



CCNA

200-301

Portable Command Guide

All the CCNA 200-301 commands in one compact, portable resource

Fifth Edition

ciscopress.com

Scott Empson

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



CCNA 200-301 Portable Command Guide

Fifth Edition

Scott Empson

Cisco Press

CCNA 200-301 Portable Command Guide, Fifth Edition

Scott Empson

Copyright© 2020 Cisco Systems, Inc.

Published by:

Cisco Press

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

ScoutAutomatedPrintCode

Library of Congress Control Number: 2019951511

ISBN-13: 978-0-13-593782-2

ISBN-10: 0-13-593782-5

Warning and Disclaimer

This book is designed to provide information about the Cisco Certified Network Associate (CCNA) exam (200-301). Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

Trademark Acknowledgments

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

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose. All such documents and related graphics are provided “as is” without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

Editor-in-Chief

Mark Taub

Alliances Manager, Cisco Press

Arezou Gol

Product Line Manager

Brett Bartow

Senior Editor

James Manly

Managing Editor

Sandra Schroeder

Development Editor

Ellie Bru

Senior Project Editor

Tonya Simpson

Copy Editor

Bill McManus

Technical Editor

Rick McDonald

Editorial Assistant

Cindy Teeters

Cover Designer

Chuti Prasertsith

Composition

codeMantra

Indexer

Lisa Stumpf

Proofreader

Abigail Bass

Contents at a Glance

Introduction xix

Part I: Network Fundamentals

- CHAPTER 1** IPv4 Addressing—How It Works 1
- CHAPTER 2** How to Subnet IPv4 Addresses 11
- CHAPTER 3** Variable Length Subnet Masking (VLSM) 23
- CHAPTER 4** Route Summarization 33
- CHAPTER 5** IPv6 Addressing—How It Works 39
- CHAPTER 6** Cables and Connections 51
- CHAPTER 7** The Command-Line Interface 59

Part II: LAN Switching Technologies

- CHAPTER 8** Configuring a Switch 67
- CHAPTER 9** VLANs 75
- CHAPTER 10** VLAN Trunking Protocol and Inter-VLAN Communication 83
- CHAPTER 11** Spanning Tree Protocol 97
- CHAPTER 12** EtherChannel 111
- CHAPTER 13** Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) 121

Part III: Routing Technologies

- CHAPTER 14** Configuring a Cisco Router 125
- CHAPTER 15** Static Routing 141
- CHAPTER 16** Open Shortest Path First (OSPF) 149

Part IV: IP Services

- CHAPTER 17** DHCP 159
- CHAPTER 18** Network Address Translation (NAT) 165
- CHAPTER 19** Configuring Network Time Protocol (NTP) 175


Part V: Security Fundamentals**CHAPTER 20** Layer Two Security Features 187**CHAPTER 21** Managing Traffic Using Access Control Lists (ACLs) 197**CHAPTER 22** Device Monitoring and Hardening 213**Part VI: Wireless Technologies****CHAPTER 23** Configuring and Securing a WLAN AP 223**Part VII Appendices****APPENDIX A** How to Count in Decimal, Binary, and Hexadecimal 251**APPENDIX B** How to Convert Between Number Systems 259**APPENDIX C** Binary/Hex/Decimal Conversion Chart 267**APPENDIX D** Create Your Own Journal Here 275**INDEX** 277

Contents

Introduction xix

Part I: Network Fundamentals

CHAPTER 1	IPv4 Addressing—How It Works	1
	What Are IPv4 Addresses Used For?	1
	What Does an IPv4 Address Look Like?	2
	Network and Subnetwork Masks	2
	Ways to Write a Network or Subnet Mask	3
	Network, Node, and Broadcast Addresses	3
	Classes of IPv4 Addresses	4
	Network vs. Node (Host) Bits	5
	RFC (Private) 1918 Addresses	6
	Local vs. Remote Addresses	7
	Classless Addressing	7
	Lessons Learned	9
CHAPTER 2	How to Subnet IPv4 Addresses	11
	Subnetting a Class C Network Using Binary	12
	Subnetting a Class B Network Using Binary	15
	Binary ANDing	17
	So Why AND?	19
	Shortcuts in Binary ANDing	20
CHAPTER 3	Variable Length Subnet Masking (VLSM)	23
	IP Subnet Zero	23
	VLSM Example	24
	Step 1: Determine How Many H Bits Will Be Needed to Satisfy the <i>Largest</i> Network	25
	Step 2: Pick a Subnet for the Largest Network to Use	25
	Step 3: Pick the Next Largest Network to Work With	26
	Step 4: Pick the Third Largest Network to Work With	28
	Step 5: Determine Network Numbers for Serial Links	30
CHAPTER 4	Route Summarization	33
	Example for Understanding Route Summarization	33
	Step 1: Summarize Winnipeg’s Routes	34
	Step 2: Summarize Calgary’s Routes	35

	Step 3: Summarize Edmonton's Routes	35
	Step 4: Summarize Vancouver's Routes	36
	Route Summarization and Route Flapping	38
	Requirements for Route Summarization	38
CHAPTER 5	IPv6 Addressing—How It Works	39
	IPv6: A Very Brief Introduction	39
	What Does an IPv6 Address Look Like?	40
	Reducing the Notation of an IPv6 Address	41
	Rule 1: Omit Leading 0s	41
	Rule 2: Omit All-0s Hextet	42
	Combining Rule 1 and Rule 2	42
	Prefix Length Notation	43
	IPv6 Address Types	44
	Unicast Addresses	45
	Multicast Addresses	48
	Anycast Addresses	50
CHAPTER 6	Cables and Connections	51
	Connecting a Rollover Cable to Your Router or Switch	51
	Using a USB Cable to Connect to Your Router or Switch	51
	Terminal Settings	52
	LAN Connections	53
	Serial Cable Types	53
	Which Cable to Use?	55
	ANSI/TIA Cabling Standards	56
	T568A Versus T568B Cables	57
CHAPTER 7	The Command-Line Interface	59
	Shortcuts for Entering Commands	59
	Using the  Key to Complete Commands	60
	Console Error Messages	60
	Using the Question Mark for Help	60
	enable Command	61
	exit Command	61
	end Command	61
	disable Command	61
	logout Command	62
	Setup Mode	62
	Keyboard Help	62

History Commands	63
terminal Commands	64
show Commands	64
Using the Pipe Parameter () with the show or more Commands	64
Using the no and default Forms of Commands	66

Part II: LAN Switching Technologies

CHAPTER 8 Configuring a Switch 67

Help Commands	68
Command Modes	68
Verifying Commands	68
Resetting Switch Configuration	69
Setting Host Names	69
Setting Passwords	69
Setting IP Addresses and Default Gateways	70
Setting Interface Descriptions	70
The mdix auto Command	70
Setting Duplex Operation	71
Setting Operation Speed	71
Managing the MAC Address Table	72
Configuration Example	72

CHAPTER 9 VLANs 75

Creating Static VLANs	75
Creating Static VLANs Using VLAN Configuration Mode	75
Assigning Ports to VLANs	76
Using the range Command	76
Configuring a Voice VLAN	76
Configuring Voice and Data with Trust	77
Configuring Voice and Data Without Trust	78
Verifying VLAN Information	78
Saving VLAN Configurations	79
Erasing VLAN Configurations	79
Configuration Example: VLANs	80
2960 Switch	80

CHAPTER 10 VLAN Trunking Protocol and Inter-VLAN Communication 83

Dynamic Trunking Protocol (DTP)	83
Setting the VLAN Encapsulation Type	84

VLAN Trunking Protocol (VTP)	84
Verifying VTP	86
Inter-VLAN Communication Using an External Router: Router-on-a-Stick	87
Inter-VLAN Communication on a Multilayer Switch Through a Switch Virtual Interface	88
Removing L2 Switchport Capability of an Interface on an L3 Switch	88
Configuring Inter-VLAN Communication on an L3 Switch	88
Inter-VLAN Communication Tips	88
Configuration Example: Inter-VLAN Communication	89
ISP Router	89
CORP Router	90
L2Switch2 (Catalyst 2960)	92
L3Switch1 (Catalyst 3560/3650/3750)	94
L2Switch1 (Catalyst 2960)	95
CHAPTER 11 Spanning Tree Protocol	97
Spanning Tree Protocol Definition	97
Enabling Spanning Tree Protocol	98
Changing the Spanning-Tree Mode	99
BPDU Guard (3650/9xxx Series)	99
Configuring the Root Switch	100
Configuring a Secondary Root Switch	100
Configuring Port Priority	100
Configuring the Path Cost	101
Configuring the Switch Priority of a VLAN	101
Configuring STP Timers	102
Configuring Optional Spanning-Tree Features	102
PortFast	102
BPDU Guard (2xxx/Older 3xxx Series)	103
Enabling the Extended System ID	103
Verifying STP	104
Troubleshooting Spanning Tree Protocol	104
Configuration Example: PVST+	104
Core Switch (3650)	105
Distribution 1 Switch (3650)	106
Distribution 2 Switch (3650)	106
Access 1 Switch (2960)	107
Access 2 Switch (2960)	107

Spanning-Tree Migration Example: PVST+ to Rapid-PVST+	108
Access 1 Switch (2960)	108
Access 2 Switch (2960)	108
Distribution 1 Switch (3650)	109
Distribution 2 Switch (3650)	109
Core Switch (3650)	109

CHAPTER 12 EtherChannel 111

EtherChannel	111
Interface Modes in EtherChannel	111
Default EtherChannel Configuration	112
Guidelines for Configuring EtherChannel	112
Configuring Layer 2 EtherChannel	113
Configuring Layer 3 EtherChannel	114
Configuring EtherChannel Load Balancing	114
Configuring LACP Hot-Standby Ports	115
Monitoring and Verifying EtherChannel	116
Configuration Example: EtherChannel	117
DLSwitch (3560 or 9300)	117
ALSwitch1 (2960 or 9200)	118
ALSwitch2 (2960 or 9200)	119

CHAPTER 13 Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) 121

Cisco Discovery Protocol	121
Configuring CDP	121
Verifying and Troubleshooting CDP	122
CDP Design Tips	122
Link Layer Discovery Protocol (802.1AB)	123
Configuring LLDP (802.1AB)	123
Verifying and Troubleshooting LLDP	124

Part III: Routing Technologies

CHAPTER 14 Configuring a Cisco Router 125

Router Modes	126
Entering Global Configuration Mode	126
Configuring a Router Name	126
Configuring Passwords	126
Password Encryption	127

Interface Names	127
Moving Between Interfaces	131
Configuring a Serial Interface	132
Assigning an IPv4 Address to a Fast Ethernet Interface	132
Assigning an IPv4 Address to a Gigabit Ethernet Interface	132
Assigning IPv6 Addresses to Interfaces	133
Creating a Message-of-the-Day Banner	133
Creating a Login Banner	134
Mapping a Local Host Name to a Remote IP Address	134
The no ip domain-lookup Command	134
Working with DNS on a Router	134
The logging synchronous Command	135
The exec-timeout Command	136
Saving Configurations	136
Erasing Configurations	136
The write Command	137
Verifying Your Configurations Using show Commands	137
EXEC Commands in Configuration Mode: The do Command	138
Configuration Example: Basic Router Configuration	138
Boston Router	138
CHAPTER 15 Static Routing	141
Configuring an IPv4 Static Route	141
Static Routes and Recursive Lookups	142
The permanent Keyword	142
Floating Static Routes in IPv4 and Administrative Distance	143
Configuring an IPv4 Default Route	144
Verifying IPv4 Static Routes	144
Configuration Example: IPv4 Static Routes	144
Ketchikan Router	145
Juneau Router	145
Sitka Router	146
Configuring an IPv6 Static Route	146
Floating Static Routes in IPv6	147
Configuring an IPv6 Default Route	147
Verifying IPv6 Static Routes	147
CHAPTER 16 Open Shortest Path First (OSPF)	149
OSPFv2 Versus OSPFv3	149
Configuring OSPF	150

- Using Wildcard Masks with OSPF Areas 150
- Loopback Interfaces 152
- Router ID 152
- DR/BDR Elections 153
- Timers 153
- Verifying OSPFv2 Configurations 153
- Troubleshooting OSPFv2 154
- Configuration Example: Single-Area OSPF 154
 - Austin Router 155
 - Houston Router 156
 - Galveston Router 157

Part IV: IP Services

CHAPTER 17 DHCP 159

- Configuring a DHCP Server on an IOS Router 159
- Using Cisco IP Phones with a DHCP Server 160
- Verifying and Troubleshooting DHCP Configuration 160
- Configuring a DHCP Helper Address 161
- Configuring a DHCP Client on a Cisco IOS Software Ethernet Interface 162
- Configuration Example: DHCP 162
 - Edmonton Router 162
 - Gibbons Router 164

CHAPTER 18 Network Address Translation (NAT) 165

- Private IP Addresses: RFC 1918 165
- Configuring Dynamic NAT: One Private to One Public Address Translation 165
- Configuring PAT: Many Private to One Public Address Translation 167
- Configuring Static NAT: One Private to One Permanent Public Address Translation 169
- Verifying NAT and PAT Configurations 170
- Troubleshooting NAT and PAT Configurations 171
- Configuration Example: PAT 171
 - ISP Router 171
 - Company Router 172

CHAPTER 19 Configuring Network Time Protocol (NTP) 175

- NTP Configuration 175
- NTP Design 176

Securing NTP	177
Enabling NTP Authentication	177
Limiting NTP Access with Access Lists	178
Verifying and Troubleshooting NTP	178
Setting the Clock on a Router	179
Using Time Stamps	182
Configuration Example: NTP	182
Core1 Router	183
Core2 Router	184
DLSwitch1	185
DLSwitch2	185
ALSwitch1	186
ALSwitch2	186

Part V: Security Fundamentals

CHAPTER 20 Layer Two Security Features 187

Setting Passwords on a Switch	187
Configuring Static MAC Addresses	188
Configuring Switch Port Security	188
Configuring Sticky MAC Addresses	189
Verifying Switch Port Security	189
Recovering Automatically from Error-Disabled Ports	190
Verifying Autorecovery of Error-Disabled Ports	190
Configuring DHCP Snooping	191
Verifying DHCP Snooping	192
Configuring Dynamic ARP Inspection (DAI)	193
Verifying Dynamic ARP Inspection	193
Configuration Example: Switch Security	194

