

31 Days Before Your **CCNA** Exam (200-301)

A Day-By-Day Review Guide for the
CCNA 200-301 Certification Exam

2nd Edition

ciscopress.com

Allan Johnson

FREE SAMPLE CHAPTER |



31 Days Before Your CCNA Exam

A Day-by-Day Review
Guide for the CCNA 200-301
Certification Exam

Second Edition

Allan Johnson

31 Days Before Your CCNA Exam

Allan Johnson

Copyright© 2025 Cisco Systems, Inc.

Published by:
Cisco Press

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 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: 2024944817

ISBN-13: 978-0-13-821425-8

ISBN-10: 0-13-821425-5

Warning and Disclaimer

This book is designed to provide information about exam topics for the Cisco Certified Networking Associate (CCNA) certification. 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.

Please contact us with concerns about any potential bias at <https://www.pearson.com/report-bias.html>.

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.

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.

Microsoft® Windows®, and Microsoft Office® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

Special Sales

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

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

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Feedback Information

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

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

We greatly appreciate your assistance.

Please contact us with concerns about any potential bias at <https://www.pearson.com/report-bias.html>.

GM K12, Early Career and Professional Learning

Alliances Manager, Cisco Press

Director, ITP Product Management

Executive Editor

Managing Editor

Development Editor

Senior Project Editor

Copy Editor

Editorial Assistant

Designer

Composition

Indexer

Proofreader

Soo Kang

Caroline Antonio

Brett Bartow

James Manly

Sandra Schroeder

Christopher Cleveland

Mandie Frank

Kitty Wilson

Cindy Teeters

Chuti Prasertsith

codeMantra

Timothy Wright

Donna E. Mulder

About the Author

Allan Johnson entered the academic world in 1999 after 10 years as a business owner/operator to dedicate his efforts to his passion for teaching. He holds both an MBA and an MEd in training and development. He taught CCNA courses at the high school level for 7 years and has taught both CCNA and CCNP courses at Del Mar College in Corpus Christi, Texas. In 2003, Allan began to commit much of his time and energy to the CCNA Instructional Support Team, providing services to Networking Academy instructors worldwide and creating training materials. He now splits his time between working as a Curriculum Lead for Cisco Networking Academy and as Account Lead for Unicon (unicon.net), supporting Cisco's educational efforts.

Dedications

For my wife, Becky. Thank you for all your support during this crazy whirlwind of a year. You are the stabilizing force that keeps me grounded.

Acknowledgments

As a technical author, I relied heavily on my technical editor. During the heavy revision of this book back in 2019, Steve Stiles had my back for this work. Steve Stiles did arduous review work necessary to make sure that you get a book that is both technically accurate and unambiguous.

Wendell Odom's *CCNA 200-301 Official Cert Guide, Volume 1* and *Volume 2* were two of my main sources. These two books have the breadth and depth needed to master the CCNA exam topics.

The Cisco Networking Academy authors for the online curriculum and series of Companion Guides take the reader deeper, past the CCNA exam topics, with the ultimate goal of preparing the student not only for CCNA certification but for more advanced college-level technology courses and degrees as well. Thank you especially to Rick Graziani, Bob Vachon, John Pickard, Dave Holzinger, Jane Gibbons, Martin Benson, Suk-Yi Pennock, Allan Reid, Jane Brooke, Anna Bolen, Telethia Willis, and the rest of the ACE team. Their excellent treatment of the material is reflected throughout this book.

James Manly, executive editor, daily juggles multiple projects simultaneously, steering each from beginning to end. James and I have completed many projects together. Thank you again, James, for shepherding this project for me.

Thank you to development editor Christopher Cleveland and project editor Mandie Frank for their professional and thorough review of this work. I've worked with the stellar Chris and Mandie on many previous projects. Their combined efforts ensure that what I authored is ready for publication.

And to the rest of the Pearson family who contributes in countless ways to bring a book to the reader, thank you for all your hard work.

Contents at a Glance

Introduction	xxviii
Day 31: Networking Models, Devices, and Components	1
Day 30: Ethernet Switching	29
Day 29: Switch Configuration Basics	41
Day 28: IPv4 Addressing	57
Day 27: IPv6 Addressing	67
Day 26: VLAN and Trunking Concepts and Configurations	85
Day 25: STP	103
Day 24: EtherChannel and HSRP	121
Day 23: DHCP and DNS	137
Day 22: Wireless Concepts	159
Day 21: WLAN Configuration	173
Day 20: LAN Security and Device Hardening	183
Day 19: Basic Routing Concepts	203
Day 18: Basic Router Configuration	217
Day 17: The Routing Table	235
Day 16: Inter-VLAN Routing	243
Day 15: Static and Default Route Configuration	251
Day 14: OSPF Operation	265
Day 13: Single-Area OSPF Implementation	275
Day 12: Fine-Tuning and Troubleshooting OSPF	285
Day 11: Network Security Concepts	295

Day 10: ACL Concepts	307
Day 9: ACL Implementation	313
Day 8: NAT	329
Day 7: WAN, VPN, and IPsec	339
Day 6: QoS	357
Day 5: CDP and LLDP	365
Day 4: Device Monitoring, Management, and Maintenance	375
Day 3: Cloud, Virtualization, and SDN	395
Day 2: Cisco SD-Access, Ansible, and Terraform	407
Day 1: Data Formats, REST, and AI	429
Exam Day	443
Post-Exam Information	445
CCNA Countdown Calendar	447
Exam Checklist	449
Index	453

Reader Services

Register your copy of this book at www.ciscopress.com/title/9780138214258 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. (Be sure to check the box indicating that you would like to hear from us to receive exclusive discounts on future editions of this product.) Enter the product ISBN 9780138214258 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

Contents

Introduction xxviii

Day 31: Networking Models, Devices, and Components 1

- CCNA 200-301 Exam Topics 1
- Key Points 1
- The OSI and TCP/IP Models 1
 - OSI Layers 2
 - TCP/IP Layers and Protocols 3
 - Protocol Data Units and Encapsulation 4
- The TCP/IP Application Layer 5
- The TCP/IP Transport Layer 5
 - TCP Header 6
 - Port Numbers 7
 - Error Recovery 7
 - Flow Control 8
 - Connection Establishment and Termination 9
 - UDP 9
- The TCP/IP Internet Layer 10
- The TCP/IP Network Access Layer 11
- Data Encapsulation Summary 12
- Networking Icons 13
- Devices 14
 - Switches 14
 - Access Layer Switches 14
 - Distribution Layer Switches 14
 - Core Layer Switches 15
 - Routers 15
 - Specialty Devices 16
 - Firewalls 16
 - IDS and IPS 16
 - Next-Generation Firewalls 18
 - Access Points and Wireless LAN Controllers 19
- Physical Layer 20
 - Network Media Forms and Standards 21
- LAN Device Connection Guidelines 22
- LANs and WANs 23

Small Office/Home Office (SOHO) 23
SOHO Routers 24

Physical and Logical Topologies 25

Hierarchical Campus Designs 25

Study Resources 27

Day 30: Ethernet Switching 29

CCNA 200-301 Exam Topics 29

Key Topics 29

Evolution to Switching 29

Switching Logic 30

Collision and Broadcast Domains 31

Frame Forwarding 31

Switch Forwarding Methods 31

Symmetric and Asymmetric Switching 32

Memory Buffering 32

Layer 2 and Layer 3 Switching 32

Ethernet Overview 32

Legacy Ethernet Technologies 33

CSMA/CD 34

Legacy Ethernet Summary 35

Current Ethernet Technologies 35

UTP Cabling 36

Benefits of Using Switches 37

Ethernet Addressing 37

Ethernet Framing 38

The Role of the Physical Layer 39

Study Resources 40

Day 29: Switch Configuration Basics 41

CCNA 200-301 Exam Topics 41

Key Topics 41

Accessing and Navigating the Cisco IOS 41

Connecting to Cisco Devices 41

WebUI 42

WebUI Connection 43

- CLI EXEC Sessions 43
- Using the Help Facility 43
- CLI Navigation and Editing Shortcuts 44
- Command History 45
- IOS Examination Commands 45
- Subconfiguration Modes 46

