Routing and Switching Essentials v6 Companion Guide

Cisco Networking Academy
Copyright © 2017 Cisco Systems, Inc.

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, 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 2016

Library of Congress Control Number: 2016956756

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy Routing and Switching Essentials course. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

The opinions expressed in this book belong to the 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 government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.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.
About the Contributing Authors

**Bob Vachon** is a professor in the Computer Systems Technology program at Cambrian College in Sudbury, Ontario, Canada, where he teaches networking infrastructure courses. He has worked and taught in the computer networking and information technology field since 1984. He has collaborated on various CCNA, CCNA Security, CCNP, and IoT projects for the Cisco Networking Academy as team lead, lead author, and subject matter expert. He enjoys playing guitar and being outdoors.

**Allan Johnson** entered the academic world in 1999 after 10 years as a business owner/operator to dedicate his efforts to his passion for teaching. He holds both an MBA and an M.Ed in training and development. He taught CCNA courses at the high school level for seven years and has taught both CCNA and CCNP courses at Del Mar College in Corpus Christi, Texas. In 2003, Allan began to commit much of his time and energy to the CCNA Instructional Support Team providing services to Networking Academy instructors worldwide and creating training materials. He now works full time for Cisco Networking Academy as Curriculum Lead.
Contents at a Glance

Introduction  xxi

Chapter 1  Routing Concepts  1
Chapter 2  Static Routing  75
Chapter 3  Dynamic Routing  127
Chapter 4  Switched Networks  171
Chapter 5  Switch Configuration  203
Chapter 6  VLANs  245
Chapter 7  Access Control Lists  309
Chapter 8  DHCP  361
Chapter 9  NAT for IPv4  415
Chapter 10  Device Discovery, Management, and Maintenance  475

Appendix A  Answers to the “Check Your Understanding” Questions  541

Glossary  555

Index  575
Contents

Introduction xxi

Chapter 1 Routing Concepts 1

Objectives 1

Key Terms 1

Introduction (1.0.1.1) 3

Router Initial Configuration (1.1) 4

Router Functions (1.1.1) 4

Characteristics of a Network (1.1.1.1) 4

Why Routing? (1.1.1.2) 6

Routers Are Computers (1.1.1.3) 7

Routers Interconnect Networks (1.1.1.4) 9

Routers Choose Best Paths (1.1.1.5) 10

Packet-Forwarding Mechanisms (1.1.1.6) 11

Connect Devices (1.1.2) 14

Connect to a Network (1.1.2.1) 14

Default Gateways (1.1.2.2) 16

Document Network Addressing (1.1.2.3) 17

Enable IP on a Host (1.1.2.4) 18

Device LEDs (1.1.2.5) 19

Console Access (1.1.2.6) 21

Enable IP on a Switch (1.1.2.7) 22

Router Basic Settings (1.1.3) 23

Configure Basic Router Settings (1.1.3.1) 23

Configure an IPv4 Router Interface (1.1.3.2) 24

Configure an IPv6 Router Interface (1.1.3.3) 26

Configure an IPv4 Loopback Interface (1.1.3.4) 29

Verify Connectivity of Directly Connected Networks (1.1.4) 30

Verify Interface Settings (1.1.4.1) 30

Verify IPv6 Interface Settings (1.1.4.2) 32

Filter Show Command Output (1.1.4.3) 35

Command History Feature (1.1.4.4) 36

Routing Decisions (1.2) 37

Switching Packets Between Networks (1.2.1) 37

Router Switching Function (1.2.1.1) 38

Send a Packet (1.2.1.2) 39

Forward to the Next Hop (1.2.1.3) 40

Packet Routing (1.2.1.4) 42

Reach the Destination (1.2.1.5) 43
Types of Static Routes (2.1.2) 80
  Static Route Applications (2.1.2.1) 80
  Standard Static Route (2.1.2.2) 81
  Default Static Route (2.1.2.3) 81
  Summary Static Route (2.1.2.4) 82
  Floating Static Route (2.1.2.5) 83

Configure Static and Default Routes (2.2) 84
  Configure IPv4 Static Routes (2.2.1) 84
    The ip route Command (2.2.1.1) 84
    Next-Hop Options (2.2.1.2) 85
    Configure a Next-Hop Static Route (2.2.1.3) 87
    Configure a Directly Connected Static Route (2.2.1.4) 88
    Configure a Fully Specified Static Route (2.2.1.5) 90
    Verify a Static Route (2.2.1.6) 92
  Configure IPv4 Default Routes (2.2.2) 93
    Default Static Route (2.2.2.1) 93
    Configure a Default Static Route (2.2.2.2) 93
    Verify a Default Static Route (2.2.2.3) 94
  Configure IPv6 Static Routes (2.2.3) 95
    The ipv6 route Command (2.2.3.1) 95
    Next-Hop Options (2.2.3.2) 96
    Configure a Next-Hop Static IPv6 Route (2.2.3.3) 99
    Configure a Directly Connected Static IPv6 Route (2.2.3.4) 100
    Configure a Fully Specified Static IPv6 Route (2.2.3.5) 102
    Verify IPv6 Static Routes (2.2.3.6) 103
  Configure IPv6 Default Routes (2.2.4) 104
    Default Static IPv6 Route (2.2.4.1) 104
    Configure a Default Static IPv6 Route (2.2.4.2) 105
    Verify a Default Static Route (2.2.4.3) 105
  Configure Floating Static Routes (2.2.5) 106
    Floating Static Routes (2.2.5.1) 106
    Configure an IPv4 Floating Static Route (2.2.5.2) 107
    Test the IPv4 Floating Static Route (2.2.5.3) 108
    Configure an IPv6 Floating Static Route (2.2.5.4) 110
  Configure Static Host Routes (2.2.6) 111
    Automatically Installed Host Routes (2.2.6.1) 111
    Configure IPv4 and IPv6 Static Host Routes (2.2.6.2) 113

Troubleshoot Static and Default Route (2.3) 115
  Packet Processing with Static Routes (2.3.1) 115
    Static Routes and Packet Forwarding (2.3.1.1) 115
Switch Forwarding Methods (4.2.1.3) 189
Store-and-Forward Switching (4.2.1.4) 190
Cut-Through Switching (4.2.1.5) 191
Switching Domains (4.2.2) 193
Collision Domains (4.2.2.1) 193
Broadcast Domains (4.2.2.2) 194
Alleviating Network Congestion (4.2.2.3) 195

Summary (4.3) 197
Practice 198
Class Activities 198
Check Your Understanding Questions 199

Chapter 5 Switch Configuration 203
Objectives 203
Key Terms 203
Introduction (5.0.1.1) 204

Basic Switch Configuration (5.1) 205
Configure a Switch with Initial Settings (5.1.1) 205
Switch Boot Sequence (5.1.1.1) 205
Recovering from a System Crash (5.1.1.2) 206
Switch LED Indicators (5.1.1.3) 207
Preparing for Basic Switch Management (5.1.1.4) 209
Configuring Basic Switch Management Access with IPv4 (5.1.1.5) 210
Configure Switch Ports (5.1.2) 213
Duplex Communication (5.1.2.1) 213
Configure Switch Ports at the Physical Layer (5.1.2.2) 214
Auto-MDIX (5.1.2.3) 215
Verifying Switch Port Configuration (5.1.2.4) 216
Network Access Layer Issues (5.1.2.5) 218
Troubleshooting Network Access Layer Issues (5.1.2.6) 221

Switch Security (5.2) 222
Secure Remote Access (5.2.1) 222
SSH Operation (5.2.1.1) 222
Configuring SSH (5.2.1.2) 225
Verifying SSH (5.2.1.3) 227
Switch Port Security (5.2.2) 229
Secure Unused Ports (5.2.2.1) 229
Port Security: Operation (5.2.2.2) 230
Chapter 6  VLANs  245

Objectives  245

Key Terms  245

Introduction (6.0.1.1)  247

VLAN Segmentation (6.1)  248

Overview of VLANs (6.1.1)  248
  VLAN Definitions (6.1.1.1)  248
  Benefits of VLANs (6.1.1.2)  249
  Types of VLANs (6.1.1.3)  250
  Voice VLANs (6.1.1.4)  252

VLANs in a Multiswitched Environment (6.1.2)  253
  VLAN Trunks (6.1.2.1)  253
  Controlling Broadcast Domains with VLANs (6.1.2.2)  254
  Tagging Ethernet Frames for VLAN Identification (6.1.2.3)  256
  Native VLANs and 802.1Q Tagging (6.1.2.4)  257
  Voice VLAN Tagging (6.1.2.5)  258

VLAN Implementations (6.2)  260

VLAN Assignment (6.2.1)  260
  VLAN Ranges on Catalyst Switches (6.2.1.1)  260
  Creating a VLAN (6.2.1.2)  262
  Assigning Ports to VLANs (6.2.1.3)  263
  Changing VLAN Port Membership (6.2.1.4)  264
  Deleting VLANs (6.2.1.5)  266
  Verifying VLAN Information (6.2.1.6)  267

VLAN Trunks (6.2.2)  270
  Configuring IEEE 802.1Q Trunk Links (6.2.2.1)  270
  Resetting the Trunk to Default State (6.2.2.2)  272
  Verifying Trunk Configuration (6.2.2.3)  273
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshoot VLANs and Trunks (6.2.3)</td>
<td>275</td>
</tr>
<tr>
<td>IP Addressing Issues with VLAN (6.2.3.1)</td>
<td>275</td>
</tr>
<tr>
<td>Missing VLANs (6.2.3.2)</td>
<td>276</td>
</tr>
<tr>
<td>Introduction to Troubleshooting Trunks (6.2.3.3)</td>
<td>278</td>
</tr>
<tr>
<td>Common Problems with Trunks (6.2.3.4)</td>
<td>279</td>
</tr>
<tr>
<td>Incorrect Port Mode (6.2.3.5)</td>
<td>281</td>
</tr>
<tr>
<td>Incorrect VLAN List (6.2.3.6)</td>
<td>284</td>
</tr>
<tr>
<td>Inter-VLAN Routing Using Routers (6.3)</td>
<td>287</td>
</tr>
<tr>
<td>Inter-VLAN Routing Operation (6.3.1)</td>
<td>287</td>
</tr>
<tr>
<td>What Is Inter-VLAN Routing? (6.3.1.1)</td>
<td>287</td>
</tr>
<tr>
<td>Legacy Inter-VLAN Routing (6.3.1.2)</td>
<td>288</td>
</tr>
<tr>
<td>Router-on-a-Stick Inter-VLAN Routing (6.3.1.3)</td>
<td>290</td>
</tr>
<tr>
<td>Configure Legacy Inter-VLAN Routing (6.3.2)</td>
<td>292</td>
</tr>
<tr>
<td>Configure Legacy Inter-VLAN Routing: Preparation (6.3.2.1)</td>
<td>292</td>
</tr>
<tr>
<td>Configure Legacy Inter-VLAN Routing: Switch Configuration (6.3.2.2)</td>
<td>293</td>
</tr>
<tr>
<td>Configure Legacy Inter-VLAN Routing: Router Interface Configuration (6.3.2.3)</td>
<td>294</td>
</tr>
<tr>
<td>Configure Router-on-a-Stick Inter-VLAN Routing (6.3.3)</td>
<td>296</td>
</tr>
<tr>
<td>Configure Router-on-a-Stick: Preparation (6.3.3.1)</td>
<td>296</td>
</tr>
<tr>
<td>Configure Router-on-a-Stick: Switch Configuration (6.3.3.2)</td>
<td>297</td>
</tr>
<tr>
<td>Configure Router-on-a-Stick: Router Subinterface Configuration (6.3.3.3)</td>
<td>298</td>
</tr>
<tr>
<td>Configure Router-on-a-Stick: Verifying Subinterfaces (6.3.3.4)</td>
<td>299</td>
</tr>
<tr>
<td>Configure Router-on-a-Stick: Verifying Routing (6.3.3.5)</td>
<td>300</td>
</tr>
<tr>
<td>Summary (6.4)</td>
<td>303</td>
</tr>
<tr>
<td>Practice</td>
<td>304</td>
</tr>
<tr>
<td>Class Activities</td>
<td>305</td>
</tr>
<tr>
<td>Labs</td>
<td>305</td>
</tr>
<tr>
<td>Packet Tracer Activities</td>
<td>305</td>
</tr>
<tr>
<td>Check Your Understanding Questions</td>
<td>305</td>
</tr>
<tr>
<td>Chapter 7</td>
<td>309</td>
</tr>
<tr>
<td>Access Control Lists</td>
<td>309</td>
</tr>
<tr>
<td>Objectives</td>
<td>309</td>
</tr>
<tr>
<td>Key Terms</td>
<td>309</td>
</tr>
<tr>
<td>Introduction (7.0.1.1)</td>
<td>310</td>
</tr>
<tr>
<td>ACL Operation (7.1)</td>
<td>310</td>
</tr>
<tr>
<td>Purpose of ACLs (7.1.1)</td>
<td>311</td>
</tr>
</tbody>
</table>
What Is an ACL? (7.1.1) 311
Packet Filtering (7.1.2) 312
ACL Operation (7.1.3) 313
Wildcard Masks in ACLs (7.2) 314
   Introducing ACL Wildcard Masking (7.2.1) 314
   Wildcard Mask Examples (7.2.2) 316
   Calculating the Wildcard Mask (7.2.3) 317
   Wildcard Mask Keywords (7.2.4) 319
   Wildcard Mask Keyword Examples (7.2.5) 320
Guidelines for ACL Creation (7.3) 321
   General Guidelines for Creating ACLs (7.3.1) 321
   ACL Best Practices (7.3.2) 322
Guidelines for ACL Placement (7.4) 322
   Where to Place ACLs (7.4.1) 322
   Standard ACL Placement (7.4.2) 324
Standard IPv4 ACLs (7.2) 325
   Configure Standard IPv4 ACLs (7.2.1) 325
      Numbered Standard IPv4 ACL Syntax (7.2.1.1) 325
      Applying Standard IPv4 ACLs to Interfaces (7.2.1.2) 328
      Numbered Standard IPv4 ACL Examples (7.2.1.3) 329
      Named Standard IPv4 ACL Syntax (7.2.1.4) 330
   Modify IPv4 ACLs (7.2.2) 332
      Method 1: Use a Text Editor (7.2.2.1) 333
      Method 2: Use Sequence Numbers (7.2.2.2) 334
      Editing Standard Named ACLs (7.2.2.3) 335
      Verifying ACLs (7.2.2.4) 336
      ACL Statistics (7.2.2.5) 338
   Securing VTY Ports with a Standard IPv4 ACL (7.2.3) 339
      The access-class Command (7.2.3.1) 339
      Verifying the VTY Port Is Secured (7.2.3.2) 341
Troubleshoot ACLs (7.3) 342
   Processing Packets with ACLs (7.3.1) 342
      The Implicit Deny Any (7.3.1.1) 343
      The Order of ACEs in an ACL (7.3.1.2) 343
      Cisco IOS Reorders Standard ACLs (7.3.1.3) 344
      Routing Processes and ACLs (7.3.1.4) 347
   Common IPv4 Standard ACL Errors (7.3.2) 349
      Troubleshooting Standard IPv4 ACLs—
         Example 1 (7.3.2.1) 349
      Troubleshooting Standard IPv4 ACLs—
         Example 2 (7.3.2.2) 351
      Troubleshooting Standard IPv4 ACLs—
         Example 3 (7.3.2.3) 352
Chapter 8  DHCP  361

Objectives  361

Key Terms  361

Introduction (8.0.1.1)  363

DHCPv4 (8.1)  363

DHCPv4 Operation (8.1.1)  363
  Introducing DHCPv4 (8.1.1.1)  364
  DHCPv4 Operation (8.1.1.2)  364
  DHCPv4 Message Format (8.1.1.3)  367
  DHCPv4 Discover and Offer Messages (8.1.1.4)  369
  Configuring a Basic DHCPv4 Server (8.1.2)  370
    Configuring a Basic DHCPv4 Server (8.1.2.1)  370
    Verifying DHCPv4 (8.1.2.2)  373
    DHCPv4 Relay (8.1.2.3)  377
  Configure DHCPv4 Client (8.1.3)  380
    Configuring a Router as a DHCPv4 Client (8.1.3.1)  380
    Configuring a Wireless Router as a DHCPv4 Client (8.1.3.2)  381
  Troubleshoot DHCPv4 (8.1.4)  382
    Troubleshooting Tasks (8.1.4.1)  382
    Verify Router DHCPv4 Configuration (8.1.4.2)  384
    Debugging DHCPv4 (8.1.4.3)  385

DHCPv6 (8.2)  387

SLAAC and DHCPv6 (8.2.1)  387
  Stateless Address Autoconfiguration (SLAAC) (8.2.1.1)  387
  SLAAC Operation (8.2.1.2)  389
  SLAAC and DHCPv6 (8.2.1.3)  390
  SLAAC Option (8.2.1.4)  391
  Stateless DHCPv6 Option (8.2.1.5)  392
  Stateful DHCPv6 Option (8.2.1.6)  393
  DHCPv6 Operations (8.2.1.7)  394
  Stateless DHCPv6 (8.2.2)  395
Device Discovery (10.1)  477
Device Discovery with CDP (10.1.1)  477
  CDP Overview (10.1.1.1)  477
  Configure and Verify CDP (10.1.1.2)  478
  Discover Devices Using CDP (10.1.1.3)  480
Device Discovery with LLDP (10.1.2)  483
  LLDP Overview (10.1.2.1)  483
  Configure and Verify LLDP (10.1.2.2)  484
  Discover Devices Using LLDP (10.1.2.3)  484

Device Management (10.2)  486
NTP (10.2.1)  487
  Setting the System Clock (10.2.1.1)  487
  NTP Operation (10.2.1.2)  488
  Configure and Verify NTP (10.2.1.3)  489
Syslog Operation (10.2.2)  491
  Introduction to Syslog (10.2.2.1)  491
  Syslog Operation (10.2.2.2)  492
  Syslog Message Format (10.2.2.3)  493
  Service Timestamp (10.2.2.4)  496
Syslog Configuration (10.2.3)  497
  Syslog Server (10.2.3.1)  497
  Default Logging (10.2.3.2)  497
  Router and Switch Commands for Syslog Clients (10.2.3.3)  499
  Verifying Syslog (10.2.3.4)  500

Device Maintenance (10.3)  502
Router and Switch File Maintenance (10.3.1)  502
  Router File Systems (10.3.1.1)  502
  Switch File Systems (10.3.1.2)  505
  Backing Up and Restoring Using Text Files (10.3.1.3)  505
  Backing Up and Restoring TFTP (10.3.1.4)  507
  Using USB Ports on a Cisco Router (10.3.1.5)  508
  Backing Up and Restoring Using a USB (10.3.1.6)  508
  Password Recovery (10.3.1.7)  511
IOS System Files (10.3.2)  514
  IOS 15 System Image Packaging (10.3.2.1)  514
  IOS Image Filenames (10.3.2.2)  515
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).
Introduction

Routing and Switching Essentials v6 Companion Guide is the official supplemental textbook for the Cisco Network Academy CCNA Routing and Switching Essentials course. Cisco Networking Academy is a comprehensive program that delivers information technology skills to students around the world. The curriculum emphasizes real-world practical application, while providing opportunities for you to gain the skills and hands-on experience needed to design, install, operate, and maintain networks in small- to medium-sized businesses, as well as enterprise and service provider environments.

As a textbook, this book provides a ready reference to explain the same networking concepts, technologies, protocols, and devices as the online curriculum. This book emphasizes key topics, terms, and activities and provides some alternate explanations and examples as compared with the course. You can use the online curriculum as directed by your instructor and then use this Companion Guide's study tools to help solidify your understanding of all the topics.

Who Should Read This Book

The book, as well as the course, is designed as an introduction to data network technology for those pursuing careers as network professionals as well as those who need only an introduction to network technology for professional growth. Topics are presented concisely, starting with the most fundamental concepts and progressing to a comprehensive understanding of network communication. The content of this text provides the foundation for additional Cisco Networking Academy courses and preparation for the CCENT and CCNA Routing and Switching certifications.

Book Features

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

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

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

- **Notes**—These are short sidebars that point out interesting facts, timesaving methods, and important safety issues.

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

- **Practice**—At the end of chapters is a full list of all the labs, class activities, and Packet Tracer activities to refer back to for study time.

Readability

The following features have been updated to assist your understanding of the networking vocabulary:

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

- **Glossary**—This book contains an all-new Glossary with more than 200 terms.

Practice

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

- **Check Your Understanding questions and answer key**—Review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions that you see in the online course. Appendix A, “Answers to the ‘Check Your Understanding’ Questions,” provides an answer key to all the questions and includes an explanation of each answer.
**Labs and activities**—Throughout each chapter, you will be directed back to the online course to take advantage of the activities created to reinforce concepts. In addition, at the end of each chapter, there is a practice section that collects a list of all the labs and activities to provide practice with the topics introduced in this chapter. The Labs, class activities, and Packet Tracer instructions are available in the companion *Routing and Switching Essentials v6 Labs & Study Guide* (ISBN 9781587134265). The Packet Tracer PKA files are found in the online course.

**Page references to online course**—After headings, you will see, for example, (1.1.2.3). This number refers to the page number in the online course so that you can easily jump to that spot online to view a video, practice an activity, perform a lab, or review a topic.

## Lab Study Guide

The supplementary book *Routing and Switching Essentials v6 Labs & Study Guide*, by Allan Johnson (ISBN 9781587134265) includes a Study Guide section and a Lab section for each chapter. The Study Guide section offers exercises that help you learn the concepts, configurations, and troubleshooting skill crucial to your success as a CCNA exam candidate. Some chapters include unique Packet Tracer activities available for download from the book’s companion website. The Labs and Activities section contains all the labs, class activities, and Packet Tracer instructions from the course.

## About Packet Tracer Software and Activities

Interspersed throughout the chapters you’ll find many activities to work with the Cisco Packet Tracer tool. Packet Tracer allows you to create networks, visualize how packets flow in the network, and use basic testing tools to determine whether the network would work. When you see this icon, you can use Packet Tracer with the listed file to perform a task suggested in this book. The activity files are available in the course. Packet Tracer software is available through the Cisco Networking Academy website. Ask your instructor for access to Packet Tracer.

## Companion Website

Register this book to get information about Packet Tracer and access to other study materials plus additional bonus content to help you succeed with this course and the certification exam. Check this site regularly for any updates or errata that might
become available for this book. Be sure to check the box that you would like to hear from us to receive news of updates and exclusive discounts on related products.

To access this companion website, follow these steps:

1. Go to www.ciscopress.com/register and log in or create a new account.
2. Enter the ISBN: 9781587134289.
3. Answer the challenge question as proof of purchase.
4. Click the “Access Bonus Content” link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files. If you are unable to locate the files for this title by following the steps, please visit www.ciscopress.com/contact and select Site Problems/Comments under the Select a Topic drop-down.

How This Book Is Organized

This book corresponds closely to the Cisco Academy Routing and Switching Essentials course and is divided into 10 chapters, one appendix, and a glossary of key terms:

- **Chapter 1, “Routing Concepts”**: Introduces basic routing concepts including how to complete an initial router configuration and how routers make decisions. Routers use the routing table to determine the next hop for a packet. This chapter explores how the routing table is built with connected, statically learned, and dynamically learned routes.

- **Chapter 2, “Static Routing”**: Focuses on the configuration, verification, and troubleshooting of static routes for IPv4 and IPv6, including default routes, floating static routes, and static host routes.

