



CCNA 200-301

Portable Command Guide Sixth Edition

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



ciscopress.com

SCOTT EMPSON

FREE SAMPLE CHAPTER |



CCNA 200-301 Portable Command Guide

Sixth Edition

Scott Empson



CCNA 200-301 Portable Command Guide, Sixth Edition

Scott Empson

Copyright © 2026 Pearson Education, Inc.

Published by: Cisco Press

Hoboken, New Jersey

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit <https://www.pearson.com/global-permission-granting.html>.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

\$PrintCode

Library of Congress Control Number: 2025948568

ISBN-13: 978-0-13-820868-4

ISBN-10: 0-13-820868-9

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 Trademark Disclaimer

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

**Head of IT &
Professional Learning,
Enterprise Learning
and Skills**

Julie Phifer

Executive Editor

James Manly

**Cisco Alliance
Manager**

Caroline Antonio

Managing Editor

Sandra Schroeder

Development Editor

Ellie Bru

Senior Project Editor

Tonya Simpson

Copy Editor

Chuck Hutchinson

Technical Editor

Patrick Gargano

Cover Designer

Chuti Prasertsith

Composition

codeMantra

Indexer

Brad Herriman

Proofreader

Barbara Mack

with the use or performance of information available from the services. The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screen shots may be viewed in full within the software version specified.

Feedback Information

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

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

We greatly appreciate your assistance.

Contents at a Glance

Introduction xxi

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 69
- CHAPTER 9** VLANs 81
- CHAPTER 10** VLAN Trunking Protocol and Inter-VLAN Communication 89
- CHAPTER 11** Spanning Tree Protocol 103
- CHAPTER 12** EtherChannel 119
- CHAPTER 13** Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) 129

Part III: Routing Technologies

- CHAPTER 14** Configuring a Cisco Router 133
- CHAPTER 15** Interpreting the Routing Table and Configuring Static Routes 149
- CHAPTER 16** Open Shortest Path First (OSPF) 161

Part IV: IP Services

- CHAPTER 17** DHCP 173
- CHAPTER 18** Network Address Translation (NAT) 181
- CHAPTER 19** Configuring Network Time Protocol (NTP) 191

Part V: Security Fundamentals

- CHAPTER 20** Layer Two Security Features 203
- CHAPTER 21** Managing Traffic Using Access Control Lists (ACLs) 215
- CHAPTER 22** Device Monitoring and Hardening 233

Part VI: Infrastructure Management

- CHAPTER 23** Troubleshooting and Verification 243
- CHAPTER 24** Backing Up and Restoring Cisco IOS Software and Configurations 255

Part VII: Wireless Technologies

- CHAPTER 25** Configuring Secure Wireless Access 267

Part VII: Appendices

- APPENDIX A** How to Count in Decimal, Binary, and Hexadecimal 277
- APPENDIX B** How to Convert Between Number Systems 285
- APPENDIX C** Binary/Hex/Decimal Conversion Chart 293
- APPENDIX D** Password Recovery Procedures and the Configuration Register 301
- APPENDIX E** Create Your Own Journal Here 309
- Index 327

Table of Contents

Introduction xxi

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 (Console) Cable to Your Router or Switch	51
	Using a USB Cable to Connect to Your Router or Switch	52
	Configuring a Terminal Emulator	52
	LAN Connections	53
	Serial Cable Types	53
	Which Cable to Use?	56
	ANSI/TIA Cabling Standards	57
	T568A Versus T568B Cables	58
CHAPTER 7	The Command-Line Interface	59
	Shortcuts for Entering Commands	59
	Using the Tab 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	62
logout Command	62
reload Command	62
Setup Mode	62
Keyboard Help	63
History Commands	64
terminal Commands	64
show Commands	65
Using the Pipe Parameter () with the show or more Commands	65
Using the no and default Forms of Commands	66

Part II: LAN Switching Technologies

CHAPTER 8 Configuring a Switch 69

Help Commands	70
Command Modes	70
Verifying Commands	70
Resetting Switch Configuration	71
Setting Host Names	71
Setting Passwords	72
Setting IP Addresses and Default Gateways	73
The Ethernet Management Port	73
Supported Features on the Ethernet Management Port	74
Configuring and Verifying the Ethernet Management Port	74
Setting Interface Descriptions	75
The mdix auto Command	75
Setting Duplex Operation	76
Setting Operation Speed	76
Setting the Maximum Aging Time of the MAC Table	77
Managing the MAC Address Table	77
Configuration Example	77

CHAPTER 9 VLANs 81

Creating Static VLANs	81
Creating Static VLANs Using VLAN Configuration Mode	81
Assigning Ports to VLANs	82
Using the range Command	82
Configuring a Voice VLAN	82

Verifying VLAN Information	83
Saving VLAN Configurations	84
Erasing VLAN Configurations	84
Shutting Down or Suspending VLANs	85
Configuration Example: VLANs	87
9200 Switch	87
CHAPTER 10 VLAN Trunking Protocol and Inter-VLAN Communication	89
Dynamic Trunking Protocol (DTP)	90
Setting the VLAN Encapsulation Type	90
VLAN Trunking Protocol (VTP)	91
Configuring a VTP Version 3 Primary Server	92
Verifying VTP	93
Inter-VLAN Communication Using an External Router: Router-on-a-Stick	93
Inter-VLAN Communication on a Layer 3 Switch Through a Switch Virtual Interface	94
The autostate command	94
Removing Layer 2 Switchport Capability of an Interface on a Layer 3 Switch	95
Configuring Inter-VLAN Communication on a Layer 3 Switch	95
Inter-VLAN Communication Tips	95
Configuration Example: Inter-VLAN Communication	96
ISP Router	96
CORP Router	97
L2Switch2 (Catalyst 9200)	99
L3Switch1 (Catalyst 9300)	100
L2Switch1 (Catalyst 9200)	102
CHAPTER 11 Spanning Tree Protocol	103
Spanning Tree Protocol Definition	104
Enabling Spanning Tree Protocol	105
Changing the Spanning-Tree Mode	105
Configuring the Root Switch	106
Configuring a Secondary Root Switch	106
Configuring the Switch Priority of a VLAN	106
Configuring Port Priority	107
Path Cost: Short vs. Long	107

- Configuring the Path Cost 108
- Configuring STP Timers 109
- Configuring Optional Spanning-Tree Features 109
 - PortFast 109
 - BPDU Guard (2xxx/Older 3xxx Series) 110
 - BPDU Guard (3650/9xxx Series) 111
 - BPDU Filter 111
 - Root Guard 112
- Enabling the Extended System ID 112
- Verifying STP 113
- Troubleshooting Spanning Tree Protocol 113
- Configuration Example: PVST+ 113
 - Core Switch (9300) 114
 - Distribution 1 Switch (9300) 115
 - Distribution 2 Switch (9300) 115
 - Access 1 Switch (9200) 116
 - Access 2 Switch (9200) 116

CHAPTER 12 EtherChannel 119

- EtherChannel 119
 - Interface Modes in EtherChannel 119
 - Default EtherChannel Configuration 120
 - Guidelines for Configuring EtherChannel 120
 - Configuring Layer 2 EtherChannel 122
 - Configuring Layer 3 EtherChannel 122
 - Configuring EtherChannel Load Balancing 123
 - Configuring LACP Hot-Standby Ports 124
 - Monitoring and Verifying EtherChannel 125
- Configuration Example: EtherChannel 125
 - DLSwitch (9300) 126
 - ALSwitch1 (9200) 127
 - ALSwitch2 (9200) 128

CHAPTER 13 Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) 129

- Cisco Discovery Protocol 129
- Configuring CDP 129
- Verifying and Troubleshooting CDP 130
- CDP Design Tips 130
- Link Layer Discovery Protocol (802.1AB) 131

Configuring LLDP (802.1AB)	131
Verifying and Troubleshooting LLDP	132

Part III: Routing Technologies

CHAPTER 14	Configuring a Cisco Router	133
	Router Modes	134
	Entering Global Configuration Mode	134
	Configuring a Router Name	134
	Configuring Passwords	134
	Password Encryption	135
	Interface Names	135
	Moving Between Interfaces	138
	Configuring a Serial Interface	139
	Assigning an IPv4 Address to a Fast Ethernet Interface	139
	Assigning an IPv4 Address to a Gigabit Ethernet Interface	139
	Assigning IPv6 Addresses to Interfaces	140
	Creating a Message-of-the-Day Banner	140
	Creating a Login Banner	141
	Mapping a Local Host Name to a Remote IP Address	141
	The no ip domain-lookup Command	141
	Working with DNS on a Router	142
	The logging synchronous Command	143
	The exec-timeout Command	143
	Saving Configurations	144
	Erasing Configurations	144
	The write Command	144
	Verifying Your Configurations Using show Commands	144
	EXEC Commands in Configuration Mode: The do Command	145
	Configuration Example: Basic Router Configuration	146
	Boston Router	146
	Buffalo Router	147
CHAPTER 15	Interpreting the Routing Table and Configuring Static Routes	149
	Interpreting the Routing Table	149
	Codes	149
	The Default Route	150