- Basic Switch Configuration Commands 46

- Half Duplex, Full Duplex, and Port Speed 48

- Automatic Medium-Dependent Interface Crossover (auto-MDIX) 48

- Verifying Network Connectivity 49

- Troubleshoot Interface and Cable Issues 52

- Media Issues 52

- Interface Status and Switch Configuration 53

- Interface Status Codes 53

- Duplex and Speed Mismatches 53

- Common Layer 1 Problems on “Up” Interfaces 55

- Study Resources 55

Day 28: IPv4 Addressing 57

- CCNA 200-301 Exam Topics 57

- Key Topics 57

- IPv4 Addressing 57

- Header Format 57

- Classes of Addresses 58

- Purpose of the Subnet Mask 59

- Private and Public IP Addressing 60

- Subnetting in Four Steps 60

- Determine How Many Bits to Borrow 61

- Determine the New Subnet Mask 62

- Determine the Subnet Multiplier 62

- List the Subnets, Host Ranges, and Broadcast Addresses 62

- Subnetting Example 1 63

- Subnetting Example 2 63

- Subnetting Example 3 64

- VLSM 64

- Study Resources 66

Day 27: IPv6 Addressing 67

CCNA 200-301 Exam Topics	67
Key Topics	67
Overview and Benefits of IPv6	67
The IPv6 Protocol	68
IPv6 Address Types	69
Unicast	69
Global Unicast Address	70
Link-Local Address	73
Loopback Address	73
Unspecified Address	73
Unique Local Address	74
IPv4 Embedded Address	74
Multicast	75
Assigned Multicast	75
Solicited-Node Multicast	76
Anycast	77
Representing the IPv6 Address	78
Conventions for Writing IPv6 Addresses	78
Conventions for Writing IPv6 Prefixes	78
IPv6 Subnetting	79
Subnetting the Subnet ID	80
Subnetting into the Interface ID	80
EUI-64 Concept	80
Stateless Address Autoconfiguration	81
Migration to IPv6	82
Study Resources	83

Day 26: VLAN and Trunking Concepts and Configurations 85

CCNA 200-301 Exam Topics	85
Key Points	85
VLAN Concepts	85
Traffic Types	86
Types of VLANs	86
Voice VLAN Example	87
Trunking VLANs	88
Dynamic Trunking Protocol	89
VLAN Configuration and Verification	90

Trunking Configuration and Verification	94
VLAN Troubleshooting	97
Disabled VLANs	98
Trunking Troubleshooting	99
Check Both Ends of a Trunk	99
Check Trunking Operational States	100
Study Resources	101

Day 25: STP 103

CCNA 200-301 Exam Topic	103
Key Topics	103
STP Concepts and Operation	103
STP Algorithm	104
STP Convergence	105
STP Varieties	106
PVST Operation	107
Port States	108
Extended System ID	108
Rapid PVST+ Operation	109
RSTP Interface Behavior	110
RSTP Port Roles	110
Edge Ports	111
Configuring and Verifying Varieties of STP	112
STP Configuration Overview	112
Configuring Rapid PVST+	113
Configuring and Verifying the BID	114
Configuring PortFast and BPDU Guard	116
Configuring BPDU Filter	116
Configuring Root Guard	117
Configuring Loop Guard	118
Verifying STP	118
Study Resources	119

Day 24: EtherChannel and HSRP 121

CCNA 200-301 Exam Topics	121
Key Topics	121
EtherChannel Operation	121
Benefits of EtherChannel	122
Implementation Restrictions	122

- EtherChannel Protocols 123
 - Port Aggregation Protocol 123
 - Link Aggregation Control Protocol 124
- Configuring EtherChannel 124
- Verifying EtherChannel 125
- Troubleshooting EtherChannel 127
- First-Hop Redundancy Concepts 128
- FHRPs 129
- HSRP Operation 130
 - HSRP Versions 130
 - HSRP Priority and Preemption 131
- HSRP Configuration and Verification 131
- HSRP Load Balancing 132
- Troubleshooting HSRP 135
- VRRP and GLBP 135
 - VRRP 135
 - GLBP 136
- Study Resources 136

Day 23: DHCP and DNS 137

- CCNA 200-301 Exam Topics 137
- Key Topics 137
- DHCPv4 137
- DHCPv4 Configuration Options 138
 - Configuring a Router as a DHCPv4 Server 138
 - Configuring a Router to Relay DHCPv4 Requests 142
 - Configuring a Router as a DHCPv4 Client 143
- DHCPv6 144
 - SLAAC 144
 - Stateless DHCPv6 146
 - Stateful DHCPv6 146
 - Stateless and Stateful DHCPv6 Operation 146
- DHCPv6 Configuration Options 147
 - Configuring a Router as a Stateless DHCPv6 Server 147
 - Configuring a Router as a Stateful DHCPv6 Server 149

DHCP Troubleshooting	149
Resolving IPv4 Address Conflicts	149
Testing Connectivity Using a Static IP Address	150
Verifying Switch Port Configuration	150
Testing DHCPv4 Operation on the Same Subnet or VLAN	150

DNS Operation 150

Troubleshooting DNS 152

Verifying Host IP Configuration 153

 IP Settings 153

 Host IP Settings on Windows 153

 Host IP Settings on macOS 155

 Host IP Settings on Linux 156

Study Resources 158

Day 22: Wireless Concepts 159

CCNA 200-301 Exam Topics 159

Key Topics 159

Wireless Standards 159

 RF Spectrum 159

 Channels 159

 802.11 Standards 161

Wireless Topologies 163

 Infrastructure Mode 163

 IBSS, or Ad Hoc Mode 164

 Mesh 164

AP Architectures 165

 Autonomous AP Architecture 165

 Cloud-Based AP Architecture 166

 Lightweight AP Architectures 166

 CAPWAP Operation 167

Wireless Security Protocols 168

 Wireless Authentication Methods 168

 WPA and WPA2 170

 802.1X/EAP 170

 WPA3 170

 Wireless Encryption Methods 171

Study Resources 172

Day 21: WLAN Configuration 173

CCNA 200-301 Exam Topics 173

Key Topics 173

Logging Into a Cisco WLC 173

Configuring a WLC with a WLAN 175

 Configuring a RADIUS Server 176

 Configuring a New Interface 176

 Configuring a WPA2 Enterprise WLAN 178

Study Resources 181

Day 20: LAN Security and Device Hardening 183

CCNA 200-301 Exam Topics 183

Key Topics 183

Access Control 183

 Local Authentication 183

 SSH Configuration 184

 Switch Port Hardening 186

 AAA 186

 802.1X 187

Port Security 189

 Port Security Configuration 189

 Port Security Aging 191

 Port Restoration After a Violation 192

LAN Threat Mitigation 193

 Native and Management VLAN Modification 193

 VLAN Attacks 194

 VLAN Attack Mitigation 195

 DHCP Attacks 196

 DHCP Starvation Attacks 196

 DHCP Spoofing Attacks 196

 DHCP Snooping 196

 ARP Attacks 198

 Dynamic ARP Inspection 199

Study Resources 201

Day 19: Basic Routing Concepts 203

CCNA 200-301 Exam Topics 203

Key Topics 203

Packet Forwarding 203

 Path Determination and Switching Function Example 204

Routing Methods	205
Classifying Dynamic Routing Protocols	206
IGP and EGP	206
Distance Vector Routing Protocols	207
Link-State Routing Protocols	207
Classful Routing Protocols	208
Classless Routing Protocols	208
Dynamic Routing Metrics	208
Administrative Distance	209
IGP Comparison Summary	211
Routing Loop Prevention	211
Link-State Routing Protocol Features	212
Building the LSDB	212
Calculating the Dijkstra Algorithm	213
Convergence with Link-State Protocols	214
Study Resources	215

Day 18: Basic Router Configuration 217

CCNA 200-301 Exam Topics	217
Key Topics	217
Basic Router Configuration with IPv4	217
Command Syntax	218
Configuration Example	219
Verification Example	220
Basic Router Configuration with IPv6	225
Command Syntax	226
Configuration Example	226
Verifying IPv4 and IPv6 Network Connectivity	229
Small Office or Home Office Routers	231
Basic IP Addressing Troubleshooting	233
Default Gateway	233
Duplicate IP Addresses	234
Study Resources	234