- **Chapter 3, “Dynamic Routing”**: Introduces all the important IPv4 and IPv6 dynamic routing protocols. RIPv2 is used to demonstrate basic routing protocol configuration. The chapter concludes with an in-depth analysis of the IPv4 and IPv6 routing tables and the route lookup process.

- **Chapter 4, “Switched Networks”**: Introduces the concepts of a converged network, hierarchical network design, and the role of switches in the network. Switching operation, including frame forwarding, broadcast domains, and collision domains, is discussed.

- **Chapter 5, “Switch Configuration”**: Focuses on the implementation of a basic switch configuration, verifying the configuration, and troubleshooting the
configuration. Switch security is then discussed, including configuring secure remote access with SSH and securing switch ports.

- Chapter 6, “VLANs”: Introduces the concepts of VLANs, including how VLANs segment broadcast domains. VLAN implementation, including configuration, verification, and troubleshooting, is then covered. The chapter concludes with configuring router-on-a-stick inter-VLAN routing.

- Chapter 7, “Access Control Lists”: Introduces the concept of using ACLs to filter traffic. Configuration, verification, and troubleshooting of standard IPv4 ACLs are covered. Securing remote access with an ACL is also discussed.

- Chapter 8, “DHCP”: Dynamically assigning IP addressing to hosts is introduced. The operation of DHCPv4 and DHCPv6 is discussed. Configuration, verification, and troubleshooting of DHCPv4 and DHCPv6 implementations are covered.

- Chapter 9, “NAT for IPv4”: Translating private IPv4 addresses to another IPv4 address using NAT for IPv4 is introduced. Configuration, verification, and troubleshooting of NAT for IPv4 are covered.

- Chapter 10, “Device Discovery, Management, and Maintenance”: Introduces the concept of device discovery using CDP and LLDP. Device management topics include NTP and Syslog. The chapter concludes with a discussion of how to manage IOS and configuration files as well as IOS licenses.

- Appendix A, “Answers to the ‘Check Your Understanding’ Questions”: This appendix lists the answers to the “Check Your Understanding” review questions that are included at the end of each chapter.

- Glossary: The glossary provides definitions for all the key terms identified in each chapter.
Objectives

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

- What are the primary functions and features of a router?
- How do you connect devices for a small, routed network?
- How do you configure basic settings on a router to route between two directly connected networks, using CLI?
- How do you verify connectivity between two networks that are directly connected to a router?
- What is the encapsulation and de-encapsulation process used by routers when switching packets between interfaces?
- What is the path determination function of a router?
- What are the routing table entries for directly connected networks?
- How does a router build a routing table of directly connected networks?
- How does a router build a routing table using static routes?
- How does a router build a routing table using a dynamic routing protocol?

Key Terms

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

- topology Page 5
- physical topology Page 5
- logical topology Page 5
- speed Page 5
- availability Page 5
- scalability Page 5
- reliability Page 6
- mean time between failures (MTBF) Page 6
- routing table Page 7
- IOS Page 7
- volatile Page 7
- nonvolatile Page 7
- RAM Page 8
- ROM Page 8
- NVRAM Page 8
- flash Page 8
- Point-to-Point Protocol (PPP) Page 10
- static routes Page 11
- dynamic routing protocols Page 11
- process switching Page 11
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast switching</td>
<td>12</td>
</tr>
<tr>
<td>Fast-switching cache</td>
<td>12</td>
</tr>
<tr>
<td>Cisco Express Forwarding (CEF)</td>
<td>12</td>
</tr>
<tr>
<td>Forwarding Information Base (FIB)</td>
<td>12</td>
</tr>
<tr>
<td>Adjacency table</td>
<td>12</td>
</tr>
<tr>
<td>VoIP</td>
<td>15</td>
</tr>
<tr>
<td>Wireless access points (WAP)</td>
<td>15</td>
</tr>
<tr>
<td>Gateway of Last Resort</td>
<td>17</td>
</tr>
<tr>
<td>USB-to-RS-232 compatible serial port adapter</td>
<td>21</td>
</tr>
<tr>
<td>USB Type-A to USB Type-B (mini-B USB)</td>
<td>21</td>
</tr>
<tr>
<td>Switched virtual interface (SVI)</td>
<td>22</td>
</tr>
<tr>
<td>High-Speed WAN Interface Card (HWIC) slots</td>
<td>24</td>
</tr>
<tr>
<td>IPv6 link-local address</td>
<td>26</td>
</tr>
<tr>
<td>IPv6 global unicast address</td>
<td>26</td>
</tr>
<tr>
<td>EUI-64</td>
<td>27</td>
</tr>
<tr>
<td>Loopback interface</td>
<td>29</td>
</tr>
<tr>
<td>PPP</td>
<td>39</td>
</tr>
<tr>
<td>ICMPv6 Neighbor Solicitation and Neighbor Advertisement messages</td>
<td>40</td>
</tr>
<tr>
<td>Neighbor cache</td>
<td>40</td>
</tr>
<tr>
<td>Metric</td>
<td>45</td>
</tr>
<tr>
<td>Equal cost load balancing</td>
<td>46</td>
</tr>
<tr>
<td>Unequal cost load balancing</td>
<td>47</td>
</tr>
<tr>
<td>Administrative distance (AD)</td>
<td>47</td>
</tr>
<tr>
<td>Directly connected routes</td>
<td>49</td>
</tr>
<tr>
<td>Remote routes</td>
<td>49</td>
</tr>
<tr>
<td>Local route interfaces</td>
<td>50</td>
</tr>
<tr>
<td>Directly connected interfaces</td>
<td>50</td>
</tr>
<tr>
<td>Default static route</td>
<td>58</td>
</tr>
</tbody>
</table>
Introduction (1.0.1.1)

Networks allow people to communicate, collaborate, and interact in many ways. Networks are used to access web pages, talk using IP telephones, participate in video conferences, compete in interactive gaming, shop using the Internet, complete online coursework, and more.

Ethernet switches function at the data link layer, Layer 2, and are used to forward Ethernet frames between devices within the same network. However, when the source IP and destination IP addresses are on different networks, the Ethernet frame must be sent to a router.

A router connects one network to another network. The router is responsible for the delivery of packets across different networks. The destination of the IP packet might be a web server in another country or an email server on the LAN.

The router uses its routing table to determine the best path to use to forward a packet. It is the responsibility of the routers to deliver those packets in a timely manner. The effectiveness of internetwork communications depends, to a large degree, on the ability of routers to forward packets in the most efficient way possible.

When a host sends a packet to a device on a different IP network, the packet is forwarded to the default gateway because a host device cannot communicate directly with devices outside of the local network. The default gateway is the intermediary device that routes traffic from the local network to devices on remote networks. It is often used to connect a local network to the Internet.

This chapter will answer the question, “What does a router do with a packet received from one network and destined for another network?” Details of the routing table will be examined, including connected, static, and dynamic routes.

Because the router can route packets between networks, devices on different networks can communicate. This chapter introduces the router, its role in networks, its main hardware and software components, and the routing process. Exercises that demonstrate how to access the router, configure basic router settings, and verify settings are provided.

Activity 1.0.1.2: Do We Really Need a Map?

This modeling activity asks you to research travel directions from source to destination. Its purpose is to compare those types of directions to network routing directions.

Scenario

Using the Internet and Google Maps, located at http://maps.google.com, find a route between the capital city of your country and some other distant town or between
two places within your own city. Pay close attention to the driving or walking
directions that Google Maps suggests.

Notice that in many cases, Google Maps suggests more than one route between the
two locations you chose. It also allows you to put additional constraints on the route,
such as avoiding highways or tolls.

Copy at least two route instructions supplied by Google Maps for this activity. Place
your copies into a word processing document and save it for use with the next step.

Open the .pdf accompanying this modeling activity and complete it with a fellow
student. Discuss the reflection questions listed on the .pdf and record your answers.

Be prepared to present your answers to the class.

**Router Initial Configuration (1.1)**

A router must be configured with specific settings before it can be deployed. New
routers are not configured. They must be initially configured using the console port.

In this section, you learn how to configure basic settings on a router.

**Router Functions (1.1.1)**

Modern routers are capable of providing many network connectivity functions. The
focus of this topic is to examine how routers route packets to their destinations.

**Characteristics of a Network (1.1.1.1)**

Networks have had a significant impact on our lives. They have changed the way we
live, work, and play. They allow us to communicate, collaborate, and interact in
ways we never did before. We use the network in a variety of ways, including
web applications, IP telephony, video conferencing, interactive gaming, electronic
commerce, education, and more.

As shown in Figure 1-1, there are many key structures and performance-related
characteristics referred to when discussing networks:
Figure 1-1 Network Characteristics

- **Topology**—There are physical and logical topologies. The *physical topology* is the arrangement of the cables, network devices, and end systems. It describes how the network devices are actually interconnected with wires and cables. The *logical topology* is the path over which the data is transferred in a network. It describes how the network devices appear connected to network users.

- **Speed**—Speed is a measure of the data rate in bits per second (b/s) of a given link in the network.

- **Cost**—Cost indicates the general expense for purchasing of network components, and installation and maintenance of the network.

- **Security**—Security indicates how protected the network is, including the information that is transmitted over the network. The subject of security is important, and techniques and practices are constantly evolving. Consider security whenever actions are taken that affect the network.

- **Availability**—Availability is the likelihood that the network is available for use when it is required.

- **Scalability**—Scalability indicates how easily the network can accommodate more users and data transmission requirements. If a network design is optimized to only meet current requirements, it can be very difficult and expensive to meet new needs when the network grows.
- **Reliability**—Reliability indicates the dependability of the components that make up the network, such as the routers, switches, PCs, and servers. Reliability is often measured as a probability of failure or as the *mean time between failures (MTBF)*.

These characteristics and attributes provide a means to compare different networking solutions.

**Note**

Although the term “speed” is commonly used when referring to the network bandwidth, it is not technically accurate. The actual speed that the bits are transmitted does not vary over the same medium. The difference in bandwidth is due to the number of bits transmitted per second, not how fast they travel over wire or wireless medium.

**Why Routing? (1.1.1.2)**

How does clicking a link in a web browser return the desired information in mere seconds? Although there are many devices and technologies collaboratively working together to enable this, the primary device is the router. Stated simply, a router connects one network to another network.

Communication between networks would not be possible without a router determining the best path to the destination and forwarding traffic to the next router along that path. The router is responsible for the routing of traffic between networks.

In the topology in Figure 1-2, the routers interconnect the networks at the different sites.
When a packet arrives on a router interface, the router uses its routing table to determine how to reach the destination network. The destination of the IP packet might be a web server in another country or an email server on the LAN. It is the responsibility of routers to deliver those packets efficiently. The effectiveness of internetwork communications depends, to a large degree, on the ability of routers to forward packets in the most efficient way possible.

**Routers Are Computers (1.1.1.3)**

Most network-capable devices (such as computers, tablets, and smartphones) require the following components to operate, as shown in Figure 1-3:

- **CPU**
- Operating system (OS)
- Memory and storage (RAM, ROM, NVRAM, Flash, hard drive)

![Figure 1-3](image)

**Figure 1-3** The Router Connection

A router is essentially a specialized computer. It requires a CPU and memory to temporarily and permanently store data to execute operating system instructions, such as system initialization, routing functions, and switching functions.

Cisco devices also require an OS; Cisco devices commonly use the Cisco **IOS** as its system software.

Router memory is classified as **volatile** or **nonvolatile**. Volatile memory loses its content when the power is turned off, whereas nonvolatile memory does not lose its content when the power is turned off.

Table 1-1 summarizes the types of router memory, the volatility, and examples of what is stored in each.
### Table 1-1 Router Memory

<table>
<thead>
<tr>
<th>Memory</th>
<th>Description</th>
</tr>
</thead>
</table>
| **RAM** | Volatile memory that provides temporary storage for various applications and processes including the following:  
- Running IOS  
- Running configuration file  
- IP routing and ARP tables  
- Packet buffer |
| **ROM** | Nonvolatile memory that provides permanent storage for the following:  
- Bootup instructions  
- Basic diagnostic software  
- Limited IOS in case the router cannot load the full-featured IOS |
| **NVRAM** | Nonvolatile memory that provides permanent storage for the following:  
- Startup configuration file (startup-config) |
| **Flash** | Nonvolatile memory that provides permanent storage for the following:  
- IOS  
- Other system-related files |

Unlike a computer, a router does not have video adapters or sound card adapters. Instead, routers have specialized ports and network interface cards to interconnect devices to other networks. Figure 1-4 identifies some of these ports and interfaces found on a Cisco 1941 Integrated Service Router (ISR).

![Figure 1-4 Back Panel of a Router](image-url)
Routers Interconnect Networks (1.1.1.4)

Most users are unaware of the presence of numerous routers on their own network or on the Internet. Users expect to be able to access web pages, send emails, and download music, regardless of whether the server accessed is on their own network or on another network. Networking professionals know that it is the router that is responsible for forwarding packets from network to network, from the original source to the final destination.

A router connects multiple networks, which means that it has multiple interfaces that each belong to a different IP network. When a router receives an IP packet on one interface, it determines which interface to use to forward the packet to the destination. The interface that the router uses to forward the packet may be the final destination, or it may be a network connected to another router that is used to reach the destination network.

In Figure 1-5, routers R1 and R2 are responsible for receiving the packet on one network and forwarding the packet out another network toward the destination network.

Each network that a router connects to typically requires a separate interface. These interfaces are used to connect a combination of both LANs and WANs. LANs are commonly Ethernet networks that contain devices, such as PCs, printers, and servers. WANs are used to connect networks over a large geographical area. For example, a WAN connection is commonly used to connect a LAN to the Internet service provider (ISP) network.

Notice that each site in Figure 1-6 requires the use of a router to interconnect to other sites. Even the Home Office requires a router. In this topology, the router located at the Home Office is a specialized device that performs multiple services for the home network.
Following are the primary functions of a router:

- Determine the best path to send packets
- Forward packets toward their destination

The router uses its routing table to determine the best path to use to forward a packet. When the router receives a packet, it examines the destination address of the packet and uses the routing table to search for the best path to that network. The routing table also includes the interface to be used to forward packets for each known network. When a match is found, the router encapsulates the packet into the data link frame of the outgoing or exit interface, and the packet is forwarded toward its destination.

It is possible for a router to receive a packet that is encapsulated in one type of data link frame and to forward the packet out of an interface that uses a different type of data link frame. For example, a router may receive a packet on an Ethernet interface, but it must forward the packet out of an interface configured with the Point-to-Point Protocol (PPP). The data link encapsulation depends on the type of interface on the router and the type of medium to which it connects. The different data link technologies that a router can connect to include Ethernet, PPP, Frame Relay, DSL, cable, and wireless (802.11, Bluetooth, and so on).
In Figure 1-7, notice that it is the responsibility of the router to find the destination network in its routing table and forward the packet toward its destination.

![Figure 1-7 How the Router Works](image)

In this example, router R1 receives the packet encapsulated in an Ethernet frame. After de-encapsulating the packet, R1 uses the destination IP address of the packet to search its routing table for a matching network address. After a destination network address is found in the routing table, R1 encapsulates the packet inside a PPP frame and forwards the packet to R2. R2 performs a similar process.

**Note**

Routers use *static routes* and *dynamic routing protocols* to learn about remote networks and build their routing tables.

**Packet-Forwarding Mechanisms (1.1.6)**

Routers support three packet-forwarding mechanisms:

- **Process switching**—Shown in Figure 1-8, this is an older packet-forwarding mechanism still available for Cisco routers. When a packet arrives on an interface, it is forwarded to the control plane where the CPU matches the destination address with an entry in its routing table, and then it determines the exit interface and forwards the packet. It is important to understand that the router does this for every packet, even if the destination is the same for a stream of packets. This process-switching mechanism is slow and rarely implemented in modern networks.
Fast switching—Shown in Figure 1-9, this is a common packet-forwarding mechanism that uses a fast-switching cache to store next-hop information. When a packet arrives on an interface, it is forwarded to the control plane, where the CPU searches for a match in the fast-switching cache. If it is not there, it is process-switched and forwarded to the exit interface. The flow information for the packet is also stored in the fast-switching cache. If another packet going to the same destination arrives on an interface, the next-hop information in the cache is reused without CPU intervention.

Cisco Express Forwarding (CEF)—Shown in Figure 1-10, CEF is the most recent and preferred Cisco IOS packet-forwarding mechanism. Like fast switching, CEF builds a Forwarding Information Base (FIB), and an adjacency table.
However, the table entries are not packet-triggered like fast switching but change-triggered, such as when something changes in the network topology. Therefore, when a network has converged, the FIB and adjacency tables contain all the information a router would have to consider when forwarding a packet. The FIB contains precomputed reverse lookups, next-hop information for routes including the interface, and Layer 2 information. CEF is the fastest forwarding mechanism and the preferred choice on Cisco routers.

Figure 1-10  Cisco Express Forwarding

Assume that all five packets in a traffic flow are going to the same destination. As shown in Figure 1-8, with process switching, each packet must be processed by the CPU individually. Contrast this with fast switching, shown in Figure 1-9. With fast switching, notice how only the first packet of a flow is process-switched and added to the fast-switching cache. The next four packets are quickly processed based on the information in the fast-switching cache. Finally, in Figure 1-10, CEF builds the FIB and adjacency tables, after the network has converged. All five packets are quickly processed in the data plane.

A common analogy used to describe the three packet-forwarding mechanisms is as follows:

- Process switching solves a problem by doing math long hand, even if it is the identical problem.
- Fast switching solves a problem by doing math long hand one time and remembering the answer for subsequent identical problems.
- CEF solves every possible problem ahead of time in a spreadsheet.
Activity 1.1.1.7: Identify Router Components
Refer to the online course to complete this activity.

Packet Tracer 1.1.1.8: Using Traceroute to Discover the Network
The company you work for has acquired a new branch location. You asked for a topology map of the new location, but apparently one does not exist. However, you have username and password information for the new branch’s networking devices, and you know the web address for the new branch’s server. Therefore, you will verify connectivity and use the tracert command to determine the path to the location. You will connect to the edge router of the new location to determine the devices and networks attached. As a part of this process, you will use various show commands to gather the necessary information to finish documenting the IP addressing scheme and create a diagram of the topology.

Lab 1.1.1.9: Mapping the Internet
In this lab, you will complete the following objectives:
- Part 1: Determine Network Connectivity to a Destination Host
- Part 2: Trace a Route to a Remote Server Using Tracert

Connect Devices (1.1.2)
LAN hosts typically connect to a router using Layer 3 IP addresses. The focus of this topic is to examine how devices connect to a small, routed network.

Connect to a Network (1.1.2.1)
Network devices and end users typically connect to a network using a wired Ethernet or wireless connection. Refer to Figure 1-11 as a sample reference topology. The LANs in the figure serve as an example of how users and network devices can connect to networks.
Home Office devices can connect as follows:

- Laptops and tablets connect wirelessly to a home router.
- A network printer connects using an Ethernet cable to the switch port on the home router.
- The home router connects to the service provider cable modem using an Ethernet cable.
- The cable modem connects to the ISP network.

The Branch site devices connect as follows:

- Corporate resources (that is, file servers and printers) connect to Layer 2 switches using Ethernet cables.
- Desktop PCs and VoIP phones connect to Layer 2 switches using Ethernet cables.
- Laptops and smartphones connect wirelessly to wireless access points (WAP).
- The WAPs connect to switches using Ethernet cables.
- Layer 2 switches connect to an Ethernet interface on the edge router using Ethernet cables. An edge router is a device that sits at the edge or boundary of a network and routes between that network and another, such as between a LAN and a WAN.
- The edge router connects to a WAN service provider (SP).
- The edge router also connects to an ISP for backup purposes.
The Central site devices connect as follows:

- Desktop PCs and VoIP phones connect to Layer 2 switches using Ethernet cables.
- Layer 2 switches connect redundantly to multilayer Layer 3 switches using Ethernet fiber-optic cables (orange connections).
- Layer 3 multilayer switches connect to an Ethernet interface on the edge router using Ethernet cables.
- The corporate website server is connected using an Ethernet cable to the edge router interface.
- The edge router connects to a WAN SP.
- The edge router also connects to an ISP for backup purposes.

In the Branch and Central LANs, hosts are connected either directly or indirectly (via WAPs) to the network infrastructure using a Layer 2 switch.

**Default Gateways (1.1.2.2)**

To enable network access, devices must be configured with IP address information to identify the appropriate:

- **IP address**—Identifies a unique host on a local network.
- **Subnet mask**—Identifies with which network subnet the host can communicate.
- **Default gateway**—Identifies the IP address of the router to send a packet to when the destination is not on the same local network subnet.

When a host sends a packet to a device that is on the same IP network, the packet is simply forwarded out of the host interface to the destination device.

When a host sends a packet to a device on a different IP network, the packet is forwarded to the default gateway because a host device cannot communicate directly with devices outside of the local network. The default gateway is the destination that routes traffic from the local network to devices on remote networks. It is often used to connect a local network to the Internet.

The default gateway is usually the address of the interface on the router connected to the local network. The router maintains routing table entries of all connected networks as well as entries of remote networks, and it determines the best path to reach those destinations.

For example, if PC1 sends a packet to the Web Server located at 176.16.1.99, it would discover that the Web Server is not on the local network. It would therefore send the packet to the MAC address of its default gateway. The packet protocol data unit (PDU) at the top in Figure 1-12 identifies the source and destination IP and MAC addresses.
Note

A router is also usually configured with its own default gateway. This is known as the *Gateway of Last Resort*.

Document Network Addressing (1.1.2.3)

When designing a new network or mapping an existing network, document the network. At a minimum, the documentation should identify the following:

- Device names
- Interfaces used in the design
- IP addresses and subnet masks
- Default gateway addresses

This information is captured by creating two useful network documents:

- **Topology diagram**—As shown in Figure 1-13, the topology diagram provides a visual reference that indicates the physical connectivity and logical Layer 3 addressing. Often created using diagramming software, such as Microsoft Visio.

Figure 1-13  Topology Diagram

- **An addressing table**—A table, such as Table 1-2, is used to capture device names, interfaces, IPv4 addresses, subnet masks, and default gateway addresses.
### Addressing Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Default Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Fa0/0</td>
<td>192.168.1.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>So0/0/0</td>
<td>192.168.2.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td>R2</td>
<td>Fa0/0</td>
<td>192.168.3.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>So0/0/0</td>
<td>192.168.2.2</td>
<td>255.255.255.0</td>
<td>N/A</td>
</tr>
<tr>
<td>PC1</td>
<td>N/A</td>
<td>192.168.1.10</td>
<td>255.255.255.0</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td>PC2</td>
<td>N/A</td>
<td>192.168.3.10</td>
<td>255.255.255.0</td>
<td>192.168.3.1</td>
</tr>
</tbody>
</table>

### Enable IP on a Host (1.1.2.4)

A host can be assigned IP address information in one of two ways:

- **Statically**—The host is manually assigned a unique IP address, subnet mask, and default gateway. The DNS server IP address can also be configured.

- **Dynamically**—The host receives its IP address information automatically from a DHCP server. The DHCP server offers the host a valid IP address, subnet mask, and default gateway information. The DHCP server may provide other information.

Figure 1-14 provides a static IPv4 configuration example.
Figure 1-15 provides a dynamic IPv4 address configuration examples.