The Default Route on a Client Machine	150
Routes	152
Configuring an IPv4 Static Route	153
Static Routes and Recursive Lookups	154
The permanent Keyword	155
Floating Static Routes and Administrative Distance	155
Configuring an IPv4 Default Route	156
Verifying IPv4 Static Routes	156
Configuration Example: IPv4 Static Routes	157
Ketchikan Router	157
Juneau Router	158
Sitka Router	158
Configuring an IPv6 Static Route	158
Floating Static Routes in IPv6	159
Configuring an IPv6 Default Route	160
Verifying IPv6 Static Routes	160
CHAPTER 16 Open Shortest Path First (OSPF)	161
OSPFv2 Versus OSPFv3	161
OSPF Network Types	162
Configuring OSPF	162
Using Wildcard Masks with OSPF Areas	163
Configuring OSPFv2 Using Interface Subcommands	164
Converting from Traditional Configuration to Interface Configuration Mode	165
Optimizing OSPF Parameters	166
Loopback Interfaces	166
Router ID	166
DR/BDR Elections	167
Timers	167
Propagating a Default Route	167
Verifying OSPFv2 Configurations	168
Troubleshooting OSPFv2	169
Configuration Example: Single-Area OSPF	169
Austin Router	170
Houston Router	170
Galveston Router	171

Part IV: IP Services**CHAPTER 17 DHCP 173**

- Configuring a DHCP Server on an IOS or IOS XE Router 173
- Using Cisco IP Phones with a DHCP Server 174
- Configuring DHCP Option 43 for Access Points 174
- Verifying and Troubleshooting DHCP Configuration 175
- Configuring a DHCP Helper Address 176
- Configuring a DHCP Client on a Cisco IOS or IOS XE Software Ethernet Interface 177
- Configuration Example: DHCP 177
 - Edmonton Router 178
 - Gibbons Router 179

CHAPTER 18 Network Address Translation (NAT) 181

- Private IP Addresses: RFC 1918 181
- Configuring Dynamic NAT: One Private to One Public Address Translation 181
- Configuring PAT: Many Private to One Public Address Translation 183
- Configuring Static NAT: One Private to One Permanent Public Address Translation 185
- Verifying NAT and PAT Configurations 186
- Troubleshooting NAT and PAT Configurations 187
- Configuration Example: PAT 187
 - ISP Router 187
 - Company Router 188

CHAPTER 19 Configuring Network Time Protocol (NTP) 191

- NTP Configuration 191
- NTP Design 192
- Securing NTP 193
 - Enabling NTP Authentication 193
 - Limiting NTP Access with Access Lists 194
- Verifying and Troubleshooting NTP 195
- Setting the Clock on a Router 195
- Using Timestamps 199
- Configuration Example: NTP 199
 - Core1 Router 200
 - Core2 Router 200
 - DLSwitch1 201

DLSwitch2	201
ALSwitch1	202
ALSwitch2	202

Part V: Security Fundamentals

CHAPTER 20 Layer Two Security Features 203

Setting Passwords on a Switch	203
Configuring Static MAC Addresses	204
Configuring Switch Port Security	205
Configuring Sticky MAC Addresses	205
Verifying Switch Port Security	206
Recovering Automatically from Error-Disabled Ports	207
Verifying Autorecovery of Error-Disabled Ports	207
Configuring DHCP Snooping	207
Verifying DHCP Snooping	209
Configuring Dynamic ARP Inspection (DAI)	209
Verifying Dynamic ARP Inspection	210
Configuration Example: Switch Security	210

CHAPTER 21 Managing Traffic Using Access Control Lists (ACLs) 215

Access List Numbers	216
Using Wildcard Masks	216
ACL Keywords	217
Creating Standard ACLs	217
Applying Standard ACLs to an Interface	218
Verifying ACLs	218
Removing ACLs	218
Creating Extended ACLs	219
Applying Extended ACLs to an Interface	220
The established Keyword	220
The log Keyword	220
Creating Named ACLs Using ACL Configuration Mode	221
Using Sequence Numbers in Named ACLs	222
Removing Specific Lines in Named ACLs Using Sequence Numbers	223
Sequence Number Tips	223
Including Comments in ACLs	224
Restricting Virtual Terminal Access	224

Tips for Configuring ACLs	225
Comparing ACLs in IOS and IOS XE	225
Using a Second (Common) Interface ACL in IOS XE	226
Matching Multiple Nonconsecutive Ports with eq in IOS XE	227
IPv6 ACLs	227
Verifying IPv6 ACLs	227
Configuration Examples: IPv4 ACLs	228
Configuration Examples: IPv6 ACLs	230
CHAPTER 22 Device Monitoring and Hardening	233
Device Monitoring	233
Configuration Backups	233
Implementing Logging	234
Configuring Syslog	235
Syslog Message Format	235
Syslog Severity Levels	236
Syslog Message Example	236
Device Hardening	236
Configuring Passwords	237
Password Encryption	238
Password Encryption Algorithm Types	238
Configuring the enable secret Password Using Encryption Algorithm Types	239
Configuring SSH	240
Verifying SSH	241
Restricting Virtual Terminal Access	241
Disabling Unneeded Services	242
Part VI: Infrastructure Management	
CHAPTER 23 Troubleshooting and Verification	243
Viewing the Routing Table	243
Clearing the Routing Table	244
Determining the Gateway of Last Resort	244
Determining the Last Routing Update	244
Internet Control Message Protocol Redirect Messages	245
The ping Command	245
Examples of Using the ping and the Extended ping Commands	246

Interpreting the show interface Command	247
Clearing Interface Counters	249
Using CDP to Troubleshoot	249
The traceroute Command	249
The show controllers Command	250
debug Commands	250
Using Timestamps	250
Generic Host Networking Commands	251
The ip http server Command	252
Configuring a Device to Accept a Remote Telnet Connection	252
Using Telnet to Remotely Connect to Other Devices	253
Verifying Telnet	254

CHAPTER 24 Backing Up and Restoring Cisco IOS Software and Configurations 255

Boot System Commands	255
The Cisco IOS File System	256
Viewing the Cisco IOS File System	256
Commonly Used URL Prefixes for Cisco Network Devices	256
Deciphering IOS Image Filenames	257
Backing Up Configurations to a TFTP Server	258
Restoring Configurations from a TFTP Server	258
Backing Up the Cisco IOS Software to a TFTP Server	259
Restoring/Upgrading the Cisco IOS Software from a TFTP Server	259
Restoring the Cisco IOS Software from ROM Monitor Mode Using Xmodem	260
Restoring the Cisco IOS Software Using the ROM Monitor Environmental Variables and tftpdnld Command	262
Secure Copy	263
Configuring a Secure Copy Server	263
Verifying and Troubleshooting Secure Copy	264
Configuration Example: Using Secure Copy	264

Part VII: Wireless Technologies

CHAPTER 25 Configuring Secure Wireless Access 267

Connecting to a Cisco Wireless LAN Controller (WLC)	267
Configuring a WLAN Using WPA2 PSK	269

APPENDIX A	How to Count in Decimal, Binary, and Hexadecimal	277
	How to Count in Decimal	277
	How to Count in Binary	279
	How to Count in Hexadecimal	280
	Representing Decimal, Binary, and Hexadecimal Numbers	282
APPENDIX B	How to Convert Between Number Systems	285
	How to Convert from Decimal to Binary	285
	How to Convert from Binary to Decimal	286
	How to Convert from Decimal IP Addresses to Binary and from Binary IP Addresses to Decimal	287
	A Bit of Perspective	288
	How to Convert from Hexadecimal to Binary	288
	How to Convert from Binary to Hexadecimal	289
	How to Convert from Decimal to Hexadecimal	290
	How to Convert from Hexadecimal to Decimal	291
APPENDIX C	Binary/Hex/Decimal Conversion Chart	293
APPENDIX D	Password Recovery Procedures and the Configuration Register	301
	The Configuration Register	301
	A Visual Representation of the Configuration Register	301
	What the Bits Mean	302
	The Boot Field	302
	Console Terminal Baud Rate Settings	303
	Changing the Console Line Speed: CLI	303
	Changing the Console Line Speed: ROM Monitor Mode	304
	Password-Recovery Procedures for Cisco Routers	305
	Password Recovery for Catalyst 9000/9200/9300 Series Switches	306
	Password Recovery for Standalone Switches	306
	Password Recovery for Stackwise Deployments	307
APPENDIX E	Create Your Own Journal Here	309
INDEX		327

About the Author



Scott Empson is enjoying being *mostly retired* after working for more than 30 years as a teacher—4 years in the Alberta K-12 public school system and 27 years as an instructor/program chair at the Northern Alberta Institute of Technology in Edmonton, Alberta, Canada. He taught a variety of technical courses in Cisco-related topics and soft-skills courses like professional develop-

ment, organizational behavior, and leadership. Scott also worked with students as they moved from being students to IT professionals through internships and co-op classes. 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, Canada, with his wife, Trina, who is still processing that he gets to stay at home while she still must go to work. His children have left the nest and are living their best lives. Scott is now upset that he must do all the yardwork, including shoveling snow during Canadian winters.

