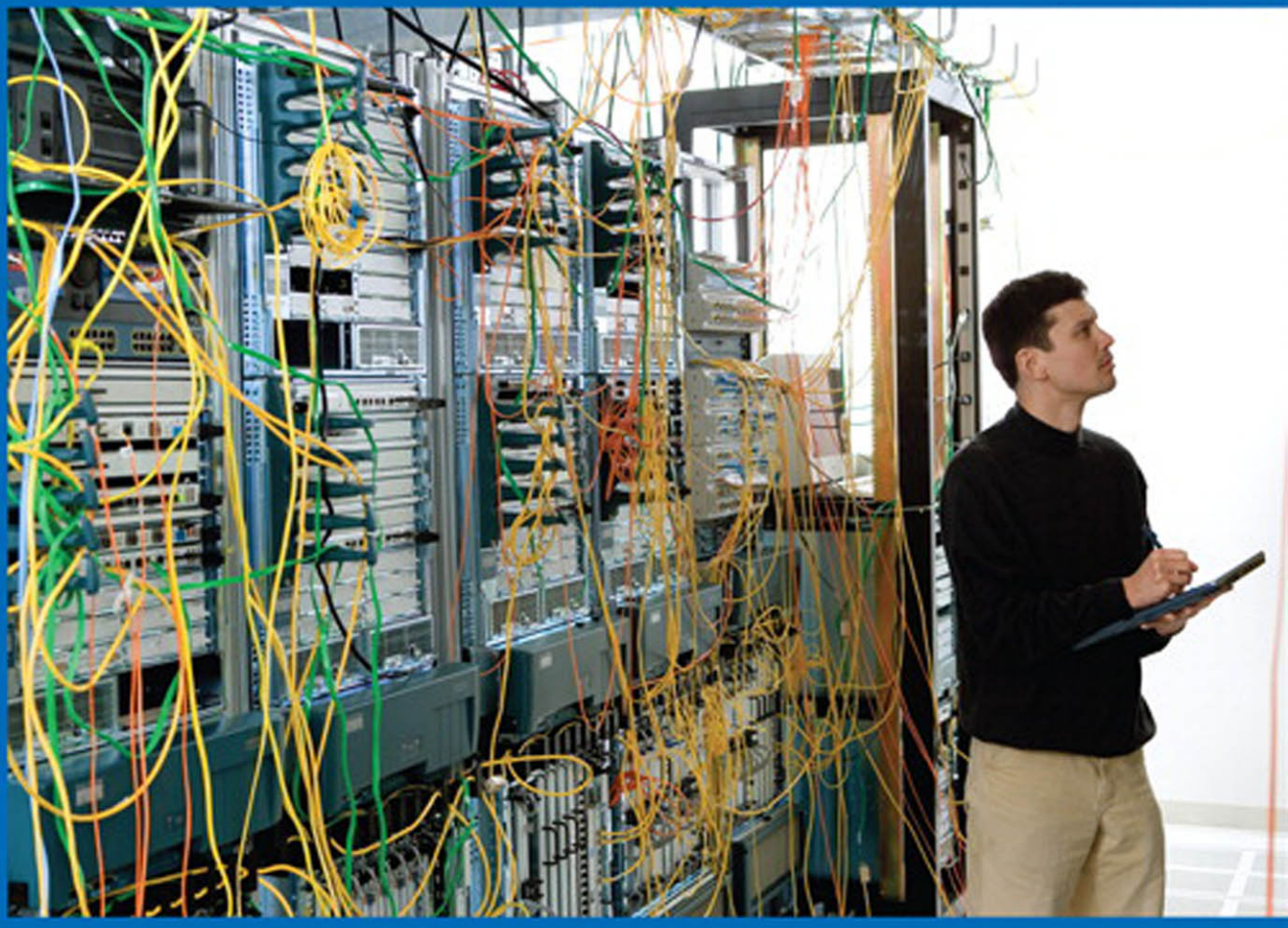
Routing Protocols

Companion Guide



Cisco | Networking Academy®
Mind Wide Open™

Routing Protocols

Companion Guide

Cisco Networking Academy

Cisco Press
800 East 96th Street
Indianapolis, Indiana 46240 USA

Routing Protocols Companion Guide

Cisco Networking Academy

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

Printed in the United States of America

First Printing February 2014

Library of Congress Control Number: 2013957291

ISBN-13: 978-1-58713-323-7

ISBN-10: 1-58713-323-7

Warning and Disclaimer

This book is designed to provide information about the Cisco Networking Academy Routing Protocols 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.

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

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

Publisher
Paul Boger

Associate Publisher
Dave Dusthimer

Business Operation Manager, Cisco Press
Jan Cornelssen

Executive Editor
Mary Beth Ray

Managing Editor
Sandra Schroeder

Development Editor
Ellie C. Bru

Project Editor
Mandie Frank

Copy Editor
Bill McManus

Technical Editor
Bruce Brumley

Editorial Assistant
Vanessa Evans

Designer
Mark Shirar

Composition
Tricia Bronkella

Indexer
Brad Herriman

Proofreader
Debbie Williams

Trademark Acknowledgements

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

Special Sales

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

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

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

Feedback Information

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

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

We greatly appreciate your assistance.

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

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

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

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

About the Contributing Authors

Rick Graziani teaches computer science and computer networking courses at Cabrillo College in Aptos, California. Prior to teaching, Rick worked in the information technology field for Santa Cruz Operation, Tandem Computers, and Lockheed Missiles and Space Corporation. He holds an M.A. in Computer Science and Systems Theory from California State University Monterey Bay. Rick is also a member of the Curriculum Development team for the Cisco Networking Academy since 1999.

Rick has authored multiple books for Cisco Press and multiple online courses for the Cisco Networking Academy. Rick is the author of the Cisco Press book *IPv6 Fundamentals* and has presented on IPv6 at several Cisco Academy conferences.

When Rick is not working, he is most likely surfing at one of his favorite Santa Cruz surf breaks.

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 more than 30 years of work and teaching experience in the computer networking and information technology field.

Since 2001, Bob has collaborated as team lead, lead author, and subject matter expert on various CCNA, CCNA-S, and CCNP projects for Cisco and the Cisco Networking Academy. He also co-authored *Accessing the WAN, CCNA Exploration Companion Guide* and authored *CCNA Security (640-554) Portable Command Guide*.

In his downtime, Bob enjoys playing the guitar, shooting darts or pool, and either working in his gardens or white-water canoe tripping.

Contents at a Glance

	Introduction	xxiv
Chapter 1	Routing Concepts	1
Chapter 2	Static Routing	73
Chapter 3	Routing Dynamically	155
Chapter 4	EIGRP	239
Chapter 5	EIGRP Advanced Configurations and Troubleshooting	333
Chapter 6	Single-Area OSPF	393
Chapter 7	Adjust and Troubleshoot Single-Area OSPF	461
Chapter 8	Multiarea OSPF	527
Chapter 9	Access Control Lists	565
Chapter 10	IOS Images and Licensing	653
Appendix A	Answers to the “Check Your Understanding” Questions	693
	Glossary	709
	Index	723

Contents

Introduction xxiv

Chapter 1 Routing Concepts 1

Objectives 1

Key Terms 1

Introduction (1.0.1.1) 3

Initial Configuration of a Router (1.1) 4

Characteristics of a Network (1.1.1.1) 4

Why Routing? (1.1.1.2) 5

Routers Are Computers (1.1.1.3) 6

Routers Interconnect Networks (1.1.1.4) 7

Routers Choose Best Paths (1.1.1.5) 9

Packet Forwarding Mechanisms (1.1.1.6) 9

Connect Devices (1.1.2) 12

Connect to a Network (1.1.2.1) 13

Default Gateways (1.1.2.2) 14

Document Network Addressing (1.1.2.3) 15

Enable IP on a Host (1.1.2.4) 16

Device LEDs (1.1.2.5) 18

Console Access (1.1.2.6) 19

Enable IP on a Switch (1.1.2.7) 20

Basic Settings on a Router (1.1.3) 22

Configure Basic Router Settings (1.1.3.1) 22

Configure an IPv4 Router Interface (1.1.3.2) 24

Configure an IPv6 Router Interface (1.1.3.3) 25

Configure an IPv4 Loopback Interface (1.1.3.4) 28

Verify Connectivity of Directly Connected Networks (1.1.4) 29

Verify Interface Settings (1.1.4.1) 29

Verify IPv6 Interface Settings (1.1.4.2) 31

Filter Show Command Output (1.1.4.3) 34

Command History Feature (1.1.4.4) 36

Routing Decisions (1.2) 38

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) 41
Reach the Destination (1.2.1.5) 42

Path Determination (1.2.2) 43

Routing Decisions (1.2.2.1) 43
Best Path (1.2.2.2) 44
Load Balancing (1.2.2.3) 45
Administrative Distance (1.2.2.4) 46

Router Operation (1.3) 47

Analyze the Routing Table (1.3.1) 47
The Routing Table (1.3.1.1) 47
Routing Table Sources (1.3.1.2) 48
Remote Network Routing Entries (1.3.1.3) 49
Directly Connected Routes (1.3.2) 51
Directly Connected Interfaces (1.3.2.1) 51
Directly Connected Route Table Entries (1.3.2.2) 51
Directly Connected Examples (1.3.2.3) 52
Directly Connected IPv6 Example (1.3.2.4) 53
Statically Learned Routes (1.3.3) 56
Static Routes (1.3.3.1) 56
Static Route Examples (1.3.3.2) 57
Static IPv6 Route Examples (1.3.3.3) 59
Dynamic Routing Protocols (1.3.4) 61
Dynamic Routing (1.3.4.1) 61
IPv4 Routing Protocols (1.3.4.2) 62
IPv4 Dynamic Routing Examples (1.3.4.3) 63
IPv6 Routing Protocols (1.3.4.4) 64
IPv6 Dynamic Routing Examples (1.3.4.5) 64

Summary (1.4) 66

Practice 67

Class Activities 67
Labs 67
Packet Tracer Activities 67

Check Your Understanding Questions 68

Chapter 2 Static Routing 73

Objectives 73

Key Terms 73

Introduction (2.0.1.1) 74

Static Routing Implementation (2.1) 75

Reach Remote Networks (2.1.1.1) 75

Why Use Static Routing? (2.1.1.2) 76

When to Use Static Routes (2.1.1.3) 77

Static Route Applications (2.1.2.1) 78

Standard Static Route (2.1.2.2) 79

Default Static Route (2.1.2.3) 79

Summary Static Route (2.1.2.4) 80

Floating Static Route (2.1.2.5) 81

Configure Static and Default Routes (2.2) 82

Configure IPv4 Static Routes (2.2.1) 82

ip route Command (2.2.1.1) 82

Next-Hop Options (2.2.1.2) 84

Configure a Next-Hop Static Route (2.2.1.3) 85

Configure a Directly Connected Static Route (2.2.1.4) 87

Configure a Fully Specified Static Route (2.2.1.5) 89

Verify a Static Route (2.2.1.6) 91

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) 94

Verify a Default Static Route (2.2.2.3) 94

Configure IPv6 Static Routes (2.2.3) 96

The ipv6 route Command (2.2.3.1) 96

Next-Hop Options (2.2.3.2) 97

Configure a Next-Hop Static IPv6 Route (2.2.3.3) 100

Configure a Directly Connected Static IPv6 Route (2.2.3.4) 102

Configure a Fully Specified Static IPv6 Route (2.2.3.5) 104

Verify IPv6 Static Routes (2.2.3.6) 105

Configure IPv6 Default Routes (2.2.4) 106

Default Static IPv6 Route (2.2.4.1) 106

Configure a Default Static IPv6 Route (2.2.4.2) 107

Verify a Default Static Route (2.2.4.3) 108

Review of CIDR and VLSM (2.3) 109

Classful Addressing (2.3.1) 109

Classful Network Addressing (2.3.1.1) 109

Classful Subnet Masks (2.3.1.2) 110

Classful Routing Protocol Example (2.3.1.3) 112

Classful Addressing Waste (2.3.1.4) 113

CIDR (2.3.2) 114

Classless Inter-Domain Routing (2.3.2.1) 114

Classless Inter-Domain Routing (2.3.2.2) 115

Static Routing CIDR Example (2.3.2.3) *117*
Classless Routing Protocol Example (2.3.2.4) *118*
VLSM (2.3.3) 119
Fixed-Length Subnet Masking (2.3.3.1) *119*
Variable-Length Subnet Masking (2.3.3.2) *121*
VLSM in Action (2.3.3.3) *122*
Subnetting Subnets (2.3.3.4) *123*
VLSM Example (2.3.3.5) *125*