![Figure 1-15 Dynamically Assigning an IPv4 Address]

Statically assigned addresses are commonly used to identify specific network resources, such as network servers and printers. They can also be used in smaller networks with few hosts. However, most host devices acquire their IPv4 address information by accessing a DHCPv4 server. In large enterprises, dedicated DHCPv4 servers providing services to many LANs are implemented. In a smaller branch or small office setting, DHCPv4 services can be provided by a Cisco Catalyst switch or a Cisco ISR.

**Device LEDs (1.1.2.5)**

Host computers connect to a wired network using a network interface and RJ-45 Ethernet cable. Most network interfaces have one or two LED link indicators next to the interface. The significance and meaning of the LED colors vary between manufacturers. However, a green LED typically means a good connection, whereas a blinking green LED indicates network activity.

If the link light is not on, there may be a problem with either the network cable or the network itself. The switch port where the connection terminates would also have an LED indicator lit. If one or both ends are not lit, try a different network cable.

**Note**

The actual function of the LEDs varies between computer manufacturers.

Similarly, network infrastructure devices commonly use multiple LED indicators to provide a quick status view. For example, a Cisco Catalyst 2960 switch has several status LEDs to help monitor system activity and performance. These LEDs are
generally lit green when the switch is functioning normally and lit amber when there is a malfunction.

Cisco ISRs use various LED indicators to provide status information. A Cisco 1941 router is shown in Figure 1-16.

![Cisco 1941 LEDs](image)

**Figure 1-16** Cisco 1941 LEDs

Table 1-3 lists the LED descriptions for the Cisco 1941 router.

<table>
<thead>
<tr>
<th>#</th>
<th>Port</th>
<th>LED</th>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GE0/0 and GE0/1</td>
<td>S (Speed)</td>
<td>1 blink + pause</td>
<td>Port operating at 10 Mb/s</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2 blink + pause</td>
<td>Port operating at 100 Mb/s</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 blink + pause</td>
<td>Port operating at 1000 Mb/s</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L (Link)</td>
<td>Green</td>
<td>Link is active</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Off</td>
<td>Link is inactive</td>
</tr>
<tr>
<td>2</td>
<td>Console</td>
<td>EN</td>
<td>Green</td>
<td>Port is active</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Off</td>
<td>Port is inactive</td>
</tr>
<tr>
<td>3</td>
<td>USB</td>
<td>EN</td>
<td>Green</td>
<td>Port is active</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Off</td>
<td>Port is inactive</td>
</tr>
</tbody>
</table>

The LEDs on the router can help a network administrator quickly conduct some basic troubleshooting. Each device has a unique set of LEDs, and it is advisable that you become familiar with the significance of these LEDs. Consult the device-specific documentation for an accurate description of the LEDs.
Console Access (1.1.2.6)

In a working network environment, infrastructure devices are commonly accessed remotely using Secure Shell (SSH) or Hypertext Transfer Protocol Secure (HTTPS). Console access is really only required when initially configuring a device, or if remote access fails.

Console access requires the following:

- **Console cable**—RJ-45-to-DB-9 serial cable or a USB serial cable
- **Terminal emulation software**—Tera Term, PuTTY

The cable is connected between the serial port of the host and the console port on the device. Most computers and notebooks no longer include built-in serial ports; therefore, a USB port can establish a console connection. However, a special *USB-to-RS-232 compatible serial port adapter* is required when using the USB port.

The Cisco ISR G2 supports a USB serial console connection. To establish connectivity, a *USB Type-A to USB Type-B* is required, as well as an operating system device driver. This device driver is available from www.cisco.com. Although these routers have two console ports, only one console port can be active at a time. When a cable is plugged into the USB console port, the RJ-45 port becomes inactive. When the USB cable is removed from the USB port, the RJ-45 port becomes active.

The table in Figure 1-17 summarizes the console connection requirements.

![Figure 1-17 Console Connection Requirements](image-url)
Figure 1-18 displays the various ports and cables required.

![Ports and Cables](image)

**Figure 1-18  Ports and Cables**

**Enable IP on a Switch (1.1.2.7)**

Network infrastructure devices require IP addresses to enable remote management. Using the device IP address, the network administrator can remotely connect to the device using Telnet, SSH, HTTP, or HTTPS.

A switch does not have a dedicated interface to which an IP address can be assigned. Instead, the IP address information is configured on a virtual interface called a **switched virtual interface (SVI)**.

For example, in Figure 1-19, the SVI on the Layer 2 switch S1 is assigned the IP address 192.168.10.2/24 and a default gateway of 192.168.10.1.

![Configure the Switch Management Interface](image)

**Figure 1-19  Configure the Switch Management Interface**
Activity 1.1.2.8: Document an Addressing Scheme
Refer to the online course to complete this activity.

Packet Tracer 1.1.2.9: Documenting the Network
Background/Scenario
Your job is to document the addressing scheme and connections used in the Central portion of the network. You need to use a variety of commands to gather the required information.

Router Basic Settings (1.1.3)
Every network has unique settings that must be configured on a router. This topic introduces basic IOS commands that are required to configure a router.

Configure Basic Router Settings (1.1.3.1)
Cisco routers and Cisco switches are a lot alike. They support a similar modal operating system, similar command structures, and many of the same commands. In addition, both devices have similar initial configuration steps.

For instance, the following configuration tasks should always be performed:

- **Name the device**—Distinguishes it from other routers.
- **Secure management access**—Secures privileged EXEC, user EXEC, and remote access.
- **Configure a banner**—Provides legal notification of unauthorized access.

Always save the changes on a router and verify the basic configuration and router operations.

Figure 1-20 shows the topology used for example configurations.

**Figure 1-20** IPv4 Configuration Topology
Example 1-1 shows the basic router settings configured for R1.

**Example 1-1 Basic Router Settings**

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)# banner motd $ Authorized Access Only! $
R1(config)# end
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

**Configure an IPv4 Router Interface (1.1.3.2)**

One distinguishing feature between switches and routers is the type of interfaces supported by each. For example, Layer 2 switches support LANs and, therefore, have multiple FastEthernet or Gigabit Ethernet ports.

Routers support LANs and WANs and can interconnect different types of networks; therefore, they support many types of interfaces. For example, G2 ISRs have one or two integrated Gigabit Ethernet interfaces and *High-Speed WAN Interface Card (HWIC) slots* to accommodate other types of network interfaces, including serial, DSL, and cable interfaces.

To be available, an interface must be both of the following:

- **Configured with an IP address and a subnet mask**—Use the `ip address` `ip-address subnet-mask` interface configuration command.

- **Activated**—By default, LAN and WAN interfaces are not activated (`shutdown`). To enable an interface, it must be activated using the `no shutdown` command.
(This is similar to powering on the interface.) The interface must also be connected to another device such as a switch or another router for the physical layer to be active.

Optionally, the interface could also be configured with a short description of up to 240 characters using the `description` command. It is good practice to configure a description on each interface. On production networks, the benefits of interface descriptions are quickly realized because they are helpful in troubleshooting and identifying a third-party connection and contact information.

Depending on the type of interface, additional parameters may be required. For example, in our lab environment, the serial interface connecting to the serial cable end labeled DCE must be configured with the `clock rate` command.

**Note**

The service provider router would typically provide the clock rate to the customer router. However, in a lab environment, the `clock rate` command is required on the DCE end when interconnecting two serial interfaces.

**Note**

Accidentally using the `clock rate` command on a DTE interface generates the following informational message:

```
%Error: This command applies only to DCE interface
```

Example 1-2 shows the router interfaces configuration for R1. Notice that the state of Serial0/0/0 is “down”. The status will change to “up” when the Serial0/0/0 interface on R2 is configured and activated.

**Example 1-2 Router Interface Configurations for IPv4**

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit

*Jan 30 22:04:47.551: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down
*Jan 30 22:04:50.899: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Jan 30 22:04:51.899: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R1(config)# interface gigabitethernet 0/1
R1(config-if)# description Link to LAN 2
```
Configure an IPv6 Router Interface (1.1.3.3)

Configuring an IPv6 interface is similar to configuring an interface for IPv4. Most IPv6 configuration and verification commands in the Cisco IOS are similar to their IPv4 counterparts. In many cases, the only difference is the use of `ipv6` in place of `ip` in commands.

An IPv6 interface must be

- **Configured with IPv6 address and subnet mask**—Use the `ipv6 address ipv6-address/prefix-length [link-local | eui-64]` interface configuration command.

- **Activated**—The interface must be activated using the `no shutdown` command.

**Note**

An interface can generate its own IPv6 link-local address without having a global unicast address by using the `ipv6 enable` interface configuration command.

Unlike IPv4, IPv6 interfaces will typically have more than one IPv6 address. At a minimum, an IPv6 device must have an **IPv6 link-local address** but will most likely also have an **IPv6 global unicast address**. IPv6 also supports the ability for an interface to have multiple IPv6 global unicast addresses from the same subnet.
The following commands can be used to statically create a global unicast or link-local IPv6 address:

- `ipv6 address ipv6-address/prefix-length` — Creates a global unicast IPv6 address as specified.

- `ipv6 address ipv6-address/prefix-length eui-64` — Configures a global unicast IPv6 address with an interface identifier (ID) in the low-order 64 bits of the IPv6 address using the *EUI-64* process.

- `ipv6 address ipv6-address/prefix-length link-local` — Configures a static link-local address on the interface that is used instead of the link-local address that is automatically configured when the global unicast IPv6 address is assigned to the interface or enabled using the `ipv6 enable` interface command. Recall that the `ipv6 enable` interface command is used to automatically create an IPv6 link-local address whether or not an IPv6 global unicast address has been assigned.

In the example topology shown in Figure 1-21, R1 must be configured to support the following IPv6 network addresses:

- 2001:0DB8:ACAD:0001:/64 or equivalently 2001:DB8:ACAD:1::/64
- 2001:0DB8:ACAD:0002:/64 or equivalently 2001:DB8:ACAD:2::/64
- 2001:0DB8:ACAD:0003:/64 or equivalently 2001:DB8:ACAD:3::/64

![Figure 1-21 IPv6 Configuration Topology](image-url)

When the router is configured using the `ipv6 unicast-routing` global configuration command, the router begins sending ICMPv6 Router Advertisement messages out the interface. This enables a PC connected to the interface to automatically configure an IPv6 address and to set a default gateway without needing the services of a DHCPv6 server. Alternatively, a PC connected to the IPv6 network can have an IPv6 address manually configured, as shown in Figure 1-22. Notice that the default gateway address configured for PC1 is the IPv6 global unicast address of the R1 GigabitEthernet 0/0 interface.
The router interfaces in the Figure 1-21 must be configured and enabled, as shown in Example 1-3.

Example 1-3 Router Interface Configurations for IPv6

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
*Feb  3 21:38:37.279: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down
*Feb  3 21:38:40.967: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Feb  3 21:39:21.867: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R1(config)# interface gigabitethernet 0/1
R1(config-if)# description Link to LAN 2
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
*Feb  3 21:39:21.867: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
*Feb  3 21:39:24.967: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Feb  3 21:39:25.967: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```
Configure an IPv4 Loopback Interface (1.1.3.4)

Another common configuration of Cisco IOS routers is enabling a *loopback interface*.

The loopback interface is a logical interface internal to the router. It is not assigned to a physical port and can therefore never be connected to any other device. It is considered a software interface that is automatically placed in an “up” state, as long as the router is functioning.

The loopback interface is useful in testing and managing a Cisco IOS device because it ensures that at least one interface will always be available. For example, it can be used for testing purposes, such as testing internal routing processes, by emulating networks behind the router.

Additionally, the IPv4 address assigned to the loopback interface can be significant to processes on the router that use an interface IPv4 address for identification purposes, such as the Open Shortest Path First (OSPF) routing process. By enabling a loopback interface, the router will use the always available loopback interface address for identification, rather than an IP address assigned to a physical port that may go down.

The task of enabling and assigning a loopback address is simple:

```
Router(config)# interface loopback number
Router(config-if)# ip address ip-address subnet-mask
Router(config-if)# exit
```

Example 1-4 shows the loopback configuration for R1.

**Example 1-4 Configure a Loopback Interface**

```
R1(config)# interface loopback 0
R1(config-if)# ip address 10.0.0.1 255.255.255.0
R1(config-if)# end
R1(config)#
*Jan 30 22:04:50.899: %LINK-3-UPDOWN: Interface loopback0, changed state to up
*Jan 30 22:04:51.899: %LINEPROTO-5-UPDOWN: Line protocol on Interface loopback0, changed state to up
```
Multiple loopback interfaces can be enabled on a router. The IPv4 address for each loopback interface must be unique and unused by any other interface.

Packet Tracer 1.1.3.5: Configuring IPv4 and IPv6 Interfaces

Background/Scenario

Routers R1 and R2 each have two LANs. Your task is to configure the appropriate addressing on each device and verify connectivity between the LANs.

Verify Connectivity of Directly Connected Networks (1.1.4)

It is always important to know how to troubleshoot and verify whether a device is configured correctly. The focus of this topic is on how to verify connectivity between two networks that are directly connected to a router.

Verify Interface Settings (1.1.4.1)

There are several privileged EXEC mode `show` commands that can be used to verify the operation and configuration of an interface. The following three commands are especially useful to quickly identify an interface status:

- `show ip interface brief`—Displays a summary for all interfaces, including the IPv4 address of the interface and current operational status.

- `show ip route`—Displays the contents of the IPv4 routing table stored in RAM. In Cisco IOS 15, active interfaces should appear in the routing table with two related entries identified by the code ‘C’ (Connected) or ‘L’ (Local). In previous IOS versions, only a single entry with the code ‘C’ will appear.

- `show running-config interface interface-id`—Displays the commands configured on the specified interface.

Example 1-5 displays the output of the `show ip interface brief` command. The output reveals that the LAN interfaces and the WAN link are activated and operational, as indicated by the Status of “up” and Protocol of “up.” A different output would indicate a problem with either the configuration or the cabling.
Example 1-5 Verify the IPv4 Interface Status

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK? Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded-Service-Engine0/0</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>GigabitEthernet0/0</td>
<td>192.168.10.1</td>
<td>YES manual</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>GigabitEthernet0/1</td>
<td>192.168.11.1</td>
<td>YES manual</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>Serial0/0/0</td>
<td>209.165.200.225</td>
<td>YES manual</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>Serial0/0/1</td>
<td>unassigned</td>
<td>YES unset</td>
<td>administratively down</td>
<td>down</td>
</tr>
</tbody>
</table>

Note

In Example 1-5, the Embedded-Service-Engine0/0 interface is displayed because Cisco ISRs G2 have dual core CPUs on the motherboard. The Embedded-Service-Engine0/0 interface is outside the scope of this course.

Example 1-6 displays the output of the `show ip route` command. Notice the three directly connected network entries and the three local host route interface entries. A local host route has an administrative distance of 0. It also has a /32 mask for IPv4, and a /128 mask for IPv6. The local host route is for routes on the router owning the IP address. It is used to allow the router to process packets destined to that IP.

Example 1-6 Verify the IPv4 Routing Table

<table>
<thead>
<tr>
<th>Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP</th>
</tr>
</thead>
</table>

Gateway of last resort is not set

```
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly connected, GigabitEthernet0/0
L 192.168.10.1/32 is directly connected, GigabitEthernet0/0

192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.11.0/24 is directly connected, GigabitEthernet0/1
L 192.168.11.1/32 is directly connected, GigabitEthernet0/1

209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.224/30 is directly connected, Serial0/0/0
L 209.165.200.225/32 is directly connected, Serial0/0/0
```
Example 1-7 displays the output of the `show running-config interface` command. The output displays the current commands configured on the specified interface.

**Example 1-7 Verify the IPv4 Interface Configuration**

```bash
R1# show running-config interface gigabitEthernet 0/0
Building configuration...

Current configuration : 128 bytes

interface GigabitEthernet0/0
  description Link to LAN 1
  ip address 192.168.10.1 255.255.255.0
duplex auto
  speed auto
end

R1#
```

The following two commands are used to gather more detailed interface information:

- **show interfaces**—Displays interface information and packet flow count for all interfaces on the device.
- **show ip interface**—Displays the IPv4-related information for all interfaces on a router.

**Verify IPv6 Interface Settings (1.1.4.2)**

The commands to verify the IPv6 interface configuration are similar to the commands used for IPv4.

The `show ipv6 interface brief` command in Example 1-8 displays a summary for each of the interfaces for the R1 router in Figure 1-21. The “up/up” output on the same line as the interface name indicates the Layer 1/Layer 2 interface state. This is the same as the Status and Protocol columns in the equivalent IPv4 command.

**Example 1-8 Verify the IPv6 Interface Status**

```bash
R1# show ipv6 interface brief
GigabitEthernet0/0     [up/up]
  FE80::FE99:47FF:FE75:C3E0
  2001:DB8:ACAD:1::1
GigabitEthernet0/1     [up/up]
  FE80::FE99:47FF:FE75:C3E1
  2001:DB8:ACAD:2::1
```
Chapter 1: Routing Concepts

The output displays two configured IPv6 addresses per interface. One address is the IPv6 global unicast address that was manually entered. The other address, which begins with FE80, is the link-local unicast address for the interface. A link-local address is automatically added to an interface whenever a global unicast address is assigned. An IPv6 network interface is required to have a link-local address, but not necessarily a global unicast address.

The show ipv6 interface gigabitethernet 0/0 command output shown in Example 1-9 displays the interface status and all the IPv6 addresses belonging to the interface. Along with the link-local address and global unicast address, the output includes the multicast addresses assigned to the interface, beginning with prefix FF02.

Example 1-9 Verify the IPv6 Interface Configuration

```
R1# show ipv6 interface gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::32F7:DFF:FEA3:DA0
No Virtual link-local address(es):
Global unicast address(es):
  2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
Joined group address(es):
  FF02::1
  FF02::1:FF00:1
  FF02::1:FFA3:DA0
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND NS retransmit interval is 1000 milliseconds
R1#
```

The show ipv6 route command shown in Example 1-10 can be used to verify that IPv6 networks and specific IPv6 interface addresses have been installed in the IPv6 routing table. The show ipv6 route command will only display IPv6 networks, not IPv4 networks.
Example 1-10 Verify the IPv6 Routing Table

```
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static

<output omitted>

C  2001:DB8:ACAD:1::/64 [0/0]
   via GigabitEthernet0/0, directly connected
L  2001:DB8:ACAD:1::1/128 [0/0]
   via GigabitEthernet0/0, receive
C  2001:DB8:ACAD:2::/64 [0/0]
   via GigabitEthernet0/1, directly connected
L  2001:DB8:ACAD:2::1/128 [0/0]
   via GigabitEthernet0/1, receive
C  2001:DB8:ACAD:3::/64 [0/0]
   via Serial0/0/0, directly connected
L  2001:DB8:ACAD:3::1/128 [0/0]
   via Serial0/0/0, receive
L  FF00::/8 [0/0]
   via Null0, receive
R1#
```

Within the routing table, a ‘C’ next to a route indicates that this is a directly connected network. When the router interface is configured with a global unicast address and is in the “up/up” state, the IPv6 prefix and prefix length is added to the IPv6 routing table as a connected route.

The IPv6 global unicast address configured on the interface is also installed in the routing table as a local route. The local route has a /128 prefix. Local routes are used by the routing table to efficiently process packets with the interface address of the router as the destination.

The ping command for IPv6 is identical to the command used with IPv4 except that an IPv6 address is used. As shown in Example 1-11, the ping command is used to verify Layer 3 connectivity between R1 and PC1.

Example 1-11 Verify R1 Connectivity to PC1

```
R1# ping 2001:db8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5)
R1#
```
Filter Show Command Output (1.1.4.3)

Commands that generate multiple screens of output are, by default, paused after 24 lines. At the end of the paused output, the --More-- text displays. Pressing Enter displays the next line, and pressing the Spacebar displays the next set of lines. Use the terminal length command to specify the number of lines to be displayed. A value of 0 (zero) prevents the router from pausing between screens of output.

Another useful feature that improves the user experience in the command-line interface (CLI) is the filtering of show output. Filtering commands can be used to display specific sections of output. To enable the filtering command, enter a pipe (|) character after the show command and then enter a filtering parameter and a filtering expression.

The filtering parameters that can be configured after the pipe include these:

- **section**—Shows entire section that starts with the filtering expression
- **include**—Includes all output lines that match the filtering expression
- **exclude**—Excludes all output lines that match the filtering expression
- **begin**—Shows all the output lines from a certain point, starting with the line that matches the filtering expression

**Note**

Output filters can be used in combination with any show command.

Example 1-12 shows the usage of these various output filters.

**Example 1-12 Filtering show Commands**

```bash
R1# show running-config | section line vty
line vty 0 4
    password 7 030752180500
login
    transport input all
R1# show ip interface brief | include up
GigabitEthernet0/0        192.168.10.1      YES manual up                         up
GigabitEthernet0/1        192.168.11.1      YES manual up                         up
Serial0/0/0                     209.165.200.225       YES manual up                         up
R1# show ip interface brief | exclude unassigned
Interface                   IP-Address      OK? Method Status              Protocol
GigabitEthernet0/0        192.168.10.1      YES manual up                         up
GigabitEthernet0/1        192.168.11.1      YES manual up                         up
Serial0/0/0                     209.165.200.225       YES manual up                         up
```
Command History Feature (1.1.4.4)

The command history feature is useful because it temporarily stores the list of executed commands to be recalled.

To recall commands in the history buffer, press Ctrl+P or the Up Arrow key. The command output begins with the most recent command. Repeat the key sequence to recall successively older commands. To return to more recent commands in the history buffer, press Ctrl+N or the Down Arrow key. Repeat the key sequence to recall successively more recent commands.

By default, command history is enabled and the system captures the last 10 command lines in its history buffer. Use the `show history` privileged EXEC command to display the contents of the buffer.

It is also practical to increase the number of command lines that the history buffer records during the current terminal session only. Use the `terminal history size` user EXEC command to increase or decrease the size of the buffer.

Example 1-13 displays a sample of the `terminal history size` and `show history` commands.
Example 1-13 Command History Feature