About the Technical Reviewer

Patrick Gargano is an instructor and a lead content advocate on the Technical Education team at Learn with Cisco. Before joining Cisco in 2021, he worked as a Cisco Networking Academy instructor and instructor-trainer, and as a Certified Cisco Systems Instructor (CCSI) for Fast Lane UK, Skyline ATS, and EnterOne, teaching CCNA and CCNP courses. He has developed Cisco's official CCNA, ENCC, ENARSI, ENSDWI, SDWFND, and SDWSCS course content, and has published four Cisco Press books. His education includes CCT, CCNA, CCNA Cybersecurity, and CCNP Enterprise certifications, a bachelor of education, a bachelor of arts, and a master of professional studies degree in computer networking. He is a regular speaker at Cisco Live US, EMEA, and APJC. He lives in Ottawa, Canada, with his wife and son.

Dedications

As always, this book is dedicated to Trina, Zach, and Shae. These books used to pay for music lessons, registration fees for various sports, and travel to Disney. Now they pay for flights to visit you since you moved away from us here in the Great White North.

I love you all. 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. Julie, James, Sandra, Ellie, Tonya, Chuck, Chuti, Brad, Jayaprakash (JP), and Barbara: Thank you for your continued support and belief in my little engineering journal.

In the past 20 years that this book (and its various iterations) has been in print, my family at Cisco Press has always treated me with kindness and respect, putting up with my spelling "errors" (there is a letter *U* in *neighbour*, and you cannot tell me otherwise. In the immortal words of the great British philosopher Rick Astley, I am never going to give u up.) and keeping me focused on what is important—providing high-quality learning materials for students and IT professionals to access on their learning journeys. Thank you to all past and present members of the team.

To my technical reviewer, Patrick: Patrick is one of the most brilliant people I have ever met and is also one of the strongest instructors I have ever had the fortune to work with and learn from. He is my co-author in the more advanced *CCNP and CCIE Enterprise Core & CCNP Enterprise Advanced Routing Portable Command Guide*, he has his own books which I strongly recommend you have in your learning library (his *31 Days Before Your CCNP and CCIE Enterprise Core Exam* is a must read), and most importantly, he is my friend. I cannot put the words together that express my gratitude for working on this title with me. Thank you for correcting my mistakes and making me look smarter than I really am. Je t'aime, mon frère.

Finally, to a great friend and the creator of my icon, Dorian. You took my request to create something new and unique and absolutely nailed the assignment. The effort to draw my actual big bald head is just proof of your dedication to your craft. Your students are truly fortunate to have you leading and teaching them. You should be proud of what you have accomplished and what you will continue to do. Just remember to keep on being fabulous!

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

Reader Services

Register your copy at www.ciscopress.com/title/9780138208684 for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account*. Enter the product ISBN 9780138208684 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

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*, Sixth edition! Just like my other books in this series, I have always tried to come up with a better name for it to increase sales. So far, the publisher has rejected past requests to name an older edition *Harry Potter and the CCNA Portable Command Guide*, or *Star Wars: The Portable Command Guide Strikes Back*, and now they have also pushed back on *KPop: Portable Command Guide Hunters*. Some people have no sense of humor.

In your hands is the sixth edition of the *Portable Command Guide*. This one was a long time coming as the fifth edition came out with the 2020 Certpocalypse of most Cisco certification exams. The updates and revisions that have been made to the 200-301 exam since then have been mostly in the theoretical arena, and not in the commands, so while other titles went through a version 1.1 revision, this book did not. On the advice of some other CCNA authors (can we all agree that Wendell Odom, Jason Gooley, and Patrick Gargano are absolutely brilliant?), and the staff of Cisco Press, I undertook this project to update some specific areas of the book—diagrams, examples, use of older Cisco devices, and so on. My fifth edition was always in line with v1.1 of the exam, but now this sixth edition is a cleaner, updated release. For someone who originally thought that this book would be fewer 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 have to do only 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 25+ years; some of my courses that I taught back in the day I only did once a year, or once every second year, so the need to refresh technologies and commands was part of my daily routine. A new IOS release meant that it was time to jump back into the CLI to see what had changed; some stuff went away, but some stuff came back. And **write mem** never did leave, even though we were told it would. 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 sixth 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 200-301 certification exam, whether through self-study, on-the-job training and practice, or study within the Cisco Networking Academy program or other high school and post-secondary classes. 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 200-301 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 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, “Interpreting the Routing Table and Configuring Static Routes”**: How to interpret the Routing Table and 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, using Cisco IP Phones with a DHCP server, and configuring options for both IP Phones and access points
- **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 timestamps

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: Infrastructure Management

- **Chapter 23, “Troubleshooting and Verification”:** Viewing and clearing routing tables, interpreting the **show interface** command, using commands to view and verify your infrastructure
- **Chapter 24, “Backing Up and Restoring Cisco IOS Software and Configurations”:** Boot commands for Cisco IOS software, backing up and restoring Cisco IOS software, and Secure Copy

Part VII: Wireless Technologies

- **Chapter 25, “Configuring Secure Wireless Access”:** 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 VIII: 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, “Password Recovery Procedures and the Configuration Register”:** The configuration register, password recovery procedures for routers and switches
- **Appendix E, “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 with 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, Figure 15-2, Figure 24-1, Figure 24-2 © Microsoft, 2026.

This page intentionally left blank

Variable Length Subnet Masking (VLSM)

This chapter provides information concerning the following topics:

- IP subnet zero
- VLSM example

Variable-length subnet masking (VLSM) is the more realistic way of subnetting a network to make the most efficient use of all of the bits.

Remember that when you perform classful (or what I sometimes call classical) subnetting, all subnets have the same number of hosts because they all use the same subnet mask. This leads to inefficiencies. For example, if you borrow 4 bits on a Class C network, you end up with 16 valid subnets of 14 valid hosts per subnet. A point-to-point link to another router only needs 2 hosts, but with classical subnetting, you end up wasting 12 of those hosts. Even with the ability to use NAT and private addresses, where you should never run out of addresses in a network design, you still want to ensure that the IP plan you create is as efficient as possible. This is where VLSM comes into play.

VLSM is the process of “subnetting a subnet” and using different subnet masks for different networks in your IP plan. What you have to remember is that you need to make sure that there is no overlap in any of the addresses.

IP Subnet Zero

Historically, it was always recommended that a subnet of all 0s or a subnet of all 1s not be used. Therefore, the formula of $2^N - 2$ was used to calculate the number of valid subnets created. However, Cisco devices can use those subnets, as long as the command **ip subnet-zero** is in the configuration. This command is on by default in Cisco IOS Software Release 12.0 and later; if it was turned off for some reason, however, you can reenable it by using the following command:

```
Router(config)# ip subnet-zero
```

Now you can use the formula 2^N rather than $2^N - 2$.

2^N	Number of total subnets created	
$2^N - 2$	Number of valid subnets created	No longer needed because you have the ip subnet-zero command enabled
2^H	Number of total hosts per subnet	
$2^H - 2$	Number of valid hosts per subnet	

NOTE: All of this is explained in great detail in RFC 950, *Internet Standard for Subnetting Procedure* (August 1985).

NOTE: RFC 1878, *Variable Length Subnet Table for IPv4* (December 1995), states, “This practice [of excluding all-zeros and all-ones subnets] is obsolete. Modern software will be able to utilize all definable networks.”

VLSM Example

NOTE: In this example, I use serial links between routers to help differentiate these networks from Ethernet networks where hosts usually reside. In today’s more modern networks, Ethernet links are used almost exclusively between routers, and serial links are obsolete. However, using serial links is a very cost-effective way to set up a testing lab for learning purposes; I have seen home labs, school labs, and corporate training labs use serial links for this reason. If you were to use Ethernet links instead of serial links in this example, you would still have to follow the same rules—only two addresses are required for the connection, one per router interface.

You follow the same steps in performing VLSM as you did when performing classical subnetting.

Consider Figure 3-1 as you work through an example.