Configure Summary and Floating Static Routes (2.4) 128

Configure IPv4 Summary Routes (2.4.1) 128
Route Summarization (2.4.1.1) *128*
Calculate a Summary Route (2.4.1.2) *129*
Summary Static Route Example (2.4.1.3) *130*
Configure IPv6 Summary Routes (2.4.1) 133
Summarize IPv6 Network Addresses (2.4.2.1) *133*
Calculate IPv6 Network Addresses (2.4.2.2) *134*
Configure an IPv6 Summary Address (2.4.2.3) *137*
Configure Floating Static Routes (2.4.3) 138
Floating Static Routes (2.4.3.1) *138*
Configure a Floating Static Route (2.4.3.2) *140*
Test the Floating Static Route (2.4.3.3) *141*

Troubleshoot Static and Default Route Issues (2.5) 142

Packet Processing with Static Routes (2.5.1) 143
Static Routes and Packet Forwarding (2.5.1.1) *143*
Troubleshoot IPv4 Static and Default Route Configuration (2.5.2) 144
Troubleshooting a Missing Route (2.5.2.1) *144*
Solve a Connectivity Problem (2.5.2.2) *147*

Summary (2.6) 150

Practice 151

Class Activities 151
Labs 152
Packet Tracer Activities 152

Check Your Understanding Questions 152

Chapter 3 Routing Dynamically 155

Objectives 155

Key Terms 155

Introduction (3.0.1.1) 157

Dynamic Routing Protocols (3.1) 158
The Evolution of Dynamic Routing Protocols (3.1.1.1) 158
Purpose of Dynamic Routing Protocols (3.1.1.2) 159
The Role of Dynamic Routing Protocols (3.1.1.3) 160

Dynamic versus Static Routing (3.1.2) 161
Using Static Routing (3.1.2.1) 161
Static Routing Scorecard (3.1.2.2) 162
Using Dynamic Routing Protocols (3.1.2.3) 163
Dynamic Routing Scorecard (3.1.2.4) 163

Routing Protocol Operating Fundamentals (3.1.3) 164
Dynamic Routing Protocol Operation (3.1.3.1) 165
Cold Start (3.1.3.2) 165
Network Discovery (3.1.3.3) 166
Exchanging the Routing Information (3.1.3.4) 168
Achieving Convergence (3.1.3.5) 170

Types of Routing Protocols (3.1.4) 171
Classifying Routing Protocols (3.1.4.1) 171
IGP and EGP Routing Protocols (3.1.4.2) 172
Distance Vector Routing Protocols (3.1.4.3) 173
Link-State Routing Protocols (3.1.4.4) 174
Classful Routing Protocols (3.1.4.5) 175
Classless Routing Protocols (3.1.4.6) 177
Routing Protocol Characteristics (3.1.4.7) 179
Routing Protocol Metrics (3.1.4.8) 180

Distance Vector Dynamic Routing (3.2) 181
Distance Vector Technologies (3.2.1.1) 181
Distance Vector Algorithm (3.2.1.2) 182

Types of Distance Vector Routing Protocols (3.2.2) 183
Routing Information Protocol (3.2.2.1) 183
Enhanced Interior Gateway Routing Protocol (3.2.2.2) 184

RIP and RIPng Routing (3.3) 186
Configuring the RIP Protocol (3.3.1) 186
Router RIP Configuration Mode (3.3.1.1) 186
Advertising Networks (3.3.1.2) 188
Examining Default RIP Settings (3.3.1.3) 189
Enabling RIPv2 (3.3.1.4) 190
Disabling Auto Summarization (3.3.1.5) 192

Configuring Passive Interfaces (3.3.1.6) 193
Propagating a Default Route (3.3.1.7) 195
Configuring the RIPng Protocol (3.3.2) 196
Advertising IPv6 Networks (3.3.2.1) 196
Examining the RIPng Configuration (3.3.2.2) 198

Link-State Dynamic Routing (3.4) 200

Link-State Routing Protocol Operation (3.4.1) 200
Shortest Path First Protocols (3.4.1.1) 200
Dijkstra's Algorithm (3.4.1.2) 201
SPF Example (3.4.1.3) 202
Link-State Updates (3.4.2) 203
Link-State Routing Process (3.4.2.1) 203
Link and Link-State (3.4.2.2) 204
Say Hello (3.4.2.3) 207
Building the Link-State Packet (3.4.2.4) 208
Flooding the LSP (3.4.2.5) 209
Building the Link-State Database (3.4.2.6) 210
Building the SPF Tree (3.4.2.7) 211
Adding OSPF Routes to the Routing Table (3.4.2.8) 212
Why Use Link-State Routing Protocols? (3.4.3) 213
Why Use Link-State Protocols? (3.4.3.1) 213
Link-State Protocols Support Multiple Areas (3.4.3.2) 214
Protocols that Use Link-State (3.4.3.3) 214

The Routing Table (3.5) 215

Parts of an IPv4 Route Entry (3.5.1) 215
Routing Table Entries (3.5.1.1) 215
Directly Connected Entries (3.5.1.2) 217
Remote Network Entries (3.5.1.3) 218
Dynamically Learned IPv4 Routes (3.5.2) 219
Routing Table Terms (3.5.2.1) 219
Ultimate Route (3.5.2.2) 220
Level 1 Route (3.5.2.3) 220
Level 1 Parent Route (3.5.2.4) 221
Level 2 Child Route (3.5.2.5) 222
The IPv4 Route Lookup Process (3.5.3) 224
Route Lookup Process (3.5.3.1) 224
Best Route = Longest Match (3.5.3.2) 226
Analyze an IPv6 Routing Table (3.5.4) 227
IPv6 Routing Table Entries (3.5.4.1) 227
Directly Connected Entries (3.5.4.2) 228
Remote IPv6 Network Entries (3.5.4.3) 230

Summary (3.6) 232

Practice 233

Class Activities 233

Lab 233

Packet Tracer Activities 234

Check Your Understanding Questions 234

Chapter 4 EIGRP 239

Objectives 239

Key Terms 239

Introduction (4.0.1) 240

Characteristics of EIGRP (4.1) 240

Basic Features of EIGRP (4.1.1) 240

Features of EIGRP (4.1.1.1) 241

Protocol-Dependent Modules (4.1.1.2) 242

Reliable Transport Protocol (4.1.1.3) 243

Authentication (4.1.1.4) 244

Types of EIGRP Packets (4.1.2) 245

EIGRP Packet Types (4.1.2.1) 245

EIGRP Hello Packets (4.1.2.2) 247

EIGRP Update and Acknowledgment Packets (4.1.2.3) 248

EIGRP Query and Reply Packets (4.1.2.4) 249

EIGRP Messages (4.1.3) 251

Encapsulating EIGRP Messages (4.1.3.1) 251

EIGRP Packet Header and TLV (4.1.3.2) 252

Configuring EIGRP for IPv4 (4.2) 255

Configuring EIGRP with IPv4 (4.2.1) 255

EIGRP Network Topology (4.2.1.1) 255

Autonomous System Numbers (4.2.1.2) 257

The Router EIGRP Command (4.2.1.3) 259

EIGRP Router ID (4.2.1.4) 261

Configuring the EIGRP Router ID (4.2.1.5) 262

The Network Command (4.2.1.6) 264

The Network Command and Wildcard Mask (4.2.1.7) 266

Passive Interface (4.2.1.8) 268

Verifying EIGRP with IPv4 (4.2.2) 270

Verifying EIGRP: Examining Neighbors (4.2.2.1) 270

*Verifying EIGRP: **show ip protocols** Command (4.2.2.2) 272*

Verifying EIGRP: Examine the IPv4 Routing Table (4.2.2.3) 273

Operation of EIGRP (4.3) 277

EIGRP Initial Route Discover (4.3.1) 277

EIGRP Neighbor Adjacency (4.3.1.1) 277
EIGRP Topology Table (4.3.1.2) 278
EIGRP Convergence (4.3.1.3) 280

Metrics (4.3.2) 280

EIGRP Composite Metric (4.3.2.1) 281
Examining Interface Values (4.3.2.2) 283
Bandwidth Metric (4.3.2.3) 284
Delay Metric (4.3.2.4) 286
Calculating the EIGRP Metric (4.3.2.5) 287
Calculating the EIGRP Metric: Example (4.3.2.6) 288

DUAL and the Topology Table (4.3.3) 290

DUAL Concepts (4.3.3.1) 291
Introduction to DUAL (4.3.3.2) 291
Successor and Feasible Distance (4.3.3.3) 293
Feasible Successors, Feasibility Condition, and Reported Distance (4.3.3.4) 295
*Topology Table: **show ip eigrp topology** Command (4.3.3.5) 297*
Topology Table: No Feasible Successor (4.3.3.7) 300

DUAL and Convergence (4.3.4) 302

DUAL Finite State Machine (FSM) (4.3.4.1) 302
DUAL: Feasible Successor (4.3.4.2) 304
DUAL: No Feasible Successor (4.3.4.3) 306

Configuring EIGRP for IPv6 (4.4) 308

EIGRP for IPv4 vs. IPv6 (4.4.1) 308

EIGRP for IPv6 (4.4.1.1) 308
Comparing EIGRP for IPv4 and IPv6 (4.4.1.2) 310
IPv6 Link-local Addresses (4.4.1.3) 311

Configuring EIGRP for IPv6 (4.4.2) 312

EIGRP for IPv6 Network Topology (4.4.2.1) 312
Configuring IPv6 Link-local Addresses (4.4.2.2) 314
Configuring the EIGRP for IPv6 Routing Process (4.4.2.3) 316
ipv6 eigrp *Interface Command (4.4.2.4) 318*

Verifying EIGRP for IPv6 (4.4.3) 319

Verifying EIGRP for IPv6: Examining Neighbors (4.4.3.1) 319
Verifying EIGRP for IPv6: show ip protocols Command (4.4.3.2) 321
Verifying EIGRP for IPv6: Examine the IPv6 Routing Table (4.4.3.3) 322

Summary (4.5) 326

Practice 327

Class Activities 328

Labs 328

Packet Tracer Activities 328

Check Your Understanding Questions 328

Chapter 5 EIGRP Advanced Configurations and Troubleshooting 333

Objectives 333

Key Terms 333

Introduction (5.0.1.1) 334

Advanced EIGRP Configurations (5.1) 334

Auto-summarization (5.1.1) 335

Network Topology (5.1.1.1) 335
EIGRP Auto-summarization (5.1.1.2) 337
Configuring EIGRP Auto-summarization (5.1.1.3) 338
*Verifying Auto-Summary: **show ip protocols** (5.1.1.4) 340*
Verifying Auto-Summary: Topology Table (5.1.1.5) 342
Verifying Auto-Summary: Routing Table (5.1.1.6) 343
Summary Route (5.1.1.7, 5.1.1.8) 345

Manual Summarization (5.1.2) 347

Manual Summary Routes (5.1.2.1) 347
Configuring EIGRP Manual Summary Routes (5.1.2.2) 349
Verifying Manual Summary Routes (5.1.2.3) 351
EIGRP for IPv6: Manual Summary Routes (5.1.2.4) 351

