39

log servers, 39

timer servers, 39

services

logging services, 40-41

network time services, 39-40

shoot-from-the-hip, 3

show access-list, 363

show archive, 45

show bgp ipv6 unicast, 423

show bgp ipv6 unicast summary, 423

show cdp, 410

show cdp entry, 410

show cdp interface, 411

show cdp neighbors, 411

show cdp neighbors detail, 411

show cdp traffic, 411

show command, filtering/redirecting output, 76-80

show commands, information gathering, 143

show controllers, 91

show diag, 92

show eigrp address-family {ipv4 | ipv6} [*autonomous-system-number*] [multicast] accounting, 309

show eigrp address-family interfaces detail [*interface-type interface-number*], 309

show eigrp address-family topology route-type summary, 309

show eigrp plugins, 309

show etherchannel *group_number* detail, 230

show etherchannel summary, 230

show frame-relay map, 141

show glbp brief, 241

show glbp interface *type number* [brief], 241

show interfaces, 91

show interfaces switchport, 69

show interfaces trunk, 69, 296

show interfaces Tunnel *tunnel-id*, 369

show inventory, 92

show ip access-list, 363

show ip arp, 140

show ip bgp, 282

show ip bgp neighbors *neighbor-ip-address* [routes | advertised-routes], 282

show ip bgp summary, 182, 282

show ip cache flow, 109

show ip cef exact-route source destination, 75, 140

show ip cef *ip-address*, 74, 140

show ip cef network mask, 75, 140

show ip eigrp interfaces, 267

show ip eigrp neighbors, 267

show ip eigrp topology, 309

show ip interface brief, 296

show ip interface *interface-type interface-number*, 363

show ip interface Tunnel *tunnel-id*, 369

show ip nat translations, 128

show ip ospf neighbor, 215, 366

show ip protocols, 264

show ip route, 77, 311

show ip route *ip-address*, 74, 139

show ip route longer-prefixes, 77

show ip route network mask, 74, 139

show ip route network mask longer-prefixes, 74, 140

show ip route ospfv3, 430

show ip sla application, 345

show ip ssh, 204

show ipv6 access-list, 363

show ipv6 eigrp interfaces, 420

show ipv6 eigrp neighbors, 419

show ipv6 eigrp topology, 420

show ipv6 interface *interface-type interface-number*, 364

show ipv6 ospf *process-id*, 386

show ipv6 protocols, 419

show ipv6 protocols | section rip, 358

show ipv6 rip [*name*] [database], 358

show ipv6 route [rip], 358

show ipv6 route ospf, 430

show lldp, 410

show lldp entry, 410

show lldp interface, 411

show lldp neighbors, 411

show lldp neighbors detail, 411

show lldp traffic, 411

show mac-address-table, 68-69, 187

show memory, 89

show ospfv3, 430

show ospfv3 interface, 430

show ospfv3 neighbor, 430

show platform, 91

show platform forward *interface-id*, 69

show processes cpu, 76, 87

  IP Input, 78

show running-config, 304

show running-config | include [*ACL-number*| *ACL-name*|], 364

show running-config | include interface|access-group, 363

show running-config | include interface|traffic-filter, 363

show running-config | include line|access-class, 363

show running-config | section interface, 430

show running-config | section router, 79 show running-config | section router ospfv3, 430

show spanning-tree, 402

show spanning-tree mst configuration, 402

show spanning-tree summary, 402

show vlan, 69

show vlan [brief], 296

show vlan vlan-id, 296

show vrrp brief, 224

show vrrp interface, 224

size datagram-size, 81

SNMP (Simple Network Management Protocol), 105-107, 110

SNMP network management system (NMS), 106

SNMP traps, 110

software, upgrading, 32

software failures, 86

solving, problems, 24

source [address | interface], ping, 81

source-specific ping, information gathering, 155-156

SPAN (Switched Port Analyzer), 102-103

spanning tree, 399

Spanning Tree Protocol (STP), troubleshooting, 401-403

spanning-tree BPDU Guard, 152

spanning-tree mode, 400

sporadic Internet connectivity, 212-220

- TINC Garbage Disposal, 231-241, 242-249

spot-the-differences approach, 5

SSH (Secure Shell), 128-130

- configuring, 44
- troubleshooting, 206

SSH (Secure Shell) version 2 access, troubleshooting, 202-206

SSH connections, TINC Garbage Disposal, 249-252

SSH connectivity problems, 141-146

standardizing templates/procedures/conventions, 36

static routes, correcting, 319

storing FTP, HTTP usernames and passwords, 43

STP (Spanning Tree Protocol), troubleshooting, 401-403

structured network maintenance, 29-31

structured troubleshooting method, 4, 16

- bottom-up approach, 5, 7-8, 12
- compare-configurations approach, 10, 13
- divide-and-conquer approach, 5, 8-9, 12
- examples, 12-13, 25-26
- follow-the-path approach, 5, 9-10, 13
- move-the-problem approach, 5
- spot-the-differences approach, 5
- swap-components approach, 11, 13
- top-down approach, 4, 6-7, 12