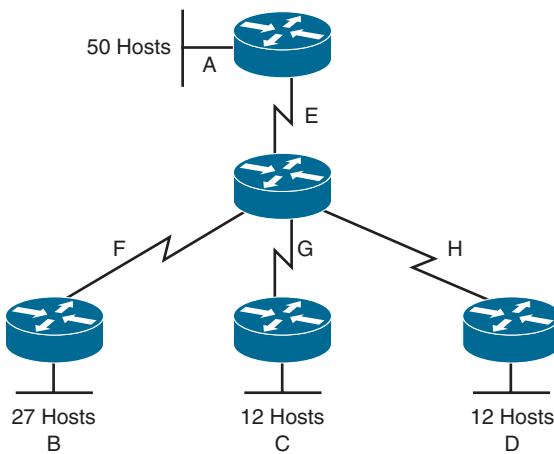


Figure 3-1 Sample Network Needing a VLSM Address Plan

A Class C network—192.168.100.0/24—is assigned. You need to create an IP plan for this network using VLSM.

Once again, you cannot use the N bits—192.168.100. You can use only the H bits. Therefore, ignore the N bits because they cannot change!

The steps to create an IP plan using VLSM for the network illustrated in Figure 3-1 are as follows:

- Step 1.** Determine how many H bits will be needed to satisfy the *largest* network.
- Step 2.** Pick a subnet for the largest network to use.
- Step 3.** Pick the next largest network to work with.

Step 4. Pick the third largest network to work with.

Step 5. Determine network numbers for serial links.

The remainder of the chapter details what is involved with each step of the process.

Step 1: Determine How Many H Bits Will Be Needed to Satisfy the *Largest* Network

Network A is the largest network with 50 hosts. Therefore, you need to know how many H bits will be needed:

If $2^H - 2 =$ Number of valid hosts per subnet

Then $2^H - 2 \geq 50$

Therefore H = 6 (6 is the smallest valid value for H)

You need 6 H bits to satisfy the requirements of Network A.

If you need 6 H bits and you started with 8 N bits, you are left with $8 - 6 = 2$ N bits to create subnets:

Started with: NNNNNNNN (these are the 8 bits in the fourth octet)

Now have: NNHHHHHH

All subnetting will now have to start at this reference point to satisfy the requirements of Network A.

Step 2: Pick a Subnet for the Largest Network to Use

You have 2 N bits to work with, leaving you with 2^N or 2^2 or 4 subnets to work with:

NN = 00HHHHHH (The Hs = The 6 H bits you need for Network A)

01HHHHHH

10HHHHHH

11HHHHHH

If you add all 0s to the H bits, you are left with the network numbers for the four subnets:

00000000 = .0

01000000 = .64

10000000 = .128

11000000 = .192

All of these subnets will have the same subnet mask, just like in classful subnetting.

Two borrowed H bits means a subnet mask of

11111111.11111111.11111111.11000000

or

255.255.255.192

or

/26

The /x notation represents how to show different subnet masks when using VLSM.

/8 means that the first 8 bits of the address are network; the remaining 24 bits are H bits.

/24 means that the first 24 bits are network; the last 8 are host. This is either a traditional default Class C address, a traditional Class A network that has borrowed 16 bits, or even a traditional Class B network that has borrowed 8 bits!

Pick *one* of these subnets to use for Network A. The rest of the networks will have to use the other three subnets.

For purposes of this example, pick the .64 network.

00000000 =	.0	
01000000 =	.64	Network A
10000000 =	.128	
11000000 =	.192	

Step 3: Pick the Next Largest Network to Work With

Network B = 27 hosts

Determine the number of H bits needed for this network:

$$2^H - 2 \geq 27$$

$$H = 5$$

You need 5 H bits to satisfy the requirements of Network B.

You started with a pattern of 2 N bits and 6 H bits for Network A. You have to maintain that pattern.

Pick one of the remaining /26 networks to work with Network B.

For the purposes of this example, select the .128/26 network:

10000000

But you need only 5 H bits, not 6. Therefore, you are left with

10N00000

where

10 represents the original pattern of subnetting.

N represents the extra bit.

00000 represents the 5 H bits you need for Network B.

Because you have this extra bit, you can create two smaller subnets from the original subnet:

10000000

10100000

Converted to decimal, these subnets are as follows:

10000000 = .128

10100000 = .160

You have now subnetted a subnet! This is the basis of VLSM.

Each of these sub-subnets will have a new subnet mask. The original subnet mask of /24 was changed into /26 for Network A. You then take one of these /26 networks and break it into two /27 networks:

10000000 and **10100000** both have 3 N bits and 5 H bits.

The mask now equals:

11111111.11111111.11111111.11100000

or

255.255.255.224

or

/27

Pick one of these new sub-subnets for Network B:

10000000 /27 = Network B

Use the remaining sub-subnet for future growth, or you can break it down further if needed.

You want to make sure the addresses are not overlapping with each other. So go back to the original table.

00000000 =	.0/26	
01000000 =	.64/26	Network A
10000000 =	.128/26	
11000000 =	.192/26	

You can now break the .128/26 network into two smaller /27 networks and assign Network B.

00000000 =	.0/26	
01000000 =	.64/26	Network A
10000000 =	.128/26	Cannot use because it has been subnetted
10000000 =	.128/27	Network B
10100000 =	.160/27	
11000000 =	.192/26	

The remaining networks are still available to be assigned to networks or subnetted further for better efficiency.

Step 4: Pick the Third Largest Network to Work With

Networks C and Network D = 12 hosts each

Determine the number of H bits needed for these networks:

$$2^H - 2 \geq 12$$

$$H = 4$$

You need 4 H bits to satisfy the requirements of Network C and Network D.

You started with a pattern of 2 N bits and 6 H bits for Network A. You have to maintain that pattern.

You now have a choice as to where to put these networks. You could go to a different /26 network, or you could go to a /27 network and try to fit them into there.

For the purposes of this example, select the other /27 network—.160/27:

10100000 (The 1 in the third bit place is no longer bold because it is part of the N bits.)

But you only need 4 H bits, not 5. Therefore, you are left with

101N0000

where

10 represents the original pattern of subnetting.

N represents the extra bit you have.

00000 represents the 5 H bits you need for Networks C and D.

Because you have this extra bit, you can create two smaller subnets from the original subnet:

101**0**0000

101**1**0000

Converted to decimal, these subnets are as follows:

101**0**0000 = .160

101**1**0000 = .176

These new sub-subnets will now have new subnet masks. Each sub-subnet now has 4 N bits and 4 H bits, so their new masks will be

11111111.11111111.11111111.11110000

or

255.255.255.240

or

/28

Pick one of these new sub-subnets for Network C and one for Network D.

00000000 =	.0/26	
01000000 =	.64/26	Network A
10000000 =	.128/26	Cannot use because it has been subnetted
10000000 =	.128/27	Network B
10100000 =	.160/27	Cannot use because it has been subnetted
10100000	.160/28	Network C
10110000	.176/28	Network D
11000000 =	.192/26	

You have now used two of the original four subnets to satisfy the requirements of four networks. Now all you need to do is determine the network numbers for the serial links between the routers.

Step 5: Determine Network Numbers for Serial Links

All serial links between routers have the same property in that they only need two addresses in a network—one for each router interface. Remember that if you use Ethernet links here instead of serial links, you still only need two addresses, one for each router interface.

Determine the number of H bits needed for these networks:

$$2^H - 2 \geq 2$$

$$H = 2$$

You need 2 H bits to satisfy the requirements of Networks E, F, G, and H.

You have two of the original subnets left to work with.

For the purposes of this example, select the .0/26 network:

00000000

But you need only 2 H bits, not 6. Therefore, you are left with

00NNNN00

where

00 represents the original pattern of subnetting.

NNNN represents the extra bits you have.

00 represents the 2 H bits you need for the serial links.

Because you have 4 N bits, you can create 16 sub-subnets from the original subnet:

00000000 = .0/30

00000100 = .4/30

00001000 = .8/30

00001100 = .12/30

00010000 = .16/30

...

00111000 = .56/30

00111100 = .60/30

You need only four of them. You can hold the rest for future expansion or recombine them for a new, larger subnet:

00010000 = .16/30

00010100 = .20/30

00011000 = .24/30

00011100 = .32/30

...