Default Route Propagation (5.1.3) 353

Propagating a Default Static Route (5.1.3.1) 353
Verifying the Propagated Default Route (5.1.3.2) 355
EIGRP for IPv6: Default Route (5.1.3.3) 355

Fine-tuning EIGRP Interfaces (5.1.4) 357

EIGRP Bandwidth Utilization (5.1.4.1) 357
Hello and Hold Timers (5.1.4.2) 359
Load Balancing IPv4 (5.1.4.3) 361
Load Balancing IPv6 (5.1.4.4) 363

Secure EIGRP (5.1.5) 364

Routing Protocol Authentication Overview (5.1.5.1) 364
Configuring EIGRP with MD5 Authentication (5.1.5.2) 365
EIGRP Authentication Example (5.1.5.3) 366
Verify Authentication (5.1.5.4) 369

Troubleshoot EIGRP (5.2) 370

Components of Troubleshooting EIGRP (5.2.1) 370

Basic EIGRP Troubleshooting Commands (5.2.1.1) 370
Components (5.2.1.2) 372

Troubleshoot EIGRP Neighbor Issues (5.2.2) 374
Layer 3 Connectivity (5.2.2.1) 374
EIGRP Parameters (5.2.2.2) 375
EIGRP Interfaces (5.2.2.3) 376
Troubleshooting EIGRP Routing Table Issues (5.2.3) 378
Passive Interface (5.2.3.1) 378
Missing Network Statement (5.2.3.2) 380
Auto-summarization (5.2.3.3) 382

Summary (5.3) 386

Practice 388

Class Activities 388

Labs 388

Packet Tracer Activities 388

Check Your Understanding Questions 389

Chapter 6 Single-Area OSPF 393

Objectives 393

Key Terms 393

Introduction (6.0.1.1) 394

Characteristics of OSPF (6.1) 394

Evolution of OSPF (6.1.1.1) 394

Features of OSPF (6.1.1.2) 395

Components of OSPF (6.1.1.3) 396

Link-State Operation (6.1.1.4) 398

Single-Area and Multiarea OSPF (6.1.1.5) 399

OSPF Messages (6.1.2) 401

Encapsulating OSPF Messages (6.1.2.1) 402

Types of OSPF Packets (6.1.2.2) 402

Hello Packet (6.1.2.3) 403

Hello Packet Intervals (6.1.2.4) 404

Link-State Updates (6.1.2.5) 405

OSPF Operation (6.1.3) 406

OSPF Operational States (6.1.3.1) 406

Establish Neighbor Adjacencies (6.1.3.2) 407

OSPF DR and BDR (6.1.3.3) 408

Synchronizing OSPF Databases (6.1.3.4) 411

Configuring Single-Area OSPFv2 (6.2) 414

OSPF Network Topology (6.2.1.1) 414

Router OSPF Configuration Mode (6.2.1.2) 415

Router IDs (6.2.1.3) 415
Configuring an OSPF Router ID (6.2.1.4) 417
Modifying a Router ID (6.2.1.5) 418
Using a Loopback Interface as the Router ID (6.2.1.6) 419
Configure Single-Area OSPFv2 (6.2.2) 420
Enabling OSPF on Interfaces (6.2.2.1) 420
Wildcard Mask (6.2.2.2) 420
The network Command (6.2.2.3) 421
Passive Interface (6.2.2.4) 422
Configuring Passive Interfaces (6.2.2.5) 423
OSPF Cost (6.2.3) 425
OSPF Metric = Cost (6.2.3.1) 425
OSPF Accumulates Costs (6.2.3.2) 426
Adjusting the Reference Bandwidth (6.2.3.3) 427
Default Interface Bandwidths (6.2.3.4) 430
Adjusting the Interface Bandwidths (6.2.3.5) 433
Manually Setting the OSPF Cost (6.2.3.6) 434
Verify OSPF (6.2.4) 435
Verify OSPF Neighbors (6.2.4.1) 435
Verify OSPF Protocol Settings (6.2.4.2) 436
Verify OSPF Process Information (6.2.4.3) 437
Verify OSPF Interface Settings (6.2.4.4) 438
Configure Single-Area OSPFv3 (6.3) 439
OSPFv3 (6.3.1.1) 439
Similarities Between OSPFv2 and OSPFv3 (6.3.1.2) 440
Differences Between OSPFv2 and OSPFv3 (6.3.1.3) 441
Link-Local Addresses (6.3.1.4) 442
Configuring OSPFv3 (6.3.2) 443
OSPFv3 Network Topology (6.3.2.1) 443
Link-Local Addresses (6.3.2.2) 444
Assigning Link-Local Addresses (6.3.2.3) 445
Configuring the OSPFv3 Router ID (6.3.2.4) 446
Modifying an OSPFv3 Router ID (6.3.2.5) 449
Enabling OSPFv3 on Interfaces (6.3.2.6) 450
Verify OSPFv3 (6.3.3) 451
Verify OSPFv3 Neighbors (6.3.3.1) 451
Verify OSPFv3 Protocol Settings (6.3.3.2) 452

Verify OSPFv3 Interfaces (6.3.3.3) 453
Verify the IPv6 Routing Table (6.3.3.4) 453

Summary (6.4) 455

Practice 456

Class Activities 456
Labs 456
Packet Tracer Activities 456

Check Your Understanding Questions 457

Chapter 7 Adjust and Troubleshoot Single-Area OSPF 461

Objectives 461

Key Terms 461

Introduction (7.0.1.1) 462

Advanced Single-Area OSPF Configurations (7.1) 462

OSPF Network Types (7.1.1.1) 462
Challenges in Multiaccess Networks (7.1.1.2) 465
OSPF Designated Router (7.1.1.3) 467
Verifying DR/BDR Roles (7.1.1.4) 469
Verifying DR/BDR Adjacencies (7.1.1.5) 472
Default DR/BDR Election Process (7.1.1.6) 474
DR/BDR Election Process (7.1.1.7) 475
The OSPF Priority (7.1.1.8) 477
Changing the OSPF Priority (7.1.1.9) 478

Default Route Propagation (7.1.2) 480

Propagating a Default Static Route in OSPFv2 (7.1.2.1) 480
Verifying the Propagated Default Route (7.1.2.2) 481
Propagating a Default Static Route in OSPFv3 (7.1.2.3) 482
Verifying the Propagated IPv6 Default Route (7.1.2.4) 484

Fine-tuning OSPF Interfaces (7.1.3) 485

OSPF Hello and Dead Intervals (7.1.3.1) 485
Modifying OSPFv2 Intervals (7.1.3.2) 486
Modifying OSPFv3 Intervals (7.1.3.3) 488

Secure OSPF (7.1.4) 489

Routers Are Targets (7.1.4.1) 489
Secure Routing Updates (7.1.4.2) 492
MD5 Authentication (7.1.4.3) 495

Configuring OSPF MD5 Authentication (7.1.4.4) 496
OSPF MD5 Authentication Example (7.1.4.5) 497
Verifying OSPF MD5 Authentication (7.1.4.6) 499

Troubleshooting Single-Area OSPF Implementations (7.2) 501
OSPF States (7.2.1.2) 501
OSPF Troubleshooting Commands (7.2.1.3) 502
Components of Troubleshooting OSPF (7.2.1.4) 505

Troubleshoot Single-Area OSPFv2 Routing Issues (7.2.2) 508
Troubleshooting Neighbor Issues (7.2.2.1) 508
Troubleshooting OSPF Routing Table Issues (7.2.2.2) 511

Troubleshoot Single-Area OSPFv3 Routing Issues (7.2.3) 514
OSPFv3 Troubleshooting Commands (7.2.3.1) 514
Troubleshooting OSPFv3 (7.2.3.2) 517

Summary (7.3) 521

Practice 523
Class Activities 523
Labs 523
Packet Tracer Activities 523

Check Your Understanding Questions 524

Chapter 8 Multiarea OSPF 527

Objectives 527

Key Terms 527

Introduction (8.0.1.1) 528

Multiarea OSPF Operation (8.1) 528
Single-Area OSPF (8.1.1.1) 528
Multiarea OSPF (8.1.1.2) 529
OSPF Two-Layer Area Hierarchy (8.1.1.3) 530
Types of OSPF Routers (8.1.1.4) 532

Multiarea OSPF LSA Operation (8.1.2) 534
OSPF LSA Types (8.1.2.1) 534
OSPF LSA Type 1 (8.1.2.2) 535
OSPF LSA Type 2 (8.1.2.3) 536
OSPF LSA Type 3 (8.1.2.4) 536
OSPF LSA Type 4 (8.1.2.5) 537
OSPF LSA Type 5 (8.1.2.6) 538

OSPF Routing Table and Types of Routes (8.1.3) 539
OSPF Routing Table Entries (8.1.3.1) 539
OSPF Route Calculation (8.1.3.2) 540
Configuring Multiarea OSPF (8.2) 541
Implementing Multiarea OSPF (8.2.1.1) 541
Configuring Multiarea OSPF (8.2.1.2) 542
Configuring Multiarea OSPFv3 (8.2.1.3) 544
OSPF Route Summarization (8.2.2.1) 545
Interarea and External Route Summarization (8.2.2.2) 546
Interarea Route Summarization (8.2.2.3) 548
Calculating the Summary Route (8.2.2.4) 550
Configuring Interarea Route Summarization (8.2.2.5) 550
Verifying Multiarea OSPF (8.2.3.1) 552
Verify General Multiarea OSPF Settings (8.2.3.2) 553
Verify the OSPF Routes (8.2.3.3) 554
Verify the Multiarea OSPF LSDB (8.2.3.4) 555
Verify Multiarea OSPFv3 (8.2.3.5) 556
Summary (8.3) 560
Practice 562
Class Activities 562
Labs 562
Packet Tracer Activities 562
Check Your Understanding Questions 562

Chapter 9 Access Control Lists 565
Objectives 565
Key Terms 565
Introduction (9.0.1.1) 566
IP ACL Operation (9.1) 567
Purpose of ACLs (9.1.1) 567
What Is an ACL? (9.1.1.1) 567
A TCP Conversation (9.1.1.2) 568
Packet Filtering (9.1.1.3) 572
Packet Filtering Example (9.1.1.4) 573
ACL Operation (9.1.1.5) 574
Standard Versus Extended IPv4 ACLs (9.1.2) 575
Types of Cisco IPv4 ACLs (9.1.2.1) 575
Numbering and Naming ACLs (9.1.2.2) 576

Wildcard Masks in ACLs (9.1.3) 577
Introducing ACL Wildcard Masking (9.1.3.1) 577
Wildcard Mask Examples (9.1.3.2) 579
Calculating the Wildcard Mask (9.1.3.3) 581
Wildcard Mask Keywords (9.1.3.4) 582
Examples Wildcard Mask Keywords (9.1.3.5) 584
Guidelines for ACL Creation (9.1.4) 584
General Guidelines for Creating ACLs (9.1.4.1) 585
ACL Best Practices (9.1.4.2) 586
Guidelines for ACL Placement (9.1.5) 587
Where to Place ACLs (9.1.5.1) 587
Standard ACL Placement (9.1.5.2) 588
Extended ACL Placement (9.1.5.3) 589

Standard IPv4 ACLs (9.2) 591

Configure Standard IPv4 ACLs (9.2.1) 591
Entering Criteria Statements (9.2.1.1) 591
Standard ACL Logic (9.2.1.2) 592
Configuring a Standard ACL (9.2.1.3) 593
Internal Logic (9.2.1.4) 595
Applying Standard ACLs to Interfaces: Permit a Specific Subnet (9.2.1.5) 596
Applying Standard ACLs to Interfaces: Deny a Specific Host (9.2.1.6) 598
Creating Named Standard ACLs (9.2.1.7) 600
Commenting ACLs (9.2.1.8) 601
Modifying IPv4 ACLs (9.2.2) 603
Editing Standard Numbered ACLs: Using a Text Editor (9.2.2.1) 603
Editing Standard Numbered ACLs: Using the Sequence Number (9.2.2.2) 604
Editing Standard Named ACLs (9.2.2.3) 605
Verifying ACLs (9.2.2.4) 606
ACL Statistics (9.2.2.5) 607
Standard ACL Sequence Numbers (9.2.2.6) 608
Securing VTY Ports with a Standard IPv4 ACL (9.2.3) 611
Configuring a Standard ACL to Secure a VTY Port (9.2.3.1) 611
Verifying a Standard ACL Used to Secure a VTY Port (9.2.3.2) 612