Day 17: The Routing Table 235

CCNA 200-301 Exam Topics	235
Key Topics	235
Two Router Functions	235

Longest Match Determines Best Path 235

Three Packet Forwarding Decisions 236

Components of the Routing Table 236

Routing Table Principles 239

Route Entry Structure 240

Study Resources 241

Day 16: Inter-VLAN Routing 243

CCNA 200-301 Exam Topics 243

Key Points 243

Inter-VLAN Routing Concepts 243

Legacy Inter-VLAN Routing 243

Router on a Stick 244

Multilayer Switching 245

Router on a Stick Configuration and Verification 245

Multilayer Switching Inter-VLAN Routing Configuration and Verification 248

Creating Additional SVIs 248

Configuring a Layer 3 Routed Port 250

Study Resources 250

Day 15: Static and Default Route Configuration 251

CCNA 200-301 Exam Topics 251

Key Topics 251

Static and Default Routing Overview 251

IPv4 Static Route Configuration 252

IPv4 Static Routes Using the Next-Hop Parameter 254

IPv4 Static Routes Using the Exit Interface Parameter 254

IPv4 Default Route Configuration 255

IPv4 Summary Static Route Configuration 258

IPv6 Static Routing 259

IPv6 Static Route Configuration 261

IPv6 Default Route Configuration 261

IPv6 Summary Static Route Configuration 262

Study Resources 264

Day 14: OSPF Operation 265

- CCNA 200-301 Exam Topics 265
- Key Topics 265
- Single-Area OSPF Operation 265
 - OSPF Message Format 265
 - OSPF Packet Types 266
 - Neighbor Establishment 266
 - Link-State Advertisements 268
 - OSPF DR and BDR 269
 - OSPF Algorithm 269
 - Link-State Routing Process 270
- OSPFv2 Versus OSPFv3 271
 - Similarities Between OSPFv2 and OSPFv3 271
 - Differences Between OSPFv2 and OSPFv3 271
- Multiarea OSPF Operation 272
 - Multiarea OSPF Design 272
 - Multiarea OSPF Improves Performance 274
- Study Resources 274

Day 13: Single-Area OSPF Implementation 275

- CCNA 200-301 Exam Topics 275
- Key Topics 275
- Single-Area OSPFv2 Configuration 275
 - The router ospf Command 276
 - Router ID 276
 - The network Command 277
 - Passive Interfaces 278
 - Modifying the OSPF Metric 278
- Verifying OSPFv2 280
- Study Resources 284

Day 12: Fine-Tuning and Troubleshooting OSPF 285

- CCNA 200-301 Exam Topics 285
- Key Topics 285
- OSPFv2 Configuration Example 285
- Modifying OSPFv2 287
 - Redistributing a Default Route 287
 - Modifying Hello and Dead Intervals 288
 - OSPF Network Types 288

DR/BDR Election 289
Controlling the DR/BDR Election 289

Troubleshooting OSPF 291
OSPF States 291
OSPF Adjacency 292
OSPF Troubleshooting Commands 292

Study Resources 293

Day 11: Network Security Concepts 295

CCNA 200-301 Exam Topics 295

Key Topics 295

Security Fundamentals 295
Security Terms 295
Attack Vectors and Data Exfiltration 296
Penetration Testing Tools 296
Attack Types 297
Types of Malware 298

Network Attacks 299
Reconnaissance Attacks 299
Access Attacks 299
Social Engineering Attacks 300
DoS and DDoS Attacks 301
IP Attacks 301
Transport Layer Attacks 302

Security Program 302

Password Vulnerabilities 303
Types of Attacks 303
Mitigation Strategies 303
Password Guidelines 303

Password Alternatives 304
Additional Password Security 305

Study Resources 306

Day 10: ACL Concepts 307

CCNA 200-301 Exam Topics 307

Key Topics 307

ACL Operation 307
Defining an ACL 307
Processing Interface ACLs 308
List Logic with IP ACLs 308

- Planning to Use ACLs 309
 - Types of ACLs 310
 - ACL Identification 311
 - ACL Design Guidelines 311
- Study Resources 312

Day 9: ACL Implementation 313

- CCNA 200-301 Exam Topics 313
- Key Topics 313
- Configuring Standard Numbered IPv4 ACLs 313
 - Standard Numbered IPv4 ACL: Permit Specific Network 314
 - Standard Numbered IPv4 ACL: Deny a Specific Host 314
 - Standard Numbered IPv4 ACL: Deny a Specific Subnet 315
 - Standard Numbered IPv4 ACL: Deny Telnet or SSH Access to the Router 315
- Configuring Extended Numbered IPv4 ACLs 315
 - Extended Numbered IPv4 ACL: Deny FTP from Subnets 316
 - Extended Numbered IPv4 ACL: Deny Only Telnet from Subnet 316
- Configuring Named IPv4 ACLs 317
 - Standard Named IPv4 ACL Steps and Syntax 317
 - Standard Named IPv4 ACL: Deny a Single Host from a Given Subnet 317
 - Extended Named IPv4 ACL Steps and Syntax 318
 - Adding Comments to Named or Numbered IPv4 ACLs 318
- Verifying IPv4 ACLs 319
- Comparing IPv4 and IPv6 ACLs 320
- Configuring IPv6 ACLs 321
 - Step 1: Name the IPv6 ACL 321
 - Step 2: Create the IPv6 ACL 321
 - Step 3: Apply the IPv6 ACL 322
 - Standard IPv6 ACL: Allow SSH Remote Access 322
 - Extended IPv6 ACL: Allow Only Web Traffic 323
- Verifying IPv6 ACLs 323
- Troubleshooting ACLs 326
- Study Resources 326

Day 8: NAT 329

- CCNA 200-301 Exam Topics 329
- Key Topics 329
- NAT Concepts 329

- A NAT Example 331
- Dynamic and Static NAT 332
- NAT Overload 332
- NAT Benefits 333
- NAT Limitations 333

- Configuring Static NAT 334
 - Configuring Dynamic NAT 334
 - Configuring NAT Overload 335

Verifying NAT 336

Troubleshooting NAT 337

Study Resources 338

Day 7: WAN, VPN, and IPsec 339

CCNA 200-301 Exam Topics 339

Key Topics 339

WAN Topologies 339

WAN Connection Options 340

- Dedicated Connection Options 341
- Circuit-Switched Connection Options 342
- Packet-Switched Connection Options 342
 - Metro Ethernet 343
 - MPLS 343
- Internet Connection Options 344
 - DSL 344
 - Cable Modem 344
 - Wireless 345
- Choosing a WAN Link Option 346

VPN Technology 346

- VPN Benefits 347
- Types of VPN Access 347
- VPN Components 350
- Establishing Secure VPN Connections 350
 - VPN Tunneling 351
 - VPN Encryption Algorithms 351
 - Hashes 352
 - VPN Authentication 352
- IPsec Security Protocols 352

Study Resources 355

Day 6: QoS 357

- CCNA 200-301 Exam Topic 357
- Key Topics 357
- QoS 357
 - Classification and Marking 358
 - DSCP and IPP 359
 - EF and AF 360
 - Congestion Management 361
 - Policing, Shaping, and TCP Discards 362
 - QoS and TCP 363
- Study Resources 364

Day 5: CDP and LLDP 365

- CCNA 200-301 Exam Topic 365
- Key Topics 365
- CDP Overview 365
 - CDP Configuration 366
 - CDP Verification 368
- LLDP Overview 371
 - LLDP Configuration 371
 - LLDP Verification 372
- Study Resources 374

Day 4: Device Monitoring, Management, and Maintenance 375

- CCNA 200-301 Exam Topics 375
- Key Topics 375
- SNMP Operation 375
 - SNMP Components 375
 - SNMP Messages 375
 - SNMP Versions 376
 - The Management Information Base 376
- Configuring SNMP 378
- Verifying SNMP 378
- Syslog 380
 - Syslog Operation 380
 - Configuring and Verifying Syslog 382
- Network Time Protocol 384

- Cisco IOS File System and Devices 385
 - IFS Commands 385
 - URL Prefixes for Specifying File Locations 388
 - Commands for Managing Configuration Files 388
- Managing Cisco IOS Images 390
 - Backing Up a Cisco IOS Image 390
 - Restoring a Cisco IOS Image 391
- Password Recovery 392
- Study Resources 393

Day 3: Cloud, Virtualization, and SDN 395

- CCNA 200-301 Exam Topics 395
- Key Topics 395
- Cloud Computing 395
 - Server Virtualization 396
 - Cloud Computing Services 397
 - Virtual Network Infrastructure 398
- Software-Defined Networking 399
 - Data, Control, and Management Planes 399
 - Controllers 400
 - Network Programmability and SDN Examples 401
 - OpenDaylight and OpenFlow 401
 - Cisco Application Centric Infrastructure (ACI) 402
- Study Resources 405