00111000 = .56/30

00111100 = .60/30

The first four of these can be combined into the following:

00010000 = .16/28

The rest of the /30 subnets can be combined into two /28 networks:

00100000 = .32/28

00110000 = .48/28

Or these two subnets can be combined into one larger /27 network:

00010000 = .32/27

Going back to the original table, you now have the following:

00000000 =	.0/26	Cannot use because it has been subnetted
00000000 =	.0/30	Network E
00000100 =	.4/30	Network F
00001000 =	.8/30	Network G
00001100 =	.12/30	Network H
00010000 =	.16/28	Future growth
00100000 =	.32/27	Future growth
01000000 =	.64/26	Network A
10000000 =	.128/26	Cannot use because it has been subnetted
10000000 =	.128/27	Network B
10100000 =	.160/27	Cannot use because it has been subnetted
10100000	.160/28	Network C
10110000	.176/28	Network D
11000000 =	.192/26	Future growth

Looking at the plan, you can see that no number is used twice. You have now created an IP plan for the network and have made the plan as efficient as possible, wasting no addresses in the serial links and leaving room for future growth. This is the power of VLSM!

Numbers

8N1 settings, 53

A

access 1 switches, configuration, 116

access 2 switches, configuration, 116

access commands, 224

Access Control Lists (ACLs). *See* ACLs
(Access Control Lists)

access lists, NTP (Network Time
Protocol), accessing, 194

access points, DHCP servers, 174–175

access switches, 105

ACLs (Access Control Lists), 215–216

application, 218

comments, 224

configuration, 225

creating named, Configuration
mode, 222–223

creating standard, 217–218

established keyword, 220

extended

applying, 220

creating, 219

interfaces, application, 218

IOS versus IOS XE, 225–226

IOS XE, second interface, 226–227

IPv4, 228–230

IPv6, 227

configuration, 230–231

keywords, 217

log keyword, 220–221

multiple nonconsecutive ports with
eq, 227

removing, 218

restricting virtual terminal access,
224

sequence numbers, 223

verification, 218

wildcard masks, 216

Active interface mode (EtherChannel), 120

AD (administrative distance), static routes,
155–156

addresses, classless, 7–9

address plans, VLSM (variable-length
subnet masking), 25

addresses

anycast, 50

broadcast, 3–4

embedded, 48

flat, 2

global unicast, 46–47

hierarchical, 1

IP, decimal/binary conversions,
287–288

IPv4, 1–2

appearance, 2

binary ANDing, 17–21

classes, 4–5

design, 3–4

masks, 2, 3

network (N) bits, 5–6

node (H) bits, 5–6

subnetting, 11–21

IPv4-mapped IPv6, 48

IPv6, 39–40

appearance, 39–40

prefix length notation, 43–44

reducing notation, 41–43

types, 45–50

- local, 7
- loopback, 47
- MAC, 2
 - configuring sticky, 205–206
- multicast, 48–50
- network, 3–4
- node, 3–4
- remote IP, local host name routing, 141
- RFC (Private) 1918, 6
- unicast, 45–46
- unique local, 47–48
- unspecified, 47

administrative distance (AD), static routes, 155–156

aging time, MAC table, setting maximum, 77

all-0's hexet, omitting, 42

ALSwitch1, configuration, 202

ALSwitch1 commands, 127

ALSwitch2, configuration, 202

ALSwitch2 commands, 128

anycast addresses, 50

APs (access points), WLANs (wireless LANs), 273–276

archive config command, 234

Austin router, 170

authentication, NTP (Network Time Protocol), 193–194

Auto interface mode (EtherChannel), 120

autosense, switches, 57

B

backing up configurations, TFTP servers, 258

binary ANDing, 17–21

binary numbers

- conversion chart, 293–296

- converting from decimals, 285–286

- converting from hexadecimal numbers, 288–289

- converting to decimals, 286–287

- converting to hexadecimal numbers, 289–290

- counting, 279–280

- representing, 282–283

bits, configuration register, 302

boot field, configuration register, 302–303

boot system commands, 255–256, 303

BPDU Filter, STP (Spanning Tree Protocol), configuration, 111

BPDU Guard, STP (Spanning Tree Protocol), configuration, 110–111

broadcast addresses, 3–4

broadcast communication, 1

Buffalo routers, 147–148

C

cables

- choosing, 56–57

- crossover, 57

- pinouts, 57

- rollover, 57, 58

- connecting, 51

- serial, 53–56

- standards, 57–58

- straight-through, 57, 58

- T568 cables, 58

- USB, connecting, 52

CAM (Content Addressable Memory) table, 204

CDP (Cisco Discovery Protocol), 129

- configuration, 129

- design, 130

- troubleshooting, 130

- verification, 130

CIDR (classless interdomain routing), 4

Cisco Discovery Protocol (CDP). *See* CDP (Cisco Discovery Protocol)

Cisco IOS File System, 256

Cisco IOS software

- backing up from TFTP server, 259

- restoring and upgrading from TFTP server, 259–260

- restoring from Xmodem, 260–263

Cisco IP phones, DHCP servers, 174

- Cisco routers
 - interfaces
 - moving between, 138
 - names, 135–138
 - serial, 139
 - IPv4 addresses, assigning, 139–140
 - local host name routing, 141
 - login banners, creating, 141
 - message-of-the-day banners, creating, 140–141
 - modes, 134
 - global configuration, 134
 - name configuration, 134
 - no ip domain-lookup command, 141–142
 - password configuration, 134–135
 - password encryption, 135
- Class B networks, subnetting via binary, 15–17
- Class C networks, subnetting via binary, 12–15
- classes, IPv4 addresses, 4–5
- classless addresses, 7–9
- classless interdomain routing (CIDR), 4
- clearing, 244
 - routing table, 244
- CLI (command-line interface). *See*
 - command-line interface, changing console line speed, 303
- clock, routers, setting, 195–198
- clock command, 251
- codes, routing table, 149–150
- command-line interface, 59
 - console error messages, 60
 - keyboard help, 63–64
 - setup mode, 62–63
- commands
 - access, 224
 - ALSwitch1, 127
 - ALSwitch2, 128
 - archive config, 234
 - boot system, 255–256, 303
 - clock, 251
 - completing with key, 60
 - copy running-config startup-config, 84
 - debug, 250
 - default, 66–67
 - disable, 62
 - DLSwitch, 126
 - do, 145
 - enable, 61, 237
 - end, 61
 - EXEC, 145
 - exec-timeout, 143–144
 - exit, 61
 - generic host networking, 251–252
 - help, switch configuration, 70
 - history, 64
 - interface vlan, 73
 - ip address dhcp, 176
 - ip default-network, 244
 - ip host, 253
 - ip http server, 252
 - ip name-server, 142
 - IP subnet-zero, 23–24
 - L2Switch1, 102
 - L2Switch2, 99–100
 - L3Switch, 122–123
 - L3Switch1, 99–101
 - logging console, 221
 - logging synchronous, 143
 - logout, 62
 - mdix auto, 75–76
 - more, pipe (|) parameter, 65–66
 - netsh, 252
 - netstat, 151–152
 - network, 164–166
 - no ip domain-lookup, 141–142
 - path, 234
 - ping, 245–247
 - question mark, 60–61
 - range, 82
 - reload, 62
 - remark, 224
 - Router, 129–130
 - shortcuts, 59
 - show, 65, 144–145
 - pipe (|) parameter, 65–66
 - show controllers, 250
 - show interface, 247–249
 - show running-config, 134

- show users, 254
- shutdown, 85–87, 248
- state, 85–87
- Switch, 122
- switchport mode access, 82
- terminal, 64–65
- traceroute, 249–250
- transport preferred none, 142
- write, 144
- write-memory, 234
- comments, ACLs (Access Control Lists), 224
- company routers, 188–189
- configuration
 - ACLs (Access Control Lists), 225
 - CDP (Cisco Discovery Protocol), 129
 - DAI (Dynamic ARP Inspection), 209–210
 - DHCP client, 177–179
 - DHCP servers, verifying and troubleshooting, 175–176
 - Dynamic NAT, 181–183
 - EtherChannel
 - default, 120
 - example, 126–128
 - guidelines, 120–121
 - Layer 2, 120–121
 - Layer 3, 122–123
 - load balancing, 123
 - Ethernet management port, 74–75
 - hot-standby ports (LACP), 124
 - IOS routers, 173–174
 - IPv6, ACLs (Access Control Lists), 230–231
 - LLDP (Link Layer Discovery Protocol), 131
 - configuration, 131
 - NAT (Network Address Translation), 181–182
 - NTP (Network Time Protocol), 191–192, 199–202
 - OSPF (Open Shortest Path First), verification, 168
 - passwords, 237
 - PAT (Public Address Translation), 183–186
 - example, 187–189
 - path cost, 108
 - ports, priority, 107–108
 - PVST+ (Per VLAN Spanning Tree), 113–117
 - root switches, 106
 - secondary, 106
 - routers
 - erasing, 144
 - example, 146–148
 - saving, 144
 - verification, 144–145
 - routing table routes, 156–157
 - SCP (Secure Copy) servers, 263–265
 - static MAC addresses, 204
 - static routes, 158–159
 - sticky MAC addresses, 205–206
 - STP (Spanning Tree Protocol)
 - BPDU Filter, 111
 - BPDU Guard, 110–111
 - extended system ID, 112
 - PortFast, 109–110
 - Root Guard, 112
 - timers, 109
 - switch port security, 205
 - switch security, configuration
 - example, 210–213
 - switches, 69
 - command modes, 70
 - command verification, 70–71
 - descriptions, 75–76
 - duplex operations, 76
 - example, 77–79
 - gateways, 73
 - help commands, 70
 - host names, 71–72
 - IP addresses, 73
 - MAC table maximum aging
 - time, 77
 - operation speed, 76
 - priority, 106–107
 - resetting, 71
 - setting passwords, 72–73