```
R1# terminal history size 200
R1# show history
  show ip interface brief
  show interface g0/0
  show ip interface g0/1
  show ip route
  show ip route 209.165.200.224
  show running-config interface s0/0/0
  terminal history size 200
  show history
R1#
```

Packet Tracer 1.1.4.5: Configuring and Verifying a Small Network

Background/Scenario

In this activity, you will configure a router with basic settings including IP addressing. You will also configure a switch for remote management and configure the PCs. After you have successfully verified connectivity, you will use `show` commands to gather information about the network.

Lab 1.1.4.6: Configuring Basic Router Settings with IOS CLI

In this lab, you will complete the following objectives:

- Part 1: Set Up the Topology and Initialize Devices
- Part 2: Configure Devices and Verify Connectivity
- Part 3: Display Router Information
- Part 4: Configure IPv6 and Verify Connectivity

Routing Decisions (1.2)

This section explains how routers use information in data packets to make forwarding decisions in a small to medium-sized business network.

Switching Packets Between Networks (1.2.1)

This topic explains the encapsulation and de-encapsulation process that routers use when switching packets between interfaces.
Router Switching Function (1.2.1.1)

A primary function of a router is to forward packets toward their destination. This is accomplished by using a switching function, which is the process used by a router to accept a packet on one interface and forward it out another interface. A key responsibility of the switching function is to encapsulate packets in the appropriate data link frame type for the outgoing data link.

Note

In this context, the term “switching” literally means moving packets from source to destination and should not be confused with the function of a Layer 2 switch.

After the router has determined the exit interface using the path determination function, the router must encapsulate the packet into the data link frame of the outgoing interface.

What does a router do with a packet received from one network and destined for another network? Refer to Figure 1-23.

![Figure 1-23  Encapsulating and De-Encapsulating Packets](image)

The router performs the following three major steps:

- **Step 1.** De-encapsulates the Layer 2 frame header and trailer to expose the Layer 3 packet.
- **Step 2.** Examines the destination IP address of the IP packet to find the best path in the routing table.
- **Step 3.** If the router finds a path to the destination, it encapsulates the Layer 3 packet into a new Layer 2 frame and forwards the frame out the exit interface.
As shown in Figure 1-23, devices have Layer 3 IPv4 addresses, and Ethernet interfaces have Layer 2 data link addresses. For example, PC1 is configured with IPv4 address 192.168.1.10 and an example MAC address of 0A-10. As a packet travels from the source device to the final destination device, the Layer 3 IP addresses do not change. However, the Layer 2 data link addresses change at every hop as the packet is de-encapsulated and re-encapsulated in a new Layer 2 frame by each router.

It is common for packets to require encapsulation into a different type of Layer 2 frame than the one in which it was received. For example, a router might receive an Ethernet encapsulated frame on a FastEthernet interface and then process that frame to be forwarded out of a serial interface.

Notice in Figure 1-23 that the ports between R2 and R3 do not have associated MAC addresses. This is because it is a serial link. MAC addresses are only required on Ethernet multiaccess networks. A serial link is a point-to-point connection and uses a different Layer 2 frame that does not require the use of a MAC address. In this example, when Ethernet frames are received on R2 from the Fa0/0 interface, destined for PC2, they are de-encapsulated and then re-encapsulated for the serial interface, such as a PPP encapsulated frame. When R3 receives the PPP frame, it is de-encapsulated again and then re-encapsulated into an Ethernet frame with a destination MAC address of 0B-20, prior to being forwarded out the Fa0/0 interface.

**Send a Packet (1.2.1.2)**

In Figure 1-24, PC1 is sending a packet to PC2. PC1 must determine if the destination IPv4 address is on the same network. PC1 determines its own subnet by doing an AND operation on its own IPv4 address and subnet mask. This produces the network address that PC1 belongs to. Next, PC1 does this same AND operation using the packet destination IPv4 address and the PC1 subnet mask.
If the destination network address is the same network as PC1, then PC1 does not use the default gateway. Instead, PC1 refers to its Address Resolution Protocol (ARP) cache for the MAC address of the device with that destination IPv4 address. If the MAC address is not in the cache, then PC1 generates an ARP request to acquire the address to complete the packet and send it to the destination. If the destination network address is on a different network, then PC1 forwards the packet to its default gateway.

To determine the MAC address of the default gateway, PC1 checks its ARP table for the IPv4 address of the default gateway and its associated MAC address.

If an ARP entry does not exist in the ARP table for the default gateway, PC1 sends an ARP request. Router R1 sends back an ARP reply. PC1 can then forward the packet to the MAC address of the default gateway, the Fa0/0 interface of router R1.

A similar process is used for IPv6 packets. However, instead of the ARP process, IPv6 address resolution uses ICMPv6 Neighbor Solicitation and Neighbor Advertisement messages. IPv6-to-MAC address mappings are kept in a table similar to the ARP cache, called the neighbor cache.

**Forward to the Next Hop (1.2.1.3)**

Figure 1-25 shows the processes that take place when R1 receives the Ethernet frame from PC1.

![Figure 1-25](image)

1. R1 examines the destination MAC address, which matches the MAC address of the receiving interface on R1, FastEthernet 0/0. R1, therefore, copies the frame into its buffer.

2. R1 identifies the Ethernet Type field as 0×800, which means that the Ethernet frame contains an IPv4 packet in the data portion of the frame.
3. R1 de-encapsulates the Ethernet frame to examine the Layer 3 information.

4. Because the destination IPv4 address of the packet does not match any of the directly connected networks of R1, R1 consults its routing table to route this packet. R1 searches the routing table for a network address that would include the destination IPv4 address of the packet as a host address within that network. In this example, the routing table has a route for the 192.168.4.0/24 network. The destination IPv4 address of the packet is 192.168.4.10, which is a host IPv4 address on that network.

The route that R1 finds to the 192.168.4.0/24 network has a next-hop IPv4 address of 192.168.2.2 and an exit interface of FastEthernet 0/1. This means that the IPv4 packet is encapsulated in a new Ethernet frame with the destination MAC address of the IPv4 address of the next-hop router.

Figure 1-26 show the processes that take place when R1 forwards the packet to R2.

Because the exit interface is on an Ethernet network, R1 must resolve the next-hop IPv4 address with a destination MAC address using ARP:

1. R1 looks up the next-hop IPv4 address of 192.168.2.2 in its ARP cache. If the entry is not in the ARP cache, R1 would send an ARP request out of its FastEthernet 0/1 interface and R2 would return an ARP reply. R1 would then update its ARP cache with an entry for 192.168.2.2 and the associated MAC address.

2. The IPv4 packet is now encapsulated into a new Ethernet frame and forwarded out the FastEthernet 0/1 interface of R1.
Packet Routing (1.2.1.4)
Figure 1-27 shows the processes that take place when R2 receives the frame on its Fa0/0 interface.

1. R2 examines the destination MAC address, which matches the MAC address of the receiving interface, FastEthernet 0/0. R2, therefore, copies the frame into its buffer.
2. R2 identifies the Ethernet Type field as $0 \times 800$, which means that the Ethernet frame contains an IPv4 packet in the data portion of the frame.
3. R2 de-encapsulates the Ethernet frame.

Figure 1-27  R2 Looks Up Route to Destination

Figure 1-28 shows the processes that take place when R2 forwards the packet to R3.

Figure 1-28  R2 Forwards Packet to R3
1. Because the destination IPv4 address of the packet does not match any of the interface addresses of R2, R2 consults its routing table to route this packet. R2 searches the routing table for the destination IPv4 address of the packet using the same process R1 used.

The routing table of R2 has a route to the 192.168.4.0/24 network, with a next-hop IPv4 address of 192.168.3.2 and an exit interface of Serial 0/0/0. Because the exit interface is not an Ethernet network, R2 does not have to resolve the next-hop IPv4 address with a destination MAC address.

2. The IPv4 packet is now encapsulated into a new data link frame and sent out the Serial 0/0/0 exit interface.

When the interface is a point-to-point (P2P) serial connection, the router encapsulates the IPv4 packet into the proper data link frame format used by the exit interface (HDLC, PPP, and so on). Because there are no MAC addresses on serial interfaces, R2 sets the data link destination address to an equivalent of a broadcast.

**Reach the Destination (1.2.1.5)**

The following processes take place when the frame arrives at R3:

1. R3 copies the data link PPP frame into its buffer.
2. R3 de-encapsulates the data link PPP frame.
3. R3 searches the routing table for the destination IPv4 address of the packet.
   - The routing table has a route to a directly connected network on R3. This means that the packet can be sent directly to the destination device and does not need to be sent to another router.

Figure 1-29 shows the processes that take place when R3 forwards the packet to PC2.
Because the exit interface is a directly connected Ethernet network, R3 must resolve the destination IPv4 address of the packet with a destination MAC address:

1. R3 searches for the destination IPv4 address of the packet in its ARP cache. If the entry is not in the ARP cache, R3 sends an ARP request out of its FastEthernet 0/0 interface. PC2 sends back an ARP reply with its MAC address. R3 then updates its ARP cache with an entry for 192.168.4.10 and the MAC address that is returned in the ARP reply.

2. The IPv4 packet is encapsulated into a new Ethernet data link frame and sent out the FastEthernet 0/0 interface of R3.

3. When PC2 receives the frame, it examines the destination MAC address, which matches the MAC address of the receiving interface, its Ethernet network interface card (NIC). PC2, therefore, copies the rest of the frame into its buffer.

4. PC2 identifies the Ethernet Type field as 0×800, which means that the Ethernet frame contains an IPv4 packet in the data portion of the frame.

5. PC2 de-encapsulates the Ethernet frame and passes the IPv4 packet to the IPv4 process of its operating system.

**Activity 1.2.1.6: Match Layer 2 and Layer 3 Addressing**

Refer to the online course to complete this activity.

**Path Determination (1.2.2)**

A router refers to its routing table when making best path decisions. In this topic, we will examine the path determination function of a router.

**Routing Decisions (1.2.2.1)**

A primary function of a router is to determine the best path to use to send packets. To determine the best path, the router searches its routing table for a network address that matches the destination IP address of the packet.

The routing table search results in one of three path determinations:

- **Directly connected network**—If the destination IP address of the packet belongs to a device on a network that is directly connected to one of the interfaces of the router, that packet is forwarded directly to the destination device. This means that the destination IP address of the packet is a host address on the same network as the interface of the router.
Remote network—If the destination IP address of the packet belongs to a remote network, then the packet is forwarded to another router. Remote networks can only be reached by forwarding packets to another router.

No route determined—If the destination IP address of the packet does not belong to either a connected or a remote network, the router determines if there is a Gateway of Last Resort available. A Gateway of Last Resort is set when a default route is configured or learned on a router. If there is a default route, the packet is forwarded to the Gateway of Last Resort. If the router does not have a default route, then the packet is discarded.

The logic flowchart in Figure 1-30 illustrates the router packet-forwarding decision process.

![Packet-Forwarding Decision Process](image)

**Figure 1-30** Packet-Forwarding Decision Process

Best Path (1.2.2.2)

Determining the best path involves the evaluation of multiple paths to the same destination network and selecting the optimum or shortest path to reach that network. Whenever multiple paths to the same network exist, each path uses a different exit interface on the router to reach that network.

The best path is selected by a routing protocol based on the value or **metric** it uses to determine the distance to reach a network. A metric is the quantitative value used to measure the distance to a given network. The best path to a network is the path with the lowest metric.
Dynamic routing protocols typically use their own rules and metrics to build and update routing tables. The routing algorithm generates a value, or a metric, for each path through the network. Metrics can be based on either a single characteristic or several characteristics of a path. Some routing protocols can base route selection on multiple metrics, combining them into a single metric.

The following lists some dynamic protocols and the metrics they use:

- **Routing Information Protocol (RIP)**—Hop count
- **Open Shortest Path First (OSPF)**—Cisco’s cost based on cumulative bandwidth from source to destination
- **Enhanced Interior Gateway Routing Protocol (EIGRP)**—Bandwidth, delay, load, reliability

Figure 1-31 highlights how the path may be different depending on the metric being used.

![Figure 1-31 Hop Count Versus Bandwidth as a Metric](image)

**Load Balancing (1.2.2.3)**

What happens if a routing table has two or more paths with identical metrics to the same destination network?

When a router has two or more paths to a destination with equal cost metrics, then the router forwards the packets using both paths equally. This is called **equal cost load balancing**. The routing table contains the single destination network but has multiple exit interfaces, one for each equal cost path. The router forwards packets using the multiple exit interfaces listed in the routing table.
If configured correctly, load balancing can increase the effectiveness and performance of the network. Equal cost load balancing can be configured to use both dynamic routing protocols and static routes.

**Note**

Only EIGRP supports *unequal cost load balancing*.

Figure 1-32 provides an example of equal cost load balancing.

**Administrative Distance (1.2.2.4)**

It is possible for a router to be configured with multiple routing protocols and static routes. If this occurs, the routing table may have more than one route source for the same destination network. For example, if both RIP and EIGRP are configured on a router, both routing protocols may learn of the same destination network. However, each routing protocol may decide on a different path to reach the destination based on the metrics of that routing protocol. RIP chooses a path based on hop count, whereas EIGRP chooses a path based on its composite metric. How does the router know which route to use?

Cisco IOS uses what is known as the *administrative distance (AD)* to determine the route to install into the IP routing table. The AD represents the “trustworthiness” of the route; the lower the AD, the more trustworthy the route source. For example, a static route has an AD of 1, whereas an EIGRP-discovered route has an AD of 90. Given two separate routes to the same destination, the router chooses the route with the lowest AD. When a router has the choice of a static route and an EIGRP route, the static route takes precedence. Similarly, a directly connected route with an AD of 0 takes precedence over a static route with an AD of 1.
Table 1-4 lists various routing protocols and their associated ADs.

**Table 1-4  Default Administrative Distances**

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Administrative Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>0</td>
</tr>
<tr>
<td>Static</td>
<td>1</td>
</tr>
<tr>
<td>EIGRP summary route</td>
<td>5</td>
</tr>
<tr>
<td>External BGP</td>
<td>20</td>
</tr>
<tr>
<td>Internal EIGRP</td>
<td>90</td>
</tr>
<tr>
<td>IGRP</td>
<td>100</td>
</tr>
<tr>
<td>OSPF</td>
<td>110</td>
</tr>
<tr>
<td>IS-IS</td>
<td>115</td>
</tr>
<tr>
<td>RIP</td>
<td>120</td>
</tr>
<tr>
<td>External EIGRP</td>
<td>170</td>
</tr>
<tr>
<td>Internal BGP</td>
<td>200</td>
</tr>
</tbody>
</table>

**Activity 1.2.2.5: Order the Steps in the Packet-Forwarding Process**

Refer to the online course to complete this activity.

**Activity 1.2.2.6: Match the Administrative Distance to the Route Source**

Refer to the online course to complete this activity.

**Router Operation (1.3)**

To make routing decisions, a router exchanges information with other routers. Alternatively, the router can also be manually configured on how to reach a specific network.

In this section you will explain how a router learns about remote networks when operating in a small to medium-sized business network.
Analyze the Routing Table (1.3.1)

The routing table is at the heart of making routing decisions. It is important that you understand the information presented in a routing table. In this topic, you will learn about routing table entries for directly connected networks.

The Routing Table (1.3.1.1)

The routing table of a router stores information about the following:

- **Directly connected routes**—These routes come from the active router interfaces. Routers add a directly connected route when an interface is configured with an IP address and is activated.

- **Remote routes**—These are remote networks connected to other routers. Routes to these networks can be either statically configured or dynamically learned through dynamic routing protocols.

Specifically, a routing table is a data file in RAM that stores route information about directly connected and remote networks. The routing table contains network or next-hop associations. These associations tell a router that a particular destination can be optimally reached by sending the packet to a specific router that represents the next hop on the way to the final destination. The next-hop association can also be the outgoing or exit interface to the next destination.

Figure 1-33 identifies the directly connected networks and remote networks of router R1.

![Figure 1-33  Directly Connected and Remote Network Routes](image)

Routing Table Sources (1.3.1.2)

On a Cisco router, the `show ip route` command is used to display the IPv4 routing table of a router. A router provides additional route information, including how
the route was learned, how long the route has been in the table, and which specific interface to use to get to a predefined destination.

Entries in the routing table can be added as follows:

- **Local route interfaces**—Added when an interface is configured and active. This entry is only displayed in IOS 15 or newer for IPv4 routes and all IOS releases for IPv6 routes.
- **Directly connected interfaces**—Added to the routing table when an interface is configured and active.
- **Static routes**—Added when a route is manually configured and the exit interface is active.
- **Dynamic routing protocol**—Added when routing protocols that dynamically learn about the network, such as EIGRP and OSPF, are implemented and networks are identified.

The sources of the routing table entries are identified by a code. The code identifies how the route was learned. For instance, common codes include the following:

- **L**—Identifies the address assigned to a router’s interface. This allows the router to efficiently determine when it receives a packet for the interface instead of being forwarded.
- **C**—Identifies a directly connected network.
- **S**—Identifies a static route created to reach a specific network.
- **D**—Identifies a dynamically learned network from another router using EIGRP.
- **O**—Identifies a dynamically learned network from another router using the OSPF routing protocol.

Example 1-14 shows the routing table for the R1 router in Figure 1-20.

**Example 1-14 Routing Table for R1**

```plaintext
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
```
Remote Network Routing Entries (1.3.1.3)

As a network administrator, it is imperative to know how to interpret the content of IPv4 and IPv6 routing tables. Figure 1-34 displays an IPv4 routing table entry on R1 for the route to remote network 10.1.1.0.

Table 1-5 describes the parts of the routing table entry shown in Figure 1-34.

<table>
<thead>
<tr>
<th>Legend</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Route Source</td>
<td>Identifies how the route was learned.</td>
</tr>
<tr>
<td>B</td>
<td>Destination Network</td>
<td>Identifies the IPv4 address of the remote network.</td>
</tr>
<tr>
<td>C</td>
<td>Administrative Distance</td>
<td>Identifies the trustworthiness of the route source. Lower values indicate preferred route source.</td>
</tr>
</tbody>
</table>
### Activity 1.3.1.4: Interpret the Content of a Routing Table Entry

Refer to the online course to complete this activity.

### Directly Connected Routes (1.3.2)

In this topic you will learn how a router builds a routing table of directly connected networks.

#### Directly Connected Interfaces (1.3.2.1)

A newly deployed router, without configured interfaces, has an empty routing table, as shown in Example 1-15.

**Example 1-15 Empty Routing Table**

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R1#
```
Before the interface state is considered up/up and added to the IPv4 routing table, the interface must

- Be assigned a valid IPv4 or IPv6 address
- Be activated with the no shutdown command
- Receive a carrier signal from another device (router, switch, host, and so on)

When the interface is up, the network of that interface is added to the routing table as a directly connected network.

Directly Connected Routing Table Entries (1.3.2.2)

An active, properly configured, directly connected interface actually creates two routing table entries. Figure 1-35 displays the IPv4 routing table entries on R1 for the directly connected network 192.168.10.0.

Figure 1-35  Directly Connected Network Entry Identifiers

The routing table entry for directly connected interfaces is simpler than the entries for remote networks. Table 1-6 describes the parts of the routing table entry shown in Figure 1-35.

Table 1-6  Parts of a Directly Connected Network Entry

<table>
<thead>
<tr>
<th>Legend</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Route Source</td>
<td>Identifies how the network was learned by the router. Directly connected interfaces have two route source codes. ‘C’ identifies a directly connected network. ‘L’ identifies the IPv4 address assigned to the router’s interface.</td>
</tr>
<tr>
<td>B</td>
<td>Destination Network</td>
<td>Identifies the destination network and how it is connected.</td>
</tr>
<tr>
<td>C</td>
<td>Outgoing Interface</td>
<td>Identifies the exit interface to use when forwarding packets to the destination network.</td>
</tr>
</tbody>
</table>
Prior to IOS 15, local route routing table entries (L) were not displayed in the IPv4 routing table. Local route (L) entries have always been part of the IPv6 routing table.

Directly Connected Examples (1.3.2.3)

Example 1-16 shows the steps to configure and activate the interfaces attached to R1 in Figure 1-20. Notice the Layer 1 and 2 informational messages generated as each interface is activated.

**Example 1-16 Configuring the Directly Connected IPv4 Interfaces**

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit

*Feb  1 13:37:35.035: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down
*Feb  1 13:37:38.211: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Feb  1 13:37:39.211: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R1(config)# interface gigabitethernet 0/1
R1(config-if)# description Link to LAN 2
R1(config-if)# ip address 192.168.11.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit

*Feb  1 13:38:01.471: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
*Feb  1 13:38:04.211: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
*Feb  1 13:38:05.211: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

R1(config)# interface serial 0/0/0
R1(config-if)# description Link to R1
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# clock rate 128000
R1(config-if)# no shutdown
R1(config-if)# end

*Feb  1 13:38:22.723: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
*Feb  1 13:38:23.723: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

R1#
As each interface is added, the routing table automatically adds the connected ('C')
and local ('L') entries. Example 1-17 provides an example of the routing table with the
directly connected interfaces of R1 configured and activated.

**Example 1-17  Verifying the Directly Connected Routing Table Entries**

```
R1# show ip route | begin Gateway
Gateway of last resort is not set

    192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
    C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
    L       192.168.10.1/32 is directly connected, GigabitEthernet0/0

    192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
    C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
    L       192.168.11.1/32 is directly connected, GigabitEthernet0/1

    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
    C       209.165.200.224/30 is directly connected, Serial0/0/0
    L       209.165.200.225/32 is directly connected, Serial0/0/0

R1#
```

**Directly Connected IPv6 Example (1.3.2.4)**

Example 1-18 shows the configuration steps for the directly connected interfaces of
R1 in Figure 1-21 with the indicated IPv6 addresses. Notice the Layer 1 and Layer 2
informational messages generated as each interface is configured and activated.

**Example 1-18  Configuring the Directly Connected IPv6 Interfaces**

```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
*Feb  3 21:38:37.279: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state
to down
*Feb  3 21:38:40.967: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state
to up
*Feb  3 21:38:41.967: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEther-
net0/0, changed state to up
R1(config)# interface gigabitethernet 0/1
R1(config-if)# description Link to LAN 2
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
```
The `show ipv6 route` command shown in Example 1-19 is used to verify that IPv6 networks and specific IPv6 interface addresses have been installed in the IPv6 routing table. Like IPv4, a ‘C’ next to a route indicates that this is a directly connected network. An ‘L’ indicates the local route. In an IPv6 network, the local route has a /128 prefix. Local routes are used by the routing table to efficiently process packets with a destination address of the interface of the router.

**Example 1-19 Verifying IPv6 Routing Table**

```
R1# show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDP - ND Prefix, DCE - Destination
       NDR - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:1:1/128 [0/0]
    via GigabitEthernet0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:2:1/128 [0/0]
    via GigabitEthernet0/1, receive
L   FF00::/8 [0/0]
    via Null0, receive
R1#
```
Notice that there is also a route installed to the FF00::/8 network. This route is required for multicast routing.

Example 1-20 displays how the `show ipv6 route` command can be combined with a specific network destination to display the details of how the router learned that route.

**Example 1-20 Verifying a Single IPv6 Route Entry**

```
R1# show ipv6 route 2001:db8:acad:1::/64
Routing entry for 2001:DB8:ACAD:1::/64
   Known via "connected", distance 0, metric 0, type connected
   Route count is 1/1, share count 0
   Routing paths:
      directly connected via GigabitEthernet0/0
      Last updated 03:14:56 ago
```

Example 1-21 displays how connectivity to R2 can be verified using the `ping` command. Notice what happens when the G0/0 LAN interface of R2 is the target of the `ping` command. The pings are unsuccessful. This is because R1 does not have an entry in the routing table to reach the 2001:DB8:ACAD:4::/64 network.

**Example 1-21 Testing Connectivity to R2**

```
R1# ping 2001:db8:acad:3::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:3::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/13/16 ms
R1# ping 2001:db8:acad:4::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:4::1, timeout is 2 seconds:

% No valid route for destination
Success rate is 0 percent (0/1)
R1#
```

R1 requires additional information to reach a remote network. Remote network route entries can be added to the routing table using either of the following:

- Static routing
- Dynamic routing protocols
Packet Tracer 1.3.2.5: Investigating Directly Connected Routes

Background

The network in the activity is already configured. You will log in to the routers and use show commands to discover and answer the questions below about the directly connected routes.

Statically Learned Routes (1.3.3)

In this topic you will learn how a router builds a routing table using static routes.

Static Routes (1.3.3.1)

After directly connected interfaces are configured and added to the routing table, static or dynamic routing can be implemented.

Static routes are manually configured. They define an explicit path between two networking devices. Unlike a dynamic routing protocol, static routes are not automatically updated and must be manually reconfigured if the network topology changes. The benefits of using static routes include improved security and resource efficiency. Static routes use less bandwidth than dynamic routing protocols, and no CPU cycles are used to calculate and communicate routes. The main disadvantage to using static routes is the lack of automatic reconfiguration if the network topology changes.