Day 2: Cisco SD-Access, Ansible, and Terraform 407

- CCNA 200-301 Exam Topics 407
- Key Topics 407
- Cisco SD-Access 407
 - Underlay 409
 - Existing Equipment for the Cisco SD-Access Underlay 409
 - New Equipment for the Cisco SD-Access Underlay 409
 - Overlay 411
 - VXLAN Tunnels in the Overlay (Data Plane) 411
 - LISP for Overlay Discovery and Location (Control Plane) 412
 - Cisco Catalyst Center 414
 - Cisco Catalyst Center and Scalable Groups 415
 - Issues with Traditional IP-Based Security 415
 - Cisco SD-Access Security Is Based on User Groups 416

Cisco Catalyst Center as a Network Management Platform	417
Cisco Catalyst Center Similarities to Traditional Management	417
Differences Between Cisco Catalyst Center and Traditional Management	418

Configuration Management Tools: Ansible and Terraform	418
Manual Configuration Management	418
Configuration Management Tool Overview	419
Configuration Provisioning	419
Configuration Templates and Variables	419
Ansible	420
Terraform	422
Ansible and Terraform Comparison	427
Explore DevNet Learning Labs	427
Study Resources	427

Day 1: Data Formats, REST, and AI 429

CCNA 200-301 Exam Topics	429
Key Topics	429
Data Formats	429
JSON Data Format	430
JSON Syntax Rules	431
RESTful APIs	432
RESTful Implementation	432
REST Authentication Types	432
RESTful API Requests	434
AI and ML in IT Operations	435
Generative AI for Network Configuration, Troubleshooting, and Simulation	436
ChatGPT Configuration Example	436
ChatGPT Troubleshooting Example	438
ChatGPT as a Network Simulator	439
Study Resources	442

Exam Day 443

What You Need for the Exam	443
What You Should Receive After Completion	443
Summary	444

Post-Exam Information 445

Receiving Your Certificate 445

Determining Career Options 445

Examining Certification Options 445

If You Did Not Pass the Exam 446

Summary 446

CCNA Countdown Calendar 447

Exam Checklist 449

Index 453

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

If you're reading this introduction, you've probably already spent a considerable amount of time and energy pursuing your CCNA 200-301 certification. Regardless of how you got to this point in your travels through your CCNA studies, *31 Days Before Your CCNA Exam* most likely represents the last leg of your journey on your way to the destination: to become a Cisco Certified Network Associate. However, if you are like me, you might be reading this book at the *beginning* of your studies. If so, this book provides an excellent overview of the material you must now spend a great deal of time studying and practicing. But I must warn you: Unless you are extremely well versed in networking technologies and have considerable experience configuring and troubleshooting Cisco routers and switches, this book will *not* serve you well as the sole resource for your exam preparations. Therefore, let me spend some time discussing my recommendations for study resources.

Study Resources

Cisco Press and Pearson IT Certification offer an abundance of CCNA-related books to serve as your primary source for learning how to install, configure, operate, and troubleshoot small to medium-size routed and switched networks.

Primary Resources

First on the list of important resources is Wendell Odom's *CCNA 200-301 Official Cert Guide Library, Volume 1* and *Volume 2*, 2nd edition (ISBN: 9780138221393). If you do not buy any other books, buy these. Wendell's method of teaching, combined with his technical expertise and down-to-earth style, is unsurpassed in our industry. As you read through his books, you sense that he is sitting right there next to you, walking you through the material. With your purchase, you get access to practice exams and study materials and other online resources that are worth the price of the book. There is no better resource on the market for a CCNA candidate.

If you are a Cisco Networking Academy student, you are blessed with access to the online version of the CCNA version 7 curriculum and the wildly popular Packet Tracer network simulator. The Cisco Network Academy curriculum has three courses. To learn more about CCNAv7 courses and to find an Academy near you, visit <http://www.netacad.com>.

However, if you are not an Academy student but want to benefit from the extensive authoring done for these courses, you can buy any or all of CCNAv7 Companion Guides (CGs) and Labs & Study Guides (LSGs) of the Academy's popular online curriculum. Although with this option you will not have access to the Packet Tracer files, you will have access to the tireless work of an outstanding team of Cisco Academy instructors dedicated to providing students with comprehensive and engaging CCNA preparation course material. The titles and ISBNs for the CCNAv7 CGs and LSGs follow:

- *Introduction to Networks v7 Companion Guide* (ISBN: 9780136633662)
- *Introduction to Networks v7 Labs & Study Guide* (ISBN: 9780136634454)
- *Switching, Routing, and Wireless Essentials v7 Companion Guide* (ISBN: 9780136729358)
- *Switching, Routing, and Wireless Essentials v7 Labs & Study Guide* (ISBN: 9780136634386)

- *Enterprise Networking, Security, and Automation v7 Companion Guide* (ISBN: 9780136634324)
- *Enterprise Networking, Security, and Automation v7 Labs & Study Guide* (ISBN: 9780136634690)

You can find these books at <http://www.ciscopress.com> by clicking the Cisco Networking Academy link.

Supplemental Resources

In addition to the book you hold in your hands, I recommend three supplemental resources to augment your final 31 days of review and preparation.

First is Scott Empson's very popular *CCNA 200-301 Portable Command Guide* (ISBN: 9780135937822). This guide is much more than just a listing of commands and what they do. Yes, it summarizes all the CCNA certification-level IOS commands, keywords, command arguments, and associated prompts. It also provides you with tips and examples of how to apply the commands to real-world scenarios. Configuration examples throughout the book provide you with a better understanding of how these commands are used in simple network designs.

Second, Jason Gooley's *CCNA 200-301 Complete Video Course*, second edition (ISBN: 9780138213596), is a comprehensive training course that brings Cisco CCNA exam topics to life through the use of real-world demonstrations, animations, live instruction, and configurations, making learning these foundational networking topics easy and fun.

Third, Wendell Odom's *IP Subnetting LiveLessons* (ISBN: 9780135497777) and *IP Subnetting Practice Questions Kit* (ISBN: 9780135647288) will help you master this crucial skill. Subnetting is not only an IPv4 address design skill, it is also a crucial skill for troubleshooting situations where IPv4 addressing has been misconfigured. You are likely to have both types of questions on the CCNA exam.

The Cisco Learning Network

Finally, if you have not done so already, you should register with The Cisco Learning Network at <https://learningnetwork.cisco.com/s/>. The Cisco Learning Network, sponsored by Cisco, is a free social learning network where IT professionals can engage in the common pursuit of enhancing and advancing their IT careers. Here you can find many resources to help you prepare for your CCNA exam, in addition to a community of like-minded people ready to answer your questions, help you with your struggles, and share in your triumphs.

So which resources should you buy? The answer to that question depends largely on how deep your pockets are and how much you like books. If you're like me, you must have it all! I admit it; my bookcase is a testament to my Cisco "geekness." But if you are on a budget, choose one of the primary study resources and one of the supplemental resources (such as Wendell Odom's certification library and Scott Empson's command guide). Whatever you choose, you will be in good hands. Any or all of these authors will serve you well.

Goals and Methods

The main goal of this book is to provide you with a clear and succinct review of the CCNA objectives. Each day's exam topics are grouped into a common conceptual framework and use the following format:

- A title for the day that concisely states the overall topic
- A list of one or more CCNA 200-301 exam topics to be reviewed
- A “Key Topics” section that introduces the review material and quickly orients you to the day's focus
- An extensive review section consisting of short paragraphs, lists, tables, examples, and graphics
- A “Study Resources” section that gives you a quick reference for locating more in-depth treatment of the day's topics

The book counts down starting with Day 31, continues through exam day, and provides post-test information. This book also provides a calendar and a checklist that you can tear out and use during your exam preparation.

Use the calendar to enter each actual date beside the countdown day and the exact day, time, and location of your CCNA exam. The calendar provides a visual for the time you can dedicate to each CCNA exam topic.

The checklist highlights important tasks and deadlines leading up to your exam. Use it to help map out your studies.

Who Should Read This Book?

The audience for this book is anyone finishing preparation for taking the CCNA 200-301 exam. A secondary audience is anyone needing a refresher review of CCNA exam topics—possibly before attempting to recertify or sit for another certification for which the CCNA is a prerequisite.

Getting to Know the CCNA 200-301 Exam

For the current certification announced in August 2024, Cisco made minor revisions to the CCNA 200-301 exam. This book focuses on the entire list of topics published for the exam. It is a 120-minute exam associated with the CCNA certification. This exam tests a candidate's knowledge and skills related to network fundamentals, network access, IP connectivity, IP services, security fundamentals, and automation and programmability. Use the following steps to access a tutorial at home that demonstrates the exam environment before you go to take the exam:

Step 1. Visit <https://home.pearsonvue.com/cisco> and go through the signup process or log in.