- syslog, 235
- terminal emulators, 52–53
- VLANs
 - erasing, 84–85
 - example, 87–88
 - path cost, 108
 - port priority, 107–108
 - saving, 84
 - switch priority, 106–107
- WLANs (wireless LANs), 271–272
- configuration menu, IOS XE WLC, 268
- Configuration mode, named ACLs, 222–223
- configuration register, 301–302
 - bits, 302
 - console terminal baud rate settings, 303
- connections
 - LANs (local area networks), 53
 - ports, 57
 - rollover cables, 51
 - serial, 53
 - USB cables, 52
- console line speed
 - changing
 - CLI (command-line interface), 303
 - ROM Monitor mode (Xmodem), 304–305
- console terminal baud rate settings, configuration register, 303
- Content Addressable Memory (CAM), 204
- conversion chart, binary numbers, decimals, and hexadecimal numbers, 293–296
- copy running-config startup-config command, 84
- core switches, configuration, 114–115
- Core1 routers, configuration, 199–200
- Core2 routers, configuration, 200–201
- CORP routers, inter-VLAN communication, 97–99
- counting in
 - binary numbers, 279–280
 - decimals, 277–279
 - hexadecimal numbers, 280–282
- crossover cables, 57

D

- DAI (Dynamic ARP Inspection), configuration, 209–210
- dashboard, IOS XE WLC, 268
- Data VLANs, 82
- debug command, 250
- decimals
 - conversion chart, 293–296
 - converting from binary numbers, 286–287
 - converting from hexadecimal numbers, 291–292
 - converting to binary numbers, 285–286
 - converting to hexadecimal numbers, 290–291
 - counting, 277–279
 - representing, 282–283
- default commands, 66–67
- default route, routing table, 150–153
- deny statement, 218, 231
- design, NTP (Network Time Protocol), 192–193
- Desirable interface mode (EtherChannel), 120
- devices
 - hardening, 236
 - disabling unneeded services, 242
 - password configuration, 237
 - password encryption, 238–239
 - restricting virtual terminal access, 241
 - SSH (Secure Shell), 240–241
 - monitoring, 233
 - configuration backups, 233–234
 - logging, 234–236
 - remote Telnet connection, 252–253
 - URL prefixes, 256–257
- DHCP (Dynamic Host Configuration Protocol)
 - helper address, 176–177
 - snooping, 207–209
- DHCP client, configuring, 177–179

DHCP servers

- access points, 174–175
 - Cisco IP phones, 174
 - configuration, verifying and troubleshooting, 175–176
 - IOS routers, configuring, 173–174
- disable command, 62
- distribution 1 switches, configuration, 115
- distribution 2 switches, configuration, 115
- DLSwitch commands, 126
- DLSwitch1, configuration, 201
- DLSwitch2, configuration, 201
- do command, 145
- DTP (Dynamic Trunking Protocol), 90
- duplex operations, switches, 76
- Dynamic NAT, 181–183
- Dynamic Trunking Protocol (DTP), 90

E

- Edmonton router, 178–179
- embedded addresses, 48
- enable command, 61
- enable commands, 237
- encapsulation types, VLANs, 90–91
- encryption, passwords, 238–239
- end command, 61
- erasing configurations, routers, 144
- error messages, console, 60
- error-disabled ports, recovering
 - automatically, 207
- established keyword, ACLs (Access Control Lists), 220
- EtherChannel, 119
 - configuration, example, 126–128
 - configuring
 - guidelines, 120–121
 - Layer 2, 120–121
 - Layer 3, 122–123
 - load balancing, 123
 - default configuration, 120
 - interface modes, 119–120
 - LACP (Link Aggregation Control Protocol), 119
 - configuring hot-standby ports, 124

monitoring, 125

PAP (Port Aggregation Protocol), 119

verification, 125

Ethernet cables, 53

Ethernet management port, 73–75

EXEC commands, 145

exec-timeout command, 143–144

exit command, 61

extended ACLs

applying, 220

creating, 219

extended system ID, STP (Spanning Tree Protocol), 112

F

- Fast Ethernet interface, IPv4 addresses,
 - assigning, 139
- flat addresses, 2
- floating static routes, 155–156
- fully specified static routes, 154

G

- Galveston router, 171–172
- gateways, switches, configuring, 73
- General tab, 269
- generic host networking commands, 251–252
- Gibbons router, 179
- Gigabit Ethernet interface, IPv4 addresses,
 - assigning, 139–140
- Gio/0 port, 73–75
- global configuration mode, Cisco routers, 134
- global unicast addresses, 46–47
- Graziani, Rick, 39–40

H

- hardening devices, 236
 - password configuration, 237
 - password encryption, 238–239
 - restricting virtual terminal access, 241

SSH (Secure Shell), 240–241
 unneeded services, disabling, 242

Help, commands, 60–61

help commands, switch configuration, 70

hexadecimal numbers
 conversion chart, 293–296
 converting from binary numbers, 289–290
 converting from decimals, 290–291
 converting to binary numbers, 288–289
 converting to decimals, 291–292
 counting, 280–282
 representing, 282–283

hextets, 40

hierarchical addresses, 1

history commands, 64

host names, setting, 71–72

host networking commands, 251–252

hot-standby ports (LACP), configuration, 124

Houston router, 170–171

I

ICMP (Internet Control Message Protocol), 245

IFS (IOS File System), 256

image filenames (IOS), deciphering image, 257

interface configuration mode, OSPF (Open Shortest Path First), 165–166

interface counters, clearing, 249

interface modes, EtherChannel, 119–120

interface vlan command, 73

interfaces
 ACLs (Access Control Lists), applying, 218
 Cisco routers
 names, 135–138
 serial, 139
 status codes, 247–249

Internet Control Message Protocol (ICMP), 245

interpreting, routing table, 149

inter-VLAN communication
 CORP routers, 97–99
 ISP routers, 96–97
 Layer 3 switches, 94–96
 routers, 93–94
 switches, L2Switch2, 97–99

IOS
 ACLs (Access Control Lists), versus IOS XE, 225–226
 deciphering image filenames, 257

IOS File System (IFS), 256

IOS routers, configuring, 173–174

IOS software
 backing up from TFTP server, 259
 restoring and upgrading from TFTP server, 259–260
 restoring from Xmodem, 260–263

IOS XE
 ACLs (Access Control Lists)
 versus IOS, 225–226
 second interface, 226–227
 WLC (wireless LAN controller), connecting to, 267–276

ip address dhcp command, 176

IP addresses
 decimal, binary conversions, 287–288
 switches, configuring, 73

ip default-network command, 244

ip host command, 253

ip http server command, 252

ip name-server command, 142

IP phones, DHCP servers, 174

IP subnet-zero command, 23–24

IPv4, ACLs (Access Control Lists), 228–230

IPv4 addresses, 1–2. *See also* routing table
 appearance, 2
 binary ANDing, 17–21
 classes, 4–5
 design, 3–4
 embedded, 48
 Fast Ethernet interface, assigning to, 139–140
 masks, 2
 writing, 3
 network (N) bits, 5–6

- node (H) bits, 5–6
- subnetting, 11–12
 - Class B via binary, 15–17
 - Class C via binary, 12–15
- IPv6, ACLs (Access Control Lists), 227, 230–231
- IPv6 addresses, 39–40
 - appearance, 39–40
 - prefix length notation, 43–44
 - reducing notation, 41–43
 - types, 45–50
- IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6*, 39–40
- ISP routers, 187–188
 - inter-VLAN communication, 96–97

J

- Juneau router, 158

K

- Ketcikan router, 157–158
- keyboard help, 63–64
- keywords, ACLs (Access Control Lists), 217

L

- L2Switch1 commands, 102
- L2Switch2 commands, 99–100
- L3Switch commands, 122–123
- L3Switch1 commands, 99–101
- LACP (Link Aggregation Control Protocol), 119
 - hot-standby ports, configuring, 124
- LANs (local area networks)
 - connections, 53
 - WLC (wireless LAN controller), connecting to, 267–276
- Layer 2 EtherChannel, configuration, 122
- Layer 3 EtherChannel, configuration, 122–123
- Layer 3 switches, inter-VLAN communication, 94–96