There are two common types of static routes in the routing table:

- Static route to a specific network
- Default static route

A static route can be configured to reach a specific remote network. IPv4 static routes are configured using the following command:

```
Router(config)# ip route network mask { next-hop-ip | exit-intf }
```

A static route is identified in the routing table with the code ‘S.’

A default static route is similar to a default gateway on a host. The default static route specifies the exit point to use when the routing table does not contain a path for the destination network. A default static route is useful when a router has only one exit point to another router, such as when the router connects to a central router or service provider.

To configure an IPv4 default static route, use the following command:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 { exit-intf | next-hop }
```
Figure 1-36 provides a simple scenario of how default and static routes can be applied.

**Figure 1-36  Static and Default Route Scenario**

**Static Route Examples (1.3.3.2)**

Example 1-22 shows the configuration and verification of an IPv4 default static route on R1 from Figure 1-20. The static route is using Serial 0/0/0 as the exit interface. Notice that the configuration of the route generated an ‘S*’ entry in the routing table. The ‘S’ signifies that the route source is a static route, whereas the asterisk (*) identifies this route as a possible candidate to be the default route. In fact, it has been chosen as the default route as evidenced by the line that reads, “Gateway of Last Resort is 0.0.0.0 to network 0.0.0.0.”

**Example 1-22 Configuring and Verifying a Default Static IPv4 Route**

```
R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/0
R1(config)# exit
R1#
Feb 1 10:19:34.483: %SYS-5-CONFIG_I: Configured from console by console
R1# show ip route | begin Gateway
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, Serial0/0/0
    192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
    192.168.10.0/24 is directly connected, GigabitEthernet0/0
C    192.168.10.0/24 is directly connected, GigabitEthernet0/0
L    192.168.10.1/32 is directly connected, GigabitEthernet0/0
L    192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
```
Example 1-23 shows the configuration and verification of two static routes from R2 to reach the two LANs on R1. The route to 192.168.10.0/24 has been configured using the exit interface while the route to 192.168.11.0/24 has been configured using the next-hop IPv4 address. Although both are acceptable, there are some differences in how they operate. For instance, notice how different they look in the routing table. Also notice that because these static routes were to specific networks, the output indicates that the Gateway of Last Resort is not set.

**Example 1-23 Configuring and Verifying Static IPv4 Routes**

```bash
R2(config)# ip route 192.168.10.0 255.255.255.0 s0/0/0
R2(config)# ip route 192.168.11.0 255.255.255.0 209.165.200.225
R2(config)# exit
R2# show ip route | begin Gateway
Gateway of last resort is not set

  10.0.0.0/8 is variably sub net ted, 4 sub nets, 2 masks
C 10.1.1.0/24 is directly connected, GigabitEthernet0/0
L 10.1.1.1/32 is directly connected, GigabitEthernet0/0
C 10.1.2.0/24 is directly connected, GigabitEthernet0/1
L 10.1.2.1/32 is directly connected, GigabitEthernet0/1
S 192.168.10.0/24 is directly connected, Serial0/0/0
S 192.168.11.0/24 [1/0] via 209.165.200.225

  209.165.200.0/24 is variably sub net ted, 2 sub nets, 2 masks
C 209.165.200.224/30 is directly connected, Serial0/0/0
L 209.165.200.226/32 is directly connected, Serial0/0/0
R2#
```

**Note**

Static and default static routes are discussed in detail in the next chapter.
Static IPv6 Route Examples (1.3.3.3)

Like IPv4, IPv6 supports static and default static routes. They are used and configured like IPv4 static routes.

To configure a default static IPv6 route, use the `ipv6 route ::/0 {ipv6-address | interface-type interface-number}` global configuration command.

Example 1-24 shows the configuration and verification of a default static route on R1 from Figure 1-21. The static route is using Serial 0/0/0 as the exit interface.

**Example 1-24 Configuring and Verifying a Default Static IPv6 Route**

```
R1(config)# ipv6 route ::/0 s0/0/0
R1(config)# exit
```

```
R1# show ipv6 route
IPv6 Routing Table - default - 8 entries
Codes:  C - Connected, L - Local, S - Static, U - Per-user Static route
        B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
        I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
        EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
        NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
        OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
$ ::/0 [1/0]
    via Serial0/0/0, directly connected
```

Notice in the output that the default static route configuration generated an ‘S’ entry in the routing table. The ‘S’ signifies that the route source is a static route. Unlike the IPv4 static route, there is no asterisk (*) or Gateway of Last Resort explicitly identified.

Like IPv4, static routes are routes explicitly configured to reach a specific remote network. Static IPv6 routes are configured using the `ipv6 route ipv6-prefix/prefix-length {ipv6-address|interface-type interface-number}` global configuration command.

Example 1-25 shows the configuration and verification of two static routes from R2 to reach the two LANs on R1. The route to the 2001:0DB8:ACAD:2::/64 LAN is configured with an exit interface, whereas the route to the 2001:0DB8:ACAD:1::/64 LAN is configured with the next-hop IPv6 address. The next-hop IPv6 address can be either an IPv6 global unicast or a link-local address.
Example 1-25 Configuring and Verifying Static IPv6 Routes

```plaintext
R2(config)# ipv6 route 2001:DB8:ACAD:1::/64 2001:DB8:ACAD:3::1
R2(config)# ipv6 route 2001:DB8:ACAD:2::/64 s0/0/0
R2(config)# end
R2# show ipv6 route
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S  2001:DB8:ACAD:1::/64 [1/0]
   via 2001:DB8:ACAD:3::1
S  2001:DB8:ACAD:2::/64 [1/0]
   via Serial0/0/0, directly connected
<output omitted>
```

Example 1-26 confirms remote network connectivity to the 2001:0DB8:ACAD:4::/64 LAN on R2 from R1.

Example 1-26 Verify Connectivity to Remote Network

```plaintext
R1# ping 2001:db8:acad:4::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:4::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/13/16 ms
R1#
```

Dynamic Routing Protocols (1.3.4)

In this topic you will learn how a router builds a routing table using dynamic routes.

Dynamic Routing (1.3.4.1)

Dynamic routing protocols are used by routers to share information about the reachability and status of remote networks. Dynamic routing protocols perform several activities, including network discovery and maintaining routing tables.

Network discovery is the ability of a routing protocol to share information about the networks that it knows about with other routers that are also using the same routing protocol. Instead of depending on manually configured static routes to remote networks on every router, a dynamic routing protocol allows the routers to
automatically learn about these networks from other routers. These networks, and
the best path to each, are added to the routing table of the router and identified as a
network learned by a specific dynamic routing protocol.

During network discovery, routers exchange routes and update their routing tables.
Routers have converged after they have finished exchanging and updating their
routing tables. Routers then maintain the networks in their routing tables.

Figure 1-37 provides a simple scenario of how two neighboring routers would
initially exchange routing information. In this simplified exchange, R1 introduces
itself and the networks it can reach. R2 responds with its list of networks.

Figure 1-37 Dynamic Routing Scenario

IPv4 Routing Protocols (1.3.4.2)
A router running a dynamic routing protocol does not only make a best path
determination to a network; it also determines a new best path if the initial path
becomes unusable (or if the topology changes). For these reasons, dynamic routing
protocols have an advantage over static routes. Routers that use dynamic routing
protocols automatically share routing information with other routers and compensate
for any topology changes without involving the network administrator.

Cisco routers can support a variety of dynamic IPv4 routing protocols, including these:

- **EIGRP**—Enhanced Interior Gateway Routing Protocol
- **OSPF**—Open Shortest Path First
- **IS-IS**—Intermediate System-to-Intermediate System
- **RIP**—Routing Information Protocol
To determine which routing protocols the IOS supports, use the `router ?` command in global configuration mode, as shown in Example 1-27.

**Example 1-27 IPv4 Routing Protocols**

```
R1(config)# router ?
  bgp       Border Gateway Protocol (BGP)
  eigrp     Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis      ISO IS-IS
  iso-igrp  IGRP for OSI networks
  mobile    Mobile routes
  odr       On Demand stub Routes
  ospf      Open Shortest Path First (OSPF)
  ospfv3    OSPFv3
  rip       Routing Information Protocol (RIP)
```

**IPv4 Dynamic Routing Examples (1.3.4.3)**

In this dynamic routing example, assume that R1 and R2 have been configured to support the dynamic routing protocol EIGRP. R2 now has a connection to the Internet, as shown in Figure 1-38. The routers also advertise directly connected networks. R2 advertises that it is the default gateway to other networks.

![IPv4 Topology with Connection to the Internet](image)

**Figure 1-38 IPv4 Topology with Connection to the Internet**

The output in Example 1-28 displays the routing table of R1 after the routers have exchanged updates and converged.

**Example 1-28 Verify Dynamic IPv4 Routes**

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
D*EX  0.0.0.0/0 [170/2297856] via 209.165.200.226, 00:07:29, Serial0/0/0
10.0.0.0/24 is subjetted, 2 subnets
```
Along with the connected and link-local interfaces, there are three ‘D’ entries in the routing table.

- The entry beginning with ‘D’EX’ identifies that the source of this entry was EIGRP (‘D’). The route is a candidate to be a default route (**”), and the route is an external route (“EX”) forwarded by EIGRP.

- The other two ‘D’ entries are routes installed in the routing table based on the update from R2 advertising its LANs.

**IPv6 Routing Protocols (1.3.4.4)**

ISR devices support the dynamic IPv6 routing protocols shown in Example 1-29.

**Example 1-29  IPv6 Routing Protocols**

```
R1(config)# ipv6 router ?
eigrp     Enhanced Interior Gateway Routing Protocol (EIGRP)
ospf      Open Shortest Path First (OSPF)
rip       IPv6 Routing Information Protocol (RIPv6)
```

Support for dynamic IPv6 routing protocols is dependent on hardware and IOS version. Most of the modifications in the routing protocols are to support the longer IPv6 addresses and different header structures.

IPv6 routing is not enabled by default. Therefore, to enable IPv6 routers to forward traffic, you must configure the ipv6 unicast-routing global configuration command.
IPv6 Dynamic Routing Examples (1.3.4.5)

Routers R1 and R2 in Figure 1-21 have been configured with the dynamic routing protocol EIGRP for IPv6. (This is the IPv6 equivalent of EIGRP for IPv4.)

To view the routing table on R1, enter the `show ipv6 route` command, as shown in Example 1-30.

**Example 1-30 Verify Dynamic IPv6 Routes**

```
R1# show ipv6 route
IPv6 Routing Table - default - 9 entries
Codes:  C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, Ndp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
    via GigabitEthernet0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
    via GigabitEthernet0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
    via Serial0/0/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
    via Serial0/0/0, receive
D   2001:DB8:ACAD:4::/64 [90/2172416]
    via FE80::D68C:B5FF:FECE:A120, Serial0/0/0
D   2001:DB8:ACAD:5::/64 [90/2172416]
    via FE80::D68C:B5FF:FECE:A120, Serial0/0/0
L   FF00::/8 [0/0]
    via Null0, receive
R1#
```

The output shows the routing table of R1 after the routers have exchanged updates and converged. Along with the connected and local routes, there are two ‘D’ entries (EIGRP routes) in the routing table.
Summary (1.4)

Class Activity 1.4.1.1: We Really Could Use a Map!

Scenario

Use the Ashland and Richmond routing tables shown in the file provided with this activity.

With the help of a classmate, draw a network topology using the information from the tables.

To assist you with this activity, follow these guidelines:

- Start with the Ashland router; use its routing table to identify ports and IP addresses/networks.
- Add the Richmond router; use its routing table to identify ports and IP addresses/networks.
- Add any other intermediary and end devices as specified by the tables.

In addition, record answers from your group to the reflection questions provided with this activity.

Be prepared to share your work with another group or the class.

There are many key structures and performance-related characteristics referred to when discussing networks: topology, speed, cost, security, availability, scalability, and reliability.

Cisco routers and Cisco switches have many similarities. They support a similar modal operating system, similar command structures, and many of the same commands. One distinguishing feature between switches and routers is the type of interfaces supported by each. Once an interface is configured on both devices, the appropriate `show` commands need to be used to verify a working interface.

The main purpose of a router is to connect multiple networks and forward packets from one network to the next. This means that a router typically has multiple interfaces. Each interface is a member or host on a different IP network.

Cisco IOS uses what is known as the administrative distance (AD) to determine the route to install into the IP routing table. The routing table is a list of networks the router knows. The routing table includes network addresses for its own interfaces, which are the directly connected networks, as well as network addresses for remote networks. A remote network is a network that can only be reached by forwarding the packet to another router.
Remote networks are added to the routing table in two ways: either by the network administrator manually configuring static routes or by implementing a dynamic routing protocol. Static routes do not have as much overhead as dynamic routing protocols; however, static routes can require more maintenance if the topology is constantly changing or is unstable.

Dynamic routing protocols automatically adjust to changes without intervention from the network administrator. Dynamic routing protocols require more CPU processing and use a certain amount of link capacity for routing updates and messages. In many cases, a routing table will contain both static and dynamic routes.

Routers make their primary forwarding decision at Layer 3, the network layer. However, router interfaces participate in Layers 1, 2, and 3. Layer 3 IP packets are encapsulated into a Layer 2 data link frame and encoded into bits at Layer 1. Router interfaces participate in Layer 2 processes associated with their encapsulation. For example, an Ethernet interface on a router participates in the ARP process like other hosts on that LAN.

The Cisco IP routing table is not a flat database. The routing table is actually a hierarchical structure that is used to speed up the lookup process when locating routes and forwarding packets.

Components of the IPv6 routing table are similar to the IPv4 routing table. For instance, it is populated using directly connected interfaces, static routes, and dynamically learned routes.

**Practice**

The following activities provide practice with the topics introduced in this chapter. The Labs and Class Activities are available in the companion *Routing and Switching Essentials v6 Labs and Study Guide* (ISBN 9781587134265). The Packet Tracer Activities PKA files are found in the online course.

**Class Activities**

Class Activity 1.0.1.2: Do We Really Need a Map Final

Class Activity 1.4.1.1: We Really Could Use A Map

**Labs**

Lab 1.1.1.9: Mapping the Internet

Lab 1.1.4.6: Configuring Basic Router Settings with IOS CLI
Packet Tracer Activities
Packet Tracer 1.1.1.8: Using Traceroute to Discover the Network
Packet Tracer 1.1.2.9: Documenting the Network
Packet Tracer 1.1.3.5: Configuring IPv4 and IPv6 Interfaces
Packet Tracer 1.1.4.5: Configuring and Verifying a Small Network
Packet Tracer 1.3.2.5: Investigating Directly Connected Routes

Check Your Understanding Questions
Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. The appendix, “Answers to the ‘Check Your Understanding’ Questions,” lists the answers.

1. Which of the following correctly explains a network characteristic?
   A. Availability indicates how easily the network can accommodate more users and data transmission requirements.
   B. Reliability is often measured as a probability of failure or as the mean time between failures (MTBF).
   C. Scalability is the likelihood that the network is available for use when it is required.
   D. Usability is how effectively end users can use the network.

2. What are two functions of a router? (Choose two.)
   A. It connects multiple IP networks.
   B. It controls the flow of data via the use of Layer 2 addresses.
   C. It determines the best path to send packets.
   D. It increases the size of the broadcast domain.
   E. It manages the VLAN database.

3. Which two statements correctly describe the concepts of administrative distance and metric? (Choose two.)
   A. Administrative distance refers to the trustworthiness of a particular route.
   B. A router first installs routes with higher administrative distances.
   C. Routes with the smallest metric to a destination indicate the best path.
   D. The metric is always determined based on hop count.
E. The metric varies depending which Layer 3 protocol is being routed, such as IP.
F. The value of the administrative distance cannot be altered by the network administrator.

4. For packets to be sent to a remote destination, what three pieces of information must be configured on a host? (Choose three.)
   A. Default gateway
   B. DHCP server address
   C. DNS server address
   D. Hostname
   E. IP address
   F. Subnet mask

5. What is a characteristic of an IPv4 loopback interface on a Cisco IOS router?
   A. It is a logical interface internal to the router.
   B. It is assigned to a physical port and can be connected to other devices.
   C. Only one loopback interface can be enabled on a router.
   D. The `no shutdown` command is required to place this interface in an “up” state.

6. What two pieces of information are displayed in the output of the `show ip interface brief` command? (Choose two.)
   A. Interface descriptions
   B. IP addresses
   C. Layer 1 statuses
   D. MAC addresses
   E. Next-hop addresses
   F. Speed and duplex settings

7. A packet moves from a host on one network to a device on a remote network within the same company. In most cases, which two items remain unchanged during the transfer of the packet from source to destination? (Choose two.)
   A. Destination MAC address
   B. Destination IP address
   C. Layer 2 header
   D. Source ARP table
   E. Source MAC address
   F. Source IP address
8. Which two items are used by a host device when performing an ANDing operation to determine whether a destination address is on the same local network? (Choose two.)
   A. Destination MAC address
   B. Destination IP address
   C. Network number
   D. Source MAC address
   E. Subnet mask

9. Refer to Example 1-28. What will the router do with a packet that has a destination IP address of 192.168.12.227?
   A. Drop the packet.
   B. Send the packet out the GigabitEthernet0/0 interface.
   C. Send the packet out the GigabitEthernet0/1 interface.
   D. Send the packet out the Serial0/0/0 interface.

10. Which two parameters does EIGRP use as metrics to select the best path to reach a network? (Choose two.)
    A. Bandwidth
    B. Confidentiality
    C. Delay
    D. Hop count
    E. Jitter
    F. Resiliency

11. What route would have the lowest administrative distance?
    A. A directly connected network
    B. A route received through the EIGRP routing protocol
    C. A route received through the OSPF routing protocol
    D. A static route

12. Consider the following routing table entry for R1:
    
    D 10.1.1.0/24 [90/2170112] via 10.2.1.1, 00:00:05, Serial0/0/0
    
    What is the significance of the Serial0/0/0?
    A. It is the interface on R1 used to send data that is destined for 10.1.1.0/24.
    B. It is the interface on the final destination router that is directly connected to the 10.1.1.0/24 network.
C. It is the interface on the next-hop router when the destination IP address is on the 10.1.1.0/24 network.
D. It is the R1 interface through which the EIGRP update was learned.

13. Refer to Example 1-19. A network administrator issues the `show ipv6 route` command on R1. What two conclusions can be drawn from the routing table? (Choose two.)
   A. Interface G0/1 is configured with IPv6 address 2001:DB8:ACAD:2::12.
   B. Network FF00::/8 was learned from a static route.
   C. Packets destined for the network 2001:DB8:ACAD:1::/64 will be forwarded through G0/1.
   D. Packets destined for the network 2001:DB8:ACAD:2::/64 will be forwarded through G0/1.
   E. R1 does not have any remote network routes.

14. A network administrator configures interface G0/0 on R1 with the `ip address 172.16.1.254 255.255.255.0` command. However, when the administrator issues the `show ip route` command, the routing table does not show the directly connected network. What is the possible cause of the problem?
   A. Interface G0/0 has not been activated.
   B. No packets with a destination network of 172.16.1.0 have been sent to R1.
   C. The configuration needs to be saved first.
   D. The subnet mask is incorrect for the IPv4 address.

15. A network administrator configures a router using the command `ip route 0.0.0.0 0.0.0.0 209.165.200.226`. What is the purpose of this command?
   A. To add a dynamic route for the destination network 0.0.0.0 to the routing table
   B. To forward all packets to the device with IP address 209.165.200.226
   C. To forward packets destined for the network 0.0.0.0 to the device with IP address 209.165.200.226
   D. To provide a route to forward packets for which there is no route in the routing table

16. What are two common types of static routes in routing tables? (Choose two.)
   A. A built-in static route by IOS
   B. A default static route
   C. A static route converted from a route that is learned through a dynamic routing protocol
D. A static route that is dynamically created between two neighboring routers
E. A static route to a specific network

17. What command will enable a router to begin sending messages that allow it to configure a link-local address without using an IPv6 DHCP server?