CHAPTER 21 Managing Traffic Using Access Control Lists (ACLs) 197

Access List Numbers	197
Using Wildcard Masks	198
ACL Keywords	198
Creating Standard ACLs	198
Applying Standard ACLs to an Interface	199
Verifying ACLs	200
Removing ACLs	200
Creating Extended ACLs	200
Applying Extended ACLs to an Interface	201

- The established Keyword 201
- The log Keyword 202
- Creating Named ACLs 203
- Using Sequence Numbers in Named ACLs 203
- Removing Specific Lines in Named ACLs Using Sequence Numbers 204
- Sequence Number Tips 204
- Including Comments About Entries in ACLs 205
- Restricting Virtual Terminal Access 206
- Tips for Configuring ACLs 206
- IPv6 ACLs 207
- Verifying IPv6 ACLs 207
- Configuration Examples: IPv4 ACLs 208
- Configuration Examples: IPv6 ACLs 210

CHAPTER 22 Device Monitoring and Hardening 213

- Device Monitoring 213
- Configuration Backups 213
- Implementing Logging 214
 - Configuring Syslog 215
 - Syslog Message Format 215
 - Syslog Severity Levels 216
 - Syslog Message Example 216
- Device Hardening 217
 - Configuring Passwords 217
 - Password Encryption 218
 - Password Encryption Algorithm Types 218
 - Configuring SSH 219
 - Verifying SSH 220
 - Restricting Virtual Terminal Access 220
 - Disabling Unneeded Services 221

Part VI: Wireless Technologies

CHAPTER 23 Configuring and Securing a WLAN AP 223

- Initial Setup of a Wireless LAN Controller (WLC) 223
- Monitoring the WLC 229
- Configuring a VLAN (Dynamic) Interface 230
- Configuring a DHCP Scope 234
- Configuring a WLAN 237

Defining a RADIUS Server	239
Exploring Management Options	242
Configuring a WLAN Using WPA2 PSK	246

Part VII: Appendices

APPENDIX A	How to Count in Decimal, Binary, and Hexadecimal	251
	How to Count in Decimal	251
	How to Count in Binary	253
	How to Count in Hexadecimal	254
	Representing Decimal, Binary, and Hexadecimal Numbers	256
APPENDIX B	How to Convert Between Number Systems	259
	How to Convert from Decimal to Binary	259
	How to Convert from Binary to Decimal	260
	How to Convert from Decimal IP Addresses to Binary and from Binary IP Addresses to Decimal	261
	A Bit of Perspective	262
	How to Convert from Hexadecimal to Binary	262
	How to Convert from Binary to Hexadecimal	263
	How to Convert from Decimal to Hexadecimal	264
	How to Convert from Hexadecimal to Decimal	265
APPENDIX C	Binary/Hex/Decimal Conversion Chart	267
APPENDIX D	Create Your Own Journal Here	275
INDEX		277

About the Author

Scott Empson is an instructor in the Department of Information Systems Technology at the Northern Alberta Institute of Technology in Edmonton, Alberta, Canada, where he has taught for more than 20 years. He teaches technical courses in Cisco routing and switching, along with courses in professional development and leadership. He has a Master of Education degree along with three undergraduate degrees: a Bachelor of Arts, with a major in English; a Bachelor of Education, again with a major in English/language arts; and a Bachelor of Applied Information Systems Technology, with a major in network management. Scott lives in Edmonton, Alberta, with his wife, Trina, and two university-attending-but-still-haven't-moved-out-yet-but-hope-to-move-out-as-soon-as-possible-after-graduation-so-Dad-can-have-the-TV-room-back children, Zachariah and Shaelyn.

About the Technical Reviewer

Rick McDonald teaches computer and networking courses at the University of Alaska Southeast in Ketchikan, Alaska. He holds a B.A. degree in English and an M.A. degree in Educational Technology from Gonzaga University in Spokane, WA. After several years in the airline industry, Rick returned to full-time teaching. Rick started in the Cisco Academy in North Carolina and taught CCNA and CCNP courses to students and was a CCNA Instructor Trainer. Previous Academy projects include authoring CCNP study guides and technical editing a previous edition of the CCNA 2 and 3 textbook. His current project is developing methods for delivering hands-on training via distance in Alaska using web conferencing and NETLAB tools.

Dedications

As always, this book is dedicated to Trina, Zach, and Shae. Now that you are older and are in university, do you even know what I do when I write these books, or are you just happy that I can afford to take you to Disney again? Or pay for your tuition. Pick one... xxxooo :)

Acknowledgments

Just as it takes many villagers to raise a child, it takes many people to create a book. Without the following, I wouldn't be able to call myself an author; my title would probably be village idiot. Therefore, I must thank:

The team at Cisco Press. Once again, you amaze me with your professionalism and the ability to make me look good. James, Ellie, Bill, Tonya, and Vaishnavi: Thank you for your continued support and belief in my little engineering journal.

To my technical reviewer, Rick: We finally get to work together! Rick was one of the first people I met when getting involved with Cisco and the Cisco Academy all those years ago (2001?). I first met you in Las Vegas at a Networkers conference. You were brilliant then, and you are brilliant now. Thanks for correcting my mistakes and making me look smarter than I really am.

A special thanks to Mary Beth Ray: You were my first editor with Cisco Press and you were with me for every step over the last 15 years. Thank you for taking a risk on me and my idea. I hope that your post-publishing career is just as exciting and rewarding as your time was with us. I bow to the divine in you. Namaste.

If you like this book, it is all because of them. Any errors in this book are all on me.

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

Welcome to *CCNA 200-301 Portable Command Guide*! As most of you know, Cisco has announced a complete revamp and update to its certifications. What you have here is the latest Portable Command Guide as part of these new outcomes and exams. For someone who originally thought that this book would be less than 100 pages in length and limited to the Cisco Networking Academy program for its complete audience, I am continually amazed that my little engineering journal has caught on with such a wide range of people throughout the IT community.

I have long been a fan of what I call the “engineering journal,” a small notebook that can be carried around and that contains little nuggets of information—commands that you forget, the IP addressing scheme of some remote part of the network, little reminders about how to do something you only have to do once or twice a year (but is vital to the integrity and maintenance of your network). This journal has been a constant companion by my side for the past 20 years; I only teach some of these concepts every second or third year, so I constantly need to refresh commands and concepts and learn new commands and ideas as Cisco releases them. My journals are the best way for me to review because they are written in my own words (words that I can understand). At least, I had better understand them because if I can’t, I have only myself to blame.

My first published engineering journal was the *CCNA Quick Command Guide*; it was organized to match the (then) order of the Cisco Networking Academy program. That book then morphed into the *Portable Command Guide*, the fifth edition of which you are reading right now. This book is my “industry” edition of the engineering journal. It contains a different logical flow to the topics, one more suited to someone working in the field. Like topics are grouped together: routing protocols, switches, troubleshooting. More complex examples are given. IPv6 has now been integrated directly into the content chapters themselves. IPv6 is not something new that can be introduced in a separate chapter; it is part of network designs all around the globe, and we need to be as comfortable with it as we are with IPv4. The popular “Create Your Own Journal” appendix is still here (blank pages for you to add in your own commands that you need in your specific job). We all recognize the fact that no network administrator’s job can be so easily pigeonholed as to just working with CCNA topics; you all have your own specific jobs and duties assigned to you. That is why you will find those blank pages at the end of the book. Make this book your own; personalize it with what you need to make it more effective. This way your journal will not look like mine.

Private Addressing Used in This Book

This book uses RFC 1918 addressing throughout. Because I do not have permission to use public addresses in my examples, I have done everything with private addressing. Private addressing is perfect for use in a lab environment or in a testing situation because it works exactly like public addressing, with the exception that it cannot be routed across a public network.

Who Should Read This Book

This book is for those people preparing for the CCNA certification exam, whether through self-study, on-the-job training and practice, or study within the Cisco Networking Academy program. There are also some handy hints and tips along the way to make life a bit easier for you in this endeavor. This book is small enough that you will find it easy to carry around with you. Big, heavy textbooks might look impressive on your bookshelf in your office, but can you really carry them around with you when you are working in some server room or equipment closet somewhere?

Optional Sections

A few sections in this book have been marked as optional. These sections cover topics that are not on the CCNA certification exam, but they are valuable topics that should be known by someone at a CCNA level. Some of the optional topics might also be concepts that are covered in the Cisco Networking Academy program courses.

Organization of This Book

This book follows a logical approach to configuring a small to mid-size network. It is an approach that I give to my students when they invariably ask for some sort of outline to plan and then configure a network. Specifically, this approach is as follows:

Part I: Network Fundamentals

- **Chapter 1, “IPv4 Addressing—How It Works”:** An overview of the rules of IPv4 addressing—how it works, what it is used for, and how to correctly write out an IPv4 address
- **Chapter 2, “How to Subnet IPv4 Addresses”:** An overview of how to subnet, examples of subnetting (both a Class B and a Class C address), and using the binary AND operation
- **Chapter 3, “Variable Length Subnet Masking (VLSM)”:** An overview of VLSM, and an example of using VLSM to make your IP plan more efficient
- **Chapter 4, “Route Summarization”:** Using route summarization to make your routing updates more efficient, an example of how to summarize a network, and necessary requirements for summarizing your network
- **Chapter 5, “IPv6 Addressing—How It Works”:** An overview of the rules for working with IPv6 addressing, including how it works, what it is used for, how to correctly write out an IPv6 address, and the different types of IPv6 addresses
- **Chapter 6, “Cables and Connections”:** An overview of how to connect to Cisco devices, which cables to use for which interfaces, and the differences between the TIA/EIA 568A and 568B wiring standards for UTP
- **Chapter 7, “The Command-Line Interface”:** How to navigate through Cisco IOS Software: editing commands, using keyboard shortcuts for commands, and using help commands

Part II: LAN Switching Technologies

- **Chapter 8, “Configuring a Switch”:** Commands to configure Catalyst switches: names, passwords, IP addresses, default gateways, port speed and duplex, and static MAC addresses
- **Chapter 9, “VLANs”:** Configuring static VLANs, troubleshooting VLANs, saving and deleting VLAN information, and configuring voice VLANs with and without trust
- **Chapter 10, “VLAN Trunking Protocol and Inter-VLAN Communication”:** Configuring a VLAN trunk link, configuring VTP, verifying VTP, and configuring inter-VLAN communication using router-on-a-stick, subinterfaces, and SVIs
- **Chapter 11, “Spanning Tree Protocol”:** Verifying STP, setting switch priorities, working with optional features, and enabling Rapid Spanning Tree
- **Chapter 12, “EtherChannel”:** Creating and verifying Layer 2 and Layer 3 EtherChannel groups between switches
- **Chapter 13, “Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP)”:** Customizing and verifying both CDP and LLDP

Part III: Routing Technologies

- **Chapter 14, “Configuring a Cisco Router”:** Commands needed to configure a single router: names, passwords, configuring interfaces, MOTD and login banners, IP host tables, saving and erasing your configurations
- **Chapter 15, “Static Routing”:** Configuring IPv4 and IPv6 static routes in your internetwork
- **Chapter 16, “Open Shortest Path First (OSPF)”:** Configuring and verifying OSPFv2 in single-area designs

Part IV: IP Services

- **Chapter 17, “DHCP”:** Configuring and verifying DHCP on a Cisco IOS router, and using Cisco IP Phones with a DHCP server
- **Chapter 18, “Network Address Translation (NAT)”:** Configuring and verifying NAT and PAT
- **Chapter 19, “Configuring Network Time Protocol (NTP)”:** Configuring and verifying NTP, setting the local clock, and using time stamps

Part V: Security Fundamentals

- **Chapter 20, “Layer Two Security Features”:** Setting passwords, configuring switch port security, using static and sticky MAC addresses, configuring and verifying DHCP snooping, and configuring and verifying Dynamic ARP Inspection (DAI)

- **Chapter 21, “Managing Traffic Using Access Control Lists (ACLs)”:** Configuring standard ACLs, using wildcard masks, creating extended ACLs, creating named ACLs, using sequence numbers in named ACLs, verifying and removing ACLs, and configuring and verifying IPv6 ACLs
- **Chapter 22, “Device Monitoring and Hardening”:** Device monitoring, backups, logging and the use of syslog, syslog message formats, configuring and encrypting passwords, configuring and verifying SSH, restricting virtual terminal access, and disabling unused services

Part VI: Wireless Technologies

- **Chapter 23, “Configuring and Securing a WLAN AP”:** The initial setup for a Wireless LAN Controller, monitoring a WLC, configuring VLANs, DHCP, WLAN, RADIUS servers, other management options, and security on a WLC

Part VII: Appendices

- **Appendix A, “How to Count in Decimal, Binary, and Hexadecimal”:** A refresher on how to count in decimal, and using those rules to count in binary and hexadecimal
- **Appendix B, “How to Convert Between Number Systems”:** Rules to follow when converting between the three numbering systems used most often in IT: decimal, binary, and hexadecimal
- **Appendix C, “Binary/Hex/Decimal Conversion Chart”:** A chart showing numbers 0 through 255 in the three numbering systems of binary, hexadecimal, and decimal
- **Appendix D, “Create Your Own Journal Here”:** Some blank pages for you to add in your own specific commands that might not be in this book

Did I Miss Anything?

I am always interested to hear how my students, and now readers of my books, do on both certification exams and future studies. If you would like to contact me and let me know how this book helped you in your certification goals, please do so. Did I miss anything? Let me know. Contact me at PCG@empson.ca or through the Cisco Press website, <http://www.ciscopress.com>.

Figure Credits

Figure 6-3, screenshot of PC Settings © Microsoft, 2019.

Figure 23-7, 23 Logging into the WLC Screenshot of Logging into © Microsoft, 2019.

Figure 23-15, screenshot of Interface Address © Microsoft, 2019.

Figure 23-16, screenshot of Interface Address © Microsoft, 2019.

Figure 23-17, screenshot of Success ping message © Microsoft, 2019.

Figure 23-24, screenshot of Saving configuration © Microsoft, 2019.