Extended IPv4 ACLs (9.3) 614

Structure of an Extended IPv4 ACL (9.3.1) 614
Extended ACLs: Testing Packets (9.3.1.1) 614
Extended ACLs: Testing Ports and Services (9.3.1.2) 615

Configure Extended IPv4 ACLs (9.3.2) 616
Configuring Extended ACLs (9.3.2.1) 616
Applying Extended ACLs to Interfaces (9.3.2.2) 618
Filtering Traffic with Extended ACLs (9.3.2.3) 620
Creating Named Extended ACLs (9.3.2.4) 621
Verifying Extended ACLs (9.3.2.5) 622
Editing Extended ACLs (9.3.2.6) 623

Troubleshoot ACLs (9.4) 625

Processing Packets with ACLs (9.4.1) 625
Inbound and Outbound ACL Logic (9.4.1.1) 625
ACL Logic Operations (9.4.1.2) 627
Standard ACL Decision Process (9.4.1.3) 628
Extended ACL Decision Process (9.4.1.4) 629
Common ACL Errors (9.4.2) 629
Troubleshooting Common ACL Errors - Example 1 (9.4.2.1) 629
Troubleshooting Common ACL Errors - Example 2 (9.4.2.2) 630
Troubleshooting Common ACL Errors - Example 3 (9.4.2.3) 632
Troubleshooting Common ACL Errors - Example 4 (9.4.2.4) 632
Troubleshooting Common ACL Errors - Example 5 (9.4.2.5) 633

IPv6 ACLs (9.5) 635

IPv6 ACL Creation (9.5.1) 635
Type of IPv6 ACLs (9.5.1.1) 635
Comparing IPv4 and IPv6 ACLs (9.5.1.2) 636
Configuring IPv6 ACLs (9.5.2) 637
Configuring IPv6 Topology (9.5.2.1) 637
Syntax for Configuring IPv6 ACLs (9.5.2.2) 639
Applying an IPv6 ACL to an Interface (9.5.2.3) 641
IPv6 ACL Examples (9.5.2.4) 642
Verifying IPv6 ACLs (9.5.2.5) 643

Summary (9.6) 646

Practice 648

Class Activities 648
Labs 648
Packet Tracer Activities 648

Check Your Understanding Questions 649

Chapter 10 IOS Images and Licensing 653

Objectives 653

Key Terms 653

Introduction (10.0.1.1) 654

Managing IOS System Files (10.1) 654

Naming Conventions (10.1.1) 654

Cisco IOS Software Release Families and Trains (10.1.1.1) 655
Cisco IOS 12.4 Mainline and T Trains (10.1.1.2) 655
Cisco IOS 12.4 Mainline and T Numbering (10.1.1.3) 657
Cisco IOS 12.4 System Image Packaging (10.1.1.4) 658
Cisco IOS 15.0 M and T Trains (10.1.1.5) 659
Cisco IOS 15 Train Numbering (10.1.1.6) 661
IOS 15 System Image Packaging (10.1.1.7) 662
IOS Image Filenames (10.1.1.8) 663

Managing Cisco IOS Images (10.1.2) 667

TFTP Servers as a Backup Location (10.1.2.1) 667
Creating Cisco IOS Image Backup (10.1.2.2) 667
Copying a Cisco IOS Image (10.1.2.3) 669
Boot System (10.1.2.4) 670

IOS Licensing (10.2) 672

Software Licensing (10.2.1) 672

Licensing Overview (10.2.1.1) 672
Licensing Process (10.2.1.2) 674
Step 1. Purchase the Software Package or Feature to Install (10.2.1.3) 675
Step 2. Obtain a License (10.2.1.4) 675
Step 3. Install the License (10.2.1.5) 677

License Verification and Management (10.2.2) 678

License Verification (10.2.2.1) 678
Activate an Evaluation Right-To-Use License (10.2.2.2) 680
Back Up the License (10.2.2.3) 682
Uninstall the License (10.2.2.4) 682

Summary (10.3) 685

Practice 688

Class Activities 688

Packet Tracer Activities 688

Check Your Understanding Questions 688

Appendix A Answers to the "Check Your Understanding" Questions 693

Glossary 709

Index 723

Icons Used in This Book

Command Syntax Conventions

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

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Routing Protocols Companion Guide is the official supplemental textbook for the Cisco Network Academy CCNA Routing Protocols 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 routing protocols for those pursuing careers as network professionals as well as those who need only an introduction to routing protocols for professional growth. Topics are presented concisely, starting with the most fundamental concepts and progressing to a comprehensive understanding of routing protocols. The content of this text provides the foundation for additional Cisco 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.

- **"How-to" feature:** When this book covers a set of steps that you need to perform for certain tasks, the text lists the steps as a how-to list. When you are studying, the icon helps you easily refer to this feature as you skim through the book.
- **Notes:** These are short sidebars that point out interesting facts, timesaving methods, and important safety issues.
- **Chapter summaries:** Each chapter includes a summary of the chapter's key concepts. It provides a synopsis of the chapter and serves as a study aid.
- **"Practice" section:** The end of each chapter includes 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 for each key term. The key 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 approximately 175 terms.

Practice

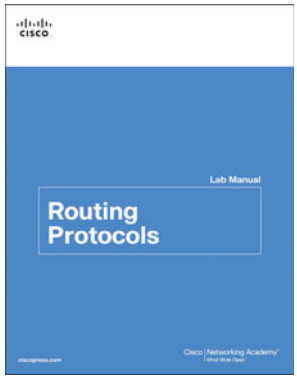
Practice makes perfect. This new Companion Guide offers you ample opportunities to put what you learn into practice. You will find the following features valuable and effective in reinforcing the instruction that you receive:

- **Check Your Understanding Questions and answer key:** Updated review questions are presented at the end of each chapter as a self-assessment tool. These questions match the style of questions that you see in the online course. Appendix A, "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, the end of each chapter includes a "Practice" section that collects a list of all the labs and activities to provide practice with the topics introduced in that chapter. The labs and class activities are available in the companion *Routing Protocols Lab Manual* (ISBN 978-1-58713-322-0). The Packet Tracer Activities PKA files are found in the online course.
- **Page references to online course:** After each heading, 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.

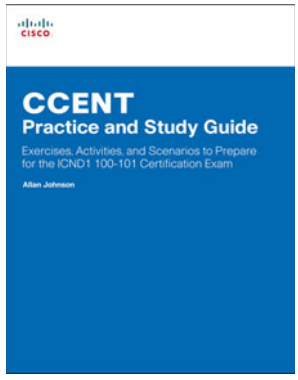
Lab Manual

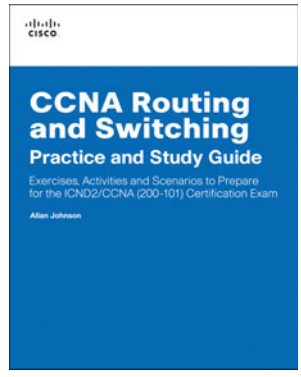
The supplementary book *Routing Protocols Lab Manual*, by Cisco Press (ISBN 978-1-58713-322-0), contains all the labs and class activities from the course.



Practice and Study Guides

Additional Study Guide exercises, activities, and scenarios are available in the new *CCENT Practice and Study Guide* (978-158713-345-9) and *CCNA Routing and Switching Practice and Study Guide* (978-158713-344-2) books by Allan Johnson. Each Practice and Study Guide coordinates with the recommended curriculum sequence—the CCENT book follows the course outlines for *Introduction to Networks* and *Routing and Switching Essentials*, and the CCNA book follows the course outlines for *Scaling Networks* and *Connecting Networks*.





Packet Tracer Activity

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 only through the Cisco Networking Academy website. Ask your instructor for access to Packet Tracer.

How This Book Is Organized

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

- **Chapter 1, "Routing Concepts":** Introduces initial router configuration, directly connected networks, static routing, and dynamic routing protocols. The process of packet forwarding is also reviewed, including the path determination and switching functions.
- **Chapter 2, "Static Routing":** Introduces the use of static routes and the role they play in modern networks. This chapter describes the advantages, uses, and configuration of IPv4 and IPv6 static routes using next-hop IP addresses and exit interfaces. Floating static routes and summary routes are also discussed. The chapter includes a review of VLSM and CIDR.
- **Chapter 3, "Routing Dynamically":** Examines the purpose of dynamic routing protocols and compares their use to static routing. Distance vector and link-state routing protocols are discussed, along with the IP routing table. RIP and RIPng routing protocols are introduced as a foundation for understanding other routing protocols discussed in this book. This chapter serves as an introduction to terms and concepts that are examined more fully in later chapters.

- **Chapter 4, "EIGRP":** Introduces the routing protocol EIGRP. EIGRP is a Cisco-proprietary, advanced distance vector routing protocol. This chapter describes the basic features and operations of EIGRP, EIGRP packet formats, and how the composite metric is calculated by EIGRP. The concepts and operations of DUAL (Diffusing Update Algorithm) are discussed, and how DUAL determines best path and loop-free back up paths. This chapter includes the basic configuration and verification of EIGRP for IPv4 and EIGRP for IPv6.
- **Chapter 5, "EIGRP Advanced Configurations and Troubleshooting":** This chapter includes the configuration and verification of advanced EIGRP features such as automatic summarization, manual summarization, default route propagation, EIGRP authentication of routing updates, and fine-tuning EIGRP interfaces. The components of troubleshooting EIGRP are discussed along with neighbor and routing table issues.
- **Chapter 6, "Single-Area OSPF":** Introduces the link-state routing protocol OSPF. Single-area OSPF operations are discussed, including how routers achieve convergence in an OSPF network, the OSPF metric of cost, OSPF messages, and the use of the OSPF router ID. This chapter includes the configuration and verification of single-area OSPFv2 (OSPF for IPv4) and OSPFv3 (OSPF for IPv6).
- **Chapter 7, "Adjust and Troubleshoot Single-Area OSPF":** Focuses on advanced features of OSPF. The OSPF DR/BDR election process is discussed along with OSPF link-state advertisements, propagating a default route with an OSPF routing domain, neighbor adjacencies, modifying OSPF interface settings to improve network performance, and configuring OSPF authentication. This chapter includes troubleshooting OSPF missing route entries for OSPFv2 and OSPFv3.
- **Chapter 8, "Multiarea OSPF":** Examines the purpose and advantages of multiarea OSPF. Multiarea OSPF link-state advertisements are discussed along with implementing multiarea OSPF. This chapter includes the configuration and verification of multiarea OSPFv2 and OSPFv3.
- **Chapter 9, "Access Control Lists":** Examines how access control lists (ACLs) are used to filter traffic in IPv4 and IPv6 networks. The use of wildcard masks for IPv4 ACLs is discussed along with the guidelines for creating ACLs and the placement of ACLs. The configuration and verification of IPv4 standard named and extended ACLs (both named and numbered) are discussed. The use of ACLs to limit debug output and secure VTY access is demonstrated. The configuration and verification of IPv6 ACLs are also examined.

- **Chapter 10, "IOS Images and Licensing":** Explains the IOS image and naming conventions for IOS 12.4 and IOS 15. The IOS 15 licensing process is discussed along with how to install an IOS 15 software image license.
- **Appendix A, "Answers to the 'Check Your Understanding' Questions":** Lists the answers to the "Check Your Understanding" review questions that are included at the end of each chapter.
- **Glossary:** Provides you with definitions for all the key terms identified in each chapter.