Step 2. On the right side, click the **Certification Tutorial** link.

When you get to the testing center and check in, the proctor verifies your identity, gives you some general instructions, and takes you into a quiet room containing a PC. When you're at the PC, you have a few things to do before the timer starts on your exam. For instance, you can take the tutorial to get accustomed to the PC and the testing engine. Every time I sit for an exam, I go

through the tutorial even though I know how the test engine works. It helps me settle my nerves and get focused. Anyone who has user-level skills in getting around a PC should have no problem with the testing environment.

NOTE: You can also take the exam at home. For more information, visit <https://home.pearsonvue.com/cisco/online>.

When you start the exam, you are asked a series of questions. The questions are presented one at a time, and you must answer each one before you can move on to the next question. The exam engine does not let you go back and change any answers. Each exam question is in one of the following formats:

- Multiple choice
- Fill in the blank
- Drag and drop
- Testlet
- Simlet
- Simulation

The multiple-choice format simply requires that you point and click a circle or checkbox next to the correct answer(s). Cisco traditionally tells you how many answers you need to choose, and the testing software prevents you from choosing too many or too few.

Fill-in-the-blank questions usually require you only to type numbers. However, if words are requested, the case does not matter unless the answer is a command that is case sensitive (such as passwords and device names when you're configuring authentication).

Drag-and-drop questions require you to click and hold, move a button or an icon to another area, and release the mouse button to place the object somewhere else—usually in a list. For some questions, to get the question correct, you might need to put a list of five things in the proper order.

A testlet contains one general scenario and several multiple-choice questions about the scenario. Testlets are ideal if you are confident in your knowledge of the scenario's content because you can leverage your strength over multiple questions.

A simlet is similar to a testlet, in that you are given a scenario with several multiple-choice questions. However, a simlet uses a network simulator to allow you access to a simulation of the Cisco IOS Software command line. You can use **show** commands to examine a network's current behavior and answer the question.

A simulation also involves a network simulator, but you are given a task to accomplish, such as implementing a network solution or troubleshooting an existing network implementation. You do this by configuring one or more routers and switches. The exam grades the question based on the configuration you changed or added. A newer form of the simulation question is the GUI-based simulation, which simulates a graphical interface such as that found on a Linksys router or the Cisco Security Device Manager.

Registering for the CCNA 200-301 Exam

If you are starting this book 31 days before you take the CCNA 200-301 exam, register for the exam right now. In my testing experience, there is no better motivator than a scheduled test date staring me in the face. I'm willing to bet the same holds true for you. Don't worry about unforeseen circumstances. You can cancel your exam registration for a full refund up to 24 hours before the scheduled exam time. So if you're ready, gather the following information and register right now!

- Legal name
- Social Security or passport number
- Company name
- Valid email address
- Method of payment

You can schedule your exam at any time by visiting www.pearsonvue.com/cisco/. I recommend that you schedule it for 31 days from now. The process and available test times vary based on the local testing center you choose.

Remember: There is no better motivation for study than an actual test date. *Sign up today.*

Topics Covered on the CCNA Exam

Table I-1 summarizes the six domains of the CCNA 200-301 exam.

Table I-1 CCNA 200-301 Exam Domains and Weightings

Domain	Percentage of Exam
1.0 Network Fundamentals	20%
2.0 Network Access	20%
3.0 IP Connectivity	25%
4.0 IP Services	10%
5.0 Security Fundamentals	15%
6.0 Automation and Programmability	10%

Although Cisco outlines general exam topics, not all topics might appear on the CCNA exam; likewise, topics that are not specifically listed might appear on the exam. The exam topics that Cisco provides and that this book covers provide a general framework for exam preparation. Be sure to check Cisco's website for the latest exam topics.

Exam Topics Cross-reference

To give you a quick reference to help find which exam topics are covered on which days, I created two cross-reference tables. You can use Table I-2 to look up an exam topic and find the day or days on which it is covered. Use Table I-3 to find out which exam topics are covered on each day.

Table I-2 Days on Which Each Exam Topic Is Covered

Exam Topic	Day(s)
1.1 Explain the role and function of network components	31, 30, 22, 19
1.2 Describe characteristics of network topology architectures	31, 18, 7, 3
1.3 Compare physical interface and cabling types	31
1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)	31, 29, 18
1.5 Compare TCP to UDP	31
1.6 Configure and verify IPv4 addressing and subnetting	29, 28, 18
1.7 Describe private IPv4 addressing	28
1.8 Configure and verify IPv6 addressing and prefix	27, 18
1.9 Describe IPv6 address types	27
1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux)	23
1.11 Describe wireless principles	22
1.12 Explain virtualization fundamentals (server virtualization, containers, and VRFs)	3
1.13 Describe switching concepts	30
2.1 Configure and verify VLANs (normal range) spanning multiple switches	26, 16
2.2 Configure and verify interswitch connectivity	26, 16
2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)	5
2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)	24
2.5 Interpret basic operations of Rapid PVST+ Spanning Tree Protocol	25
2.6 Describe Cisco Wireless Architectures and AP modes	22
2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)	22
2.8 Describe network device management access (Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS, and cloud managed)	29
2.9 Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings	21
3.1 Interpret the components of routing table	17
3.2 Determine how a router makes a forwarding decision by default	19, 17
3.3 Configure and verify IPv4 and IPv6 static routing	15
3.4 Configure and verify single area OSPFv2	14, 13, 12
3.5 Describe the purpose, functions, and concepts of first hop redundancy protocols	24
4.1 Configure and verify inside source NAT using static and pools	8
4.2 Configure and verify NTP operating in a client and server mode	4
4.3 Explain the role of DHCP and DNS within the network	23
4.4 Explain the function of SNMP in network operations	4
4.5 Describe the use of syslog features, including facilities and severity levels	4
4.6 Configure and verify DHCP client and relay	23

Exam Topic	Day(s)
4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, and shaping	6
4.8 Configure network devices for remote access using SSH	20
4.9 Describe the capabilities and functions of TFTP/FTP in the network	4
5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)	11
5.2 Describe security program elements (user awareness, training, and physical access control)	11
5.3 Configure and verify device access control using local passwords	20
5.4 Describe security password policy elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)	11
5.5 Describe IPsec remote access and site-to-site VPNs	7
5.6 Configure and verify access control lists	10, 9
5.7 Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)	20
5.8 Compare authentication, authorization, and accounting concepts	20
5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)	22
5.10 Configure and verify WLAN within the GUI using WPA2 PSK	21
6.1 Explain how automation impacts network management	2
6.2 Compare traditional networks with controller-based networking	3
6.3 Describe controller-based, software defined architecture (overlay, underlay, and fabric)	3, 2
6.4 Explain AI (generative and predictive) and machine learning in network operations	1
6.5 Describe characteristics of REST-based APIs (authentication types, CRUD, HTTP verbs, and data encoding)	1
6.6 Recognize the capabilities of configuration management mechanisms such as Ansible and Terraform	2
6.7 Recognize components of JSON-encoded data	1

Table I-3 Exam Topics Covered on Each Day

Day	Exam Topic(s)
31	1.1 Explain the role and function of network components
	1.2 Describe characteristics of network topology architectures
	1.3 Compare physical interface and cabling types
	1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
	1.5 Compare TCP to UDP
30	1.1 Explain the role and function of network components
	1.13 Describe switching concepts

Day	Exam Topic(s)
29	1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
	1.6 Configure and verify IPv4 addressing and subnetting
	2.8 Describe network device management access (Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS, and cloud managed)
28	1.6 Configure and verify IPv4 addressing and subnetting
	1.7 Describe private IPv4 addressing
27	1.8 Configure and verify IPv6 addressing and prefix
	1.9 Describe IPv6 address types
26	2.1 Configure and verify VLANs (normal range) spanning multiple switches
	2.2 Configure and verify interswitch connectivity
25	2.5 Interpret basic operations of Rapid PVST+ Spanning Tree Protocol
24	2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
	3.5 Describe the purpose, functions, and concepts of first hop redundancy protocols
23	1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux)
	4.3 Explain the role of DHCP and DNS within the network
	4.6 Configure and verify DHCP client and relay
22	1.1 Explain the role and function of network components
	1.11 Describe wireless principles
	2.6 Describe Cisco Wireless Architectures and AP modes
	2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
	5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)
21	2.9 Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings
	5.10 Configure and verify WLAN within the GUI using WPA2 PSK
20	4.8 Configure network devices for remote access using SSH
	5.3 Configure and verify device access control using local passwords
	5.7 Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
	5.8 Compare authentication, authorization, and accounting concepts
19	1.1 Explain the role and function of network components
	3.2 Determine how a router makes a forwarding decision by default
18	1.2 Describe characteristics of network topology architectures
	1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
	1.6 Configure and verify IPv4 addressing and subnetting
	1.8 Configure and verify IPv6 addressing and prefix