This page intentionally left blank

Route Summarization

This chapter provides information concerning the following topics:

- Example for understanding route summarization
- Route summarization and route flapping
- Requirements for route summarization

Route summarization, or supernetting, is needed to reduce the number of routes that a router advertises to its neighbor. Remember that for every route you advertise, the size of your update grows. It has been said that if there were no route summarization, the Internet backbone would have collapsed from the sheer size of its own routing tables back in 1997!

Routing updates, whether done with a distance-vector protocol or a link-state protocol, grow with the number of routes you need to advertise. In simple terms, a router that needs to advertise ten routes needs ten specific lines in its update packet. The more routes you have to advertise, the bigger the packet. The bigger the packet, the more bandwidth the update takes, reducing the bandwidth available to transfer data. But with route summarization, you can advertise many routes with only one line in an update packet. This reduces the size of the update, allowing you more bandwidth for data transfer.

Also, when a new data flow enters a router, the router must do a lookup in its routing table to determine which interface the traffic must be sent out. The larger the routing tables, the longer this takes, leading to more used router CPU cycles to perform the lookup. Therefore, a second reason for route summarization is that you want to minimize the amount of time and router CPU cycles that are used to route traffic.

NOTE: This example is a very simplified explanation of how routers send updates to each other. For a more in-depth description, I highly recommend you go out and read Jeff Doyle and Jennifer Carroll's book *Routing TCP/IP, Volume I*, Second Edition (Cisco Press, 2005). This book has been around for many years and is considered by most to be the authority on how the different routing protocols work. If you are considering continuing on in your certification path to try and achieve the CCIE, you need to buy Doyle's book—and memorize it; it's that good.

Example for Understanding Route Summarization

Refer to Figure 4-1 to assist you as you go through the following explanation of an example of route summarization.

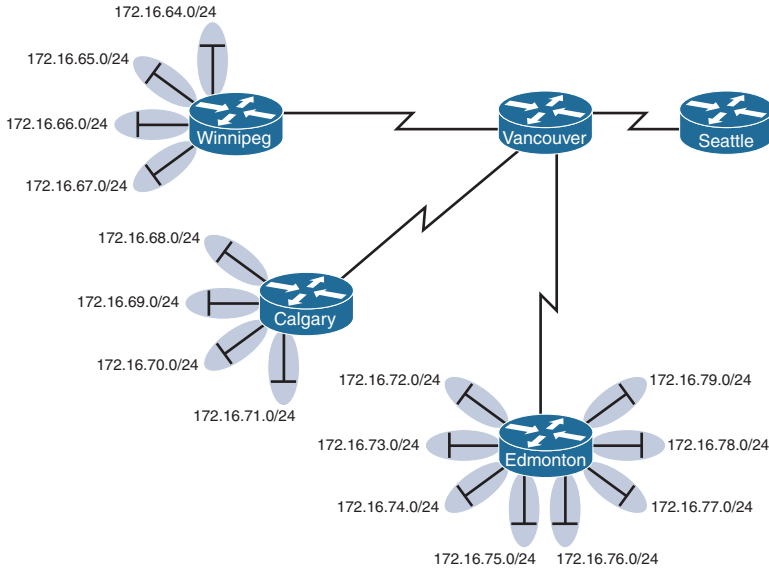


Figure 4-1 Four-City Network Without Route Summarization

As you can see from Figure 4-1, Winnipeg, Calgary, and Edmonton each have to advertise internal networks to the main router located in Vancouver. Without route summarization, Vancouver would have to advertise 16 networks to Seattle. You want to use route summarization to reduce the burden on this upstream router.

Step 1: Summarize Winnipeg’s Routes

To do this, you need to look at the routes in binary to see if there are any specific bit patterns that you can use to your advantage. What you are looking for are common bits on the network side of the addresses. Because all of these networks are /24 networks, you want to see which of the first 24 bits are common to all four networks.

- 172.16.64.0 = **10101100.00010000.01000000.00000000**
- 172.16.65.0 = **10101100.00010000.01000001.00000000**
- 172.16.66.0 = **10101100.00010000.01000010.00000000**
- 172.16.67.0 = **10101100.00010000.01000011.00000000**
- Common bits: **10101100.00010000.010000xx**

You see that the first 22 bits of the four networks are common. Therefore, you can summarize the four routes by using a subnet mask that reflects that the first 22 bits are common. This is a /22 mask, or 255.255.252.0. You are left with the summarized address of

172.16.64.0/22

This address, when sent to the upstream Vancouver router, will tell Vancouver: “If you have any packets that are addressed to networks that have the first 22 bits in the pattern of 10101100.00010000.010000xx.xxxxxxxx, then send them to me here in Winnipeg.”

By sending one route to Vancouver with this supernetted subnet mask, you have advertised four routes in one line instead of using four lines. Much more efficient!

Step 2: Summarize Calgary's Routes

For Calgary, you do the same thing that you did for Winnipeg—look for common bit patterns in the routes:

172.16.68.0 = **10101100.00010000.010001**00.00000000

172.16.69.0 = **10101100.00010000.010001**01.00000000

172.16.70.0 = **10101100.00010000.010001**10.00000000

172.16.71.0 = **10101100.00010000.010001**11.00000000

Common bits: **10101100.00010000.010001**xx

Once again, the first 22 bits are common. The summarized route is therefore

172.16.68.0/22

Step 3: Summarize Edmonton's Routes

For Edmonton, you do the same thing that you did for Winnipeg and Calgary—look for common bit patterns in the routes:

172.16.72.0 = **10101100.00010000.01001**000.00000000

172.16.73.0 = **10101100.00010000.01001**001.00000000

172.16.74.0 = **10101100.00010000.01001**010.00000000

172.16.75.0 = **10101100.00010000.01001**011.00000000

172.16.76.0 = **10101100.00010000.01001**100.00000000

172.16.77.0 = **10101100.00010000.01001**101.00000000

172.16.78.0 = **10101100.00010000.01001**110.00000000

172.16.79.0 = **10101100.00010000.01001**111.00000000

Common bits: **10101100.00010000.01001**xxx

For Edmonton, the first 21 bits are common. The summarized route is therefore

172.16.72.0/21

Figure 4-2 shows what the network looks like, with Winnipeg, Calgary, and Edmonton sending their summarized routes to Vancouver.

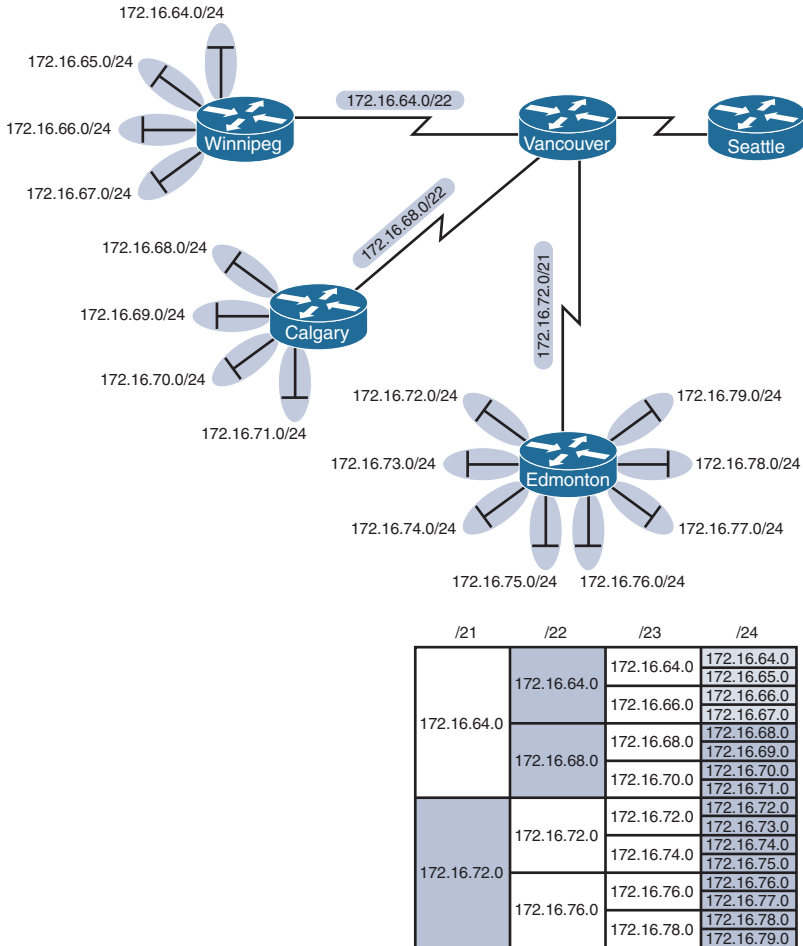


Figure 4-2 Four-City Network with Edge Cities Summarizing Routes

Step 4: Summarize Vancouver's Routes

Yes, you can summarize Vancouver's routes to Seattle. You continue in the same format as before. Take the routes that Winnipeg, Calgary, and Edmonton sent to Vancouver, and look for common bit patterns:

172.16.64.0 = 10101100.00010000.01000000.00000000

172.16.68.0 = 10101100.00010000.01000100.00000000

172.16.72.0 = 10101100.00010000.01001000.00000000

Common bits: 10101100.00010000.0100xxxx

Because there are 20 bits that are common, you can create one summary route for Vancouver to send to Seattle:

172.16.64.0/20

Vancouver has now told Seattle that in one line of a routing update, 16 different networks are being advertised. This is much more efficient than sending 16 lines in a routing update to be processed.

Figure 4-3 shows what the routing updates would look like with route summarization taking place.

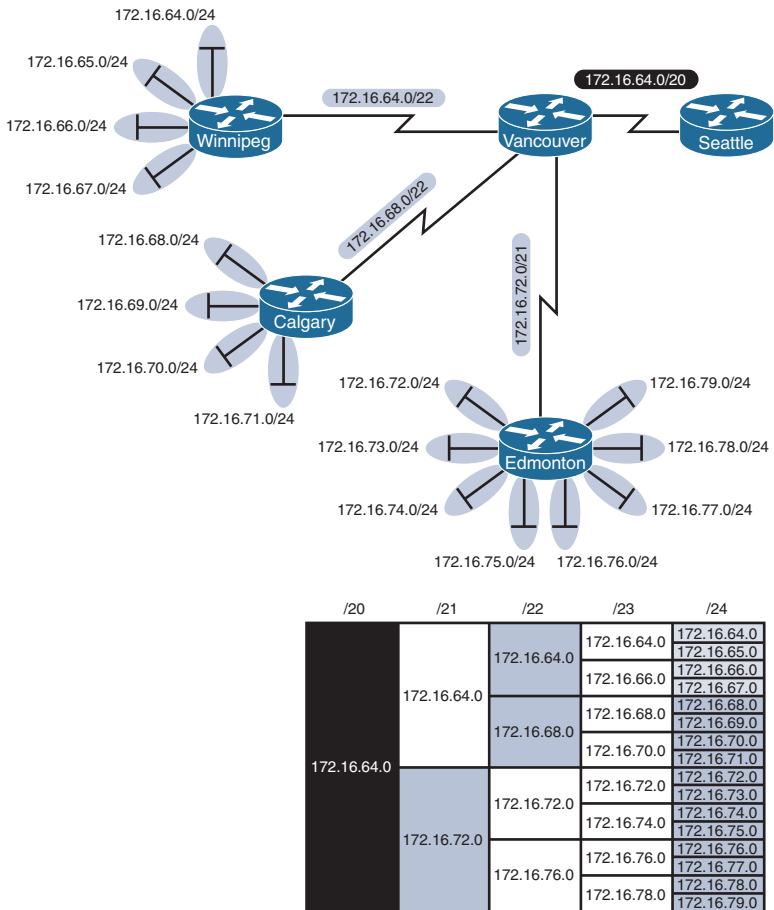


Figure 4-3 Four-City Network with Complete Route Summarization

Route Summarization and Route Flapping

Another positive aspect of route summarization has to do with route flapping. *Route flapping* is when a network, for whatever reason (such as interface hardware failure or misconfiguration), goes up and down on a router, causing that router to constantly advertise changes about that network. Route summarization can help insulate upstream neighbors from these problems.

Consider router Edmonton from Figure 4-1. Suppose that network 172.16.74.0/24 goes down. Without route summarization, Edmonton would advertise Vancouver to remove that network. Vancouver would forward that same message upstream to Calgary, Winnipeg, Seattle, and so on. Now assume the network comes back online a few seconds later. Edmonton would have to send another update informing Vancouver of the change. Each time a change needs to be advertised, the router must use CPU resources. If that route were to flap, the routers would constantly have to update their own tables, as well as advertise changes to their neighbors. In a CPU-intensive protocol such as OSPF, the constant hit on the CPU might make a noticeable change to the speed at which network traffic reaches its destination.

Route summarization enables you to avoid this problem. Even though Edmonton would still have to deal with the route constantly going up and down, no one else would notice. Edmonton advertises a single summarized route, 172.16.72.0/21, to Vancouver. Even though one of the networks is going up and down, this does not invalidate the route to the other networks that were summarized. Edmonton will deal with its own route flap, but Vancouver will be unaware of the problem downstream in Edmonton. Summarization can effectively protect or insulate other routers from route flaps.

Requirements for Route Summarization

To create route summarization, there are some necessary requirements:

- Routers need to be running a classless routing protocol, as they carry subnet mask information with them in routing updates. (Examples are RIP v2, OSPF, EIGRP, IS-IS, and BGP.)
- Addresses need to be assigned in a hierarchical fashion for the summarized address to have the same high-order bits. It does no good if Winnipeg has network 172.16.64.0 and 172.16.67.0 while 172.16.65.0 resides in Calgary and 172.16.66.0 is assigned in Edmonton. No summarization could take place from the edge routers to Vancouver.

TIP: Because most networks use NAT and the RFC 10.0.0.0/8 network internally, it is important when creating your network design that you assign network subnets in a way that they can be easily summarized. A little more planning now can save you a lot of grief later.