A. A static route
B. The `ip routing` command
C. The `ipv6 route ::/0` command
D. The `ipv6 unicast-routing` command
This page intentionally left blank
Symbols

* (asterisk), 59
: (colon), 452
? (question mark) command, 532
802.1Q tagging, 257–258

A

access control entries. See ACEs (access control entries)
access control lists. See ACLs (access control lists)
access layer, 179
access-class command, 339–341
accessing infrastructure devices, 21–22
access-list command, 325–326, 437–438
ACEs (access control entries)
definition of, 312
order of, 343–344
ACLs (access control lists)
ACEs (access control entries)
definition of, 312
order of, 343–344
best practices, 322
definition of, 311–312
extended ACLs (access control lists), 312–313
guidelines for creating, 321–322
inbound ACLs, 313–314
outbound ACLs, 313–314
packet filtering, 312–313
placement of, 322–325
processing packets withCisco IOS reordering of ACLs, 343–344
implicit deny any, 343
order of ACEs (access control entries), 343–344
routing processes, 347–349
securing VTY ports with, 339–342
standard IPv4 ACL configuration
links to interfaces, 328–329
named standard ACL syntax, 330–332
numbered standard ACL examples, 329–330
numbered standard ACL syntax, 325–327
standard IPv4 ACL modification
with sequence numbers, 334–335
standard named ACLs, 335–336
with text editor, 333–334
statistics, 338–339
verification, 336–337
wildcard masks
calculating, 317–319
examples, 316–317
keywords, 319–320
overview, 314–315
activating Evaluation Right-to-Use (RTU) licenses, 529–531
AD (administrative distance)
default administrative distances, 47–48
dynamic routing
definition of, 79
IPv4, 151
IPv6, 163
overview, 133, 162
static routing, 107
adapters, USB-to-RS-232 compatible, 21
address pool (PAT), 443–445
address prefix command, 399–400, 406
Address Resolution Protocol (ARP) cache, 40
document network addressing, 17–18
hierarchical network-addressing scheme, 249
IP (Internet Protocol). See IPv4; IPv6
MAC (media access control). See MAC address tables
NAT (network address translation). See NAT
(address network translation)
addressing tables, 17–18
adjacency tables, 12–13
administrative distance. See AD (administrative distance)
Advanced Research Projects Agency Network (ARPANET), 130
ADVERTISE message, 394
advertising networks, 138–139
algorithms, 132
alleviation of network congestion, 195–196
analysis
NAT (network address translation)
dynamic NAT, 438–440
static NAT, 433–434
PAT (Port Address Translation), 446–448
routing tables
overview, 49
remote network routing entries, 51–52
sources, 49–51
any keyword, 319–320
application-specific-integrated circuits (ASICs), 189
ARP (Address Resolution Protocol) cache, 40
ARPANET (Advanced Research Projects Agency
Network), 130
ASICs (application-specific-integrated circuits), 189
assigning ports to VLANs, 263
asterisk (*), 59
authoritative time sources, 488
automated attendants, 176
automatic buffering, 191
automatic medium-dependent interface crossover
(auto-MDIX), 215–216
automatic summarization, 142–143
automatically installed host routes, 111–113
auto-MDIX, 215–216
autonegotiation, 193
availability, 5

B
backing up
IOS images, 517–519
software licenses, 531–532
to text files, 505–507
with TFTP (Trivial File Transfer Protocol), 507–508
with USB flash drives, 508–510
balancing load, 46–47
bandwidth, wasted, 144
basic router settings, 23–24
best path, determining, 45–46
BGP (Border Gateway Protocol), 131
bits per second (b/s), 5

BOOT environment variable, 206
boot loader
boot sequence, 205–206
system crash recovery, 205–206
boot sequence (switches), 205–206
boot system command, 206, 521–522
Border Gateway Protocol (BGP), 131
borderless switched networks
Cisco Borderless Networks, 176–177
hierarchical design frameworks, 177–179
Branch site devices, 15
break sequences, 511
bridges (Ethernet), 189
broadcast domains
controlling with VLANs, 254–256
overview, 194–195, 250
b/s (bits per second), 5
buffering, automatic, 191

C

cache
ARP (Address Resolution Protocol) cache, 40
fast-switching cache, 12
neighbor cache, 40
calculating wildcard masks, 317–319
call control, 176
CAM (content addressable memory), 186
CAM tables. See MAC address tables
Canonical Format Identifier (CFI), 257
cd command, 504
CDP (Cisco Discovery Protocol)
configuration, 478–480
disabling, 478
discovering devices with, 480–483
overview, 477–478
packets, 258
verification, 478–480
cdp enable command, 479
cdp run command, 478
CEF (Cisco Express Forwarding), 12–13, 90, 158
Central site devices, 16
Cerf, Vint, 417
CFI (Canonical Format Identifier), 257
derive directory (cd) command, 504
CIADDR (client IPv4 address), 369
CIDR (classless inter-domain routing) prefix, 418
Cisco 1941 router LEDs, 19–20
Cisco Borderless Networks, 176–177
Cisco Discovery Protocol. See CDP (Cisco Discovery Protocol)
Cisco Express Forwarding (CEF), 12–13, 90, 158
Cisco IOS, 7
Cisco License Manager (CLM), 525
Cisco License Registration Portal, 525
Cisco StackPower technology, 185
Cisco StackWise technology, 185
class of service (CoS), 258
classful routing protocols, 139, 141
classless inter-domain routing (CIDR) prefix, 418
clear access-list counters command, 338–339, 353
clear ip nat statistics command, 435
clear ip nat translation command, 441
clearing
   NAT translations, 441
   software licenses, 502, 532–533
CLI (command-line interface), 493
client IPv4 address (CIADDR), 369
clients
   DHCPv4
      configuring wired routers as, 380–381
      configuring wireless routers as, 381–382
   DHCPv6
      configuration, 396–399
      stateful DHCPv6, 401
CLM (Cisco License Manager), 525
clock, setting, 487
clock command, 487
clock rate command, 25
collapsed core layer model, 177–181
collision domains, 193–194
collisions
   collision domains, 193–194
   half-duplex versus full-duplex operations, 220
   late collisions, 222
colon (:), 452
command history feature, 36–37
command-line interface (CLI), 493
commands
   access-class, 339–341
   access-list, 325–326, 437–438
   address prefix, 399–400, 406
boot system, 206, 521–522
cd, 504
cdp enable, 479
cdp run, 478
clear access-list counters, 338–339, 353
clear ip nat statistics, 435
clear ip nat translation, 441
clock, 487
clock rate, 25
command history feature, 36–37
confreg, 511
copy, 520
copy run usbflash0:/509
copy running-config startup-config, 212, 262, 294, 512
copy running-config tftp, 507
crypto key generate rsa, 225
crypto key zeroize rsa, 225
debug ip dhcp server events, 386
debug ip nat, 462–464
debug ip packet, 386
debug ipv6 dhcp detail, 398–399, 407–408
default-information originate, 146
default-router, 372
delete flash:vlan.dat, 266–267
description, 25
dir, 207, 503–504, 510
dns-server, 372, 395, 400
domain-name, 372, 396, 400
duplex, 214
encapsulation, 298
erase startup-config, 267
implicit deny any, 343
interface loopback, 29
interface range, 230, 263
ip access-group, 328–329
ip access-list standard, 335
ip address, 24, 294
ip address dhcp, 380–381
ip default-gateway, 240
ip dhcp excluded-address, 371
ip dhcp pool, 371
ip domain-name, 225
ip helper-address, 378–380, 384
ip nat inside, 432, 438
ip nat inside source, 454–455
578 commands

ip nat inside source list, 438
ip nat inside source static, 432
ip nat outside, 432, 438
ip nat pool, 437
ip route, 58, 84–85, 93, 107
ipconfig, 275
ipconfig all, 376–377
ipconfig release, 378
ipconfig /renew, 378
ipv6 address, 26–27
ipv6 address autoconfig, 397
ipv6 address dhcp, 401
ipv6 dhcp pool, 395, 399
ipv6 dhcp relay destination, 403, 405
ipv6 dhcp server, 396, 400
ipv6 enable, 397, 401
ipv6 nd managed-config-flag, 400, 406
ipv6 nd other-config-flag, 392–393, 396, 406
ipv6 route, 61, 95–96, 104–105, 110
ipv6 unicast-routing, 27, 65, 96, 389, 395, 399
lease, 372
license accept end user agreement, 529
license boot module, 530, 532, 532
license clear, 532
license install, 526, 531
license save, 531
line vty, 226
lldp run, 484
logging, 499
logging buffered, 497–498
logging console, 497–498
logging source-interface, 499
logging trap, 499
login local, 226
mdix, 214
more, 510
name, 262
network, 138–139, 372
no access-list, 326, 334
no auto-summary, 143
no cdp enable, 479
no cdp run, 478
no ip access-group, 328
no ipv6 nd managed-config-flag, 392
no license boot module, 532
no lldp run, 484
no passive-interface, 145
no router rip, 138
no service dhcp, 373, 385
no shutdown, 26, 229, 295, 298
no switchport access vlan, 264, 278
no switchport trunk allowed vlan, 272
no switchport trunk native vlan, 272
no version, 142
no vlan, 266
ntp server, 489
passive-interface, 144–145
passive-interface default, 145
ping, 34, 57, 87, 98, 106, 117, 119, 276, 300–301
pwd, 505
reload, 527, 530
router ?64
router rip, 137
service dhcp, 373
service timestamps log datetime, 496
show
filtering output of, 35–36
options, 216–217
show access-list, 350–351
show access-lists, 326, 337–338, 341, 345–346, 347
show boot, 206
show cdp, 478
show cdp interface, 479–480
show cdp neighbors, 118, 479, 480–482
show clock, 489
show controllers ethernet-controller, 216
show file systems, 502–503, 505
show flash, 515
show interface, 214
show interfaces, 217–222, 268–270, 383
show interfaces interface-id switchport, 259, 264,
272, 273, 278
show interfaces trunk, 279, 280, 281–282, 284–285
show ip dhcp binding, 374–376
show ip dhcp conflict, 383
show ip dhcp server statistics, 374–376
show ip interface, 336–337, 381
show ip interface brief, 30–31, 32, 118, 211
show ip nat, 460–462
show ip nat statistics, 435, 442, 449–450, 464–467
show ip nat translations, 434–435, 440–441, 449,
455, 464–467
configuration  579

show ip ntp associations, 490–491
show ip protocols, 139, 141, 143, 144–145
show ip route static, 92, 94
show ip ssh, 225, 228
show ipv6 dhcp binding, 401–402
show ipv6 dhcp conflict, 404
show ipv6 dhcp interface, 403
show ipv6 dhcp pool, 397, 401
show ipv6 interface, 397–398, 402
show ipv6 interface gigabitethernet 0/0, 33
show ipv6 route static, 103, 105, 111
show license, 528–529, 531
show license feature, 523
show license udi, 525–526
show lldp neighbors, 484–485
show lldp neighbors detail, 485–486
show logging, 498–499, 500–501
show mac address-table, 277
show ntp status, 490–491
show port-security address, 235–236
show port-security interface, 234–235, 236–237
show run, 351
show running-config, 217, 333–334, 346, 384
show running-config | include no service dhcp, 385
show running-config | section dhcp, 373–374
show running-config interface, 30, 32
show ssh, 228
show version, 224, 527
show vlan, 267–268, 277
show vlan brief, 250–251, 261, 264, 266
shutdown, 229, 298
speed, 214
switchport access vlan, 263, 294
switchport mode access, 263, 272, 282
switchport mode trunk, 270–271, 280, 281, 297
switchport port-security, 234
switchport port-security mac-address, 231
switchport port-security mac-address sticky, 231
switchport port-security violation, 233
switchport trunk allowed vlan, 270, 284, 285
switchport trunk native vlan, 270
traceroute, 109–110, 117, 119
tracert, 301–302
transport input ssh, 226
version 2, 141
vlan, 262
complexity of converged networks, 174–175
configuration
CDP (Cisco Discovery Protocol), 478–480
DHCPv4 servers
  command syntax, 371–372
  DHCPv4 pool, 371
disabling DHCPv4, 373
example, 372–373
IPv4 addresses, excluding, 371
relay, 377–380
topology, 370–371
verification, 373–377
DHCPv6
debugging, 407–408
verification, 405–407
IPv4 default static routes
  example, 93
  ip route command, 93
overview, 81–82
verification, 94–95
IPv4 floating static routes, 106–110
IPv4 standard static routes
directly connected static routes, 88–90
fully specified static routes, 90–91
ip route command, 84–85
next-hop options, 85–87
next-hop route configuration, 87–88
overview, 81
verification, 92, 103–104
IPv6 default static routes
  example, 105
ipv6 route command, 104–105
overview, 81–82
verification, 105–106
IPv6 floating static routes, 110–111
IPv6 standard static routes
directly connected static routes, 100–102
fully specified static routes, 102–103
ipv6 route command, 95–96
next-hop options, 95–96
next-hop route configuration, 99–100
overview, 81
legacy inter-VLAN routing
  preparation for, 292–293
  router interface configuration, 294–295
  switch configuration, 293–294
LLDP (Link Layer Discovery Protocol), 484
NAT (network address translation)
  dynamic NAT, 437–438
  port forwarding, 453–456
  static NAT, 432–433
NTP (Network Time Protocol), 489–491
PAT (Port Address Translation)
  address pool, 443–445
  single addresses, 445–446
port security, 233–234
RIPv2
  advertising networks, 138–139
  automatic summarization, 142–143
  configuration mode, 136–138
  default route propagation, 145–147
  passive interfaces, 143–145
router-on-a-stick inter-VLAN routing
  preparation for, 296–297
  subinterfaces, 299–300
  switch configuration, 298–299
  verification, 300–302
routers
  basic router settings, 23–24
  IPv4 loopback interfaces, 29–30
  IPv4 router interfaces, 24–26
  IPv6 router interfaces, 26–29
SLAAC (Stateless Address Autoconfiguration)
  SLAAC Option, 390–391
  Stateful DHCPv6 Option, 393
  Stateless DHCPv6 Option, 392–393
SSH (Secure Shell), 225–226
standard IPv4 ACLs
  links to interfaces, 328–329
  named standard ACL syntax, 330–332
  numbered standard ACL examples, 329–330
  numbered standard ACL syntax, 325–327
stateful DHCPv6
  clients, 401
  relay agents, 402–403
  servers, 399–400
stateless DHCPv6
  clients, 396–399
  servers, 395–396
static host routes
  automatically installed host routes, 111–113
  IPv4, 113–114
  IPv6, 113–114
switch ports
  auto-MDIX, 215–216
  DHCPv4, 383
duplex communication, 213–214
network access layer issues, 218–222
physical layer, 214–215
verification, 216–218
switches, 210–212
Syslog
  default logging, 497–499
  router and switch commands, 499–500
switches
  basic router settings, 23–24
  IPv4 loopback interfaces, 29–30
  IPv4 router interfaces, 24–26
  IPv6 router interfaces, 26–29
  SLAAC (Stateless Address Autoconfiguration)
  SLAAC Option, 390–391
  Stateful DHCPv6 Option, 393
  Stateless DHCPv6 Option, 392–393
configuration mode commands. See commands
  configuration register, 511–513
conflicts (DHCP), 404
confreg command, 511
core layer, 180–181
distribution layer, 179
elements of, 175–176
hierarchical design frameworks, 177–179
IEEE 802.1Q trunk links, 270–271
resetting to default state, 272–273
verification, 273–274
converged networks
  access layer, 179
  Cisco Borderless Networks, 176–177
  complexity of, 174–175
content addressable memory (CAM), 186
connectivity problems, troubleshooting,
  118–120
console access, 21–22
core layer, 180–181
distribution layer, 179
copy command, 520
copy run usbflash0:/ command, 509
copy running-config startup-config command, 212, 262, 294, 512
copy running-config tftp command, 507
copying IOS images to devices, 519–520
core layer, 180–181
CoS (class of service), 258
CoS priority values, 258
cost
  of networks, 5
  reduction with VLANs, 250
CPU POST (power-on self-test), 205
CRC (cyclic redundancy check)
  errors, 220
  overview, 189
creating, See also configuration
  ACLs (access control lists)
    best practices, 322
    guidelines for creating, 321–322
    placement of, 322–325
  VLANs (virtual LANs), 262
crypto key generate rsa global configuration mode command, 225
crypto key zeroize rsa global configuration mode command, 225
cut-through switching, 190, 191–193
cyclic redundancy check (CRC)
  errors, 220
  overview, 189

D

DAD (duplicate address detection), 390
DAs (destination addresses), 427
Data license, 523
data structures, 132
data VLANs (virtual LANs), 251–252
datetime keyword, 496
debug ip dhcp server events command, 386
debug ip nat commands, 462–464
debug ip packet command, 386
debug ipv6 dhcp detail command, 398–399, 407–408
debugging
  DHCPv4, 385–387
  DHCPv6, 407–408
  Debugging Levels (Syslog), 494
de-encapsulating packets, 38
default administrative distances, 47–48
default gateway address (GIADDR), 369
default gateways, 16–17
default logging (Syslog), 497–499
default port assignments (VLANs), 250–251
default route propagation, 145–147
default state, resetting trunks to, 272–273
default static routes
  default static routes, 153
IPv4
  configuration, 93
  example, 59–60
  ip route command, 93
  verification, 94–95
IPv6
  configuration, 105
  example, 61
  ipv6 route command, 104–105
  verification, 105–106
  overview, 81–82
default VLANs (virtual LANs), 250–251
default-information originate command, 146
default-router command, 372
delete flash: vlan.dat command, 266–267
deleting
  RSA key pairs, 225
  VLANs (virtual LANs), 266–267
density of ports, 195
deny any statement, 338, 343
deny statement, 338
description command, 25
destination, processing packets at, 43–44
destination addresses (DAs), 427
detail keyword, 489
determining path. See path determination
device connections
  Branch site devices, 15
  Central site devices, 16
  console access, 21–22
  default gateways, 16–17
  device LEDs, 19–20
document network addressing, 17–18
  Home Office devices, 15
IP configuration on hosts, 18–19
IP configuration on switches, 22–23

device discovery
CDP (Cisco Discovery Protocol)
  configuration, 478–480
  disabling, 478
  discovering devices with, 480–483
  overview, 477–478
  verification, 478–480
LLDP (Link Layer Discovery Protocol)
  configuration, 484
  overview, 483
  verification, 484

device LEDs, 19–20

device maintenance
backup and restore
  with text files, 505–507
  with TFTP (Trivial File Transfer Protocol), 507–508
  with USB flash drives, 508–510
IOS images
  backing up to TFTP servers, 517–519
  boot system command, 521–522
  copying to devices, 519–520
IOS system files
  filenames, 515–517
  IOS 15 system image packaging, 514–515
password recovery, 511–513
router file systems, 502–505
software licenses
  backing up, 531–532
  EULA (End User License Agreement), 524
  Evaluation Right-to-Use (RTU) licenses, activating, 529–531
  installing, 526–527
  overview, 522–523
  PAKs (Product Activation Keys), 524–526
  technology package licenses, 522–523
uninstalling, 532–533
verification, 527–529
switch file systems, 505

device management
NTP (Network Time Protocol)
  configuration, 489–491
  system clock, setting, 487
  verification, 489–491
Syslog
  default logging, 497–499
  facilities, 494–495
  message format, 493–495
  operation, 492–493
  overview, 491–492
  router and switch commands, 499–500
  server configuration, 496
  service timestamps, 496
  verification, 500–501
DHCPACK message, 366–367
DHCPDISCOVER message, 365, 369–370
DHCPOFFER message, 365, 369
DHCPREQUEST message, 365–367
DHCPv4. See also DHCPv6
  clients
    configuring wired routers as, 380–381
    configuring wireless routers as, 381–382
  debugging, 385–387
  disabling, 373
  leases
    origination, 365–366
    renewal, 366–367
  messages
    DHCPACK, 366–367
    DHCPDISCOVER, 365, 369–370
    DHCPOFFER, 365, 369
    DHCPREQUEST, 365–367
    message format, 367–368
  overview, 363–364
  relay, 377–380
  servers
    command syntax, 371–372
    DHCPv4 pool, 371
    example, 372–373
    IPv4 addresses, excluding, 371
    topology, 370–371
  troubleshooting
    IPv4 address conflicts, 383
    physical connectivity, 383–384
    switch port configuration, 384
    testing, 384
  verifying configuration of, 373–377, 384–385
DHCPv6. See also DHCPv4
  ADVERTISE message, 394
  debugging, 407–408
INFORMATION-REQUEST message, 394
operations summary, 393
SLAAC (Stateless Address Autoconfiguration)
   host configuration methods, 387–390
   operation, 389–390
   overview, 388–389
   SLAAC Option, 390–391
   Stateful DHCPv6 Option, 393
   Stateless DHCPv6 Option, 392–393
SOLICIT message, 394
stateful DHCPv6
   client configuration, 401
   overview, 393
   relay agent configuration, 402–403
   server configuration, 399–400
   verifying configuration of, 401–402, 406–407
stateless DHCPv6
   client configuration, 396–399
   overview, 392–393
   server configuration, 395–396
   verifying configuration of, 397–399, 405–406
troubleshooting tasks, 404–405
   verifying configuration of, 405–407
diagrams, topology, 17
dir command, 207, 503–504, 510
directly connected entries
IPv4, 149–150
IPv6, 160–162
directly connected networks
routings to, 44
   verifying connectivity of
      command history feature, 36–37
      IPv4 interface settings, 30–32
      IPv6 interface settings, 32–34
      show command output, filtering, 35–36
directly connected static routes
examples, 54–57
interfaces, 52–53
IPv4, 88–90
IPv6, 100–102
routing table entries, 53
disabling
   automatic summarization, 142–143
   CDP (Cisco Discovery Protocol), 478
   DHCPv4, 373
   unused ports, 229–230
discontiguous networks, 148
discovery. See device discovery
distribution layer, 179
dns-server command, 372, 400
dns-server commands, 395
document network addressing, 17–18
domain-name command, 372, 396, 400
domains
   broadcast domains, 194–195
   broadcast domains, controlling with VLANs, 254–256
   collision domains, 193–194
drives, USB flash drives, 508–510
dTP (Dynamic Trunking Protocol), 270
dual-stack, 459
duplex communication, 193, 213–214
duplex interface configuration mode command, 214
duplex mismatch, 222
duplicate address detection (DAD), 390
Dynamic Host Configuration Protocol. See DHCPv4; DHCPv6
dynamic NAT (network address translation)
   address pool configuration, 443–445
   analysis, 438–440, 446–448
   configuration, 437–438
   operation, 436–437
   overview, 425–426
   single address configuration, 445–446
   verification, 440–442, 449–450
dynamic routing
   advantages/disadvantages, 135–136
   compared to static routing, 79
   EIGRP (Enhanced IGRP), 63, 130
   IPv4 routing examples, 64–65
   IPv4 routing tables
      directly connected entries, 149–150
      level 1 parent routes, 154–155
      level 1 routes, 153–154
      level 2 child routes, 155–156
      overview, 147–149
      remote network entries, 150–151
      route lookup process, 156–159
      ultimate routes, 152
   IPv6 routing examples, 66
   IPv6 routing protocols, 65
   IPv6 routing tables
directly connected entries, 160–162
overview, 159–160
remote network entries, 162–164
IS-IS (Intermediate System-to-Intermediate System), 63, 130
OSPF (Open Shortest Path First), 63, 130
overview, 62–63
protocol components, 63–64, 132–133
protocol evolution, 130–132
RIPv2
advertising networks, 138–139
automatic summarization, 142–143
configuration mode, 136–138
default route propagation, 145–147
overview, 63
passive interfaces, 143–145
topology, 137
verification, 139–142
when to use, 134–135
dynamic secure MAC addresses, 231
Dynamic Trunking Protocol (DTP), 270

E

dynamic routing

eedge routers, 145
egress, 186
egress ports, 191
EIGRP (Enhanced IGRP), 46, 63, 130
Emergency Levels (Syslog), 494
capsulating packets, 38
capsulation command, 298
End User License Agreement (EULA), 524
Enhanced IGRP (EIGRP), 46, 63, 130
environment variables, BOOT, 206
equal cost load balancing, 46–47
erase startup-config command, 267
error checking, 190–191
error disabled state, 236–237
errors
ACL (access control list) errors, 349–353
input errors, 220
output errors, 220–221
Ethernet bridges, 189
EUI-64, 27, 390
EULA (End User License Agreement), 524
evaluation licenses, 524
Evaluation Right-to-Use (RTU) licenses, activating, 529–531
evolution of routing protocols, 130–132
excluding IPv4 addresses, 371
exit interfaces, finding, 88
extended ACLs (access control lists), 312–313
extended range VLANs (virtual LANs), 261

F

facilities (Syslog), 494–495
fast switching, 12
fast-switching cache, 12
FCS (frame-check-sequence), 190–191, 256
FDDI (Fiber Distributed Data Interface)
VLANs, 261
FIB (Forwarding Information Base), 12–13, 90
Fiber Distributed Data Interface (FDDI)
VLANs, 261
file system maintenance
router file systems, 502–505
switch file systems, 505
filenames of IOS system files, 515–517
files
backup and restore
with text files, 505–507
with TFTP (Trivial File Transfer Protocol), 507–508
with USB flash drives, 508–510
IOS images
backing up to TFTP servers, 517–519
boot system command, 521–522
copying to devices, 519–520
IOS system files
filenames, 515–517
IOS 15 system image packaging, 514–515
maintenance
router file systems, 502–505
switch file systems, 505
password recovery, 511–513
startup-config, 206
vlan.dat file, 261
zipping, 517
filtering
packets, 312–313
show command output, 35–36
IGRP (Interior Gateway Routing Protocol) 585

finding exit interfaces, 88
fixed configuration switches, 184
flash drives, 508–510
flash file system, 503–504
flash memory, 8
floating static routes
  IPv4 route configuration, 106–110
  IPv6 route configuration, 110–111
overview, 83–84
form factors for switched networks, 183–185
forwarding
  frame forwarding
    cut-through switching, 190, 191–193
    LAN switching examples, 186–188
    MAC address tables, 188–189
    store-and-forward switching, 189–191
  packet forwarding
    to next hop, 39–40
    packet processing, 11–13
port forwarding
  configuration, 453–456
  overview, 451–452
  wireless router example, 452–453
Forwarding Information Base (FIB), 12–13, 90
fragment-free switching, 192–193
frame buffers, 183
frame forwarding
  cut-through switching, 190, 191–193
  LAN switching examples, 186–188
  MAC address tables, 188–189
  store-and-forward switching, 189–191
frame-check-sequence (FCS), 190–191, 256
frames
  frame buffers, 183
  frame forwarding
    cut-through switching, 190, 191–193
    LAN switching examples, 186–188
    MAC address tables, 188–189
    store-and-forward switching, 189–191
giants, 220
runt frames, 220
full-duplex communication, 193, 213–214
fully specified static routes
  IPv4, 90–91
  IPv6, 102–103