Day	Exam Topic(s)
17	3.1 Interpret the components of routing table
	3.2 Determine how a router makes a forwarding decision by default
16	2.1 Configure and verify VLANs (normal range) spanning multiple switches
	2.2 Configure and verify interswitch connectivity
15	3.3 Configure and verify IPv4 and IPv6 static routing
14	3.4 Configure and verify single area OSPFv2
13	3.4 Configure and verify single area OSPFv2
12	3.4 Configure and verify single area OSPFv2
11	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
	5.2 Describe security program elements (user awareness, training, and physical access control)
	5.4 Describe security password policy elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
10	5.6 Configure and verify access control lists
9	5.6 Configure and verify access control lists
8	4.1 Configure and verify inside source NAT using static and pools
7	1.2 Describe characteristics of network topology architectures
	5.5 Describe IPsec remote access and site-to-site VPNs
6	4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, and shaping
5	2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
4	4.2 Configure and verify NTP operating in a client and server mode
	4.4 Explain the function of SNMP in network operations
	4.5 Describe the use of syslog features, including facilities and severity levels
	4.9 Describe the capabilities and functions of TFTP/FTP in the network
3	1.2 Describe characteristics of network topology architectures
	1.12 Explain virtualization fundamentals (server virtualization, containers, and VRFs)
	6.2 Compare traditional networks with controller-based networking
	6.3 Describe controller-based, software defined architecture (overlay, underlay, and fabric)
2	6.1 Explain how automation impacts network management
	6.3 Describe controller-based, software defined architecture (overlay, underlay, and fabric)
	6.6 Recognize the capabilities of configuration management mechanisms such as Ansible and Terraform
1	6.4 Explain AI (generative and predictive) and machine learning in network operations
	6.5 Describe characteristics of REST-based APIs (authentication types, CRUD, HTTP verbs, and data encoding)
	6.7 Recognize components of JSON-encoded data

Credits

Figure 23.10 – Microsoft Corporation

Figure 23.11 – Apple Inc.

Figure 23.12 – Ubuntu

This page intentionally left blank

Wireless Concepts

CCNA 200-301 Exam Topics

- 1.1 Explain the role and function of network components
 - 1.11 Describe wireless principles
 - 2.6 Describe Cisco Wireless Architectures and AP modes
 - 2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, LAG)
 - 5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)
-

Key Topics

Wireless specifications are detailed in the IEEE 802.11 family of standards, including wireless topologies, spectrum allocation, and wireless security. Today we review basic wireless network concepts.

Wireless Standards

The IEEE 802.11 WLAN standards define how radio frequencies (RFs) are used for wireless links. To avoid interference, different channels within an RF can be used.

RF Spectrum

The RF spectrum, shown in Figure 22-1, includes all types of radio communications, including the 2.4-GHz and 5-GHz frequencies used by wireless devices.

Channels

A frequency range is typically called a *band* of frequencies. For example, a wireless LAN device with a 2.4-GHz antenna can actually use any frequency from 2.4000 to 2.4835 GHz. The 5-GHz band lies between 5.150 and 5.825 GHz.

The bands are further subdivided into frequency channels. Channels become particularly important when the wireless devices in a specific area become saturated. Each channel is known by a channel number and is assigned to a specific frequency. As long as the channels are defined by a national or international standards body, they can be used consistently in all locations. Figure 22-2 and Figure 22-3 show the channel layouts for the 2.4- and 5-GHz bands, respectively.

Figure 22-1 RF Spectrum

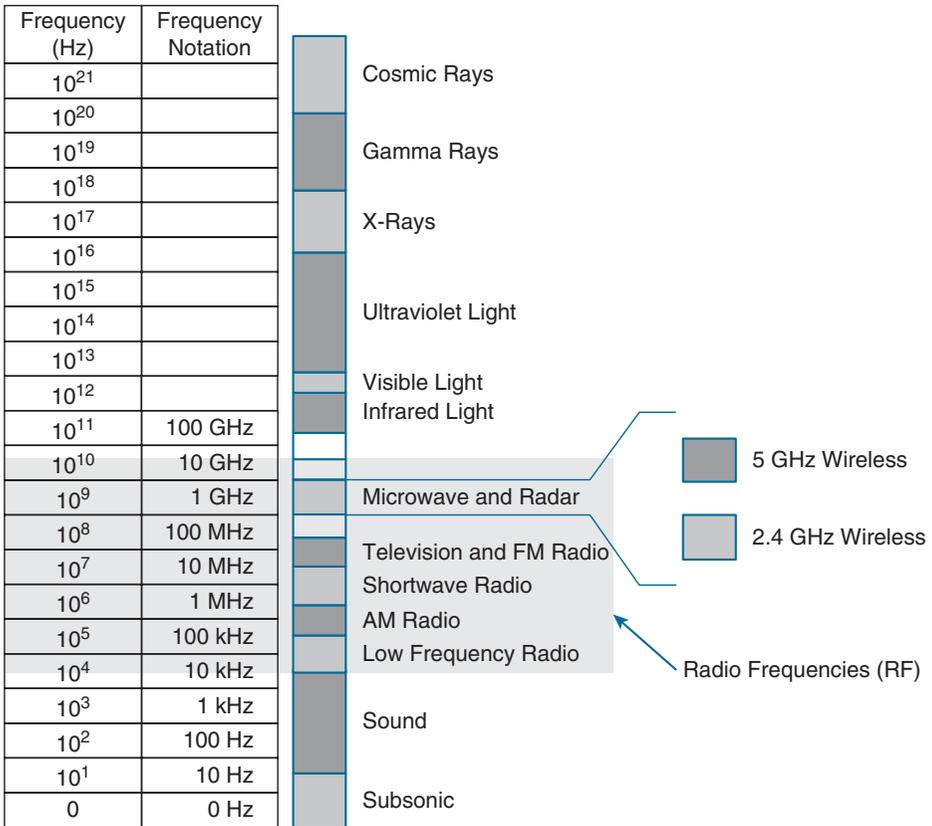
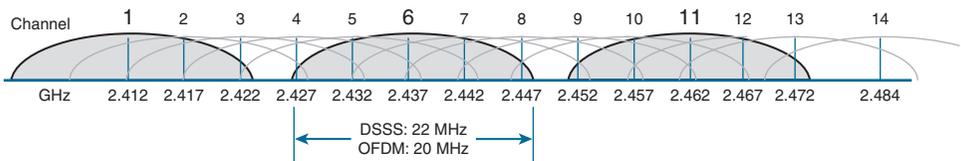
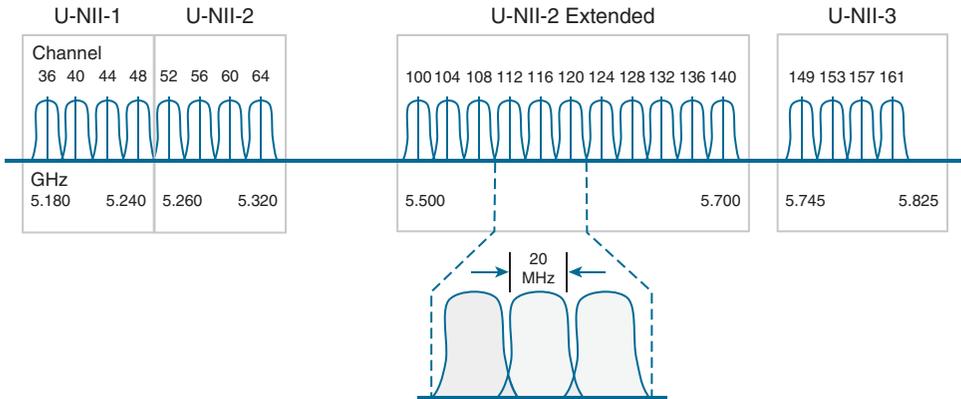


Figure 22-2 2.4-GHz Channels



Notice in Figure 22-3 that the 5-GHz band consists of nonoverlapping channels. Each channel is allocated a frequency range that does not encroach on or overlap the frequencies allocated for any other channel. The same is not true of the 2.4-GHz band in Figure 22-2. The only way to avoid any overlap between adjacent channels is to configure access points (APs) to use only channels 1, 6, and 11.