summarization, 350-353

- EIGRP, 353
- OSPF, 374
- route summarization, 369-374

summary, 352

swap-components approach, 13

sweep range of sizes, ping, 83

Switched Port Analyzer (SPAN), 102-103

switches, mitigating unauthorized switches added by employees, 398-403

switching methods, CEF (Cisco Express Forwarding), 141

symbols, ping, 84

syslog, 110

T

TAC (Technical Assistance Center), 248-249

TCP

- connection setup procedures, 145-146
- three-way handshake, 145-146, 270

TDR (Time Domain Reflectometer), 92

tee, 79-80

| tee option, 80

Telnet

- information gathering, 142
- PILE Forensic Accounting, 274-275
- testing network connectivity, 84
- troubleshooting, 206

templates, standardizing, 36

testing network connectivity

- ping, 81-84
- Telnet, 84

three-way handshake, TCP, 145-146, 270

Time Domain Reflectometer (TDR), 92

timer servers, 39

timers, 345

TINC Garbage Disposal, 173

- trouble ticket 1, 174
  - *lack of backup Internet connectivity through GW2, 174-182*
  - *PC1's connectivity problems, 182-187*
  - *PC2's connectivity problems, 187-193*
- trouble ticket 2, 193-194
  - *duplicate address problems discovered through log messages, 207-212*
  - *OSPF neighbor relation problems with router R1, 194-202*
  - *SSH version 2 access, 202-206*
- trouble ticket 3, 212
  - *EtherChannel, 224-231*
  - *sporadic Internet connectivity, 212-220*
- trouble ticket 4, 231
  - *sporadic Internet connectivity, 231-249*
  - *SSH connections, 249-252*

TINC Garbage Disposal trouble ticket 3 multiple masters within VRRP, 220-224

tools

- traffic-capturing, 101-102
- troubleshooting tools. *See* troubleshooting tools

top-down approach to troubleshooting, 4, 6-7, 12

totally stubby areas

- Bank of POLONA, 386-391
- OSPF, 391

traceroute mac, 69

tracking options, FHRP (first-hop routing protocol), 344-345

traffic-capturing, 101-102

- RSPAN (Remote Switched Port Analyzer), 103-105
- SPAN (Switched Port Analyzer), 102-103

trap receivers, 111

troubleshooting

- AAA, 377-378
- ACL (access control lists), 362-364

BGP, 281-282
BGP neighbor relationships, 181-182
BGP route selection, 321-322
DHCP, 160
DNS (Domain Name System), 300
EIGRP adjacency, 266-267
EIGRP summarization, 353
erroneous routing information, 218-220
error-disabled ports, 151-152
EtherChannel, 229-231
Ethernet trunks, SECHNIK Networking, 122-123
FHRP (first-hop routing protocol), 241
GRE tunnels, 368-369
HSRP, 211-212
inter-VLAN routing, 296-297
IP SLA, 349
IPv6 address assignment on clients, 133-134
MP-BGP, 423
NAT (Network Address Translation), SECHNIK Networking, 127-128
network device interfaces, 130
network layer connectivity, 138-141
NTP (Network Time Protocol), 286-287
OSPF adjacency, 201-202
OSPF for IPv6, 385-386
OSPFv3 address families feature, 429-430
policy-based routing, 407
port security, 186-187
redistribution, 339-340
RIPng, 357-358
secondary Internet connections through ISP2, 267-274
SSH (Secure Shell), 206
SSH (Secure Shell) version 2 access, 202-206
STP (Spanning Tree Protocol), 401-403
Telnet, 206
VLANs, 192-193
VRRP, 224

troubleshooting approaches, 4-5
bottom-up approach, 5, 7-8, 12
compare-configurations approach, 10, 13
divide-and-conquer approach, 5, 8-9, 12
examples, 12-13
follow-the-path approach, 5, 9-10, 13
move-the-problem approach, 5
spot-the-differences approach, 5
swap-components approach, 11, 13
top-down approach to troubleshooting, 4, 6-7, 12

troubleshooting principles, 1-4

troubleshooting processes, 2-3, 16-17
analyzing information, 20-21
communication, 51-52
defining problems, 17-18
eliminating possible causes, 21
examples, 25-26
gathering information, 18-20
proposing, hypothesis, 21-22
solving problems and documenting work, 24
testing hypothesis, 23-24

troubleshooting tools
categories of, 100-101
network event notification, 109-112

traffic-capturing, 101-102
RSPAN (Remote Switched Port Analyzer), 103-105
SPAN (Switched Port Analyzer), 102-103

U

U, symbols in ping, 84
UDLD (unidirectional link detection), 152
unauthorized Telnet access, 322-326
undesired external OSPF routes in DST's routing table, RADULKO Transport, 434-439
unidirectional link detection (UDLD), 152
updating documentation, 49
upgrading software, 32