G

Gateway of Last Resort, 17, 81
gateways
default gateways, 16–17
Gateway of Last Resort, 17, 45
GIADDR (default gateway address), 369
generating RSA key pairs, 225
GIADDR (default gateway address), 369
giants, 220
global addresses, 421
global unicast addresses, 26–27

H

half-duplex communication, 193, 213–214
help. See troubleshooting
hierarchical design of borderless switched networks, 177–179
hierarchical network-addressing scheme, 249
high port density, 195
high-performance computing (HPC) applications, 193
High-Speed WAN Interface Card (HWIC), 24
Home Office devices, 15
host keyword, 319–320
host routes. See static host routes
hosts
  IP configuration on, 18–19
  matching with wildcard masks, 316–317
HPC (high-performance computing) applications, 193
HWIC (High-Speed WAN Interface Card), 24

I

IAB (Internet Architecture Board), 457
IANA (Internet Assigned Numbers Authority), 457
ICMPv6 (Internet Control Message Protocol version 6)
  Neighbor Solicitation and Neighbor Advertisement messages, 40
  overview, 388
  Router Advertisement messages, 27
IEEE 802.1Q standard, 256
IEEE 802.1Q trunk links, configuring, 270–271
IFS (IOS File System), 502
IGRP (Interior Gateway Routing Protocol), 130
images (IOS)
backing up to TFTP servers, 517–519
  copying to devices, 517–519
implicit deny any command, 343
inbound ACLs (access control lists), 313–314
  include Auto-MDIX filter, 216
indicator lights
  device LEDs, 19–20
  switch LEDs, 207–209
INFORMATION-REQUEST message, 394
ingress, 186
ingress ports, 186–187
input errors, 220
inside addresses, 421
inside global addresses, 422
inside local addresses, 422
inside networks, 420
installing software licenses, 526–527
Integrated Services Routers Generation Two (ISR G2), 514–515
interface identifier (ID), 27
interface loopback command, 29
interface range command, 230, 263
interfaces
  directly connected interfaces, 52–57
  directly connected networks, verifying connectivity of
    command history feature, 36–37
    IPv4 interface settings, 30–32
    IPv6 interface settings, 32–34
    show command output, filtering, 35–36
    IPv4 loopback interfaces, 29–30
  legacy inter-VLAN routing, 294–295
router interfaces
  IPv4 router interface configuration, 24–26
  IPv6 router interface configuration, 26–29
  legacy inter-VLAN routing configuration, 294–295
router-on-a-stick inter-VLAN routing configuration, 299–300
SVI (switched virtual interface), 22, 252
Interior Gateway Routing Protocol (IGRP), 130
Intermediate System-to-Intermediate System (IS-IS), 63, 130
Internet Architecture Board (IAB), 457
Internet Assigned Numbers Authority (IANA), 457
Internet Control Message Protocol version 6 (ICMPv6), 388
inter-VLAN routing
  definition of, 287–288
  legacy inter-VLAN routing
    example, 289
    explained, 287–288
    preparation for, 292–293
  router interface configuration, 294–295
  switch configuration, 293–294
router-on-a-stick inter-VLAN routing
  explained, 290–291
  preparation for, 296–297
  subinterfaces, 299–300
  switch configuration, 298–299
  verification, 300–302
inverse masks. See wildcard masks
IOS 15 system image packaging, 514–515
IOS File System (IFS), 502
IOS images
  backing up to TFTP servers, 517–519
  copying to devices, 517–519
IOS system files
  filenames, 515–517
  IOS 15 system image packaging, 514–515
  ip access-group command, 328–329
  ip access-list standard command, 335
  ip address command, 24, 294
  ip address dhcp command, 380–381
  IP Base license, 522–523
  ip default-gateway command, 240
  ip dhcp excluded-address command, 371
  ip dhcp pool command, 371
  ip domain-name command, 225
  ip helper-address command, 378–380, 384
  ip nat inside command, 432, 438
  ip nat inside source command, 454–455
  ip nat inside source list command, 438
  ip nat inside source static command, 432
  ip nat outside command, 432, 438
  ip nat pool command, 437
  ip route command, 58, 84–85, 93, 107
  ipconfig command, 275
  ipconfig /all, 376–377
  ipconfig /release, 378
  ipconfig /renew, 378
**IPv4**

addresses
- **addressing space**, 131–132
- **conflicts, troubleshooting**, 383
- **excluding in DHCPv4**, 371
- **private address space**, 418–419
- **private addresses**, 418–419
- **public addresses**, 418–419
configuration on switches, 22–23
default static routes
- **example**, 59–60, 93
- **ip route command**, 93
- **overview**, 81–82
- **verification**, 94–95
dynamic routing examples, 64–65
EIGRP (Enhanced IGRP), 46, 63, 130
exit interfaces, finding, 88
floating static routes
- **configuration**, 106–110
- **overview**, 83–84
IS-IS (Intermediate System-to-Intermediate System), 63, 130
loopback interface configuration, 29–30
NAT (network address translation). See NAT
- (network address translation)
next-hop IP addresses, 122
OSPF (Open Shortest Path First), 29, 46, 63, 130
RIPv2
- **advertising networks**, 138–139
- **automatic summarization**, 142–143
- **configuration mode**, 136–138
- **default route propagation**, 145–147
- **overview**, 63
- **passive interfaces**, 143–145
- **topology**, 137
- **verification**, 139–142
router interface configuration, 24–26
routing tables
- **directly connected entries**, 149–150
- **directly connected routing table entries**, 53
on hosts, 18–19
- **level 1 parent routes**, 154–155
- **level 1 routes**, 153–154
- **level 2 child routes**, 155–156
- **overview**, 49, 147–149
remote network entries, 150–151

**IPv6**

default static routes
- **example**, 61, 105
- **ipv6 route command**, 104–105
- **overview**, 81–82
- **verification**, 105–106
dynamic routing examples, 66
EUI-64, 27
floating static routes
- **configuration**, 110–111
- **overview**, 83–84
global unicast addresses, 26–27
link-local address, 26–27
link-local addresses, 102, 114
NAT (network address translation)
IPv4-to-IPv6 scenarios, 458–459
overview, 456–457
ULAs (unique local addresses), 457–458
router interface configuration, 26–29
routing protocols, 65
routing tables
directly connected entries, 160–162
overview, 159–160
remote network entries, 162–164
verification, 96–98, 99–101, 103–104, 105
standard static routes
directly connected static routes, 100–102
example, 61–62
fully specified static routes, 102–103
ipv6 route command, 95–96
next-hop options, 95–96
next-hop route configuration, 99–100
overview, 81
verification, 103–104
static host routes
automatically installed host routes, 111–113
IPv4, 113–114
IPv6, 113–114
overview, 113–114
ipv6 address autoconfig command, 397
ipv6 address command, 26–27
ipv6 address dhcp command, 401
ipv6 dhcp pool command, 395, 399
ipv6 dhcp relay destination command, 403, 405
ipv6 dhcp server command, 396, 400
ipv6 enable command, 397, 401
ipv6 nd managed-config-flag command,
393, 400, 406
ipv6 nd other-config-flag command, 392–393,
396, 406
ipv6 route command, 61, 95–96, 104–105, 110
ipv6 unicast-routing command, 27, 65, 96, 389,
395, 399
IS-IS (Intermediate System-to-Intermediate System),
63, 130
ISR G2 (Integrated Services Routers Generation Two), 514–515
keywords. See also commands
any, 319–320
datetime, 496
detail, 489
host, 319–320
remark, 327
verbose, 441
LAN (local area network) design. See also VLANs (virtual LANs)
converged networks
access layer, 179
Cisco Borderless Networks, 176–177
complexity of, 174–175
core layer, 180–181
distribution layer, 179
elements of, 175–176
hierarchical design frameworks, 177–179
switched networks. See switched networks
late collisions, 221
layers
access layer, 179
core layer, 180–181
distribution layer, 179
network access layer issues
configuration, 218–221
troubleshooting, 221–222
leaking (VLAN), 278
lease command, 372
leases (DHCP)
origination, 365–366
renewal, 366–367
LED indicator lights
device LEDs, 19–20
switch LEDs, 207–209
legacy inter-VLAN routing
example, 289
explained, 287–288
preparation for, 292–293
router interface configuration, 294–295
switch configuration, 293–294
level 1 parent routes, 154–155
level 1 routes, 153–154
level 2 child routes, 155–156
Kahn, Bob, 417
key pairs (RSA), 225
levels of severity (Syslog), 494
license accept end user agreement command, 529
license boot module command, 530, 532, 532
license clear command, 532
license install command, 526, 531
license save command, 531
licenses (software)
backing up, 531–532
EULA (End User License Agreement), 524
Evaluation Right-to-Use (RTU) licenses, activating, 529–531
installation, 526–527
overview, 522–523
PAKs (Product Activation Keys), 524–526
technology package licenses, 522–523
uninstallation, 532–533
verification, 526–527
line cards, 184
line vty command, 226
Link Layer Discovery Protocol. See LLDP
(Link Layer Discovery Protocol)
link-local addresses (IPv6), 26–27, 102, 114
links, IEEE 802.1Q trunk links, 270–271
lists (VLAN), troubleshooting, 281–283, 284–286
LLDP (Link Layer Discovery Protocol)
configuration, 484
overview, 483
verification, 484
lldp run command, 484
load balancing, 46–47
local addresses, 421
local host routes. See static host routes
local route routing table entries, 54
logging buffered command, 497–498
logging command, 499
logging console command, 497–498
logging source-interface command, 499
logging trap command, 499
logging with Syslog
default logging, 497–499
facilities, 494–495
message format, 493–495
operation, 492–493
overview, 491–492
router and switch commands, 499–500
server configuration, 497
service timestamps, 496
verification, 500–501
logical topology, 5
login local command, 226
lookup process (IPv4), 156–158

M
M flag (Managed Address Configuration flag), 390
MAC address tables
overview, 188–189
secure MAC addresses, 231
sticky secure MAC addresses, 231–232
maintenance
backup and restore
with text files, 505–507
with TFTP (Trivial File Transfer Protocol), 507–508
with USB flash drives, 508–510
IOS images
backing up to TFTP servers, 517–519
boot system command, 521–522
copying to devices, 519–520
IOS system files
filenames, 515–517
IOS 15 system image packaging, 514–515
password recovery, 511–513
router file systems, 502–505
software licenses
backing up, 531–532
EULA (End User License Agreement), 524
Evaluation Right-to-Use (RTU) licenses, activating, 529–531
installing, 526–527
overview, 522–523
PAKs (Product Activation Keys), 524–526
technology package licenses, 522–523
uninstalling, 532–533
verification, 527–529
switch file systems, 505
Managed Address Configuration flag (M flag), 390
management of devices. See device management
management VLANs (virtual LANs), 252
matching
hosts, 316–317
ranges, 317
subnets, 316–317
mdix auto interface configuration mode command, 215
mean time between failures (MTBF), 6
memory
ARP (Address Resolution Protocol) cache, 40
fast-switching cache, 12
neighbor cache, 40
routers, 7–8
volatile versus nonvolatile, 7
messages
DHCPv4
DHCPACK, 366–367
DHCPDISCOVER, 365, 369–370
DHCPOFFER, 365, 369
DHCPREQUEST, 365–367
message format, 367–368
DHCPv6
ADVERTISE, 394
INFORMATION-REQUEST, 394
SOLICIT, 394
ICMPv6
Neighbor Solicitation and Neighbor Advertisement messages, 40
Router Advertisement messages, 27
NS (neighbor solicitation) messages, 390
RA (router advertisement) message, 389
routing protocol messages, 132
RS (router solicitation) message, 388
Syslog
message format, 493–495
service timestamps, 496
metrics, 45–46
microsegmented LANs, 213
mismatched port modes, 281–283
missing routes, troubleshooting, 116–118
missing VLANs (virtual LANs), troubleshooting, 276–278
Mode button, 207
modifying standard IPv4 ACLs
with sequence numbers, 334–335
standard named ACLs, 335–336
with text editor, 333–334
modular configuration switches, 184
more command, 510
MTBF (mean time between failures), 6
multiswitched environments, VLANs (virtual LANs) in
802.1Q tagging, 257–258
broadcast domains, controlling, 254–256
trunks, 253–254
VLAN tag field, 256–257
voice VLAN tagging, 258–259
N
name command, 262
named standard ACLs
configuration, 330–332
modifying, 335–336
NAT (network address translation)
address translations, 428–429
addresses, 420–423
advantages, 430
definition of, 419–420
disadvantages, 430–431
dynamic NAT
analysis, 438–440
configuration, 437–438
operation, 436–437
overview, 425–426
verification, 440–442
how it works, 423–424
inside networks, 420
NAT for IPv6
IPv4-to-IPv6 scenarios, 458–459
overview, 456–457
ULAs (unique local addresses), 457–458
NAT64, 459
NAT-PT (Network Address Translation-Protocol Translation), 459
outside networks, 420
overview, 418–419
PAT (Port Address Translation)
address pool configuration, 443–445
address translations, 428–429
analysis, 446–448
overview, 426–427
single address configuration, 445–446
source port reassignment, 427–428
verification, 449–450
pool, 419–420
port forwarding
configuration, 453–456
overview, 451–452
wireless router example, 452–453
static NAT
analysis, 433–434
configuration, 432–433
overview, 424–425
verification, 434–435
troubleshooting commands
debug ip nat command, 462–464
show ip nat commands, 460–462
troubleshooting scenario, 464–467
NAT overloading. See PAT (Port Address Translation)
NAT64, 459
native keyword, 298–299
native VLANs (virtual LANs)
802.1Q tagging, 257–258
overview, 251
NAT-PT (Network Address Translation-Protocol Translation), 459
neighbor cache, 40
Neighbor Solicitation and Neighbor Advertisement messages (ICMPv6), 40
neighbor solicitation (NS) messages, 390
netbios-name-server command, 372
network access layer issues
configuration, 218–221
troubleshooting, 221–222
network address translation. See NAT (network address translation)
Network Address Translation-Protocol Translation (NAT-PT), 459
network command, 138–139, 372
network congestion, alleviating, 195–196
network routes, 153
Network Time Protocol. See NTP (Network Time Protocol)
networks
converged networks
access layer, 179
Cisco Borderless Networks, 176–177
complexity of, 174–175
core layer, 180–181
distribution layer, 179
elements of, 175–176
hierarchical design frameworks, 177–179
device connections
Branch site devices, 15
Central site devices, 16
cable access, 21–22
default gateways, 16–17
device LEDs, 19–20
document network addressing, 17–18
Home Office devices, 15
IP configuration on hosts, 18–19, 22–23
IP configuration on switches, 22–23
directly connected networks, routing to, 44
directly connected networks, verifying connectivity of
command history feature, 36–37
IPv4 interface settings, 30–32
IPv6 interface settings, 32–34
show command output, filtering, 35–36
form factors, 183–185
frame forwarding
cut-through switching, 190, 191–193
LAN switching examples, 186–188
MAC address tables, 188–189
store-and-forward switching, 189–191
inside networks, 420
logging with Syslog
default logging, 497–499
facilities, 494–495
message format, 493–495
operation, 492–493
overview, 491–492
router and switch commands, 499–500
server configuration, 497
service timestamps, 496
verification, 500–501
network characteristics, 4–6
outside networks, 420
overview, 173
packets
encapsulation/de-encapsulation, 36–37
forwarding to next hop, 39–40
processing at destination, 43–44
routing, 42–43
sending, 39–40
routers
 basic router settings, 23–24
 components of, 7–8
 connections, 4–6, 9–10
directly connected static routes, 52–57
dynamic routing. See dynamic routing
edge routers, 145
Gateway of Last Resort, 17, 45
IPv4 loopback interfaces, 29–30
IPv4 router interface configuration, 24–26
IPv6 router interface configuration, 26–29
memory, 7–8
network characteristics and, 4–6
network connectivity functions, 4–13
packet forwarding mechanisms, 11–13
packet switching between networks, 36–44
path determination, 10–11, 44–48
routing tables. See routing tables
static routing. See static routing
stub routers, 79–80
security. See security
stub networks, 420
switch port configuration
 auto-MDIX, 215–216
duplex communication, 213–214
network access layer issues, 218–222
physical layer, 214–215
verifying configuration of, 216–218
switch port security
 configuration, 233–234
MAC addresses, 230–232
ports in error disabled state, 236–237
secure unused ports, 229–230
verification, 234–236
violation modes, 232–233
switched networks. See switched networks
switches
 boot sequence, 205–206
IPv4 configuration, 210–212
LED indicator lights, 207–209
overview, 204
preparing for remote management, 209–210
SSH (Secure Shell), 222–229
Syslog commands, 499–500
system crash recovery, 205–206
VLAN ranges on, 260–261
switching domains
 alleviation of network congestion, 195–196
broadcast domains, 194–195
collision domains, 193–194
VLANs (virtual LANs). See VLANs (virtual LANs)
next-hop options
IPv4 static routes
 configuration, 87–88
options, 85–87
overview, 151
IPv6 static routes
 configuration, 99–100
next-hop options, 95–96
overview, 163
next-hop IP addresses, 122
packet forwarding to next hop, 39–40
no access-list command, 326, 334
no auto-summary command, 143
no cdp run command, 478
no ip access-group command, 328
no ipv6 nd managed-config-flag command, 392
no license boot module command, 532
no lldp run command, 484
no passive-interface command, 145
no router rip command, 138
no service dhcp command, 373, 385
no shutdown command, 26, 229, 295, 298
no switchport access vlan command, 264, 278
no switchport trunk allowed vlan command, 272
no switchport trunk native vlan command, 272
no version command, 142
no vlan command, 266
nonvolatile memory, 7
normal range VLANs (virtual LANs), 261
Notification Levels (Syslog), 494
NS (neighbor solicitation) messages, 390
NTP (Network Time Protocol)
 configuration, 489–491
operation, 488–489
stratum levels, 488–489
system clock, setting, 487
verification, 489–491
ntp server command, 489
numbered standard ACLs
  configuration
    examples, 329–330
    links to interfaces, 328–329
    syntax, 325–327
  modifying
    with sequence numbers, 334–335
    standard named ACLs, 335–336
    with text editor, 333–334
  statistics, 338–339
  verification, 336–337
NVRAM, 8, 504–505

O
O flag (Other Configuration flag), 390
obtaining software licenses, 525–526
Open Shortest Path First (OSPF), 29, 46, 63, 130
  order
    ACEs (access control entries), 343–344
    Cisco IOS reordering of ACLs, 343–344
    originating DHCP leases, 365–366
    OSPF (Open Shortest Path First), 29, 46, 63, 130
    Other Configuration flag (O flag), 390
    outbound ACLs (access control lists), 313–314
  output errors, 220–221
  outside addresses, 421
  outside global addresses, 422
  outside local addresses, 423
  outside networks, 420
  overload keyword, 445
  overloading (NAT). See PAT (Port Address Translation)

P
P2P (point-to-point) serial connections, 43
packaging (IOS), 514–515
packet protocol data unit (PDU), 16
  packets
    CDP (Cisco Discovery Protocol) packets, 258
    encapsulation/de-encapsulation, 36–37
    filtering, 312–313
    forwarding to next hop, 39–40
  packet forwarding mechanisms, 11–13
  path determination
    AD (administrative distance), 47–48
    best path, determining, 45–46
    load balancing, 46–47
    packet forwarding decision process, 44–45
  processing at destination, 43–44
  processing with ACLs (access control lists)
    Cisco IOS reordering of ACLs, 343–344
    implicit deny any, 343
    order of ACEs (access control entries), 343–344
    routing processes, 347–349
  processing with static routes, 115–116
  routing, 42–43
  sending, 39–40
  PAKs (Product Activation Keys), 515, 524–525
  passive interfaces, configuring, 143–145
  passive-interface command, 144–145
  passive-interface default command, 145
  password recovery, 511–513
  PAT (Port Address Translation)
    address pool configuration, 443–445
    address translations, 428–429
    analysis, 446–448
    overview, 425–426
    single address configuration, 445–446
    source port reassignment, 427–428
    verification, 449–450
  path determination
    AD (administrative distance), 47–48
    best path, 45–46
    load balancing, 46–47
    overview, 10–11
    packet forwarding decision process, 44–45
  PDU (packet protocol data unit), 16
  permanent licenses
    definition of, 524
    verification, 528
  permit statement, 338
  PHY (physical layer device), 216
  phy keyword, 216
  physical layer device (PHY), 216
  physical layer of switch ports, 214–215
  physical topology, 5
  ping command, 34, 57, 87, 98, 106, 117,
    119, 276, 300–301
  placement of ACLs (access control lists), 322–325
PoE (Power over Ethernet) Mode LED, 209
point-to-point (P2P) serial connections, 43
Point-to-Point Protocol (PPP), 10–11
pool (DHCPv4), 371
pool (NAT), 419–420
Port Address Translation. See PAT (Port Address Translation)
port density, 183
Port Duplex LED, 209
port forwarding
configuration, 453–456
overview, 451–452
wireless router example, 452–453
port modes, troubleshooting, 281–283
port speed, 183, 195
Port Speed LED, 209
Port Status LED, 208–209
Port VLAN ID (PVID), 257
ports
assigning to VLANs, 263
egress ports, 191
ingress ports, 186–187
PAT (Port Address Translation)
address pool configuration, 443–445
analysis, 446–448
overview, 426–427
single address configuration, 445–446
source port reassignment, 427–428
verification, 449–450
port density, 195
port forwarding
configuration, 453–456
overview, 451–452
wireless router example, 452–453
port modes, troubleshooting, 281–283
PVID (Port VLAN ID), 257
switch port configuration
auto-MDI X, 215–216
duplex communication, 213–214
network access layer issues, 218–222
physical layer, 214–215
verification, 216–218
switch port security
configuration, 233–234
MAC addresses, 230–232
ports in error disabled state, 236–237
secure unused ports, 229–230
verification, 234–236
violation modes, 232–233
VLAN default port assignments, 250–251
VLAN port membership, 264–265
VTY ports
securing with ACLs, 339–342
verification security on, 341–342
POST (power-on self-test), 205
Power over Ethernet (PoE) Mode LED, 209
power-on self-test (POST), 205
PPP (Point-to-Point Protocol), 10–11
preparations
for legacy inter-VLAN routing, 292–293
for router-on-a-stick inter-VLAN routing, 296–297
present working directory (pwd) command, 505
private address space (IPv4), 418–419
private IPv4 addresses, 418–419
problem solving
ACLs (access control lists), 349–353
DHCPv4
debugging, 385–387
IPv4 address conflicts, 383
physical connectivity, 383–384
switch port configuration, 383
testing, 384
verifying configuration of, 384–385
DHCPv6
debugging, 407–408
troubleshooting tasks, 404–405
verifying configuration of, 405–407
IOS troubleshooting commands
ping, 117, 119, 300–301
show cdp neighbors, 118
show ip interface brief, 118
show ip route, 117
traceroute, 117, 119
NAT (network address translation)
debug ip nat command, 462–464
show ip nat commands, 460–462
troubleshooting scenario, 464–467
network access layer issues, 221–222
static routing
connectivity problems, 118–120
missing routes, 116–118
packet processing, 115–116
trunks
  common problems, 279–281
general guidelines, 278–279
incorrect port modes, 281–283
incorrect VLAN lists, 284–286
native VLAN mismatches, 280–281
trunk mode mismatches, 280–283
VLANs (virtual LANs)
  common trunk problems, 279–281
incorrect port modes, 281–283
incorrect VLAN lists, 284–286
IP addressing issues, 275–276
missing VLANs, 276–278
native VLAN mismatches, 280–281
trunk troubleshooting guidelines, 278–279
process switching, 11–12
processing packets
  ACLs (access control lists)
    Cisco IOS reordering of ACLs, 343–344
    implicit deny any, 343
    order of ACEs (access control entries), 343–344
    routing processes, 347–349
static routing, 115–116
Product Activation Keys (PAKs), 515, 524–525
propagating default routes, 145–147
Protect mode, 232
PSTN (public switched telephone network), 186
public IPv4 addresses, 418–419
public switched telephone network (PSTN), 186
PVID (Port VLAN ID), 257
pwd command, 505