Figure 22-3 5-GHz Channels

802.11 Standards

Most of the standards specify that a wireless device must have one antenna to transmit and receive wireless signals on the specified radio frequency (2.4 GHz or 5 GHz). Some of the newer standards that transmit and receive at higher speeds require APs and wireless clients to have multiple antennas using the multiple input, multiple output (MIMO) technology. MIMO uses multiple antennas as both the transmitter and receiver to improve communication performance. Up to four antennas can be supported.

Various implementations of the IEEE 802.11 standard have been developed over the years. Table 22-1 highlights these standards.

Table 22-1 Summary of 802.11 Standards

IEEE WLAN Standard	2.4 GHz	5 GHz	6 GHz	Max Data Rate	Description
802.11-1997	Yes	No	No	2 Mbps	The original 802.11 standard, ratified in 1997
802.11a	No	Yes	No	54 Mbps	Introduced in 1999 Small coverage area Less effective at penetrating building structures Not interoperable with 802.11b and 802.11g
802.11b	Yes	No	No	11 Mbps	Introduced in 1999 Longer range than 802.11a Better able to penetrate building structures

IEEE WLAN Standard	2.4 GHz	5 GHz	6 GHz	Max Data Rate	Description
802.11g	Yes	No	No	54 Mbps	Introduced in 2003 Backward compatible with 802.11b with reduced bandwidth capacity
802.11n	Yes	Yes	No	600 Mbps	Introduced in 2009 Also known as High Throughput (HT) Distance range of up to 70 m (230 feet) APs and wireless clients require multiple antennas using MIMO technology Backward compatible with 802.11a/b/g devices with limited data rates
802.11ac	No	Yes	No	6.93 Gbps	Introduced in 2013 Also known as Very High Throughput (VHT) Uses MIMO technology Up to eight antennas can be supported Backward compatible with 802.11a/n devices with limited data rates
802.11ax	Yes	Yes	Yes	4x 802.11ac	Released in 2019 (latest standard) Also known as High-Efficiency Wireless (HEW) Higher data rates and increased capacity Handles many connected devices Improved power efficiency 1 GHz and 7 GHz capable when those frequencies become available

The Wi-Fi Alliance introduced a set of simplified names to identify each Wi-Fi generation, as listed in Table 22-2.

Table 22-2 Wi-Fi Alliance Generational Names

Wi-Fi Alliance Designation	Bands Supported	IEEE 802.11 Amendments Supported
Wi-Fi 0	2.4	802.11 (the original)
Wi-Fi 1	2.4	802.11b
Wi-Fi 2	5	802.11a
Wi-Fi 3	2.4	802.11g
Wi-Fi 4	2.4, 5	802.11n
Wi-Fi 5	5	802.11ac

Wi-Fi Alliance Designation	Bands Supported	IEEE 802.11 Amendments Supported
Wi-Fi 6	2.4, 5	802.11ax
Wi-Fi 6E	2.4, 5, 6	802.11ax
Wi-Fi 7	2.4, 5, 6	802.11be

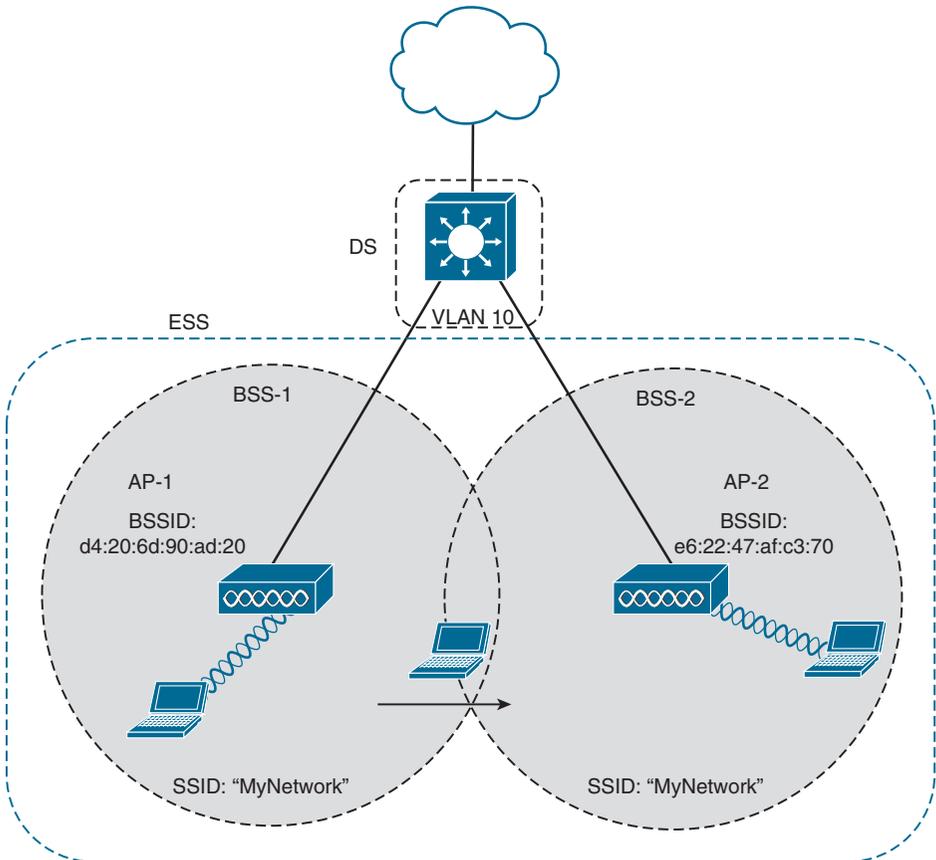
Wireless Topologies

The 802.11 standard identifies two main wireless topology modes: infrastructure mode and Independent Basic Service Set (IBSS). IBSS is also known as ad hoc mode. With the ubiquity of wireless networks, mesh topologies are now common.

Infrastructure Mode

With infrastructure mode, wireless clients interconnect via an AP. Figure 22-4 illustrates infrastructure mode terminology. Notice that the configuration of the APs to share the same SSID allows wireless clients to roam between BSAs.

Figure 22-4 Example of ESS Infrastructure Mode



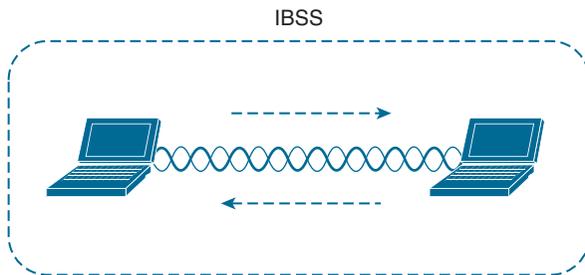
Infrastructure mode terminology includes the following:

- **Basic service set (BSS):** This consists of a single AP interconnecting all associated wireless clients.
- **Basic service area (BSA):** This is the area that is bound by the reach of the AP's signal. The BSA is also called a *cell* (the gray area in Figure 22-4).
- **Basic service set identifier (BSSID):** This is the unique, machine-readable identifier for the AP that is in the format of a MAC address and is usually derived from the AP's wireless MAC address.
- **Service set identifier (SSID):** This is a human-readable, non-unique identifier used by the AP to advertise its wireless service.
- **Distribution system (DS):** APs connect to the network infrastructure using the wired DS, such as Ethernet. An AP with a wired connection to the DS is responsible for translating frames between 802.3 Ethernet and 802.11 wireless protocols.
- **Extended service set (ESS):** When a single BSS provides insufficient coverage, two or more BSSs can be joined through a common DS into an ESS. An ESS is the union of two or more BSSs interconnected by a wired DS. Each ESS is identified by its SSID, and each BSS is identified by its BSSID.

IBSS, or Ad Hoc Mode

In the 802.11 standard, Independent Basic Service Set (IBSS) is defined as two devices connected wirelessly in a peer-to-peer (P2P) manner without the use of an AP. One device takes the role of advertising the wireless network to clients. The IBSS allows two devices to communicate directly without the need for any other wireless devices, as shown in Figure 22-5. IBSSs do not scale well beyond 8 to 10 devices.