IPv6 Addressing—How It Works

This chapter provides information concerning the following topics:

- IPv6: A very brief introduction
- What does an IPv6 address look like?
- Reducing the notation of an IPv6 address
 - Rule 1: Omit leading 0s
 - Rule 2: Omit all-0s hexet
 - Combining rule 1 and rule 2
- Prefix length notation
- IPv6 address types
 - Unicast addresses
 - Global unicast
 - Link-local
 - Loopback
 - Unspecified
 - Unique local
 - IPv4 embedded
 - Multicast addresses
 - Well-known
 - Solicited-node
 - Anycast addresses

NOTE: This chapter is meant to be a very high-level overview of IPv6 addressing. For an excellent overview of IPv6, I strongly recommend you read Rick Graziani's book from Cisco Press: *IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6*, Second Edition. It is a brilliant read, and Rick is an amazing author. I am also very fortunate to call him a friend.

IPv6: A Very Brief Introduction

When IPv4 became a standard in 1980, its 32-bit address field created a theoretical maximum of approximately 4.29 billion addresses (2^{32}). IPv4 was originally conceived as an experiment, and not for a practical implementation, so 4.29 billion was considered to be an inexhaustible amount. But with the growth of the Internet, and the need for individuals and companies to require multiple addresses—your home PC, your cell

phone, your tablet, your PC at work/school, your Internet-aware appliances—you can see that something larger than 32-bit address fields would be required. In 1993, the Internet Engineering Task Force (IETF) formed a working group called the IP Next Generation working group. In 1994 the IETF recommended an address size of 128 bits. While many people think that IPv6 is just a way to create more addresses, there are actually many enhancements that make IPv6 a superior choice to IPv4. Again, I recommend Rick Graziani's *IPv6 Fundamentals* as a must-have on your bookshelf for working with IPv6.

What Does an IPv6 Address Look Like?

The way that a computer or other digital device sees an IPv6 address and the way humans see an IPv6 address are different. A digital device looks at an IPv6 address as a 128-bit number. But humans have devised a way to convert this 128-bit number into something easier to look at and work with. For humans, an IPv6 address is a 128-bit number that is written as a string of hexadecimal digits. Hexadecimal is a natural fit for IPv6 addresses because any 4 bits can be represented as a single hexadecimal digit. Two hexadecimal digits represent a single byte, or octet (8 bits). The preferred form of an IPv6 address is $x:x:x:x:x:x:x$, where each x is a 16-bit section that can be represented using up to four hexadecimal digits. Each section is separated by a colon (:), as opposed to IPv4 addressing, which uses a period (.) to separate each section. The result is eight 16-bit sections (sometimes called *hexets*) for a total of 128 bits in the address.

Figure 5-1 shows this format.

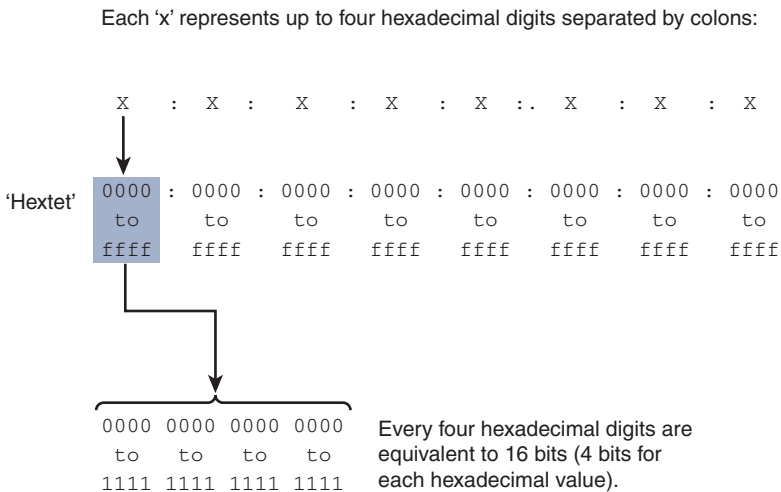


Figure 5-1 Format of an IPv6 Address

Showing all the hexadecimal digits in an IPv6 address is the longest representation of the preferred form. The next section shows you two rules for reducing the notation of an IPv6 address in the preferred format for easier use and readability.

TIP: If you need more practice working with hexadecimal and converting between hexadecimal, decimal, and binary, refer to both Appendix A, “How to Count in Decimal, Binary, and Hexadecimal,” and Appendix B, “How to Convert Between Number Systems.”

Reducing the Notation of an IPv6 Address

Looking at the longest representation of an IPv6 address can be overwhelming:

```
0000:0000:0000:0000:0000:0000:0000:0000
0000:0000:0000:0000:0000:0000:0000:0001
ff02:0000:0000:0000:0000:0000:0000:0001
fe80:0000:0000:0000:a299:9bff:fe18:50d1
2001:0db8:cafe:0001:0000:0000:0000:0200
```

There are two rules for reducing the notation.

Rule 1: Omit Leading 0s

Omit any leading 0s in any hextet (a 16-bit section). This rule applies only to leading 0s and not trailing 0s. Table 5-1 shows examples of omitting leading 0s in a hextet:

TABLE 5-1 Examples of Omitting Leading 0s in a Hextet (Leading 0s in bold; spaces retained)

Format	IPv6 Address
Preferred	0000:0000:0000:0000:0000:0000:0000:0000
Leading 0s omitted	0: 0: 0: 0: 0: 0: 0: 0 or 0:0:0:0:0:0:0:0
Preferred	0000:0000:0000:0000:0000:0000:0000:0001
Leading 0s omitted	0: 0: 0: 0: 0: 0: 0: 1 or 0:0:0:0:0:0:0:1
Preferred	ff02: 0000:0000:0000:0000:0000:0000:0000:0001
Leading 0s omitted	ff02: 0: 0: 0: 0: 0: 0: 1 or ff02:0:0:0:0:0:0:1
Preferred	2001: 0db8:1111:000a:00b0:0000:9000:0200
Leading 0s omitted	2001: db8: 1111: a: b0: 0:9000: 200 or 2001:db8:1111:a:b0:0:9000:200

Rule 2: Omit All-0s Hextet

Use a double colon (::) to represent any single, contiguous string of two or more hextets consisting of all 0s. Table 5-2 shows examples of using the double colon.

TABLE 5-2 Examples of Omitting a Single Contiguous String of All-0s Hextets (0s in Bold Replaced By a Double Colon)

Format	IPv6 Address
Preferred	0000:0000:0000:0000:0000:0000:0000
:: All-0s segments	::
Preferred	0000:0000:0000:0000:0000:0000:0000:0001
:: All-0s segments	::0001
Preferred	ff02: 0000:0000:0000:0000:0000:0000:0001
:: All-0s segments	ff02::0001
Preferred	2001:0db8:aaaa:0001: 0000:0000:0000:0100
:: All-0s segments	2001:0db8:aaaa:0001::0100
Preferred	2001:0db8: 0000:0000 :abcd:0000:0000:1234
:: All-0s segments	2001:0db8::abcd:0000:0000:1234

Only a single contiguous string of all 0s can be represented by a double colon; otherwise the address would be ambiguous. Consider the following example:

```
2001::abcd:1234
```

There are many different possible choices for the preferred address:

```
2001:0000:0000:0000:0000:abcd:0000:1234
```

```
2001:0000:0000:0000:abcd:0000:0000:1234
```

```
2001:0000:0000:abcd:0000:0000:0000:1234
```

```
2001:0000:abcd:0000:0000:0000:0000:1234
```

If two double colons are used, you cannot tell which of these addresses is correct.

If you have an address with more than one contiguous string of 0s, where should you place the double colon? RFC 5952 states that the double colon should represent

- The longest string of all-0s hextets.
- If the strings are of equal value, the first string should use the double colon notation.

Combining Rule 1 and Rule 2

You can combine the two rules to reduce an address even further. Table 5-3 shows examples of this.

TABLE 5-3 Examples of Applying Both Rule 1 and Rule 2 (Leading 0s in bold)

Format	IPv6 Address
Preferred	0000:0000:0000:0000:0000:0000:0000:0000
Leading 0s omitted	0: 0: 0: 0: 0: 0: 0: 0
(::) All-0s segments	::
Compressed	::
Preferred	0000:0000:0000:0000:0000:0000:0000:0001
Leading 0s omitted	0: 0: 0: 0: 0: 0: 0: 1
(::) All-0s segments	::1
Compressed	::1
Preferred	ff02: 0000:0000:0000:0000:0000:0000:0000:0001
Leading 0s omitted	ff02: 0: 0: 0: 0: 0: 0: 1
(::) All-0s segments	ff02::1
Compressed	ff02::1
Preferred	fe80: 0000:0000:0000:a299:9bff:fe18:50d1
Leading 0s omitted	fe80: 0: 0: 0:a299:9bff:fe18:50d1
(::) All-0s segments	fe80::a299:9bff:fe18:50d1
Compressed	fe80::a299:9bff:fe18:50d1
Preferred	2001:0db8:aaaa:0001: 0000:0000:0000:0200
Leading 0s omitted	2001: db8:aaaa: 1: 0: 0: 0: 200
(::) All-0s segments	2001: db8:aaaa: 1:: 200
Compressed	2001:db8:aaaa:1::200

Prefix Length Notation

In IPv4, the prefix of the address (the network portion) can be represented either by a dotted-decimal netmask (the subnet mask) or through CIDR notation. When we see 192.168.100.0 255.255.255.0 or 192.168.100.0/24, we know that the network portion of the address is the first 24 bits of the address (192.168.100) and that the last 8 bits (.0) are host bits. IPv6 address prefixes are represented in much the same way as IPv4 address prefixes are written in CIDR notation. IPv6 prefixes are represented using the following format:

IPv6-Address/Prefix-Length

The *prefix-length* is a decimal value showing the number of leftmost contiguous bits of the address. It identifies the prefix (the network portion) of the address. In unicast addresses, it is used to separate the prefix portion from the Interface ID. The Interface ID is equivalent to the host portion of an IPv4 address.

Looking at the address

2001:db8:aaaa:1111::100/64

we know that the leftmost 64 bits are the prefix (network portion) and the remaining bits are the Interface ID (host portion). See Figure 5-2.

Each hexadecimal digit is 4 bits; a hextet is a 16-bit segment.

2001:db8:aaaa:1111::100/64

2001 : 0db8 : aaaa : 1111 : 0000 : 0000 : 0000 : 0100

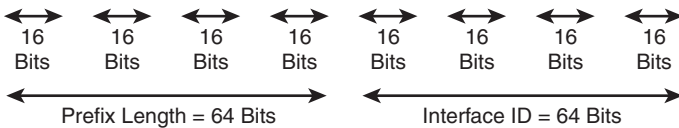


Figure 5-2 IPv6 Prefix and Prefix Length

A /64 prefix length results in an Interface ID of 64 bits. This is a common prefix length for most end-user networks. A /64 prefix length gives us 2^{64} or 18 quintillion devices on a single network (or subnet).

There are several more common prefix length examples, as shown in Figure 5-3. All of these examples fall either on a hextet boundary or on a nibble boundary (a multiple of 4 bits). Although prefix lengths do not need to fall on a nibble boundary, most usually do.

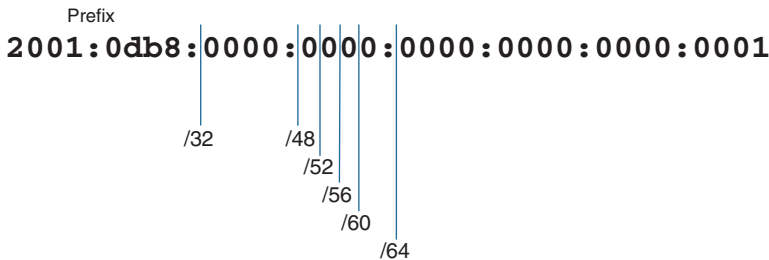


Figure 5-3 IPv6 Prefix Length Examples

IPv6 Address Types

In IPv6, there are three types of addresses: unicast, multicast, and anycast. This section gives a (very) high-level overview of these types.

NOTE: IPv6 does not have a broadcast address. There are other options that exist in IPv6 that deal with this issue, but this is beyond the scope of this book.

Figure 5-4 diagrams the three types of addresses.

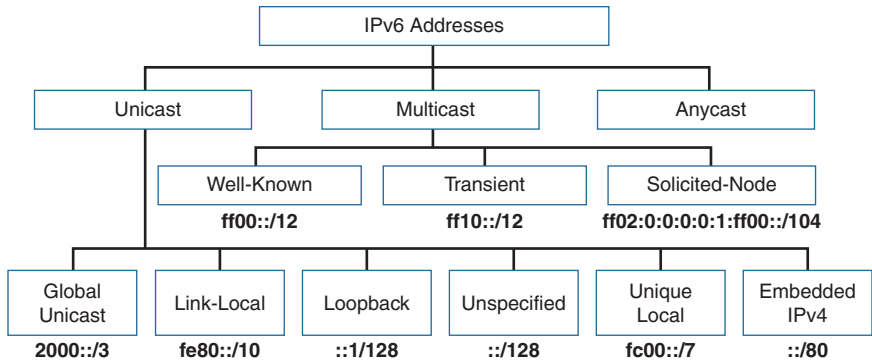


Figure 5-4 IPv6 Address Types

Unicast Addresses

A unicast address uniquely identifies an interface on an IPv6 device. A packet sent to a unicast address is received by the interface that is assigned to that address. Similar to IPv4, a source IPv6 address must be a unicast address.

As shown in Figure 5-4, there are six different types of unicast addresses:

1. **Global unicast:** A routable address in the IPv6 Internet, similar to a public IPv4 address.
2. **Link-local:** Used only to communicate with devices on the same local link.
3. **Loopback:** An address not assigned to any physical interface that can be used for a host to send an IPv6 packet to itself.
4. **Unspecified address:** Used only as a source address and indicates the absence of an IPv6 address.
5. **Unique local:** Similar to a private address in IPv4 (RFC 1918) and not intended to be routable in the IPv6 Internet. However, unlike RFC 1918 addresses, these addresses are not intended to be statefully translated to a global unicast address. Please see Rick Graziani's book *IPv6 Fundamentals* for a more detailed description of stateful translation.
6. **IPv4 embedded:** An IPv6 address that carries an IPv4 address in the low-order 32 bits of an IPv6 address.

Global Unicast Addresses

Global unicast addresses (GUAs) are globally routable and reachable in the IPv6 Internet. The generic structure of a GUA has three fields:

- **Global Routing Prefix:** The prefix or network portion of the address assigned by the provider, such as an ISP, to the customer site.