This page intentionally left blank

CHAPTER 1

Routing Concepts

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?
- Can you configure basic settings on a router to route between two directly connected networks?
- How can you verify connectivity between two networks that are directly connected to a router?
- How do routers encapsulate and de-encapsulate packets when switching packets between directly connected interfaces?
- How do routers determine the best path?
- How do routers build a routing table of directly connected networks?
- How do routers build a routing table using static routes?
- How do routers 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.

default gateway page 3

physical topology page 4

logical topology page 4

availability page 5

scalability page 5

reliability page 5

Random Access Memory (RAM) page 6

Read-Only Memory (ROM) page 6

Non-Volatile Random Access Memory (NVRAM) page 6

Flash page 6

process switching page 9

fast switching page 10

Cisco Express Forwarding (CEF) page 11

IP address page 14

subnet mask page 14

topology diagram page 16

addressing table page 16

statically assigned IP address page 16

dynamically assigned IP address page 16

console cable page 19

terminal emulation software page 19

switched virtual interface (SVI) page 20

High-Speed WAN Interface Card (HWIC) *page 24*

loopback interface *page 28*

directly connected network *page 43*

remote network *page 43*

Gateway of Last Resort *page 43*

metric *page 44*

best path *page 44*

equal cost load balancing *page 45*

unequal cost load balancing *page 45*

administrative distance *page 46*

routing table *page 47*

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.

At the core of the network is the 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 local-area network.

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 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.

This chapter will also 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 will introduce the router, its role in the networks, its main hardware and software components, and the routing process.

Class 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 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.

Initial Configuration of a Router (1.1)

A router is essentially a special-purpose computer with an internetwork operating system optimized for the purpose of routing and securing networks. This section will examine the functions of a router and how a router determines the best path. It will also review the command-line interface (CLI) commands required to configure the base settings of a router.

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.

Networks 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.

There are many terms, key structures, and performance-related characteristics that are referred to when discussing networks. These include:

- **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 a measure of the probability 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

While 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.

Video

Video 1.1.1.2: Routers Route Packets

Go to the online course and play the animation of a packet being sent through a Cisco 1841 router from sender to receiver.

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 local-area network. 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 (i.e., computers, tablets, and smartphones) require the following components to operate:

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

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.

Note

Cisco devices use the Cisco Internetwork Operating System (IOS) as the system software.

Routers store data using:

- *Random Access Memory (RAM)*: Provides temporary storage for various applications and processes, including the running IOS, the running configuration file, various tables (i.e., IP routing table, Ethernet ARP table), and buffers for packet processing. RAM is referred to as volatile because it loses its contents when power is turned off.
- *Read-Only Memory (ROM)*: Provides permanent storage for bootup instructions, basic diagnostic software, and a limited IOS in case the router cannot load the full featured IOS. ROM is firmware and referred to as non-volatile because it does not lose its contents when power is turned off.
- *Non-Volatile Random Access Memory (NVRAM)*: Provides permanent storage for the startup configuration file (startup-config). NVRAM is non-volatile and does not lose its contents when power is turned off.
- *Flash*: Provides permanent storage for the IOS and other system-related files. The IOS is copied from flash into RAM during the bootup process. Flash is non-volatile and does not lose its contents when power is turned off.

Table 1-1 provides a summary of the types of router memory, their volatility, and examples of what is stored in each.

Table 1-1 Router Memory

Memory	Volatile/Non-Volatile	Stores
RAM	Volatile	■ Running IOS ■ Running configuration file ■ IP routing and ARP tables ■ Packet buffer
ROM	Non-volatile	■ Bootup instructions ■ Basic diagnostic software ■ Limited IOS
NVRAM	Non-volatile	■ Startup configuration file
Flash	Non-volatile	■ IOS file ■ Other system 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 1-1 displays the back panel of a Cisco 1941 ISRG2 and identifies those special ports and interfaces.

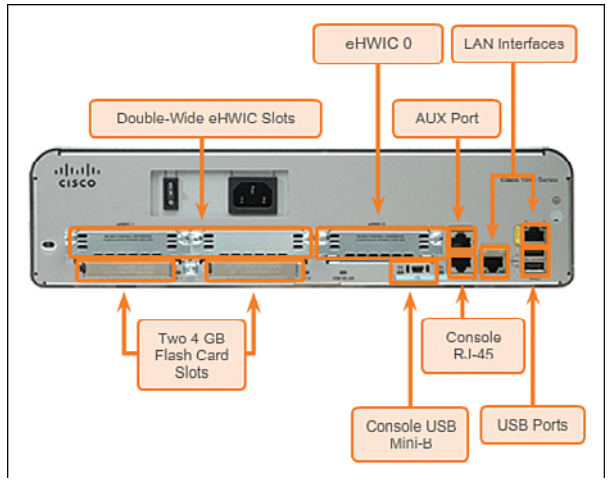


Figure 1-1 Back Panel of a 1941 ISRG2

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.

Video

Video 1.1.1.4: Routers Connect

Go to the online course and play the animation of a packet being sent through two Cisco 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 local-area networks (LANs) and wide-area networks (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 1-2 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.

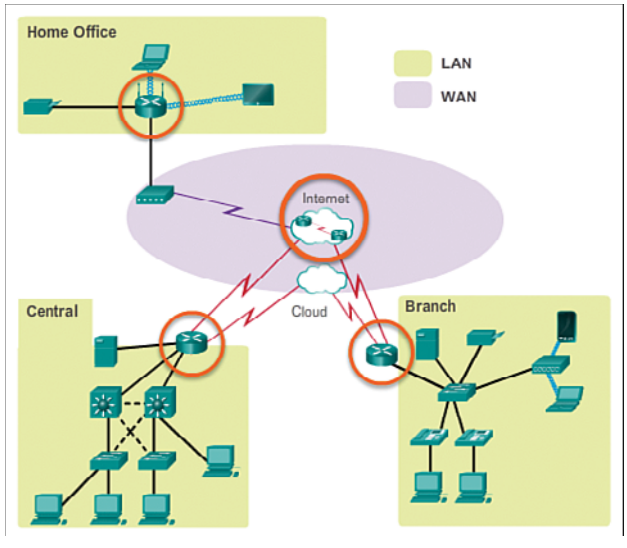


Figure 1-2 Sample Routed Topology

Routers Choose Best Paths (1.1.1.5)

The primary functions of a router are to:

- 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 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).

Video

Video 1.1.1.5: How the Router Works

Go to the online course and play the animation of a packet being sent through two routers from sender to receiver.

Note

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

Packet Forwarding Mechanisms (1.1.1.6)

Routers support three packet-forwarding mechanisms:

- *Process switching*: 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 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 very slow and

rarely implemented in modern networks. Figure 1-3 illustrates how packets are process-switched.

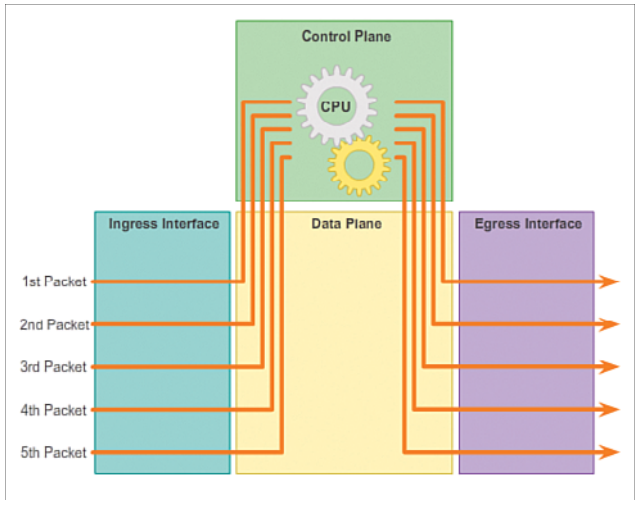


Figure 1-3 Process Switching

- *Fast switching*: This is a common packet-forwarding mechanism which 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 re-used without CPU intervention. Figure 1-4 illustrates how packets are fast-switched.

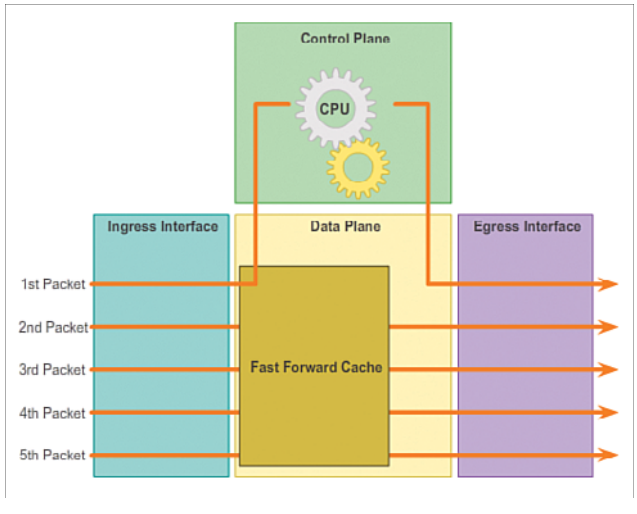


Figure 1-4 Fast Switching

- *Cisco Express Forwarding (CEF)*: 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 pre-computed reverse lookups and next-hop information for routes, including the interface and Layer 2 information. Cisco Express Forwarding is the fastest forwarding mechanism and the preferred choice on Cisco routers. Figure 1-5 illustrates how packets are forwarded using CEF.

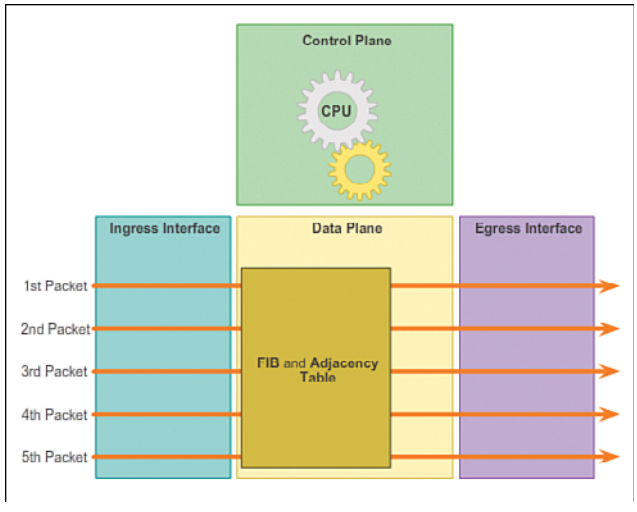


Figure 1-5 Cisco Express Forwarding

Figures 1-3 to 1-5 illustrate the differences between the three packet-forwarding mechanisms. Assume a traffic flow consisting of five packets all going to the same destination. As shown in Figure 1-3, with process switching, each packet must be processed by the CPU individually. Contrast this with fast switching, as shown in Figure 1-4. 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 1-5, 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

Go to the online course to perform this practice activity.

Packet Tracer Activity 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)

In this section, you will see how accessing a network involves connecting hosts and infrastructure devices with IP addresses, subnet masks, and default gateways. This section will also introduce how to configure the initial settings of a switch.

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 the sample reference topology in Figure 1-6. The LANs in the figure serve as an example of how users and network devices could connect to networks.