Q
Query ID, 429
question mark (?) command, 532

R
R3 G0/0 interface, 325
R3 S0/0/1 interface, 324–325
RA (router advertisement) message, 389
rack units, 183
RAM (random-access memory), 8
random-access memory (RAM), 8
ranges, matching with wildcard masks, 317
rapid frame forwarding, 192
read-only memory (ROM), 8
recovering
  passwords, 511–513
  from system crashes, 205–206
recursive lookups, 88
Redundant Power System (RPS) LED, 208
regional Internet registry (RIR), 457
registers, configuration register, 511–513
relay (DHCPv4), 377–380
relay agents (DHCPv6), 402–403
reliability, 6
reload command, 527, 530
remark keyword, 327
remote management
  overview, 227–229
  preparing switches for, 209–210
remote network entries
  IPv4, 150–151
  IPv6, 162–164
  overview, 51–52
remote networks, routing to, 45
renewing DHCP leases, 366–367
resetting trunks to default state, 272–273
restoring files
  from text files, 505–507
  with TFTP (Trivial File Transfer Protocol), 507–508
  with USB flash drives, 508–510
Restrict mode, 232
Right-to-Use (RTU) licenses, activating, 529–531
RIPv1, 130
RIPv2
  advertising networks, 138–139
  automatic summarization, 142–143
  configuration mode, 136–138
  default route propagation, 145–147
  metrics, 46
  overview, 63
  passive interfaces, 143–145
  topology, 137
  verification, 139–142
RIR (regional Internet registry), 457
ROM (read-only memory), 8
ROMMON mode, 511–512
route lookup process (IPv4), 156–159
router ? command, 64
Router Advertisement messages (ICMPv6), 27
router advertisement (RA) message, 389
router rip command, 137
router solicitation (RS) message, 388
router-on-a-stick inter-VLAN routing
   explained, 290–291
   preparation for, 296–297
   subinterfaces, 299–300
   switch configuration, 298–299
   verification, 300–302
routers/routing. See also static routing
   ACLs (access control lists) and, 347–349
   basic router settings, 23–24
   components of, 7–8
   configuring for DHCPv6
      clients, 401
      servers, 399–400
   connections, 4–6, 9–10
   device connections
      Branch site devices, 15
      Central site devices, 16
      console access, 21–22
      default gateways, 16–17
      device LEDs, 19–20
   document network addressing, 17–18
   Home Office devices, 15
   IP configuration on hosts, 18–19
   IP configuration on switches, 22–23
   as DHCPv4 clients, 380–381
   as DHCPv6 servers, 395–399
   directly connected networks, verifying connectivity of
      command history feature, 36–37
      IPv4 interface settings, 30–32
      IPv6 interface settings, 32–34
      show command output, filtering, 35–36
   directly connected static routes
      examples, 54–57
      interfaces, 52–53
      routing table entries, 53
   dynamic. See dynamic routing
   edge routers, 145
   files
      backing up/restoring with text files, 505–507
      backing up/restoring with TFTP, 507–508
   Gateway of Last Resort, 17, 45
   interfaces. See interfaces
   IPv4 router interface configuration, 24–26
   IPv4 routing tables
      directly connected entries, 149–150
      level 1 parent routes, 154–155
      level 1 routes, 153–154
      level 2 child routes, 155–156
      overview, 147–149
   remote network entries, 150–151
   route lookup process, 156–159
   ultimate routes, 152
   verification, 86, 88, 89, 91, 92
   IPv6 router interface configuration, 26–29
   IPv6 routing tables
      directly connected entries, 160–162
      overview, 159–160
   remote network entries, 162–164
   verification, 96–98, 99–101, 103–104, 105
   legacy inter-VLAN routing
      example, 289
   explained, 287–288
   preparation for, 292–293
   router interface configuration, 294–295
   switch configuration, 293–294
   memory, 7–8
   NAT (network address translation). See NAT (network address translation)
   network characteristics and, 4–6
   network connectivity functions, 222–229
   packet forwarding mechanisms, 11–13
   packets
      encapsulation/de-encapsulation, 36–37
      forwarding to next hop, 39–40
      processing at destination, 43–44
      routing, 42–43
      sending, 39–40
   path determination
      AD (administrative distance), 47–48
      best path, 45–46
      load balancing, 46–47
      overview, 10–11
      packet forwarding decision process, 44–45
   ROMMON mode, 511–512
servers  597

router file system maintenance, 502–505
router-on-a-stick inter-VLAN routing
   explained, 290–291
   preparation for, 296–297
subinterfaces, 299–300
switch configuration, 298–299
verification, 300–302
Routing Information Protocol. See RIPv2
routing protocol messages, 132
static. See static routing
stub routers, 79–80
Syslog commands, 499–500
Routing Information Protocol. See RIPv2
routing protocol messages, 132
routin...
example, 372–373
IPv4 addresses, excluding, 371
relay, 377–380
topology, 370–371
verification, 373–377
DHCPv6 servers
stateful DHCPv6, 399–400
stateless DHCPv6, 395–396
Syslog, 493–495
TFTP servers, backing up IOS images to, 517–519
service dhcp command, 373
service timestamps log datetime command, 496
service timestamps (Syslog), 496
Services on Demand process, 514
settings. See configuration
severity levels (Syslog), 494
show access-list command, 350–351
show access-lists command, 326, 337–338, 341, 345–346, 347
show boot command, 206
show cdp command, 478
show cdp neighbors command, 118, 479, 480–482
show clock command, 489
show command
filtering output of, 35–36
options, 216–217
show controllers ethernet-controller command, 216
show file systems command, 502–503, 505
show flash command, 515
show interface command, 214
show interfaces command, 217–222, 268–270, 383
show interfaces f0/1 trunk command, 280
show interfaces interface-id switchport command, 259, 264, 272, 273, 278
show interfaces trunk command, 279, 281–282, 284–285
show ip dhcp binding command, 375–376
show ip dhcp conflict command, 383
show ip dhcp server statistics command, 374–376
show ip interface brief command, 30–31, 32, 118, 211
show ip interface command, 336–337, 381
show ip nat commands, 460–462
show ip nat statistics command, 435, 442, 449–450, 464–467
show ip nat translations command, 434–435, 440–441, 449, 455, 464–467
show ip ntp associations command, 490–491
show ip protocols, 141
show ip protocols command, 139, 143, 144–145
show ip route static command, 92, 94
show ip ssh command, 225, 228
show ipv6 dhcp binding command, 401–402
show ipv6 dhcp conflict command, 404
show ipv6 dhcp interface command, 403
show ipv6 dhcp pool command, 397, 401
show ipv6 interface command, 397–398, 402
show ipv6 interface gigabitethernet 0/0
command, 33
show ipv6 route static command, 103, 105, 111
show license command, 528–529, 531
show license feature command, 523
show license udi command, 525–526
show lldp neighbors command, 484–485
show lldp neighbors detail command, 485–486
show logging command, 498–499, 500–501
show mac address-table command, 277
show ntp status command, 490–491
show port-security address command, 235–236
show port-security interface command, 234–235, 236–237
show run command, 351
show running-config command, 217, 333–334, 345, 384

show running-config | include no service dhcp, 385
show running-config | section dhcp, 373–374
show running-config interface command, 30, 32
show ssh command, 228
show version command, 224, 527
show vlan brief command, 250–251, 261, 264, 266
show vlan command, 267–268, 277
shutdown command, 229, 298
Shutdown mode, 232–233
single address configuration (PAT), 445–446
single-homed, 145
SLAAC (Stateless Address Autoconfiguration)
host configuration methods, 387–390
operation, 389–390
overview, 388–389
SLAAC Option, 390–391
Stateful DHCPv6 Option, 393
Stateless DHCPv6 Option, 392–393
software licenses
backing up, 531–532
EULA (End User License Agreement), 524
Evaluation Right-to-Use (RTU) licenses, activating, 529–531
installation, 526–527
obtaining, 525–526
overview, 522–523
PAKs (Product Activation Keys), 524–525
technology package licenses, 522–523
uninstallation, 532–533
verification, 527–529
SOLICIT message, 394
source addresses (SAs), 427
source port reassignment, 427–428
speed
of networks, 5
of ports, 183, 195
SSH (Secure Shell)
configuration, 225–226
operation, 222–224
verification, 227–229
stackable configuration switches, 185
StackPower technology, 185
StackWise technology, 185
staff efficiency, improving with VLANs, 250
standard IPv4 ACLs
configuration
links to interfaces, 328–329
named standard ACL syntax, 330–332
numbered standard ACL examples, 329–330
numbered standard ACL syntax, 325–327
modifying
with sequence numbers, 334–335
standard named ACLs, 335–336
with text editor, 333–334
statistics, 338–339
troubleshooting, 349–353
verification, 336–337
standard static routes
IPv4 standard static routes
directly connected static routes, 88–90
example, 60
fully specified static routes, 90–91
ip route command, 84–85
next-hop options, 85–87
next-hop route configuration, 87–88
verification, 92, 103–104
IPv6 standard static routes
directly connected static routes, 100–102
example, 61–62
fully specified static routes, 102–103
ipv6 route command, 95–96
next-hop options, 95–96
next-hop route configuration, 99–100
overview, 81
startup-config file, 206
stateful DHCPv6
client configuration, 401
relay agent configuration, 402–403
server configuration, 399–400
verification, 401–402
verifying configuration of, 406–407
Stateless Address Autoconfiguration. See SLAAC (Stateless Address Autoconfiguration)
stateless DHCPv6
client configuration, 396–399
server configuration, 395–396
verification, 397–399
verifying configuration of, 405–406
statements
deny, 338
deny any, 338, 343
permit, 338
static host routes
automatic summarization, 111–113
IPv4, 113–114
IPv6, 113–114
static NAT (network address translation)
analysis of, 433–434
configuration, 432–433
overview, 424–425
verification, 434–435
static route applications, 80–81
static routing
AD (administrative distance), 107
advantages/disadvantages, 77–79, 134
comparing to dynamic routing, 79
directly connected static routes
examples, 54–57
interfaces, 52–53
IPv4, 88–90
IPv6, 100–102
routing table entries, 53
IPv4 default static routes
example, 59–60, 93
ip route command, 93
overview, 81–82
verification, 94–95
IPv4 floating static routes, 106–110
IPv4 standard static routes
directly connected static routes, 88–90
example, 60
fully specified static routes, 90–91
ip route command, 84–85
next-hop options, 85–87
next-hop route configuration, 87–88
overview, 81
verification, 92
IPv4 summary static routes, 81–82
IPv6 default static routes
example, 61, 105
ipv6 route command, 104–105
overview, 81–82
verification, 105–106
IPv6 floating static routes, 110–111
IPv6 standard static routes
directly connected static routes, 100–102
example, 61–62
fully specified static routes, 102–103
ipv6 route command, 95–96
next-hop options, 95–96
next-hop route configuration, 99–100
overview, 58–59, 76
packet processing, 115–116
scenarios, 77–78
static host routes
automatically installed host routes, 111–113
IPv4, 113–114
IPv6, 113–114
summary static routes, 81–82, 83–84
troubleshooting
connectivity problems, 118–120
missing routes, 116–118
types of, 80–84
when to use, 79–80, 133
static secure MAC addresses, 231
statistics (ACL), 338–339
sticky secure MAC addresses, 231–232
store-and-forward switching, 189–191
stratum levels (NTP), 488–489
stub networks, 79, 420
stub routers, 79–80
subinterfaces, 299–300
subnets, matching with wildcard masks, 316–317
summary static routes, 81–83
supernet routes, 153
SVI (switched virtual interface), 22, 210, 252
switch: command prompt, 207
switch ports
configuration
auto-MDIX, 215–216
duplex communication, 213–214
network access layer issues, 218–222
physical layer, 214–215
verification, 216–218
security
configuration, 233–234
MAC addresses, 230–232
ports in error disabled state, 236–237
secure unused ports, 229–230
verification, 234–236
violation modes, 232–233
verification, 383
switched networks
converged networks
access layer, 179
Cisco Borderless Networks, 176–177
complexity of, 174–175
core layer, 180–181
distribution layer, 179
elements of, 175–176
hierarchical design frameworks, 177–179
form factors, 183–185
frame forwarding
cut-through switching, 190, 191–193
LAN switching examples, 186–188
MAC address tables, 188–189
store-and-forward switching, 189–191
overview, 173
packets
encapsulation/de-encapsulation, 36–37
forwarding to next hop, 39–40
processing at destination, 43–44
routing, 42–43
sending, 39–40
role of, 181–182
routers. See routers/routing
security. See security
switch port configuration
auto-MDIX, 215–216
duplex communication, 213–214
network access layer issues, 218–222
physical layer, 214–215
verifying configuration of, 216–218
switch port security
configuration, 233–234
MAC addresses, 230–232
ports in error disabled state, 236–237
secure unused ports, 229–230
verification, 234–236
violation modes, 232–233
switches
boot sequence, 205–206
IPv4 configuration, 22–23, 210–212
LED indicator lights, 207–209
overview, 204
preparing for remote management, 209–210
SSH (Secure Shell)
configuration, 225–226
overview, 222–224
verification, 227–229
switch file system maintenance, 505
Syslog commands, 499–500
system crash recovery, 205–206
VLAN ranges on, 260–261
switching domains
alleviation of network congestion, 195–196
broadcast domains, 194–195
collision domains, 193–194
switchport access vlan command, 263, 294
switchport mode access command, 263, 272, 282
switchport mode trunk command, 270–271, 280, 281, 297
switchport port-security command, 234
switchport port-security mac-address command, 231
switchport port-security mac-address sticky command, 231
switchport port-security violation command, 233
switchport trunk allowed vlan command, 270, 284, 285
switchport trunk native vlan command, 270
synchronizing time with NTP (Network Time Protocol)
configuration, 489–491
operation, 488–489
stratum levels, 488–489
system clock, setting, 487
verification, 489–491
Syslog
default logging, 497–499
facilities, 494–495
messages
message format, 493–495
service timestamps, 496
operation, 492–493
overview, 491–492
router and switch commands, 499–500
server configuration, 497
verification, 500–501
system clock, setting, 487
system crashes, recovering from, 205–206
System LED, 208

tables
addressing tables, 17–18
adjacency tables, 12–13
IPv4 routing tables
  directly connected entries, 149–150
directly connected routing table entries, 53
level 1 parent routes, 154–155
level 1 routes, 153–154
level 2 child routes, 155–156
overview, 49, 147–149
remote network entries, 150–151
remote network routing entries, 51–52
route lookup process, 156–159
sources, 49–51
ultimate routes, 152
IPv6 routing tables
  directly connected entries, 160–162
overview, 159–160
remote network entries, 162–164
MAC address tables, 188–189
overview, 188–189
secure MAC addresses, 231
sticky secure MAC addresses, 231–232
tag protocol ID (TPID), 257
tagged traffic, 251
tags (VLAN)
  802.1Q tagging, 257–258
tag field, 256–257
voice VLAN tagging, 258–259
technology package licenses, 522–523
Telnet, 222–223
temporary licenses, 524
Tera Term, 505–507
terminal emulation software, 21
testing DHCPv4, 384
text editors, modifying standard IPv4 ACLs with, 333–334
text files
  backing up to, 505–507
  restoring from, 505–507
TFTP (Trivial File Transfer Protocol)
  overview, 507–508
  TFTP servers, backing up IOS images to, 517–519
three-layer hierarchical model, 177–181
time synchronization with NTP (Network Time Protocol)
  configuration, 489–491
  operation, 488–489
  stratum levels, 488–489
  system clock, setting, 487
  verification, 489–491
timestamps (Syslog), 496
Token Ring VLANs, 261
topology
  DHCPv4 servers, 370–371
  NAT (network address translation), 419–420
  physical versus logical, 5
  RIPv2, 137
  VLANs (virtual LANs), 249
topology diagrams, 17
tPID (tag protocol ID), 257
traceroute command, 109–110, 117, 119
traceroute command, 301–302
translation, 459
transport input ssh command, 226
Trivial File Transfer Protocol (TFTP), 507–508
troubleshooting
  ACLs (access control lists), 349–353
  DHCPv4
    debugging, 385–387
    IPv4 address conflicts, 383
    physical connectivity, 383–384
    switch port configuration, 383
    testing, 384
    verifying configuration of, 384–385
  DHCPv6
    debugging, 407–408
troubleshooting tasks, 404–405
    verifying configuration of, 405–407
  IOS troubleshooting commands
    ping, 117, 119, 300–301
verification

show cdp neighbors, 118
show ip interface brief, 118
show ip route, 117
traceroute, 117, 119
NAT (network address translation)
debag ip nat command, 462–464
show ip nat commands, 460–462
troubleshooting scenario, 464–467
network access layer issues, 221–222
static routing
  connectivity problems, 118–120
  missing routes, 116–118
  packet processing, 115–116
trunks
  common problems, 279–281
  general guidelines, 278–279
  incorrect port modes, 281–283
  incorrect VLAN lists, 284–286
  native VLAN mismatches, 280–281
  trunk mode mismatches, 280–283
VLANs (virtual LANs)
  common trunk problems, 279–281
  incorrect port modes, 281–283
  incorrect VLAN lists, 284–286
  IP addressing issues, 275–276
  missing VLANs, 276–278
  native VLAN mismatches, 280–281
  trunk troubleshooting guidelines, 278–279
trunk mode mismatches, 280–283
trunks
  broadcast domains, controlling, 254–256
  DTP (Dynamic Trunking Protocol), 270
  IEEE 802.1Q trunk links, configuring, 270–271
  overview, 253–254
  resetting to default state, 272–273
troubleshooting
  common problems, 279–281
  general guidelines, 278–279
  incorrect port modes, 281–283
  incorrect VLAN lists, 284–286
  native VLAN mismatches, 280–281
  trunk mode mismatches, 280–283
verifying configuration of, 273–274
VTP (VLAN Trunking Protocol), 261
tunneling, 459
Type field (VLAN tags), 257

U

UDIs (unique device identifiers), 525
ULAs (unique local addresses), 457–458
ultimate routes, 152
unequal cost load balancing, 46–47
Unified Communications license, 523
uninstalling software licenses, 532–533
unique device identifiers (UDIs), 525
unique local addresses (ULAs), 457–458
universal images, 514
Universal Serial Bus (USB) flash drives, 508–510
universalK9 designation, 514
universalK9_npe designation, 515
untagged traffic, 251
unused ports, disabling, 229–230
upgrading IOS system images
  boot system command, 521–522
  image backups
to devices, 519–520
to TFTP server, 517–519
USB flash drives, 508–510
USB Type-A to USB Type-B connections, 21
USB-to-RS-232 compatible serial port adapters, 21
User Priority field (VLAN tags), 257

V

verbose keyword, 441
verification
  ACLs (access control lists), 336–337
  CDP (Cisco Discovery Protocol), 478–480
  DHCPv4, 373–377, 384–385
  DHCPv6, 405–407
directly connected networks
  command history feature, 36–37
  IPv4 interface settings, 30–32
  IPv6 interface settings, 32–34
  show command output, filtering, 35–36
  IPv4 routing tables, 86, 88, 89, 91, 92
  LLDP (Link Layer Discovery Protocol), 484
  NAT (network address translation)
    dynamic NAT, 440–442
    static NAT, 434–435
  NTP (Network Time Protocol), 489–491
PAT (Port Address Translation), 449–450
port security, 234–236
RIPv2, 139–142
router-on-a-stick inter-VLAN routing
routing, 300–302
subinterfaces, 299–300
software licenses, 527–529,
SSH (Secure Shell), 227–229
stateful DHCPv6, 401–402
stateless DHCPv6, 397–399
static routes
IPv4 default static routes, 94–95
IPv4 standard static routes, 92
IPv6 default static routes, 105–106
IPv6 standard static routes, 103–104
switch port configuration, 216–218, 383
Syslog commands, 500–501
trunk configuration, 273–274
USB flash drives, 509
VLANs (virtual LANs), 267–270
VTY port security, 341–342
version 2 command, 141
VID (VLAN ID), 257
violation modes, 232–233
virtual LANs. See VLANs (virtual LANs)
vlan command, 262
VLAN ID (VID), 257
VLAN lists, troubleshooting, 284–286
VLAN Trunking Protocol (VTP), 261
vlan.dat file, 261
VLANs (virtual LANs)
benefits of, 249–250
creating, 262
data VLANs, 251–252
default VLANs, 250–251
deleting, 266–267
extended range VLANs, 261
FDDI (Fiber Distributed Data Interface)
VLANs, 261
legacy inter-VLAN routing
example, 289
explained, 287–288
preparation for, 292–293
router interface configuration, 294–295
switch configuration, 293–294
management VLANs, 252
multiswitched environments
802.1Q tagging, 257–258
broadcast domains, controlling, 254–256
trunks, 253–254
VLAN tag field, 256–257
voice VLAN tagging, 258–259
native VLANs
802.1Q tagging, 257–258
overview, 251
normal range VLANs, 261
overview, 247–249
port assignment, 263
port membership, changing, 264–265
router-on-a-stick inter-VLAN routing
explained, 290–291
preparation for, 296–297
subinterfaces, 299–300
switch configuration, 298–299
verification, 300–302
switch management, 210
Token Ring VLANs, 261
topology, 249
troubleshooting
common trunk problems, 279–281
incorrect port modes, 281–283
incorrect VLAN lists, 280–281, 284–286
IP addressing issues, 275–276
missing VLANs, 276–278
trunk troubleshooting guidelines, 278–279
trunks
common problems with, 279–281
DTP (Dynamic Trunking Protocol), 270
general guidelines, 278–279
IEEE 802.1Q trunk links, configuring, 270–271
native VLAN mismatches, 280–281
port modes, troubleshooting, 281–283
resetting to default state, 272–273
verifying configuration of, 273–274
VLAN lists, troubleshooting, 284–286
verification, 267–270
VLAN leaking, 278
VLAN ranges on Catalyst switches, 260–261
vlan.dat file, 261
voice VLANs, 252–253
voice VLANs (virtual LANs)
  overview, 252–253
tagging, 258–259
VTP (VLAN Trunking Protocol), 261
voice VLANs (virtual LANs)
  overview, 252–253
tagging, 258–259
VoIP device connections, 15
volatile memory, 7
VTP (VLAN Trunking Protocol), 261
VTY ports
  securing with ACLs, 339–342
  verification security on, 341–342

W-X-Y-Z

WAP (wireless access points), 15
Warning Levels (Syslog), 494
wasted bandwidth, 144
wasted resources, 144
wildcard masks
  calculating, 317–319
  examples, 316–317
  keywords, 319–320
  overview, 314–320
wireless access points (WAP), 15
wireless routers, configuring as DHCPv4 clients, 381–382
Wireshark, 223–224
zipping files, 517