- Subnet ID:** A separate field for allocating subnets within the customer site. Unlike IPv4, it is not necessary to borrow bits from the Interface ID (host portion) to create subnets. The number of bits in the Subnet ID falls between where the Global Routing Prefix ends and the Interface ID begins.
- Interface ID:** Identifies the interface on the subnet, equivalent to the host portion of an IPv4 address. In most cases, the Interface ID is 64 bits in length.

Figure 5-5 shows the structure of a global unicast address.

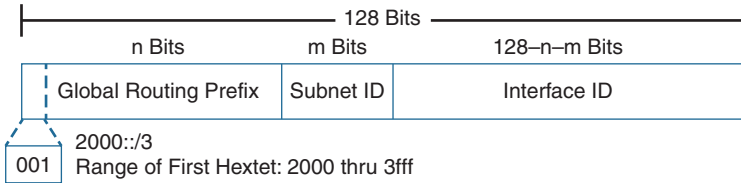


Figure 5-5 Structure of a Global Unicast Address

Link-Local Unicast Addresses

A link-local unicast address is a unicast address that is confined to a single link (a single subnet). Link-local addresses only need to be unique on the link (subnet) and do not need to be unique beyond the link. Therefore, routers do not forward packets with a link-local address.

Figure 5-6 shows the format of a link-local unicast address, which is in the range fe80::/10. Using this prefix and prefix length range results in the range of the first hexet being from fe80 to febf.

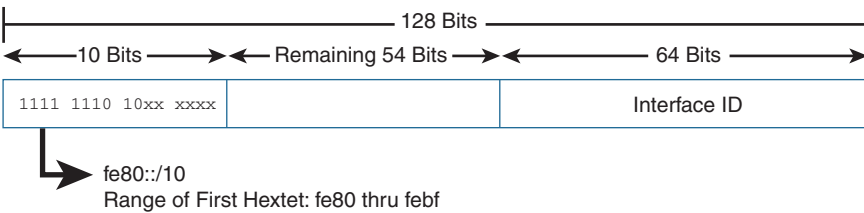


Figure 5-6 Structure of a Link-Local Unicast Address

NOTE: Using a prefix other than fe80 is permitted by RFC 4291, but the addresses should be tested prior to usage.

NOTE: To be an IPv6-enabled device, a device must have an IPv6 link-local address. You do not need to have an IPv6 global unicast address, but you must have a link-local address.

NOTE: Devices dynamically (automatically) create their own link-local IPv6 addresses upon startup. Link-local addresses can be manually configured.

NOTE: Link-local addresses only need to be unique on the link. It is very likely, and even desirable, to have the same link-local address on different interfaces that are on different links. For example, on a device named Router2, you may want all link-local interfaces to be manually configured to FE80::2, whereas all link-local interfaces on Router3 to be manually configured to FE80::3, and so on.

NOTE: There can be only one link-local address per interface. There can be multiple global unicast addresses per interface.

Loopback Addresses

An IPv6 loopback address is ::1, an all-0s address except for the last bit, which is set to 1. It is equivalent to the IPv4 address block 127.0.0.0/8, most commonly the 127.0.0.1 loopback address. The loopback address can be used by a node to send an IPv6 packet to itself, typically when testing the TCP/IP stack.

Table 5-4 shows the different formats for representing an IPv6 loopback address.

TABLE 5-4 IPv6 Loopback Address Representation

Representation	IPv6 Loopback Address
Preferred	0000:0000:0000:0000:0000:0000:0000:0001
Leading 0s omitted	0:0:0:0:0:0:0:1
Compressed	::1

NOTE: A loopback address cannot be assigned to a physical interface.

Unspecified Addresses

An unspecified unicast address is an all-0s address (see Table 5-5), used as a source address to indicate the absence of an address.

Table 5-5 shows the different formats for representing an IPv6 unspecified address.

TABLE 5-5 IPv6 Unspecified Address Representation

Representation	IPv6 Unspecified Address
Preferred	0000:0000:0000:0000:0000:0000:0000:0000
Leading 0s omitted	0:0:0:0:0:0:0:0
Compressed	::

NOTE: An unspecified address cannot be assigned to a physical interface.

Unique Local Addresses

Figure 5-7 shows the structure of the unique local address (ULA), which is the counterpart of IPv4 private addresses. ULAs are used similarly to global unicast addresses, but are for private use and cannot be routed in the global Internet. ULAs are defined in RFC 4193.

Figure 5-7 shows the different formats for representing an IPv6 unspecified address.

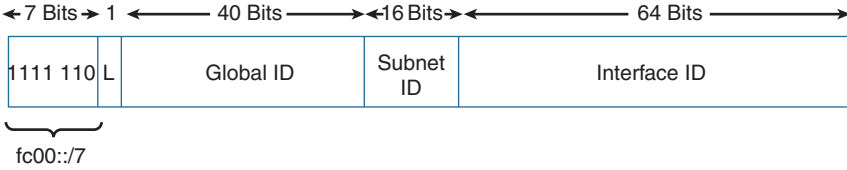


Figure 5-7 Structure of a Unique Local Unicast Address

IPv4 Embedded Addresses

Figure 5-8 shows the structure of IPv4 embedded addresses. They are used to aid in the transition from IPv4 to IPv6. IPv4 embedded addresses carry an IPv4 address in the low-order 32 bits of an IPv6 address.

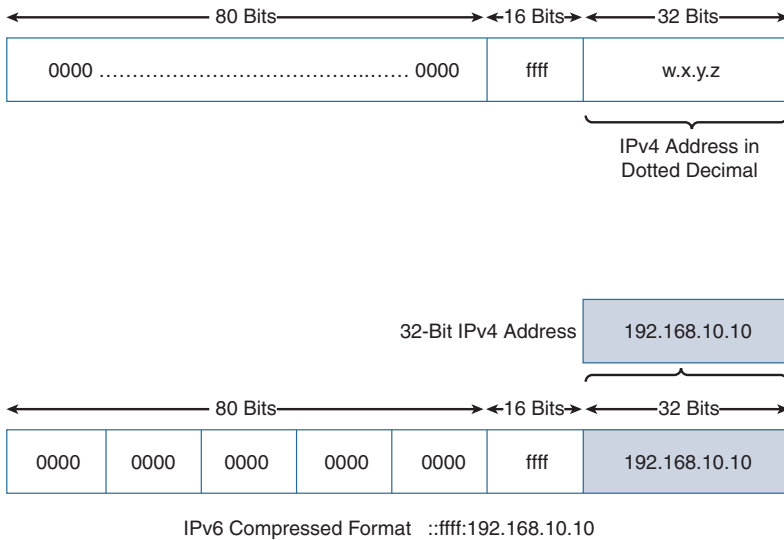


Figure 5-8 IPv4-Mapped IPv6 Address

NOTE: This is a transition technique for moving from IPv4 to IPv6 addressing. This should not be used as a permanent solution. The end goal should always be native end-to-end IPv6 connectivity.

Multicast Addresses

Multicast is a technique in which a device sends a single packet to multiple destinations simultaneously (one-to-many transmission). Multiple destinations can actually be multiple interfaces on the same device, but they are typically different devices.

An IPv6 multicast address defines a group of devices known as a multicast group. IPv6 addresses use the prefix `ff00::/8`, which is equivalent to the IPv4 multicast address `224.0.0.0/4`. A packet sent to a multicast group always has a unicast source address; a multicast address can never be the source address.

Unlike IPv4, there is no broadcast address in IPv6. Instead, IPv6 uses multicast.

Table 5-6 shows IPv6 multicast address representation.

TABLE 5-6 IPv6 Multicast Address Representation

Representation	IPv6 Multicast Address
Preferred	ff00:0000:0000:0000:0000:0000:0000/8
Leading 0s omitted	ff00:0:0:0:0:0:0/8
Compressed	ff00::/8

The structure of an IPv6 multicast is shown in Figure 5-9; the first 8 bits are 1-bits (ff) followed by 4 bits for flags and a 4-bit Scope field. The next 112 bits represent the Group ID.

8 Bits	4 Bits	4 Bits	112 Bits
1111 1111	Flags	Scope	Group ID

Figure 5-9 IPv6 Multicast Address

Although there are many different types of multicast addresses, this book defines only two of them:

- Well-known multicast addresses
- Solicited-node multicast addresses

Well-Known Multicast Addresses

Well-known multicast addresses have the prefix ff00::/12. Well-known multicast addresses are predefined or reserved multicast addresses for assigned groups of devices. These addresses are equivalent to IPv4 well-known multicast addresses in the range 224.0.0.0 to 239.255.255.255. Some examples of IPv6 well-known multicast addresses include the following:

Address	Use
ff02::1	All IPv6 devices
ff02::2	All IPv6 routers
ff02::5	All OSPFv3 routers
ff02::6	All OSPFv3 DR routers
ff02::9	All RIPng routers
ff02:a	All EIGRPv6 routers
ff02::1:2	All DHCPv6 servers and relay agents

Solicited-Node Multicast Addresses

Solicited-node multicast addresses are used as a more efficient approach to IPv4's broadcast address. A more detailed description is beyond the scope of this book.

Anycast Addresses

An IPv6 anycast address is an address that can be assigned to more than one interface (typically on different devices). In other words, multiple devices can have the same anycast address. A packet sent to an anycast address is routed to the "nearest" interface having that address, according to the router's routing table.

Figure 5-10 shows an example of anycast addressing.

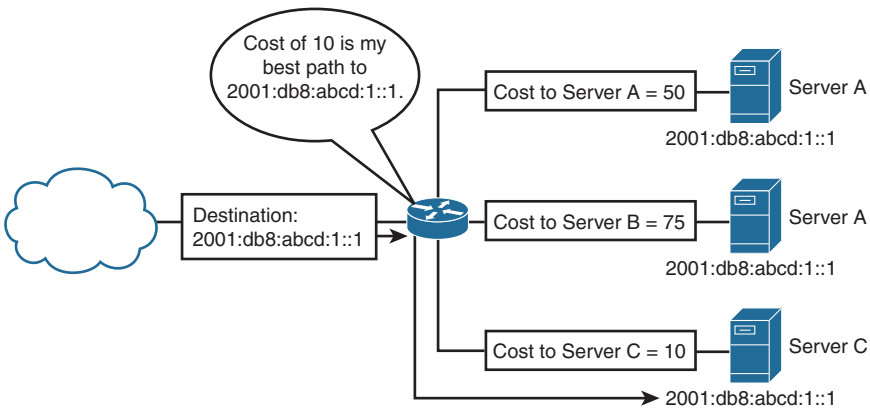


Figure 5-10 Example of Anycast Addressing

NOTE: IPv6 anycast addressing is still somewhat in the experimental stages and beyond the scope of this book.

Symbols

- :: (double colon), 42
- | (pipe parameter), 64–65
- ? (question mark), using for help, 60–61
- [tab] key, completing commands, 60

Numbers

- 0 (zero), wildcard masks, 150, 198
- 1 (one), wildcard masks, 150, 198
- 2³² bit addressing, 7
- 2xxx/3xxx series (BPDU Guard),
Spanning Tree Protocol, 103
- 9xxx Series (BPDU Guard), Spanning
Tree Protocol, 103
- 802.1AB (Link Layer Discovery Protocol),
123
- 2960 series switches, 70
 - secure configuration, 194
- 2960 switch, VLAN configurations, 80–81
- 2960/9200 series switches, 70
 - network topology, 72
- 9200 series switches, 70

A

- AAA (authentication, authorization, and
accounting) server, storing passwords,
217
- access 1 switch (2960)
 - PVST+ (Per VLAN Spanning Tree),
configuration examples, 107
 - PVST+ to Rapid-PVST+, migration
example, 108
- access 2 switch (2960)
 - PVST+ (Per VLAN Spanning
Tree), configuration examples,
107–108
 - PVST+ to Rapid-PVST+, migration
example, 108
- access control entry (ACE), 199
- access control lists. *See* ACLs (access
control lists)
- access lists, limiting NTP access, 178
- access number lists, 197
- access-class command, 220
- access-class keyword, 207
- access-group command, 220
- access-group keyword, 207
- ACE (access control entry), 199
- ACLs (access control lists), 197
 - extended ACLs
 - applying to interfaces, 201
 - creating, 200–201
 - established keyword,
201–202
 - log keyword, 202
 - including comments about entries,
205
- IPv4 ACLs, configuration examples,
208–210
- IPv6 ACLs, 207
 - configuration examples,
210–211
 - verifying, 207
- keywords, 198
- named ACLs
 - creating, 203

- removing specific lines with
 - sequence numbers, 204
 - sequence numbers, 203–204
- removing, 200
- restricting virtual terminal access, 205–206
- standard ACLs
 - applying to interfaces, 199–200
 - creating, 198–199
 - tips for configuring, 206–207
 - verifying, 200
 - wildcard masks, 198
- acronyms for time zones, 180–181
- AD (administrative distance), 143
 - floating static routes in IPv4, 143–144
- address types, IPv6 addresses
 - anycast addresses, 50
 - multicast addresses, 48–49
 - unicast addresses, 45–48
- addresses
 - broadcast addresses, 3
 - host addresses, 3
 - IPv4 addresses. *See* IPv4 addresses
 - IPv6 addresses. *See* IPv6 addresses
 - local addresses versus remote addresses, IPv4 addresses, 7
 - loopback addresses, 45, 47
 - MAC addresses, 2
 - multicast addresses. *See* multicast addresses
 - network addresses, 3
 - remote addresses versus local addresses, IPv4 addresses, 7
 - remote ip addresses, mapping local host names to, 134
 - RFC (private) 1918 addresses, 165
 - static MAC addresses, configuring, 188
 - sticky MAC addresses, configuring, 189
 - unicast addresses. *See* unicast addresses
 - unique local addresses, 45
 - unspecified addresses, 45
 - well-known multicast addresses, IPv6 addresses, 49
- administrative distance (AD), 143
 - floating static routes in IPv4, 143–144
- Advanced Monitor Summary screen, WLC (Wireless LAN Controller), 230
- algorithm types, password encryption, 218–219
- ALSwitch1 (2960 or 9200), EtherChannel (configuration examples), 118–119
- ALSwitch2 (2960 or 9200), EtherChannel (configuration examples), 119–120
- ANDing, 17–19
 - reasons for, 19–20
 - shortcuts, 20–21
- ANSI/TIA cabling standards, 56
- any keyword, 198
- anycast addresses, IPv6 addresses, 50
- appearance of
 - IPv4 addresses, 2
 - IPv6 addresses, 40
- archive config command, 214
- ARP (Address Resolution Protocol), disabling, 221
- assigning
 - IPv4 addresses to fast Ethernet interfaces, 132
 - IPv4 addresses to gigabit Ethernet interfaces, 132
 - IPv6 addresses to interfaces, 133
 - ports to VLANs, 76
- authentication, NTP (Network Time Protocol), 177
- authentication, authorization, and accounting (AAA) server, storing passwords, 217
- Authentication Key Management, 248–249
- Auto-MDIX feature, 71
- autosensing cable types, switches, 56