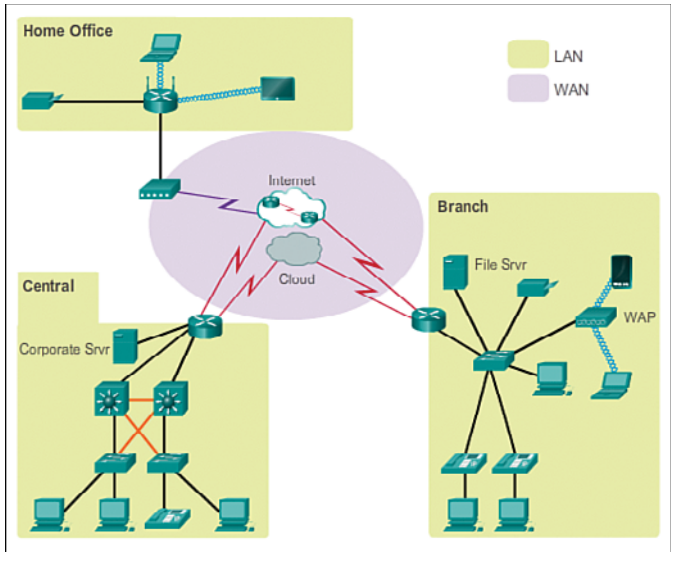


Figure 1-6 Sample LAN and WAN Connections

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 Internet service provider (ISP) network.

The Branch site devices connect as follows:

- Corporate resources (i.e., file servers and printers) connect to Layer 2 switches using Ethernet cables.
- Desktop PCs and voice over IP (VoIP) phones connect to Layer 2 switches using Ethernet cables.
- Laptops and smartphones connect wirelessly to wireless access points (WAPs).
- 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 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, then 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 determines the best path to reach those destinations.

For example, if PC1 sends a packet to the Web Server located at 172.16.1.99, it would discover that the Web Server is not on the local network and it, therefore, must send the packet to the Media Access Control (MAC) address of its default gateway. The packet protocol data unit (PDU) in Figure 1-7 identifies the source and destination IP and MAC addresses.

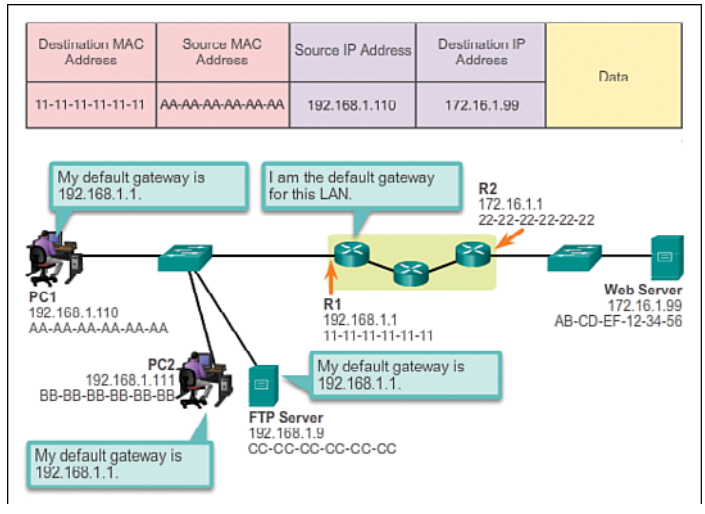


Figure 1-7 Getting the Pieces to the Correct Network

Note

A router is also usually configured with its own default gateway. This is sometimes 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:

- 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*: Provides a visual reference that indicates the physical connectivity and logical Layer 3 addressing. Often created using software, such as Microsoft Visio.
- *Addressing table*: A table that captures device names, interfaces, IPv4 addresses, subnet masks, and default gateway addresses.

Figure 1-8 displays the sample topology diagram, while Table 1-2 provides a sample addressing table for the topology.

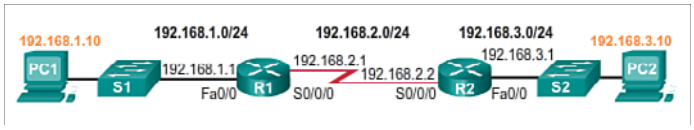


Figure 1-8 Documenting Network Addressing

Table 1-2 Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
PC1	N/A	192.168.1.10	255.255.255.0	192.168.1.1
PC2	N/A	192.168.3.10	255.255.255.0	192.168.3.1

Enable IP on a Host (1.1.2.4)

A host can be assigned its IP address information in one of two ways. A host can get a:

- *Statically Assigned IP Address*: The host is manually assigned the correct IP address, subnet mask, and default gateway. The DNS server IP address can also be configured.
- *Dynamically Assigned IP Address*: IP address information is provided by a server using the Dynamic Host Configuration Protocol (DHCP). The DHCP server provides a valid IP address, subnet mask, and default gateway for end devices. Other information may be provided by the server.

Figures 1-9 and 1-10 provide static and dynamic IPv4 address configuration examples.

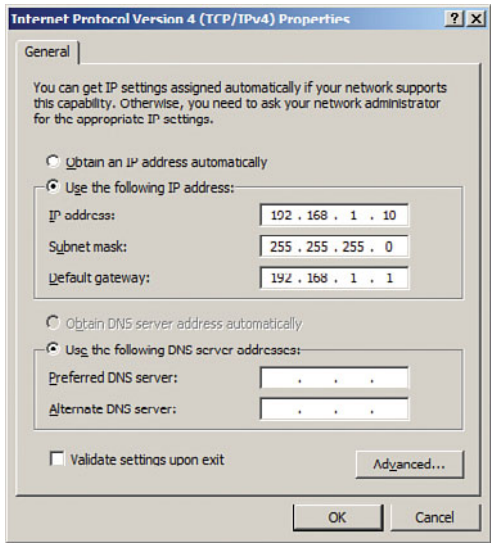


Figure 1-9 Statically Assigning an IP Address

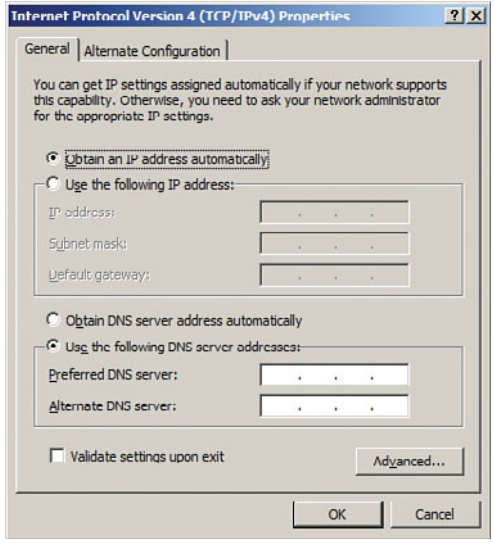


Figure 1-10 Dynamically Assigning an IP Address

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 DHCP server. In large enterprises, dedicated DHCP servers providing services to many LANs are implemented. In a smaller branch or small office setting, DHCP 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. Typically, a green LED means a good connection while a blinking green LED indicates network activity.

If the link light is not on, then 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. The LEDs on the router help the network administrator conduct some basic troubleshooting. Each device has a unique set of LEDs. Consult the device-specific documentation for an accurate description of the LEDs.

The LEDs of the Cisco 1941 router shown in Figure 1-11 are explained in Table 1-3.

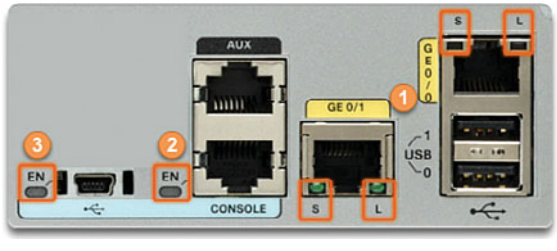


Figure 1-11 Cisco 1941 LEDs

Table 1-3 Description of the Cisco 1941 LEDs

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

Console Access (1.1.2.6)

In a production 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:

- *Console cable*: RJ-45-to-DB-9 console cable
- *Terminal emulation software*: Tera Term, PuTTY, HyperTerminal

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. If the host does not have a serial port, the USB port can be used to establish a console connection. 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 (mini-B USB) is required, as well as an operating system device driver. This device driver is available from http://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.

Table 1-4 summarizes the console connection requirements, while Figure 1-12 displays the various ports and cables required.

Table 1-4 Console Connection Requirements

Port on Computer	Cable Required	Port on ISR	Terminal Emulation
Serial Port	RJ-45 to DB-9 Console Cable	RJ-45 Console Port	Tera Term PuTTY
USB Type-A Port	USB to RS-232 compatible serial port adapter ■ Adapter may require a software driver RJ-45 to DB-9 Console Cable		
	USB Type-A to USB Type-B (Mini-B USB) ■ A device driver is required and available from Cisco.com	USB Type-B (Mini-B USB)	

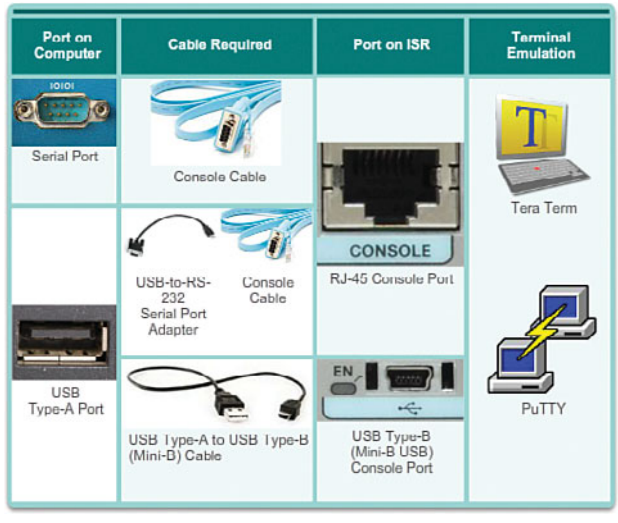


Figure 1-12 Ports and Cables

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).*

How To

The steps to configure the basic settings on a switch are as follows:

Step 1. Name the device.

Step 2. Configure the SVI. This makes the switch accessible for network management.

Step 3. Enable the SVI.

Step 4. Configure the default gateway for the switch. Packets generated by the switch and destined for an address other than its management network segment will be forwarded to this address. This default gateway is used by the switch only for the packets it generates, not any hosts connected to the switch.

For example, the following commands would configure the management VLAN interface and default gateway of switch S1 shown in Figure 1-13.