- leading 0's, omitting, 41
- leading bit patterns, 4
- Level Two security
 - DAI (Dynamic ARP Inspection), configuration, 209–210
 - DHCP snooping, 207–209
 - error-disabled ports, Autorecovery, 207
 - static MAC addresses, configuration, 204
 - sticky MAC addresses, configuration, 205–206
 - switch port
 - configuration, 205
 - verification, 206
 - switches, configuration, 210–213
- link aggregation, 119
- Link Aggregation Control Protocol (LACP). *See* LACP (Link Aggregation Control Protocol)
- Link Layer Discovery Protocol (LLDP). *See* LLDP (Link Layer Discovery Protocol)
- LLDP (Link Layer Discovery Protocol), 131
 - configuration, 131
 - troubleshooting, 132
 - verification, 132
- load balancing, EtherChannel, configuration, 123
- local addresses, 7
- local networks, 19
- log keyword, ACLs (Access Control Lists), 220–221
- logging, device monitoring, 234–236
- logging console command, 221
- logging synchronous command, 143
- login banners, creating, 141
- logout command, 62
- loopback addresses, 47

M

- MAC addresses, 2
 - configuring static, 204
 - sticky, configuration, 205–206

MAC table, maximum aging time, setting, 77

many private to one PAT, configuring, 183–185

masks, 2. *See also* VLSM (variable-length subnet masking)
writing, 3

mdix auto command, 75–76

message format, syslog, 235

message-of-the-day banners, creating, 140–141

modes, Cisco routers, 134

monitoring
devices, 233
configuration backups, 233–234
logging, 234–236
EtherChannel, 125

more commands, pipe (|) parameter, 65–66

multicast addresses, 48–50

multicast communication, 5

multiple nonconsecutive ports with eq, ACLs (Access Control Lists), 227

N

names, Cisco router interfaces, 135–138

NAT (Network Address Translation)
configuring, 181–182
troubleshooting, 187
verification, 186

netsh command, 252

netstat command, 151–152

network (N) bits, 5–6

network command, 164–166

network devices, URL prefixes, 256–257

network masks, 2
writing, 3

Network Time Protocol (NTP). *See* NTP (Network Time Protocol)

network types, OSPF (Open Shortest Path First), 161–162

networks
Class B, subnetting via binary, 15–17
Class C, subnetting via binary, 12–15
LANs (local area networks), connections, 53

local, 19
remote, 19

network addresses, 3–4

no command, 66–67

no ip domain-lookup command, 141–142

node (H) bits, 5–6

node addresses, 3–4

notation, IPv6 addresses, reducing, 41–43

NTP (Network Time Protocol), 191
authentication, 193–194
configuration, 199–202
configuring, 191–192
design, 192–193
limiting access lists, 194
setting clock on router, 195–198
time stamps, 199
troubleshooting, 195
verification, 195

O

omitting
all-0's hexet, 42
leading 0's, 41

On interface mode (EtherChannel), 119

Open Shortest Path First (OSPF). *See* OSPF (Open Shortest Path First)

operation speed, switches, 76

OSPF (Open Shortest Path First), 161
configuration verification, 168
configuring, 162–164
interface configuration mode, 165–166
network types, 161–162
OSPFv2 versus OSPFv3, 161–162
parameter optimization, 166–168
troubleshooting, 169–172
wildcard masks, 163–165

P

PAP (Port Aggregation Protocol), 119

parameters, OSPF (Open Shortest Path First), optimization, 166–168

Passive interface mode (EtherChannel), 120

passwords

- Cisco routers
 - configuration, 134–135
 - encryption, 135
- configuring, 237
- encryption, 238–239
- recovery
 - routers, 305–306
 - switches, 306–307
- secret, 239
- switches, setting, 72–73, 203–204

PAT (Public Address Translation)

- configuring, 183–186
 - example, 187–189
 - troubleshooting, 187
 - verification, 186
- many private to one PAT, 183–185
- private to one permanent PAT, 185–186

path command, 234

path cost, configuring, priority, 108

permanent keyword, routing table, 155

permit any statement, 218

ping command, 245–247

pinouts, cables, 57

pipe (|) parameter, show and more commands, 65–66

policies, WLANs (wireless LANs), creating, 272–275

Port Aggregation Protocol (PAP), 119

Portable Command Guide, 53port-channel. *See* EtherChannel

PortFast, STP (Spanning Tree Protocol), configuration, 109–110

ports

- configuration, 205
- configuring, priority, 107–108
- connections, 57
- error-disabled, Autorecovery, 207
- Ethernet management, 73–75
- hot-standby ports (LACP), configuration, 124
- verification, 206
- VLANs, assigning, 82

prefix length notation, IPv6 addresses, 43–44

prefixes, URLs, 256–257

private IP addresses, RFC (Private) 1918 addresses, 181

private to one permanent PAT, configuring, 185–186

protocols. *See also* STP (Spanning Tree Protocol); *specific protocols*

CDP (Cisco Discovery Protocol), 129

configuration, 129

design, 130

troubleshooting, 130

verification, 130

DHCP (Dynamic Host Configuration Protocol), snooping, 207–209

DTP (Dynamic Trunking Protocol), 90

ICMP (Internet Control Message Protocol), 245

LACP (Link Aggregation Control Protocol), 119

LLDP (Link Layer Discovery Protocol), 131

troubleshooting, 132

verification, 132

NTP (Network Time Protocol), 191

authentication, 193–194

configuration, 199–202

configuring, 191–192

design, 192–193

limiting access lists, 194

setting clock on router, 195–198

time stamps, 199

troubleshooting, 195

verification, 195

PAP (Port Aggregation Protocol), 119

STP (Spanning Tree Protocol), 104–105

mode changes, 105

troubleshooting, 113

VTP (VLAN Trunking Protocol), 91–93

PVST+ (Per VLAN Spanning Tree), 104 configuration, 113–117

Q

question mark, commands, 60–61

R

range command, 82

Rapid PVST+, 104

recovering passwords

 routers, 305–306

 stackwise deployments, 306–307

 switches, 306–307

recursive lookups, static routes, 153–156

reference topology, routing table, 153

reload command, 62

remark command, 224

remote IP addresses, local host name

 routing, 141

remote networks, 19

restoring configurations, TFTP servers, 258

RFC (Private) 1918 addresses, 6

 private IP addresses, 181

rollover cables, 57, 58

 connecting, 51

ROM Monitor mode (Xmodem)

 changing console line speed,

 304–305

 restoring Cisco IOS software from,

 260–263

Root Guard, STP (Spanning Tree

 Protocol), configuration, 112

root switches

 configuring, 106

 secondary, 106

route flapping, 38

route summarization, 33–38

 requirements, 38

 route flapping, 38

Router commands, 129–130

routers

 Austin, 170

 Boston, 146–147

 Buffalo, 147–148

 Cisco

 global configuration mode, 134

 modes, 134

 Cisco routers

 assigning IPv4 addresses,

 139–140

 creating login banners, 141

 creating message-of-the-day

 banners, 140–141

 interface names, 135–138

 IPv4 address assignments,

 139–140

 local host name routing, 141

 moving between interfaces, 138

 name configuration, 134

 no ip domain-lookup command,

 141–142

 password configuration, 134–135

 password encryption, 135

 serial interfaces, 139

 clock, setting, 195–198

 company, 188–189

 configuration

 erasing, 144

 example, 146–148

 NTP (Network Time Protocol),

 199–202

 saving, 144

 verification, 144–145

 connecting rollover cables, 51

 connecting USB cables, 52

 connections, 57

 CORP, inter-VLAN communication,

 97–99

 DNS, 142–143

 Edmonton, 178–179

 Galveston, 171–172

 Gibbons, 179

 Houston, 170–171

 inter-VLAN communication, 93–94

 ISP, 187–188

 inter-VLAN communication,

 96–97

 Juneau, 158

 Ketcikan, 157–158

 last routing update, 244–245

 password-recovery procedures,

 305–306

 Sitka, 158

routes

- routing table
 - configuring, 156–157
 - default, 150–153
 - static, 153–156

routing table

- clearing, 244
- codes, 149–150
- default route, 150–153
- interpreting, 149
- Juneau router, 158
- Ketcikan router, 157–158
- permanent keyword, 155
- reference topology, 153
- routes
 - configuring, 156–157
 - static, 153–156
- Sitka router, 158
- static routes, configuring, 158–159
- viewing, 243–244