B

- backup designated router (BDR), OSPF (Open Shortest Path First), 153
- backups, configuration backups, 213–214
- banners
 - login banners, 134
 - message-of-the-day banner, 133
- BDR (backup designated router), OSPF (Open Shortest Path First), 153
- binary, subnetting
 - Class B networks, 15–17
 - Class C networks, 12–15
- Binary ANDing, 17–19
 - shortcuts, 20–21
- binary math, 11
- BOOTP server, disabling, 221
- BPDU Guard (2xxx/3xxx Series), Spanning Tree Protocol, 103
- BPDU Guard (9xxx Series), Spanning Tree Protocol, 103
- broadcast addresses, 3

C

- cables
 - ANSI/TIA cabling standards, 56
 - deciding which to use, 55–56
 - rollover cables, connecting to routers or switches, 51
 - serial cable types, 53–55
 - T568A versus T568 B, 57
 - USB cables, connecting to routers or switches, 51–52
- CAM (Content Addressable Memory) table, 188
- Catalyst 9xxx series, 67
- Catalyst 2960 (L2Switch1), inter-VLAN communication (configuration examples), 92–96
- Catalyst 3560 (L3Switch1), inter-VLAN communication (configuration examples), 94–95
- Catalyst 3650 (L3Switch1), inter-VLAN communication (configuration examples), 94–95
- Catalyst 3750 (L3Switch1), inter-VLAN communication (configuration examples), 94–95
- CDP (Cisco Discovery Protocol), 76, 121
 - configuring, 121
 - design tips, 122
 - disabling, 221
 - verifying, 122
- changing spanning-tree mode, 99
- channel-group command, 114
- Cisco Discovery Protocol (CDP), 76, 121
 - configuring, 121
 - design tips, 122
 - disabling, 221
 - verifying, 122
- Cisco IP Phones
 - configuring voice and data with trust, 77
 - DHCP servers, 160
- Class A, IPv4 addresses, 4, 7
- Class B
 - IPv4 addresses, 5
 - subnetting using binary, 15–17
- Class C
 - IPv4 addresses, 5
 - subnetting using binary, 12–15
- Class D, IPv4 addresses, 5
- Class E, IPv4 addresses, 5, 7
- classes of IPv4 addresses, 4–5
 - sizing, 5–6
- classless addressing, IPv4 addresses, 7–9
- clear errdisable interface interface-id vlan, 190
- clear ip ospf process, 152
- clock rate command, 132
- clocks, setting on routers, NTP (Network Time Protocol), 179–182
- command modes
 - configuring switches, 68
 - for setting passwords, 69–70

command-line interface

- console error messages, 60
- disable command, 61
- enable command, 61
- end command, 61
- exit command, 61
- history commands, 63
- keyboard help, 62–63
- logout command, 62
- pipe parameter (|), 64–65
- question mark (?) for help, 60–61
- setup mode, 62
- shortcuts for entering commands, 59
- show commands, 64
- [tab] key, 60
- terminal commands, 64

commands, 190

- access-class, 206, 220
- access-group, 206, 220
- archive config, 214
- begin, 65
- channel-group, 114
- clear ip ospf process, 152
- clear mac address-table, 190
- clock rate, 132
- command modes, 68
- completing with [tab] key, 60
- configure terminal, 138
- copy running-config startup-config, 79, 214
- default ?, 66
- default command-name, 66
- disable, 61
- do, 138
- enable, 61
- enable password, 127, 217
- enable secret password, 127, 217
- end, 61
- erase startup-config, 69
- exec-timeout, 136
- exit, 61, 79
- forward-time, 102
- hello-time, 102
- help, 68
- history, 63
- history size, 64

- hostname, 219
- interface range, 76
- ip access-list resequence, 205
- ip forward-helper udp x, 161
- ip helper-address, 161
- ip name-server, 135
- ip route, 142
- ipv6 enable, 133
- log-adjacency-changes, 150
- logging synchronous, 135–136
- logout, 62
- MAC address table, 72
- max-age, 102
- mdix auto, 70–71
- more, 64
- network area, 150
- no cdp enable, 122
- no cdp run, 122
- no ip domain-lookup, 134–135
- no ip forward-protocol udp x, 161
- no switchport, 88
- ntp master, 176
- ntp peer, 176
- port channel, 114
- range, 76
- remark, 205
- router ospf x, 152
- service password-encryption, 217–218
- service sequence-numbers global configuration, 215
- service timestamps log datetime global configuration, 215
- setting duplex operation, 71
- for setting interface descriptions, 70
- setting operation speed, 71–72
- shortcuts for entering, 59
- show commands, 64
- show con?, 60
- show interfaces, 68
- show interfaces vlanx, 68
- show ntp associations, 176
- show running-config, 71, 126, 138, 152
- show version, 64

- show vlan privileged EXEC, 75
- spanning-tree portfast default global configuration, 102
- spanning-tree portfast disable interface configuration, 102
- spanning-tree vlan x root primary, 102
- spanning-tree vlan x root secondary, 102
- switchport mode access, 76, 84
- switchport mode dynamic desirable, 83
- switchport mode nonegotiate, 83
- switchport mode trunk, 83
- switchport trunk encapsulation negotiate, 84
- switchport trunk pruning vlan, 86
- terminal commands, 64
- terminal history size, 64
- terminal length x, 64
- transport preferred none, 135
- username, 217
- verifying commands, 68
- write, 137
- write-memory, 214
- comments, including in ACLs, 205
- completing commands with [tab] key, 60
- configuration backups, 213–214
- configuration examples, EtherChannel, 117
- configuration mode, EXEC commands (do), 138
- configurations
 - erasing, routers, 136
 - saving, routers, 136
- configure terminal command, routers, 138
- configuring
 - ACLs (access control lists), tips for, 206–207
 - CDP (Cisco Discovery Protocol), 121
 - DAI (Dynamic ARP Inspection), 193
 - DHCP clients, on IOS software ethernet interface, 162
 - DHCP helper addresses, 161
 - DHCP scope, WLC (Wireless LAN Controller), 234–237
 - DHCP servers, on IOS routers, 159–160
 - DHCP snooping, 190–192
 - Dynamic NAT, 165–167
 - EtherChannel
 - guidelines for, 112–113
 - layer 3 EtherChannel, 114
 - inter-VLAN communication, on L3 switches, 88
 - IPv4 default routes, 144
 - IPv4 static routes, 141–142
 - IPv6 default routes, 147
 - IPv6 static route configuration, 146–147
 - LACP hot-standby ports, EtherChannel, 115–116
 - layer 2 EtherChannel, 113
 - LLDP (Link Layer Discovery Protocol) (802.1AB), 123
 - load balancing, EtherChannel, 114–115
 - NTP (Network Time Protocol), 175–176
 - OSPF (Open Shortest Path First), 150
 - passwords
 - device hardening, 217
 - for routers, 126–127
 - PAT (Public Address Translation), 167–169
 - path cost, Spanning Tree Protocol, 101
 - port priority, Spanning Tree Protocol, 100–101
 - PortFast, Spanning Tree Protocol, 102–103
 - root switch, Spanning Tree Protocol, 100
 - routers
 - router names, 126
 - serial interfaces, 132
 - secondary root switches, 100
 - SSH (Secure Shell), 219–220

- static MAC addresses, 188
 - Static NAT, 169–170
 - sticky MAC addresses, 189
 - STP timers for Spanning Tree Protocol, 102
 - switch port security, 188–189
 - switch priority of VLANs, Spanning Tree Protocol, 101–102
 - switches
 - command modes, 68
 - examples, 72–74
 - help commands, 68
 - MAC address table, 72
 - mdix auto command, 70–71
 - resetting switch configuration, 69
 - setting duplex operation, 71
 - setting host names, 69
 - setting interface descriptions, 70
 - setting operation speed, 71–72
 - setting passwords, 69–70
 - setting up IP addresses and default gateways, 70
 - verifying commands, 68
 - syslog, 215
 - VLAN (Dynamic) interface, 230–234
 - VLANs (virtual LANs)
 - voice and data with trust, 77
 - voice and data without trust, 78
 - voice VLAN, 76
 - WLANs (wireless LANs), 237–239
 - with WPA2 PSK, 246–250
 - confog, 135
 - connecting
 - rollover cables to routers or switches, 51
 - routers or switches, terminal settings, 52
 - connections, LAN connections, 53
 - connectors, USB-to-serial connector for laptops, 55
 - console error messages, 60
 - Content Addressable Memory (CAM) table, 188
 - copy running-config startup-config
 - command, 79, 214
 - routers, 136
 - copy running-config tftp command, 136
 - core switch (3650)
 - PVST+ (Per VLAN Spanning Tree), configuration examples, 105–106
 - PVST+ to Rapid-PVST+, migration example, 109
 - CORP routers, inter-VLAN communication, configuration examples, 90–92
 - Create Your Wireless Networks Wizard
 - page, WLC (Wireless LAN Controller), 225–226
- ## D
- DAI (Dynamic ARP Inspection)
 - configuring, 193
 - verifying, 193
 - DCE cables, 54
 - serial interfaces, 132
 - dead interval timer, OSPF (Open Shortest Path First), 153
 - default ? command, 66
 - default command-name, 66
 - default dead interval timer, OSPF (Open Shortest Path First), 153
 - default EtherChannel configuration, 112
 - default gateways, configuring switches, 70
 - default hello timer, OSPF (Open Shortest Path First), 153
 - delimiting characters, 133–134
 - deny, ACLs (access control lists), 199
 - deny ipv6 any any command, 211
 - design, NTP (Network Time Protocol), 176–177
 - design tips, CDP (Cisco Discovery Protocol), 122
 - designated router (DR), OSPF (Open Shortest Path First), 153
 - detail keyword, 150
 - device hardening, 217
 - configuring

- SSH (Secure Shell), 219–220
 - passwords, 217
 - disabling unneeded services, 221
 - password encryption, 218
 - algorithm types, 218–219
 - restricting virtual terminal access, 220–221
 - device monitoring, 213
 - configuration backups, 213–214
 - logging, 214
 - syslog
 - configuring, 215
 - message example, 216
 - message format, 215
 - severity levels, 216
 - DHCP (Dynamic Host Configuration Protocol)
 - configuration examples, 162–164
 - disabling, 221
 - snooping, configuring, 190–192
 - DHCP address allocation, 191
 - DHCP clients, configuring on IOS
 - software ethernet interface, 162
 - DHCP helper addresses, configuring, 161
 - DHCP scope, configuring, 234–237
 - DHCP servers
 - Cisco IP Phones, 160
 - configuring on IOS routers, 159–160
 - verifying and troubleshooting, 160–161
 - DHCP snooping
 - configuring, 190–192
 - verifying, 192
 - diameter keyword, 100
 - Differentiated Services Code Point (DSCP), 77
 - disable command, 61
 - disabling unneeded services, 221
 - distribution 1 switch (3650)
 - PVST+ (Per VLAN Spanning Tree), configuration examples, 106
 - PVST+ to Rapid-PVST+, migration example, 109
 - distribution 2 switch (3650)
 - PVST+ (Per VLAN Spanning Tree), configuration examples, 106
 - PVST+ to Rapid-PVST+, migration example, 109
 - DLSwitch (3560 or 9300), EtherChannel, configuration examples, 117–118
 - DNS (Domain Name System), routers, 134–135
 - DNS name resolution, disabling, 221
 - do command, routers, 138
 - dot1q trunking, 84
 - double colon (::), 42
 - DR (designated router), OSPF (Open Shortest Path First), 153
 - DSCP (Differentiated Services Code Point), 77
 - dst-ip, 114
 - dst-mac, 114
 - dst-mixed-ip-port, 114–115
 - dst-port, 114
 - DTP (Dynamic Trunking Protocol), 83–84
 - duplex operations, configuring switches, 71
 - Dynamic ARP Inspection (DAI)
 - configuring, 193
 - verifying, 193
 - Dynamic Host Configuration Protocol (DHCP)
 - configuration examples, 162–164
 - disabling, 221
 - snooping, configuring, 190–192
 - Dynamic NAT, 165–167
 - Dynamic Trunking Protocol (DTP), 83–84
- ## E
- enable command, 61
 - enable password command, 127, 217
 - enable secret password command, 127, 217
 - end command, 61
 - erase startup-config, 69
 - routers, 136

erase startup-config command, 69

erasing

- configurations, routers, 136
- VLAN configurations, 79–80

error-disabled ports

- recovering automatically from, 190
- verifying autorecovery, 190

errors messages, console error messages, 60

established keyword, 201–202

EtherChannel, 111

- configuration examples, 117
 - ALSwitch1 (2960 or 9200), 118–119
 - ALSwitch2 (2960 or 9200), 119–120
 - DLSwitch (3560 or 9300), 117–118

configuring

- LACP hot-standby ports, 115–116
- Layer 2 EtherChannel, 113
- Layer 3 EtherChannel, 114
- load balancing, 114–115

default configuration, 112

guidelines for configuring, 112–113

interface modes, 111

monitoring, 116

verifying, 116

Ethernet links, 24

examples

DHCP configurations, 162–164

EtherChannel

- ALSwitch 1 (2960 or 9200), 118–119
- ALSwitch2 (2960 or 9200), 119–120
- DLSwitch (3560 or 9300), 117–118

inter-VLAN communication, 89

CORP routers, 90–92

ISP router, 89–90

L2Switch2 (Catalyst 2960), 92–96

L3Switch1 (Catalyst 3560/3650/3750), 94–95

IPv4 ACLs, 208–210

IPv4 static routes, 144–146

IPv6 ACLs, 210–211

NTP (Network Time Protocol), 182–186

OSPF (Open Shortest Path First), single-area OSPF, 154–157

PAT (Public Address Translation), 171–173

PVST+ (Per VLAN Spanning Tree), 104–105

router configurations, 138–140

routers, 138

switch configurations, 72–74

switch security, 194–196

VLAN configurations, 80–81

EXEC-level mode

configuration mode, do command, 138

routers, 126

exec-timeout, 136

exit, 61

extended, 115

extended ACLs

applying to interfaces, 201

creating, 200–201

established keyword, 201–202

log keyword, 202

extended system ID, enabling, for

Spanning Tree Protocol, 103

external routers, inter-VLAN

communication, with external routers (router-on-a-stick), 87

F

fast Ethernet interface, assigning IPv4 addresses, 132

flat addresses, MAC addresses, 2

floating static routes

IPv4 addresses and administrative distance (AD), 143–144

IPv6, 147

formulas for subnetting network address spaces, 12

forward-time command, 102

G

- gigabit Ethernet interfaces, assigning IPv4 addresses, 132
- global configuration mode, routers, 126
- GUAs (global unicast addresses), 45–46
- guidelines, for configuring EtherChannel, 112–113