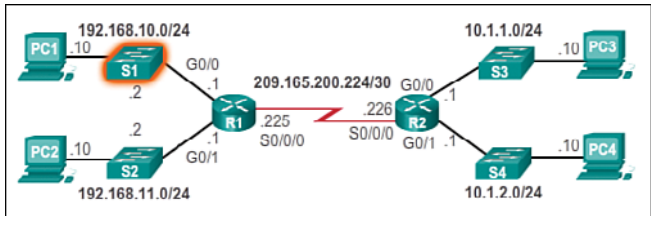


Figure 1-13 Configuring the SVI of S1

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.10.2 255.255.255.0
S1(config-if)# no shutdown
%LINK-5-CHANGED: Interface Vlan1, changed state to up
S1(config-if)# exit
S1(config)#
S1(config)# ip default-gateway 192.168.10.1
S1(config)#
```

In the example, the switch SVI is configured and enabled with the IP address 192.168.10.2/24 and a default gateway of the router located at 192.168.10.1. Packets generated by the switch and destined for an address outside of the 192.168.1.0/24 network segment will be forwarded to this address. In the example, the address is that of the G0/0 interface of R1.

Interactive Graphic

Activity 1.1.2.7: Configure the Management SVI on S2

Go to the online course to use the Syntax Checker in the second graphic to configure the S2 Layer 2 switch.

Interactive Graphic

Activity 1.1.2.8: Document an Addressing Scheme

Go to the online course to perform this practice activity.

Packet Tracer Activity

Packet Tracer Activity 1.1.2.9: Documenting the Network

Your job is to document the addressing scheme and connections used in the Central portion of the network. You will need to use a variety of commands to gather the required information.

Basic Settings on a Router (1.1.3)

The basic addressing and configuration of Cisco devices was covered in either the Introduction to Networks or Network Basics course. However, we will spend some time reviewing these topics as well as preparing you for the hands-on lab experience in this course.

Configure Basic Router Settings (1.1.3.1)

Cisco routers and Cisco switches have many similarities. 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.

When initially configuring a Cisco switch or router, the following steps should be executed:

How To

Step 1. Name the device. This changes the router prompt and helps distinguish the device from others.

Step 2. Secure management access. Specifically, secure the privileged EXEC, user EXEC, and Telnet access, and encrypt passwords to their highest level.

Step 3. Configure a banner. Although optional, this is a recommended step to provide legal notice to anyone attempting to access the device.

Step 4. Save the configuration.

For example, the following commands would configure the basic settings for router R1 shown in Figure 1-14.

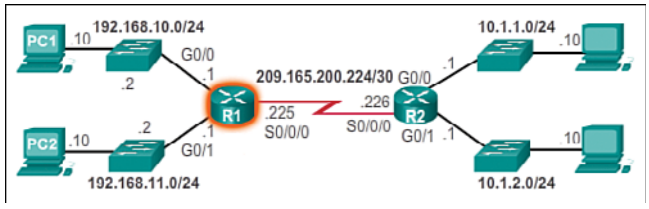


Figure 1-14 Configuring the Basic Settings of R1

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

Interactive Graphic

Activity 1.1.3.1: Configure Basic Settings on R2

Go to the online course to use the Syntax Checker in the fifth graphic to configure basic settings on R2.

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:

- **If using IPv4, configured with an 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 (a hub, a switch, or another router) for the physical layer to be active.

Optionally, the interface could also be configured with a short description. It is good practice to configure a description on each interface. The description text is limited to 240 characters. On production networks, a description can be helpful in troubleshooting by providing information about the type of network to which the interface is connected. If the interface connects to an ISP or service carrier, it is helpful to enter the third-party connection and contact information.

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

Note

Accidentally using the **clock rate** command on a DTE interface generates a "%Error: This command applies only to DCE interface" message.

The steps to configure an IPv4 interface on a router are:

Step 1. Add a description. Although optional, it is a necessary component for documenting a network.

Step 2. Configure the IPv4 address.

Step 3. Configure a clock rate on Serial interfaces. This is only necessary on the DCE device in our lab environment and does not apply to Ethernet interfaces.

Step 4. Enable the interface.

For example, the following commands would configure the three directly connected interfaces of router R1 shown in Figure 1-14 (in the previous section):

```
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
R1(config)#
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
R1(config)#
R1(config)# interface serial 0/0/0
R1(config-if)# description Link to R2
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)# exit
R1(config)#
```

Interactive Graphic

Activity 1.1.3.2: Configure the R2 Interfaces

Go to the online course to use the Syntax Checker in the fourth graphic to configure the R2 interfaces.

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 very similar to their IPv4 counterparts. In many cases, the only difference uses **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, 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.

The steps to configure an IPv6 interface on a router are:

Step 1. Add a description. Although optional, it is a necessary component for documenting a network.

Step 2. Configure the IPv6 global unicast address. Configuring a global unicast address automatically creates a link-local IPv6 address.

Step 3. Configure a link-local unicast address which automatically assigns a link-local IPv6 address and overrides any previously assigned address.

Step 4. Configure a clock rate on Serial interfaces. This is only necessary on the DCE device in our lab environment and does not apply to Ethernet interfaces.

Step 5. Enable the interface.

In the example topology shown in Figure 1-15, R1 must be configured to support the following IPv6 global network addresses:

- 2001:0DB8:ACAD:0001:/64 (2001:DB8:ACAD:1::/64)
- 2001:0DB8:ACAD:0002:/64 (2001:DB8:ACAD:2::/64)
- 2001:0DB8:ACAD:0003:/64 (2001:DB8:ACAD:3::/64)

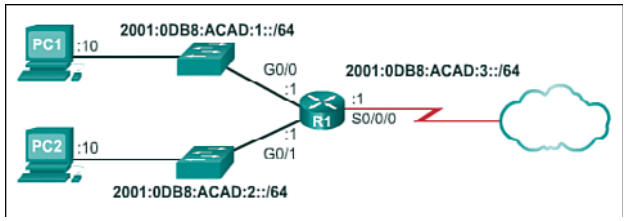


Figure 1-15 IPv6 Topology

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 get its IPv6 address statically assigned, as shown in Figure 1-16. Notice that the default gateway address configured for PC1 is the IPv6 global unicast address of the R1 Gigabit Ethernet 0/0 interface.

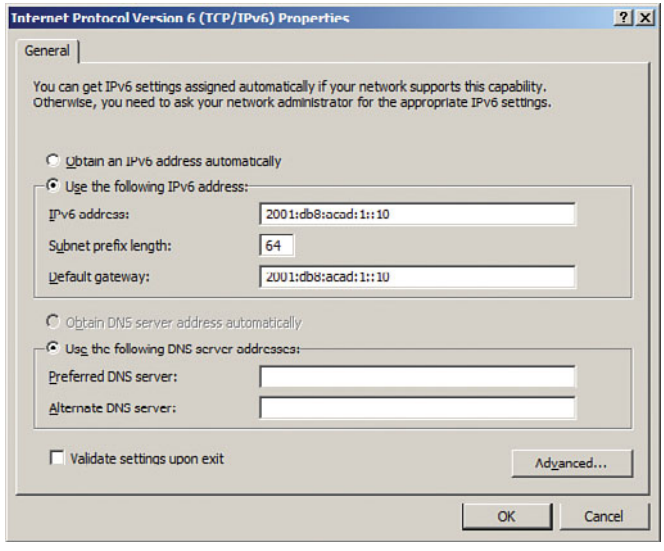


Figure 1-16 Statically Assign an IPv6 Address to PC1

For example, the following commands would configure the IPv6 global unicast addresses of the three directly connected interfaces of the R1 router shown in Figure 1-15:

```
R1# configure terminal
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
R1(config)#
```

```
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
R1(config)#
R1(config)# interface serial 0/0/0
R1(config-if)# description Link to R2
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# clock rate 128000
R1(config-if)# no shutdown
R1(config-if)#
```

Interactive Graphic

Activity 1.1.3.3: Configure the R2 Interfaces

Go to the online course to use the Syntax Checker in the sixth graphic to configure the IPv6 global unicast addresses on the R2 router.

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/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.

How To

The steps to configure a loopback interface on a router are:

Step 1. Create the loopback interface using the **interface loopback** *number* global configuration command.

Step 2. Add a description. Although optional, it is a necessary component for documenting a network.

Step 3. Configure the IP address.

For example, the following commands configure a loopback interface of the R1 router shown in Figure 1-14 (shown earlier in the chapter):

```
R1# configure terminal
R1(config)# interface loopback 0
R1(config-if)# ip address 10.0.0.1 255.255.255.0
R1(config-if)# exit
R1(config)#
```

A loopback interface is always enabled and therefore does not require a **no shutdown** command. 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 Activity

Packet Tracer Activity 1.1.3.5: Configuring IPv4 and IPv6 Interfaces

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)

The first task to undertake once the basic settings and interfaces are configured is to verify and validate the configured settings. This is an important step and should be done before any other configurations are added to the router.

Verify Interface Settings (1.1.4.1)

There are several **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.

Figure 1-17 displays the output of the **show ip interface brief** command.

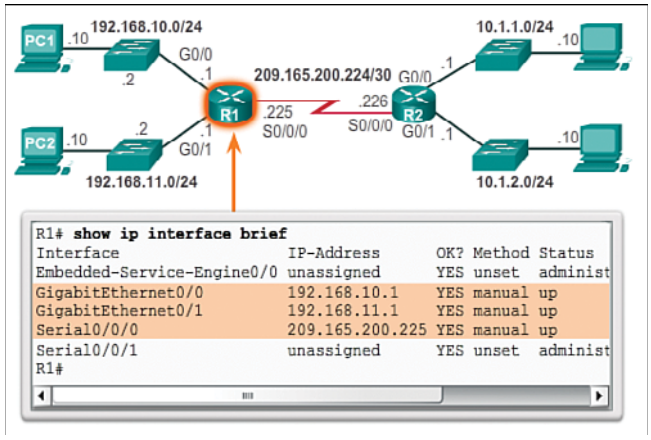


Figure 1-17 Display Interface Summaries

The output reveals that the LAN interfaces and the WAN link are all 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.

Note

The entire output of the **show ip interface brief** command in Figure 1-17 can be viewed in the online course on page 1.1.4.1 graphic number 1.

Note

In Figure 1-17, 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.

Figure 1-18 displays the output of the **show ip route** command.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mo

<output omitted>

Gateway of last resort is not set

      192.168.10.0/24 is variably subnetted, 2 subnets, 2 ma
C        192.168.10.0/24 is directly connected, GigabitEther
L        192.168.10.1/32 is directly connected, GigabitEther
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 ma
C        192.168.11.0/24 is directly connected, GigabitEther
L        192.168.11.1/32 is directly connected, GigabitEther
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 m
```

Figure 1-18 Verify the IPv4 Routing Table

Note

The entire output of the **show ip route** command in Figure 1-18 can be viewed in the online course on page 1.1.4.1 graphic number 2.

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.

Figure 1-19 displays the output of the **show running-config interface** command. The output displays the current commands configured on the specified interface.

```
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#
```

Figure 1-19 Verify an Interface Configuration

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

Interactive Graphic

Activity 1.1.4.1: Verify Router Interfaces

Go to the online course to use the Syntax Checker in the fourth and fifth graphics to verify the interfaces of the R2 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 Figure 1-20 displays a summary for each of the interfaces.

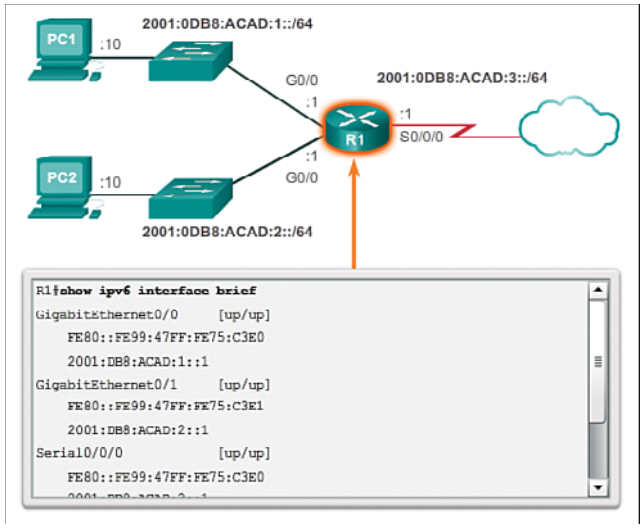


Figure 1-20 Verify the R1 IPv6 Interface Status

Note

The entire output of the **show ipv6 interface brief** command in Figure 1-20 can be viewed in the online course on page 1.1.4.2 graphic number 1.

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.

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 Figure 1-21 displays the interface status and all of 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.

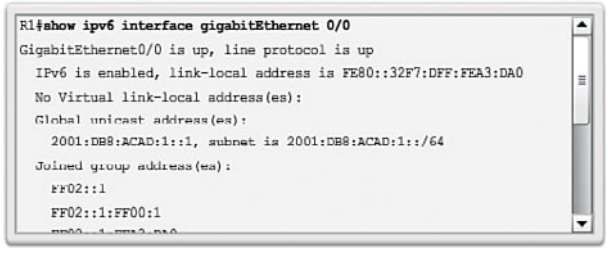


Figure 1-21 Verify the IPv6 Configuration on R1 G0/0

Note

The entire output of the **show ipv6 interface** command in Figure 1-21 can be viewed in the online course on page 1.1.4.2 graphic number 2.

The **show ipv6 route** command shown in Figure 1-22 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.