V-W-X-Y-Z

verifying
IP packet forwarding (Layer 3 data plane), 73-75
Layer 2 switching, 67-69
port security, 150-151
VLAN Trunking Protocol (VTP), 415-416
VLANs
connectivity problems, RADULKO Transport, 411-416
RSPAN (Remote Switched Port Analyzer), 103-105
troubleshooting, 192-193
VRRP
interface tracking, 340-345
multiple masters within VRRP, 220-224
troubleshooting, 224
VTP (VLAN Trunking Protocol), 415-416
vty lines, 322

PEARSON ALWAYS LEARNING

PEARSON IT CERTIFICATION

Browse by Exams ▾ | Browse by Technology ▾ | Browse by Format | Explore ▾ | I'm New Here – Help!
Store | Forums | Safari Books Online

Pearson IT Certification
THE LEADER IN IT CERTIFICATION LEARNING TOOLS

Visit **pearsonITcertification.com** today to find:

- IT CERTIFICATION EXAM information and guidance for

CISCO CompTIA Microsoft vmware

Pearson is the official publisher of Cisco Press, IBM Press, VMware Press and is a Platinum CompTIA Publishing Partner—CompTIA's highest partnership accreditation

- EXAM TIPS AND TRICKS from Pearson IT Certification's expert authors and industry experts, such as
  - *Mark Edward Soper* – CompTIA
  - *David Prowse* – CompTIA
  - *Wendell Odom* – Cisco
  - *Kevin Wallace* – Cisco and CompTIA
  - *Shon Harris* – Security
  - *Thomas Erl* – SOACP

- SPECIAL OFFERS – **pearsonITcertification.com/promotions**
- REGISTER your Pearson IT Certification products to access additional online material and receive a coupon to be used on your next purchase

Articles & Chapters
Blogs
Books
Cert Flash Cards Online
eBooks
Mobile Apps
Newsletters
Podcasts
Question of the Day
Rough Cuts
Short Cuts
Software Downloads
Videos

CONNECT WITH PEARSON IT CERTIFICATION

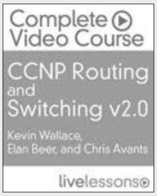
Be sure to create an account on **pearsonITcertification.com** and receive members-only offers and benefits cisco

Cisco Press

NEW Complete Video Courses for CCNP Routing & Switching 300 Series Exams

These unique products include multiple types of video presentations, including:

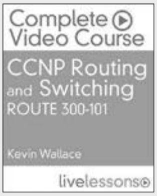
- Live instructor whiteboarding
- Real-world demonstrations
- Animations of network activity
- Dynamic KeyNote presentations
- Doodle videos
- Hands-on command-line interface (CLI) demonstrations
- Review quizzes



Complete Video Course
CCNP Routing and Switching v2.0
Kevin Wallace, Elan Beer, and Chris Avants
livelessons

9780789754493

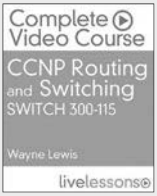
CCNP Routing and Switching v2.0 — Complete Video Course Library
Specially priced library including ALL THREE Complete Video Courses: *CCNP Routing and Switching ROUTE 300-101*, *CCNP Routing and Switching SWITCH 300-115*, and *CCNP Routing and Switching TSHOOT 300-135*.



Complete Video Course
CCNP Routing and Switching ROUTE 300-101
Kevin Wallace
livelessons

9780789753731

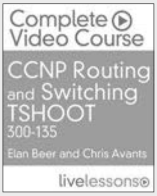
CCNP Routing and Switching ROUTE 300-101 — Complete Video Course
149 VIDEOS with 12+ HOURS of video instruction from best-selling author, expert instructor, and double CCIE Kevin Wallace walk you through the full range of topics on the CCNP Routing and Switching ROUTE 300-101 exam, including fundamental routing concepts; IGP routing protocols including RIPng, EIGRP, and OSPF; route distribution and selection; BGP; IPv6 Internet connectivity; router security; and routing protocol authentication.



Complete Video Course
CCNP Routing and Switching SWITCH 300-115
Wayne Lewis
livelessons

9780789754073

CCNP Routing and Switching SWITCH 300-115 — Complete Video Course
10+ HOURS of unique video training walks you through the full range of topics on the CCNP SWITCH 300-115 exam. This complete video course takes you from the design and architecture of switched networks through the key technologies vital to implementing a robust campus network. You will learn, step-by-step, configuration commands for configuring Cisco switches to control and scale complex switched networks.



Complete Video Course
CCNP Routing and Switching TSHOOT 300-135
Elan Beer and Chris Avants
livelessons

9780789754295

CCNP Routing and Switching TSHOOT 300-135 — Complete Video Course
10+ HOURS of unique video instruction from expert instructors and consultants Elan Beer and Chris Avants walks you through the full range of topics on the CCNP TSHOOT 300-135 exam. This complete video course teaches you the skills you need to plan and perform regular maintenance on complex enterprise routed and switched networks and how to use technology-based practices and a systematic ITIL-compliant approach to perform network troubleshooting commands for configuring Cisco switches to control and scale complex switched networks.

SAVE ON ALL NEW
CCNP R&S 300 Series Products

www.CiscoPress.com/CCNP