H

- hello interval timer, OSPF (Open Shortest Path First), 153
- hello-time command, 102
- hello-time keyword, 100
- help
 - keyboard help, 62–63
 - question mark (?), 60–61
- help commands, configuring switches, 68
- hexidecimal digits, IPv6 addresses, 40
- hierarchical addresses, IPv4 addresses, 1
- history commands, 63
- history size command, 64
- host addresses, 3
- host bits, 11
- host keyword, 198
- host names, setting for switches, 69
- hostname command, 219
- HTTP service, disabling, 221
- HTTP-HTTPS Configuration page, 244

I

- IEEE Standard 802.1Q (dot1q), 84
- IETF (Internet Engineering Task Force), 39–40
- illegal characters in host names, 69
- implementing logging, 214
- implicit deny rule, 211
- in keyword, 200
- information, verifying for VLANs, 78
- interface descriptions, configuring, switches, 70

- interface modes,
 - EtherChannel, 111
 - routers, 126
- interface names, routers, 127–131
- interface range command, 76
- interfaces, moving between, 131
- Internet Engineering Task Force (IETF), 39–40
- Inter-Switch Link (ISL), 84
- inter-VLAN communication
 - configuration examples, 89
 - CORP routers, 90–92
 - ISP router, 89–90
 - L2Switch1 (Catalyst 2960), 95–96
 - L2Switch2 (Catalyst 2960), 92–94
 - L3Switch1 (Catalyst 3560/3650/3750), 94–95
 - with external routers (router-on-a-stick), 87
 - on multilayer switches, through SVI (Switch Virtual Interface), 88
 - network topology, 89
 - tips for, 88–89
- IOS routers, configuring DHCP servers, 159–160
- IOS software ethernet interface,
 - configuring DHCP clients, 162
- ip access-list resequence command, 205
- IP addresses, configuring switches, 70
- ip forward-helper udp x, 161
- ip helper-address, 161
- ip name-server command, 135
- ip ospf process ID area area number command, 151
- IP plans, VLSM example, 24–31
- IP redirects, disabling, 221
- ip route, 141–142
- IP source routing, disabling, 221
- ip subnet zero, 23
- IPv4 ACLs, configuration examples, 208–210
- IPv4 addresses, 39–40
 - appearance of, 2

- assigning to fast Ethernet interfaces, 132
- broadcast addresses, 3–4
- classes of, 4–5
 - sizing, 5–6
- classless addressing, 7–9
- floating static routes in IPv4 and administrative distance (AD), 143–144
- local versus remote addresses, 7
- network addresses, 3–4
- network bits versus node (host) bits, 5–6
- network masks, 2
 - writing, 3
- node addresses, 3–4
- RFC (private) 1918 addresses, 6–7
- subnetwork masks, 2
 - writing, 3
- when to use, 1–2

IPv4 embedded addresses, 45

- IPv6 addresses, 48

IPv4 static routes

- configuration examples, 144–146
- configuring, 141–142
- verifying, 144

IPv6, 7

- floating static routes, 147

IPv6 ACLs, 207

- configuration examples, 210–211
- verifying, 207

IPv6 addresses, 39–40

- address types, 44–45
 - anycast addresses, 50
 - multicast addresses, 48–50
 - unicast addresses, 45–48
- appearance of, 40
- assigning to interfaces, 133
- prefix length notation, 43–44
- reducing notation of, 41–43

IPv6 default routes, configuring, 147

ipv6 enable command, 133

IPv6 static route

- configuring, 146–147
- verifying, 147

- ipv6-label, 115
- ISL (Inter-Switch Link), 84
- ISP router, inter-VLAN communication (configuration examples), 89–90

K

- keyboard help, command-line interface, 62–63
- keywords
 - access-class, 207
 - access-group, 207
 - any, 198
 - detail, 150
 - diameter, 100
 - established, 201–202
 - hello-time, 100
 - host, 198
 - in, 200
 - log, 202
 - log-input, 202
 - out, 199–200
 - overload, 168
 - permanent, 142–143
 - priority, 101
 - traffic-filter, 207
 - voice, 189

L

- L2 switchport capability, removing on L3 switches, 88
- L2Switch2 (Catalyst 2960), inter-VLAN communication (configuration examples), 92–96
- L3 switches
 - configuring inter-VLAN communication, 88
 - removing L2 switchport capability, 88
- l3-proto, 115
- L3Switch1 (Catalyst 3560/3650/3750), inter-VLAN communication (configuration examples), 94–95

LACP hot-standby ports, configuring for EtherChannel, 115–116

LAN connections, 53

Layer 2 EtherChannel, configuring, 113

Layer 3 EtherChannel, configuring, 114

leading bit pattern, 4

limiting NTP access with access lists, 178

line mode, routers, 126

Link Layer Discovery Protocol (LLDP) (802.1AB), 123

- configuring, 123
- verifying and troubleshooting, 124

link-local unicast addresses, 45–47

LLDP (Link Layer Discovery Protocol) (802.1AB), 123

- configuring, 123
- verifying and troubleshooting, 124

load balancing, configuring for EtherChannel, 114–115

local addresses versus remote addresses, IPv4 addresses, 7

local host names, mapping to remote IP addresses, 134

log keyword, 202

log-adjacency-changes, 150

logging

- implementing, 214
- into WLC, 229

logging console, 202

logging synchronous, 135–136

login banners, creating, 134

log-input keyword, 202

logout command, 62

Logs Config page, 245

loopback addresses, 45, 47

loopback interfaces, OSPF (Open Shortest Path First), 152

M

MAC address table, switches, 72

MAC addresses, 2

management options, WLC (Wireless LAN Controller), 242–245

Management Summary page, WLC (Wireless LAN Controller), 242

mapping local host names to remote ip addresses, 134

max-age command, 102

mdix auto command, configuring switches, 70–71

message-of-the-day banner, 133

messages, syslog, 216

migration example, Spanning Tree Protocol (PVST+ to Rapid-PVST+), 108–109

monitoring

- EtherChannel, 116
- WLC (Wireless LAN Controller), 229–230

more command, pipe parameter (!), 64–65

MOTD (message-of-the-day) banner, 133

moving between interfaces, 131

MSTP (Multiple Spanning Tree Protocol), 98

multiarea OSPF, 150

multicast addresses, IPv6 addresses, 48–49

- solicited-node multicast addresses, 50
- well-known multicast addresses, 49

multilayer switches, inter-VLAN communication through SVI (Switch Virtual Interface), 88

Multiple Spanning Tree Protocol (MSTP), 98

N

named ACLs

- creating, 203
- removing specific lines with sequence numbers, 204
- sequence numbers, 203–204

NAT (Network Address Translation)

- Dynamic NAT, 165–167
- PAT (Public Address Translation), 167–169
- configuration examples, 171–173

- RFC (private) 1918 addresses, 6
- Static NAT, 169–170
- troubleshooting, 171
- verifying, 170
- NDP (Neighbor Discovery Protocol), 211
- network address spaces, formulas for
 - subnetting, 12
- Network Address Translation (NAT), RFC
 - (private) 1918 addresses, 6
- network addresses, 3
- network area command, 150
- network bits, 11
 - versus node (host) bits, IPv4
 - addresses, 5–6
- network masks, IPv4 addresses, 2
 - writing, 3
- Network Time Protocol. *See* NTP (Network Time Protocol)
- network topology
 - for 2960 series switch configuration,
 - 72
 - ACL configurations, 208
 - DHCP configuration, 162
 - EtherChannel, 117
 - inter-VLAN communication, 89
 - IPv6 static route configuration, 147
 - NTP (Network Time Protocol), 183
 - PAT (Public Address Translation),
 - 167, 171
 - router configurations, 138
 - single-area OSPF, 155
 - Static NAT, 169
 - static route configuration, 145
 - STP configuration example, 105
 - switch security, 194
 - VLAN configurations, 80
- no banner login command, 134
- no banner motd command, 133
- no cdp enable command, 122
- no cdp run command, 122
- no ip domain-lookup command, 134–135
- no ip forward-protocol udp x command,
 - 161
- no switchport command, 88
- node (host) bits versus network bits, IPv4
 - addresses, 5–6

- node addresses, 3–4
- NTP (Network Time Protocol), 175
 - authentication, 177
 - configuration examples, 182–186
 - configuring, 175–176
 - design, 176–177
 - disabling, 221
 - limiting access with access lists, 178
 - securing, 177
 - setting clocks on routers, 179–182
 - single-letter time zone designators,
 - 181–182
 - time stamps, 182
 - time zone acronyms, 180–181
 - verifying and troubleshooting, 178
- ntp master command, 176
- ntp peer command, 176
- NTPv3, 176–177
- NTPv4, 176

O

- octets, 2
 - wildcard masks, 151
- omitting all-0s hexets, IPv6 addresses, 42
- omitting leading 0s, IPv6 addresses, 41
- on-board port, 128
- Open Shortest Path First. *See* OSPF
- operation speed, configuring, switches,
 - 71–72
- OSPF (Open Shortest Path First), 149
 - configuration examples, single-area
 - OSPF, 154–157
 - configuring, 150
 - DR/BDR elections, 153
 - loopback interfaces, 152
 - multiarea OSPF, 150
 - router ID, 152
 - timers, 153
 - troubleshooting, version 2, 154
 - verifying version 2, 153–154
 - version 2 versus version 3, 149–150
 - wildcard masks, 150–152
- out keyword, 199–200
- overload keyword, 168

P

- password backdoor, 127
- password encryption
 - algorithm types, 218–219
 - device hardening, 218
 - routers, 127
- passwords
 - configuring, 217
 - for routers, 126–127
 - setting for switches, 69–70
 - setting on switches, 187
 - storing, 217
 - VTP (VLAN Trunking Protocol), 85
- PAT (Public Address Translation), 167–169
 - configuration examples, 171–173
 - troubleshooting, 171
 - verifying, 170
- path cost, configuring for Spanning Tree Protocol, 101
- Per VLAN Spanning Tree (PVST+), 97–98
- permanent keyword, static routing, 142–143
- permit any command, ACLs (access control lists), 199
- permit ip any any command, 199
- pinouts for different cables, 56
- pipe parameter (l), 64–65
- pipe parameter (l) options parameter, 65
- port channel command, 114
- port priority, configuring (Spanning Tree Protocol), 100–101
- PortFast, configuring (Spanning Tree Protocol), 102–103
- ports
 - assigning to VLANs, 76
 - error-disabled ports, recovering automatically from, 190
 - RJ-45 ports, 52
- prefix length notation, IPv6 addresses, 43–44
- prefix-length, 43
- priority keyword, 101
- private IP addresses, RFC (private) 1918 addresses, 165
- privilege EXEC modes, 126, 134
- protocols
 - ARP (Address Resolution Protocol), disabling, 221
 - CDP (Cisco Discovery Protocol), 121
 - configuring, 121
 - design tips, 122
 - verifying, 122
 - DHCP. *See* DHCP (Dynamic Host Configuration Protocol)
 - DTP (Dynamic Trunking Protocol), 83–84
 - LLDP (Link Layer Discovery Protocol) (802.1AB), 123
 - configuring, 123
 - verifying, 124
 - MSTP (Multiple Spanning Tree Protocol), 98
 - NDP (Neighbor Discovery Protocol), 211
 - NTP (Network Time Protocol). *See* NTP (Network Time Protocol)
 - Proxy Address Resolution Protocol (ARP), 221
 - Spanning Tree Protocol. *See* Spanning Tree Protocol (STP)
 - RSTP (Running Spanning Tree Protocol), 98
 - VTP (VLAN Trunking Protocol), 84–86
 - passwords, 85
 - pruning, 86
 - verifying, 86
 - versions, 85–86
- Proxy Address Resolution Protocol (ARP), disabling, 221
- pruning, VTP (VLAN Trunking Protocol), 86
- Public Address Translation (PAT), 167–169
- PVST+ (Per VLAN Spanning Tree), 97–98
 - configuration examples, 104–105

access 1 switch (2960), 107
 access 2 switch (2960), 107–108
 core switch (3650), 105–106
 distribution 1 switch (3650), 106
 distribution 2 switch (3650), 106
 PVST+ to Rapid-PVST+, Spanning-Tree
 migration example, 108–109

Q

question mark (?) for help, 60–61

R

RADIUS Authentication Servers page, 241
 RADIUS servers, WLC (Wireless LAN
 Controller), 239–241
 range command, 76
 Rapid PVST+, 98
 rebooting WLC (Wireless LAN
 Controller), 229
 recovering automatically from error-
 disabled ports, 190
 recursive lookups, static routing, 142
 reducing notation of IPv6 addresses, 41–43
 reference clocks, 176
 remark command, 205
 remote addresses versus local addresses,
 IPv4 addresses, 7
 remote ip addresses, mapping local host
 names to, 134
 removing
 ACLs (access control lists), 200
 L2 switchport capability on L3
 switches, 88
 specific lines from ACLs with
 sequence numbers, 204
 requirements for route summarization, 38
 resetting switch configuration, 69
 restricting virtual terminal access
 ACLs (access control lists),
 205–206
 device hardening, 220–221
 RF Parameter Optimization settings, WLC
 (Wireless LAN Controller), 227