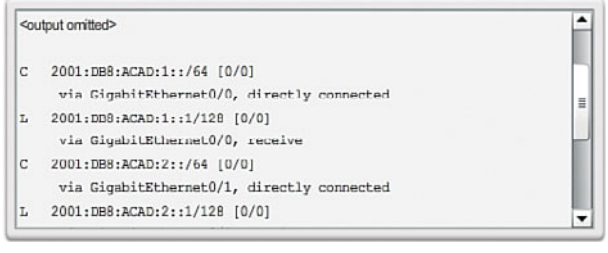


Figure 1-22 Verify the R1 IPv6 Routing Table

Note

The entire output of the **show ipv6 route** command in Figure 1-22 can be viewed in the online course on page 1.1.4.2 graphic number 3.

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, as indicated with an 'L' next to the route entry. 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 Figure 1-23, the **ping** command is used to verify Layer 3 connectivity between R1 and 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#
```

Figure 1-23 Verify Connectivity on R1

Other useful IPv6 verification commands include:

- **show interface**
- **show ipv6 routers**

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** *number* 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 very 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:

- **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.

Figures 1-24 through 1-27 provide examples of the various output filters. The example in Figure 1-24 uses the pipe character and the **section** keyword.

```
R1# show running-config | section line vty
line vty 0 4
 password 7 030752180500
 login
 transport input all
R1#
```

Figure 1-24 Filter **show** Commands by Section

The example in Figure 1-25 uses the pipe character and the **include** keyword.

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status
Embedded-Service-Engine0/0 unassigned      YES unset  administ
GigabitEthernet0/0         192.168.10.1    YES manual up
GigabitEthernet0/1         192.168.11.1    YES manual up
Serial0/0/0                209.165.200.225 YES manual up
Serial0/0/1                unassigned      YES unset  administ
R1#
R1# show ip interface brief | include up
GigabitEthernet0/0         192.168.10.1    YES manual up
GigabitEthernet0/1         192.168.11.1    YES manual up
Serial0/0/0                209.165.200.225 YES manual up
R1#
```

Figure 1-25 Filter **show** Commands by Common Keyword

Note

The entire output of the **show ip interface brief** command in Figure 1-25 can be viewed in the online course on page 1.1.4.3 graphic number 2.

The example in Figure 1-26 uses the pipe character and the **exclude** keyword.

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status
Embedded-Service-Engine0/0 unassigned      YES unset  administ
GigabitEthernet0/0         192.168.10.1    YES manual up
GigabitEthernet0/1         192.168.11.1    YES manual up
Serial0/0/0                209.165.200.225 YES manual up
Serial0/0/1                unassigned      YES unset  administ

R1# show ip interface brief | exclude unassigned
Interface                  IP-Address      OK? Method Status
GigabitEthernet0/0         192.168.10.1    YES manual up
GigabitEthernet0/1         192.168.11.1    YES manual up
Serial0/0/0                209.165.200.225 YES manual up

R1#
```

Figure 1-26 Filter **show** Commands to Exclude Rows of Output

Note

The entire output of the **show ip interface brief** command in Figure 1-26 can be viewed in the online course on page 1.1.4.3 graphic number 3.

The example in Figure 1-27 uses the pipe character and the **begin** keyword.

```
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#
```

Figure 1-27 Filter **show** Commands Beginning from a Keyword

Interactive Graphic

Activity 1.1.4.3: Filter Command Output

Go to the online course to use the Syntax Checker in the fifth graphic to practice how to filter command output on the R1 router.

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.

For example, the following displays a sample of the **terminal history size** and **show history** commands:

```
R1# terminal history size 200
R1#
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#
```

Interactive Graphic

Activity 1.1.4.4: Adjusting the Command History

Go to the online course to use the Syntax Checker in the second graphic to adjust and list the command history output on the R1 router.

Packet Tracer Activity

Packet Tracer Activity 1.1.4.5: Configuring and Verifying a Small Network

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

Lab 1.1.4.7: Configuring Basic Router Settings with CCP

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: Configure Router to Allow CCP Access
- Part 4: (Optional) Install and Set Up CCP on PC-A
- Part 5: Configure R1 Settings Using CCP
- Part 6: Use CCP Utilities

Routing Decisions (1.2)

The key to understanding the role of a router in the network is to understand that a router is a Layer 3 device responsible for forwarding packets. However, a router also operates at Layers 1 and 2.

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 of 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? The router performs the following three major steps:

Step 1. De-encapsulates the Layer 3 packet by removing the Layer 2 frame header and trailer.

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 1-28, 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 frame by each router. It is very likely that the packet is encapsulated in a different type of Layer 2 frame than the one in which it was received. For example, an Ethernet encapsulated frame might be received by the router on a FastEthernet interface, and then processed to be forwarded out of a serial interface as a Point-to-Point Protocol (PPP) encapsulated frame.

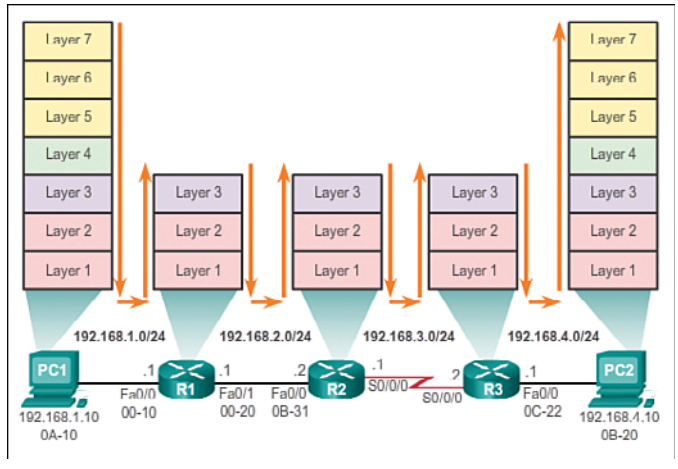


Figure 1-28 Encapsulating and De-Encapsulating Packets

Send a Packet (1.2.1.2)

In the animation in the online course, PC1 is sending a packet to PC2.

Video

Video 1.2.1.2: PC1 Sends a Packet to PC2

Go to the online course and play the animation of a packet being sent from PC1 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 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. 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)

The following processes take place when R1 receives the Ethernet frame from PC1:

1. R1 examines the destination MAC address, which matches the MAC address of the receiving interface, FastEthernet 0/0. R1, therefore, copies the frame into its buffer.
2. R1 identifies the Ethernet Type field as 0x800, which means that the Ethernet frame contains an IPv4 packet in the data portion of the frame.
3. R1 de-encapsulates the Ethernet frame.
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.

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 send back 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.

The animation in the online course illustrates how R1 forwards the packet to R2.

Video

Video 1.2.1.3: R1 Forwards the Packet to R2

Go to the online course and play the animation of a packet being sent through three routers from sender to receiver.

Packet Routing (1.2.1.4)

The following processes 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 0x800, which means that the Ethernet frame contains an IPv4 packet in the data portion of the frame.
3. R2 de-encapsulates the Ethernet frame.
4. 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.
5. 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.
6. 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, etc.). Because there are no MAC addresses on serial interfaces, R2 sets the data link destination address to an equivalent of a broadcast (MAC address: FF:FF:FF:FF:FF:FF).

The animation in the online course illustrates how R2 forwards the packet to R3.

Video

Video 1.2.1.4: R2 Forwards the Packet to R3

Go to the online course and play the animation of a packet being sent from R2 to R3.

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.

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 Address Resolution Protocol (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 0x800, 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.

The animation in the online course illustrates how R3 forwards the packet to PC2.

Video

Video 1.2.1.5: R3 Forwards the Packet to PC2

Go to the online course and play the animation of a packet being sent from R3 to PC2.

Interactive Graphic

Activity 1.2.1.6: Match Layer 2 and Layer 3 Addressing

Go to the online course to perform this practice activity.

Path Determination (1.2.2)

This section discusses the best path to send packets, load balancing, and the concept of administrative distance.

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 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 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. If the packet is discarded, the router sends an ICMP Unreachable message to the source IP address of the packet.

The logic flowchart in Figure 1-29 illustrates the router packet-forwarding decision process.

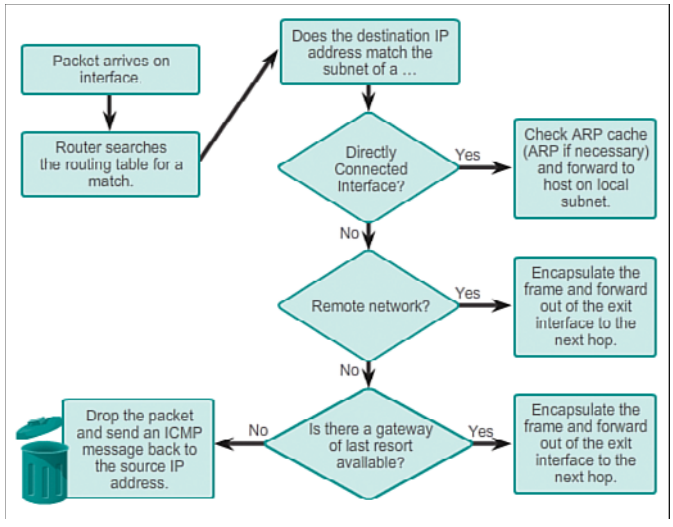


Figure 1-29 Packet Forwarding Decision Process

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 routers use a cost based on cumulative bandwidth from source to destination

- **Enhanced Interior Gateway Routing Protocol (EIGRP):** Bandwidth, delay, load, reliability

The animation in the online course highlights how the path may be different depending on the metric being used.

Video

Video 1.2.2.2: Hop Count vs. Bandwidth as a Metric

Go to the online course and play the animation showing how a network path may be different depending on the metric being used.

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.

By default, Cisco routers can load balance up to four equal cost paths. The maximum number of equal cost paths depends on the routing protocol and IOS version.

EIGRP supports equal cost load balancing and is also the only routing protocol to support *unequal cost load balancing*. Unequal cost load balancing is when a router distributes traffic over network interfaces, even those that are different distances from the destination address.

Note

EIGRP supports unequal cost load balancing by using the `variance` command.

The animation in the online course provides an example of equal cost load balancing.

Video

Video 1.2.2.3: Equal Cost Load Balancing

Go to the online course and play the animation showing 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 that routing protocol's metrics. 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 1-5 lists various routing protocols and their associated ADs.

Table 1-5 Default Administrative Distances

Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200
Unknown	255

Interactive Graphic

Activity 1.2.2.5: Order the Steps in the Packet Forwarding Process

Go to the online course to perform these four practice activities.

Router Operation (1.3)

The primary function of a router is to forward packets toward their destination network, the destination IP address of the packet. To do this, a router needs to search the routing information stored in its routing table. In the following sections, you will learn how a router builds the routing table. Then, you will learn the three basic routing principles.

Analyze the Routing Table (1.3.1)

A good understanding of routing tables is crucial for any network administrator.

The Routing Table (1.3.1.1)

The *routing table* of a router stores information about:

- **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 configured using dynamic routing protocols.

Specifically, a routing table is a data file in RAM that is used to store 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 1-30 identifies the directly connected networks and remote networks of router R1.

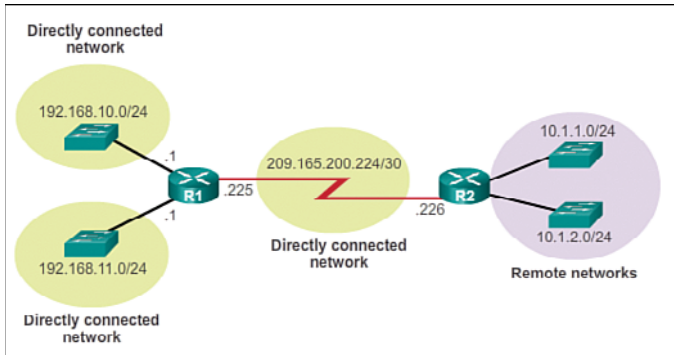


Figure 1-30 Directly Connected and Remote Network Routes

Routing Table Sources (1.3.1.2)

On a Cisco IOS router, the **show ip route** command can be 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:

- **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 or 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:

- **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.