S

saving, router configurations, 144

- SCP (Secure Copy), 263
 - configuration, 263–265
 - SSH (Secure Shell) configuration, 263
 - troubleshooting, 264
 - verification, 264

secret password, 239

Secure Copy (SCP). *See* SCP (Secure Copy)

security

- Level Two security
 - DAI (Dynamic ARP Inspection), 209–210
 - DHCP snooping, 207–209
 - error-disabled ports, 207
 - port verification, 206
 - static MAC addresses, 204
 - sticky MAC addresses, 205–206
 - switch port, 205
- NTP (Network Time Protocol)
 - authentication, 193–194
 - limiting access lists, 194

troubleshooting, 195

verification, 195

switches, configuration, 210–213

sequence numbers, ACLs (Access Control Lists), 223

serial cables, 53–56

serial interfaces, Cisco routers, configuring, 139

serial links, VLSM (variable-length subnet masking), determining network numbers, 30–31

servers

SCP (Secure Copy), configuration, 263–265

TFTP

backing up CISCO IOS software to, 259

backing up configurations, 258

restoring and upgrading CISCO IOS software from, 259–260

restoring configurations, 258

setup mode (CLI), 62–63

severity levels, syslog, 236

shortcuts

binary ANDing, 20–21

commands, 59

show commands, 65, 144–145

pipe (|) parameter, 65–66

show controllers command, 250

show interface command, 247–249

show ip route command, 152

show running-config command, 134

show users command, 254

shutdown command, 85–87, 248

shutting down VLANs, 85–87

Sitka router, 158

SLAs (service level agreements), 191

snooping, DHCP (Dynamic Host Configuration Protocol), 207–209

Spanning Tree Protocol (STP). *See* STP (Spanning Tree Protocol)

SSH (Secure Shell)

device hardening, 240–241

SCP (Secure Copy), 263

stackwise deployments, password-recovery procedures, 306–307

- standard ACLs, creating, 217–218
- standards, cables, 57–58
- state command, 85–87
- statements
 - deny, 218
 - permit any, 218
- static MAC addresses, configuring, 204
- static routes
 - configuring, 158–159
 - configuring, 153–156
- static VLANs, creating, 81–82
- status codes, interfaces, 247–249
- sticky MAC addresses, configuration, 205–206
- STP (Spanning Tree Protocol), 104
 - BPDU Filter, 111
 - BPDU Guard, 110–111
 - enabling, 105
 - extended system ID, 112
 - mode changes, 105
 - MSTP (Multiple Spanning Tree Protocol), 104
 - PortFast, 109–110
 - PVST+ (Per VLAN Spanning Tree), 104
 - configuration, 113–117
 - Rapid PVST+, 104
 - Root Guard, 112
 - switches
 - configuring root, 106
 - configuring secondary root, 106
 - timers, configuring, 109
 - troubleshooting, 113
 - verifying, 113
 - VLANs
 - configuring path cost, 108
 - configuring port priority, 107–108
 - configuring switch priority, 106
- straight-through cables, 57, 58
- subnetting, 9, 11–12. *See also* VLSM (variable-length subnet masking)
 - Class B networks via binary, 15–17
 - Class C networks via binary, 12–15
- subnetwork masks, 2
 - writing, 3
- suspending VLANs, 85–87
- Switch commands, 122
- switches, 204
 - access, 105
 - access 1, configuration, 116
 - access 2, configuration, 116
 - autosense, 57
 - configuring, 69
 - command modes, 70
 - command verification, 70–71
 - descriptions, 75–76
 - duplex operations, 76
 - example, 77–79
 - gateways, 73
 - help commands, 70
 - host names, 71–72
 - IP addresses, 73
 - MAC table maximum aging time, 77
 - operation speed, 76
 - priority, 106–107
 - resetting, 71
 - setting passwords, 72–73
 - connecting rollover cables, 51
 - connecting USB cables, 52
 - connections, 57
 - core, configuration, 114–115
 - distribution 1, configuration, 115
 - distribution 2, configuration, 115
 - inter-VLAN communication
 - L2Switch1, 102
 - L2Switch2, 97–99
 - L3Switch1, 99–101
 - Layer 3, inter-VLAN communication, 94–96
 - password-recovery procedures, 306–307
 - ports
 - configuration, 205
 - error-disabled ports, 207
 - verification, 206
 - root, configuring, 106
 - security, configuration example, 210–213
 - setting passwords, 203–204
- switchport mode access command, 82

syslog

- configuration, 235
- message example, 236
- message format, 235
- severity levels, 236

T

T568A cables, 58

T568B cables, 58

Telnet

- remotely connecting devices, 253
- verification, 254

terminal commands, 64–65

terminal emulators, configuring, 52–53

TFTP servers

- backing up CISCO IOS software to, 259
- backing up configurations, 258
- restoring and upgrading CISCO IOS software from, 259–260
- restoring configurations, 258

time stamps, NTP (Network Time Protocol), 199

timers, STP (Spanning Tree Protocol), configuration, 109

timestamps, 250–251

traceroute command, 249–250

traffic

- ACLs (Access Control Lists), 215–216
 - application, 218
 - applying extended, 220
 - comments, 224
 - configuration, 225
 - creating extended, 219
 - creating named, 222–223
 - creating standard, 217–218
 - established keyword, 220
 - IOS versus IOS XE, 225–226
 - IOS XE, 226–227
 - IPv4, 228–230
 - IPv6, 227, 230–231
 - keywords, 217
 - log keyword, 220–221

multiple nonconsecutive ports

with eq, 227

removing, 218

restricting virtual terminal access, 224

sequence numbers, 223

verification, 218

wildcard masks, 216

transport preferred none command, 142

troubleshooting

CDP (Cisco Discovery Protocol), 130

DHCP servers, configuration, 175–176

LLDP (Link Layer Discovery Protocol), 132

NAT (Network Address Translation), 187

NTP (Network Time Protocol), 195

OSPF (Open Shortest Path First), 169–172

PAT (Public Address Translation), 187

SCP (Secure Copy), 264

STP (Spanning Tree Protocol), 113

U

unicast addresses, 45–46

unicast communication, 1

unique local addresses, 47–48

unnneeded services, disabling, 242

unspecified addresses, 47

URLs, prefixes, 256–257

USB cables, connecting, 52

V

variable-length subnet masking (VLSM).

See VLSM (variable-length subnet masking)

verification

ACLs (Access Control Lists), 218

CDP (Cisco Discovery Protocol), 130

EtherChannel, 125
 LLDP (Link Layer Discovery Protocol), 132
 NAT (Network Address Translation), 186
 NTP (Network Time Protocol), 195
 PAT (Public Address Translation), 186
 router configurations, 144–145
 SCP (Secure Copy), 264
 switch port, 205–206
 Telnet, 254
 WLANs (wireless LANs), 276
 viewing, routing table, 243–244
 virtual terminal access
 ACLs (Access Control Lists)
 configuration, 225
 IOS versus IOS XE, 225–226
 IOS XE, 226–227
 restricting access, 224
 device hardening, restricting, 241
 VLANs
 assigning ports, 82
 configuring
 erasing configurations, 84–85
 example, 87–88
 path cost, 108
 port priority, 107–108
 saving configurations, 84
 switch priority, 106–107
 creating static, 81–82
 Data VLANs, 82
 encapsulation types, 90–91
 information verification, 83–84
 inter-VLAN communication
 CORP routers, 97–99
 ISP routers, 96–97
 L2Switch1 commands, 102
 L2Switch2 commands, 99–100
 L3Switch1 commands, 99–101
 Layer 3 switches, 94–96
 routers, 93–94
 shutting down, 85–87
 STP (Spanning Tree Protocol), 105
 suspending, 85–87
 Voice VLANs, configuring, 82–83

 VTP (VLAN Trunking Protocol), 91–93
 VLSM (variable-length subnet masking), 23
 address plan, 25
 choosing largest network, 26–28
 choosing subnets, 25–26
 choosing third-largest network, 28–29
 IP subnet-zero command, 23–24
 serial links, determining network numbers, 30–31
 Voice VLANs, configuring, 82–83
 VTP (VLAN Trunking Protocol), 91–93

W

wildcard masks
 ACLs (Access Control Lists), 216
 OSPF (Open Shortest Path First), 163–165
 wireless LAN controller (WLC). *See* WLC (wireless LAN controller)
 wireless LANs (WLANs). *See* WLANs (wireless LANs)
 WLANs (wireless LANs)
 adding, 269–270
 APs (access points), 273–276
 configuration, 271–272
 defining, 270
 policies, 272–275
 verification, 276
 WLC (wireless LAN controller), 267
 connecting to, 267
 workstations, configuring, 52–53
 write command, 144
 write-memory command, 234
 writing, masks, 3

X

Xmodem
 console line speed, 304–305
 restoring Cisco IOS software from, 260–263