RFC (private) 1918 addresses, 165
 IPv4 addresses, 6–7
 RJ45 Gio/o/o, 130
 RJ-45 ports, 52
 rollover cables, connecting to routers or
 switches, 51
 root switch
 configuring (Spanning Tree
 Protocol), 100
 secondary root switches,
 configuring, 100
 route flapping, route summarization, 38
 route summarization, 33
 examples, 33–37
 requirements for, 38
 route flapping, 38
 router configuration mode, routers, 126
 router configurations, network topology,
 138
 router ID, OSPF (Open Shortest Path
 First), 152
 Router Model 1721, 128
 Router Model 1760, 128
 Router Model 1841, 128
 Router Model 1941/1941W, 130
 Router Model 2501, 128
 Router Model 2514, 128
 Router Model 2610, 128
 Router Model 2611, 128
 Router Model 2620, 128
 Router Model 2621, 128
 Router Model 2801, 129
 Router Model 2811, 129
 Router Model 2901, 130
 Router Model 2911, 130
 Router Model 4221/4321, 130
 router modes, 126
 router names, configuring, 126
 router ospf x command, 152
 router-on-a-stick, inter-VLAN
 communication, 87
 routers
 assigning
 IPv4 addresses to fast Ethernet
 interfaces, 132

- IPv4 addresses to gigabit Ethernet interfaces, 132
- IPv6 addresses to interfaces, 133
- clocks, setting (NTP), 179–182
- configuration examples, 138
 - Boston Router, 138–140
- configuring
 - passwords, 126–127
 - router names, 126
 - serial interfaces, 132
- connecting
 - rollover cables, 51
 - terminal settings, 52
 - USB cables, 51–52
- CORP routers, inter-VLAN communication examples, 90–92
- DNS (Domain Name System), 134–135
- erasing configurations, 136
- EXEC commands, in configuration mode, 138
- exec-timeout, 136
- global configuration mode, 126
- interface names, 127–131
- inter-VLAN communication with external routers (router-on-a-stick), 87
- IOS routers, configuring DHCP servers on, 159–160
- ISP router, inter-VLAN communication examples, 89–90
- logging synchronous, 135–136
- login banners, creating, 134
- mapping local host names to remote ip addresses, 134
- message-of-the-day banner, 133
- moving between interfaces, 131
- password encryption, 127
- saving configurations, 136
- verifying configurations with show commands, 137–138
- write, 137
- routing, static routing. *See* static routing
- RSTP (Running Spanning Tree Protocol),

S

- samples, networks needing VLSM address plans, 24
- saving
 - configurations, routers, 136
 - VLAN configurations, 79
- secondary root switches, configuring, 100
- Secure Shell (SSH)
 - configuring, 219–220
 - verifying, 220
- securing NTP (Network Time Protocol), 177
- security, WLANs, 226
- Security Policies field, WLANs, 250
- sequence numbers
 - named ACLs, 203–204
 - tips for, 204–205
- serial cable (2500 series), 53
- serial cable types, 53–55
- serial interfaces, configuring, 132
- serial links, 24
- servers, DHCP servers. *See* DHCP servers
- service password-encryption command, 217–218
- service sequence-numbers global configuration command, 215
- service timestamps log datetime global configuration command, 215
- Set Up Your Controller Wizard page, WLC (Wireless LAN Controller), 225
- setup mode, 62
- severity levels, syslog, 216
- SFP Gio/o/o, 130
- shortcuts
 - Binary ANDing, 20–21
 - for entering commands, 59
- show commands, 64
 - pipe parameter (!), 64–65
 - verifying router configurations, 137–138
- show con? command, 60
- show errdisable recovery command, 190
- show flash command, 64

- show history command, 64
- show interfaces command, 68
- show interfaces status err-disabled command, 190
- show interfaces vlanx command, 68
- show ip interface brief command, 128
- show ntp associations command, 176
- show running-config command, 71, 126
 - OSPF (Open Shortest Path First), 152
 - routers, 138
- show version command, 64
- show vlan privileged EXEC command, 75
- Simplified Setup Start page, WLC (Wireless LAN Controller), 224
- single-area OSPF, configuration examples, 154–157
- single-letter time zone designators, 181–182
- sizing classes of IPv4 addresses, 5–6
- slots, 128
- smart serial cables, 54
- SNMP System Summary page, 242–243
- SNMP Trap Controls General Tab, 243
- solicited-node multicast addresses, IPv6 addresses, 50
- Spanning Tree Protocol (STP)
 - BPDU Guard (2xxx/3xxx Series), 103
 - BPDU Guard (9xxx Series), 103
 - changing spanning-tree mode, 99
 - configuration example, network topology, 105
 - configuring
 - path cost, 101
 - port priority, 100–101
 - PortFast, 102–103
 - root switch, 100
 - secondary root switches, 100
 - STP timers, 102
 - switch priority of VLANs, 101–102
 - definition, 97–98
 - enabling, 98
 - extended system ID, enabling, 103
 - migration example, PVST+ to Rapid-PVST+, 108–109
 - PVST+ (Per VLAN Spanning Tree)
 - access 1 switch (2960), 107
 - access 2 switch (2960), 107–108
 - configuration examples, 104–105
 - core switch (3650), 105–106
 - distribution 1 switch (3650), 106
 - distribution 2 switch (3650), 106
 - troubleshooting, 104
 - verifying, 104
- spanning-tree mode, changing, 99
- spanning-tree portfast default global configuration command, 102
- spanning-tree portfast disable interface configuration command, 102
- spanning-tree vlan x root primary command, 102
- spanning-tree vlan x root secondary command, 102
- src-dst-ip, 115
- src-dst-mac, 115
- src-dst-mixed-ip-port, 115
- src-ip, 115
- src-mac, 114–115
- src-port, 115
- SSH (Secure Shell)
 - configuring, 219–220
 - verifying, 220
- standard ACLs
 - applying to interfaces, 199–200
 - creating, 198–199
- static MAC addresses, configuring, 188
- Static NAT, 169–170
- static routing
 - configuration examples, IPv4 static routes, 144–146
 - configuring
 - IPv4 default routes, 144
 - IPv4 static routes, 141–142
 - IPv6 default routes, 147
 - IPv6 static route, 146–147

- floating static routes in IPv4 and administrative distance (AD), 143–144
- floating static routes in IPv6, 147
- permanent keyword, 142–143
- recursive lookups, 142
- verifying
 - IPv4 static routes, 144
 - IPv6 static routes, 147
- static VLANs, creating, 75
 - with VLAN configuration mode, 75–76
- sticky MAC addresses, configuring, 189
- storing passwords, 217
- STP. *See* Spanning Tree Protocol (STP)
- STP configuration example, network topology, 105
- STP timers, configuring (Spanning Tree Protocol), 102
- stratum, 176
- subinterface mode, routers, 126
- subnetting, 11
 - Binary ANDing, 17–19
 - shortcuts, 20–21
 - Class B networks, using binary, 15–17
 - Class C network, using binary, 12–15
 - IP subnet zero, 23
 - network address spaces, formulas for, 12
 - VLSM (variable-length subnet masking), 23
- subnetwork masks, IPv4 addresses, 2
 - writing, 3
- supernetting. *See* route summarization
- SVI (switched virtual interface), inter-VLAN communication, on multilayer switches, 88
- switch port security
 - configuring, 188–189
 - verifying, 189–190
- switch priority of VLANs, configuring, for Spanning Tree Protocol, 101–102
- switch security, configuration examples, 194–196
- switched virtual interfaces (SVI), inter-VLAN communication, on multilayer switches, 88
- switches
 - 2960/9200 series switches, 70
 - autosensing cable types, 56
 - configuring
 - command modes, 68
 - examples, 72–74
 - help commands, 68
 - MAC address table, 72
 - mdix auto command, 70–71
 - port security, 188–189
 - resetting switch configuration, 69
 - setting duplex operation, 71
 - setting host names, 69
 - setting interface descriptions, 70
 - setting operation speed, 71–72
 - setting passwords, 69–70
 - setting up IP addresses and default gateways, 70
 - static MAC addresses, 188
 - sticky MAC addresses, 189
 - verifying commands, 68
 - connecting
 - rollover cables, 51
 - terminal settings, 52
 - USB cables, 51–52
 - DHCP snooping, configuring, 190–192
 - inter-VLAN communication, on multilayer switches through SVI, 88
 - recovering automatically from error-disabled ports, 190
 - root switch, configuring, 100
 - secondary root switches, configuring, 100
 - setting passwords, 187

- switch port security, verifying, 189–190
 - verifying autorecovery of error-disabled ports, 190
- switchport mode access command, 76, 84
- switchport mode dynamic auto command, 83
- switchport mode dynamic desirable command, 83
- switchport mode nonegotiate command, 83
- switchport mode trunk command, 83
- switchport port-security mac-address sticky command, 189
- switchport trunk encapsulation negotiate command, 84
- switchport trunk pruning vlan command, 86
- synchronous logging, 135–136
- syslog
 - configuring, 215
 - message example, 216
 - message format, 215
 - severity levels, 216
- System Configuration Dialog (setup mode), 62

T

- T568A versus T568B cables, 57
- T568B versus T568A cables, 57
- Tech Support > System Resource Information page, 245
- Telnet-SSH configuration, 244
- terminal commands, 64
- terminal settings, connecting, routers or switches, 52
- time stamps, NTP (Network Time Protocol), 182
- time zone acronyms, 180–181
- time zone designators, 181–182
- timers, OSPF (Open Shortest Path First), 153
- traffic-filter keyword, 207
- transparent mode, VLANs, 76

- transport preferred none command, 135
- troubleshooting
 - CDP (Cisco Discovery Protocol), 122
 - DHCP configuration, 160–161
 - LLDP (Link Layer Discovery Protocol) (802.1AB), 124
 - NAT (Network Address Translation), 171
 - NTP (Network Time Protocol), 178
 - OSPF (Open Shortest Path First), version 2, 154
 - PAT (Public Address Translation), 171
 - Spanning Tree Protocol, 104
- trust, configuring voice and data VLANs with, 77

U

- unicast addresses, IPv6 addresses, 45–48
 - global unicast addresses (GUAs), 45–46
 - IPv4 embedded addresses, 48
 - link-local unicast addresses, 46–47
 - loopback addresses, 47
 - unique local addresses, 47–48
 - unspecified addresses, 47
- unicast communication, 1
- unique local addresses, 45
 - IPv6 addresses, 47–48
- unnneeded services, disabling, 221
- unspecified addresses, 45
 - IPv6 addresses, 47
- USB cables, connecting, to routers or switches, 51–52
- USB Type A to 5-pin mini type B cable, 55
- USB-to-serial connector for laptops, 55
- user EXEC mode, 134
- user mode, routers, 126
- username command, 217
- UTP wiring standards, T568A versus T568 B, 57

V

- V.35 DTE and DCE cables, 54
- variable-length subnet masking (VLSM), 23
 - examples, 24–31
- verifying
 - ACLs (access control lists), 200
 - autorecovery of error-disabled ports, 190
 - CDP (Cisco Discovery Protocol), 122
 - DAI (Dynamic ARP Inspection), 193
 - DHCP configuration, 160–161
 - DHCP snooping, 192
 - EtherChannel, 116
 - information, VLANs, 78
 - IPv4 static routes, 144
 - IPv6 ACLs, 207
 - IPv6 static route, 147
 - LLDP (Link Layer Discovery Protocol) (802.1AB), 124
 - NAT (Network Address Translation) configurations, 170
 - NTP (Network Time Protocol), 178
 - OSPF (Open Shortest Path First), version 2, 153–154
 - PAT (Public Address Translation), 170
 - router configurations with show commands, 137–138
 - Spanning Tree Protocol (STP), 104
 - SSH (Secure Shell), 220
 - switch port security, 189–190
 - VTP (VLAN Trunking Protocol), 86
- verifying commands, configuring switches, 68
- versions of VTP, 85–86
- virtual terminal access, restricting, 220–221
 - in ACLs, 205–206
- VLAN (Dynamic) interface, configuring, 230–234
- VLAN configuration mode, creating static VLANs, 75–76
- VLAN encapsulation type, setting, 84
- VLAN Trunking Protocol (VTP), 76, 84–86
 - passwords, 85
 - pruning, 86
 - verifying, 86
- VLANs (virtual LANs)
 - assigning ports to, 76
 - configuration examples, 80–81
 - configuring
 - inter-VLAN communication on L3 switches, 88
 - voice and data with trust, 77
 - voice and data without trust, 78
 - erasing configurations, 79–80
 - inter-VLAN communication. *See* inter-VLAN communication
 - with external routers (router-on-a-stick), 87
 - on multilayer switches through SVI, 88
 - network topology, configuration examples, 80
 - range command, 76
 - saving configurations, 79
 - static VLANs, creating, 75
 - with VLAN configuration mode, 75–76
 - verifying information, 78
 - voice VLAN, configuring, 76
- VLSM (variable-length subnet masking), 23
 - examples, 24–31
- voice and data, configuring
 - with trust, VLANs, 77
 - without trust, 78
- voice keyword, 189
- voice VLAN, configuring, 76
- VTP (VLAN Trunking Protocol), 76, 84–86
 - passwords, 85
 - pruning, 86
 - verifying, 86
 - versions, 85–86

W-X-Y-Z

well-known multicast addresses, IPv6 addresses, 49

wildcard masks

ACLs (access control lists), 198

OSPF (Open Shortest Path First), 150–152

Wireless LAN Controller. *See* WLC (Wireless LAN Controller)

WLANs (wireless LANs)

configuring, 237–239

with WPA2 PSK, 246–250

security, 226

WLC (Wireless LAN Controller)

configuring

DHCP scope, 234–237

VLAN (Dynamic) interface, 230–234

WLANs, 237–239

initial setup, 223–229

management options, 242–245

monitoring, 229–230

RADIUS servers, 239–241

WPA2 PSK, configuring, WLANs, 246–250

write command, routers, 137

write erase command, 137

write memory command, 137

write network command, 137

write-memory command, 214

writing

network masks, IPv4 addresses, 3

subnetwork masks, IPv4 addresses, 3