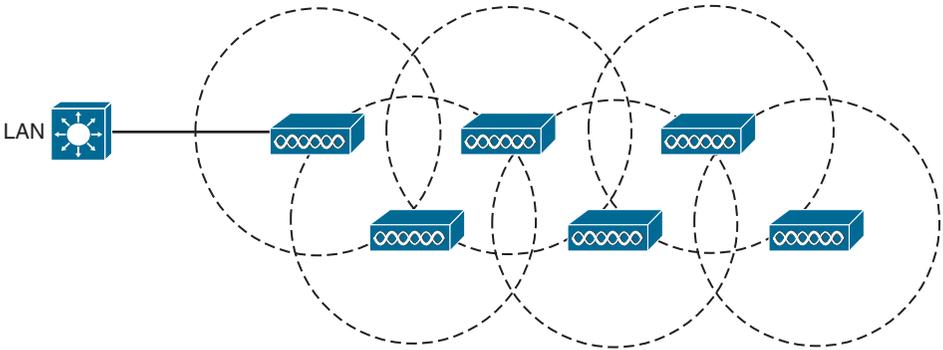
Figure 22-5 802.11 Independent Basic Service Set



Mesh

Having a wired DS connecting all APs is not always practical or necessary. Instead, APs can be configured to connect in mesh mode. In this mode, APs bridge client traffic between each other, as shown in Figure 22-6.

Each AP in the mesh maintains a BSS on one channel used by wireless clients. Then the APs bridge between each other using other channels. The mesh network runs its own dynamic routing protocol to determine the best path to the wired network.

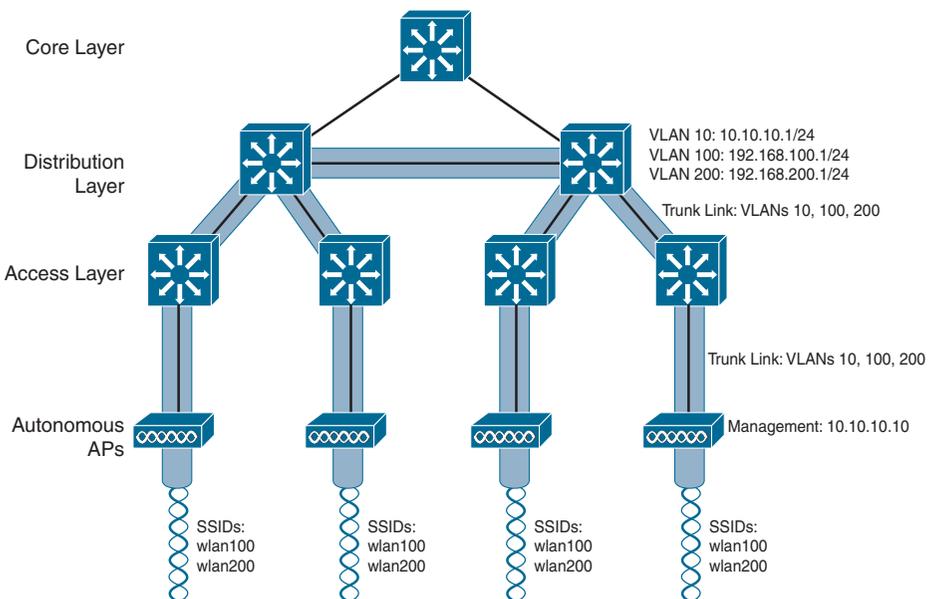
Figure 22-6 Example of a Wireless Mesh Network

AP Architectures

APs can be networked together in a variety of architectures. The size and scalability of the network determine which architecture is most suited for a given implementation.

Autonomous AP Architecture

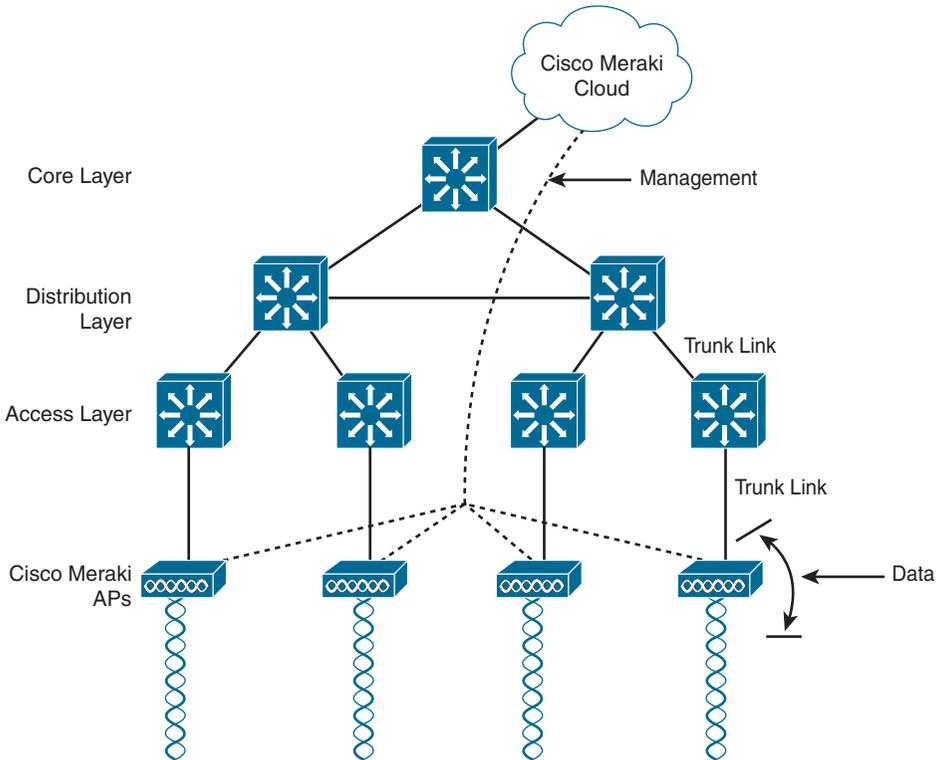
An autonomous AP is a self-contained device with both wired and wireless hardware so that it can bridge to the wired VLAN infrastructure wireless clients that belong to SSIDs, as shown in Figure 22-7. Each autonomous AP must be configured with a management IP address so that it can be remotely accessed using Telnet, SSH, or a web interface. Each AP must be individually managed and maintained unless you use a management platform such as Cisco DNA Center.

Figure 22-7 Autonomous APs

Cloud-Based AP Architecture

Cloud-based AP management is an alternative to purchasing a management platform. The AP management function is pushed into the Internet cloud. For example, Cisco Meraki is a cloud-based AP management service that allows you to automatically deploy Cisco Meraki APs. These APs can then be managed from the Meraki cloud web interface (dashboard). In Figure 22-8, the same APs shown in Figure 22-7 are now managed in the cloud.

Figure 22-8 Cisco Meraki Cloud-Based AP Management

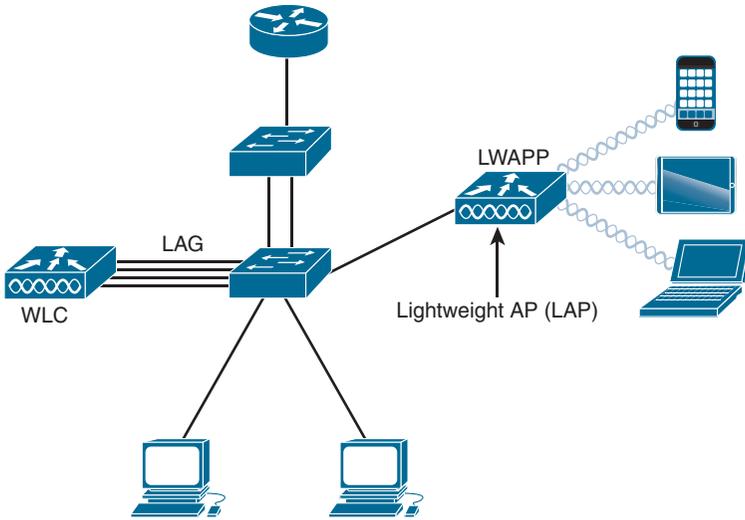


Notice that there are two distinct paths for data traffic and for management traffic, corresponding to the following two functions:

- **A control plane:** Traffic used to control, configure, manage, and monitor the AP itself
- **A data plane:** End-user traffic passing through the AP

Lightweight AP Architectures

Wireless LAN controllers (WLCs) use Lightweight Access Point Protocol (LWAPP) to communicate with lightweight APs (LAPs), as shown in Figure 22-9. LAPs are useful in situations where many APs are required in the network. They are “lightweight” because they only perform the 802.11 wireless operation for wireless clients. Each LAP is automatically configured and managed by the WLC.

Figure 22-9 Controller-Based AP Architecture

Notice in Figure 22-9 that the WLC has four ports connected to the switching infrastructure. These four ports are configured as a link aggregation group (LAG) so they can be bundled together. Much like EtherChannel, LAG provides redundancy and load balancing.

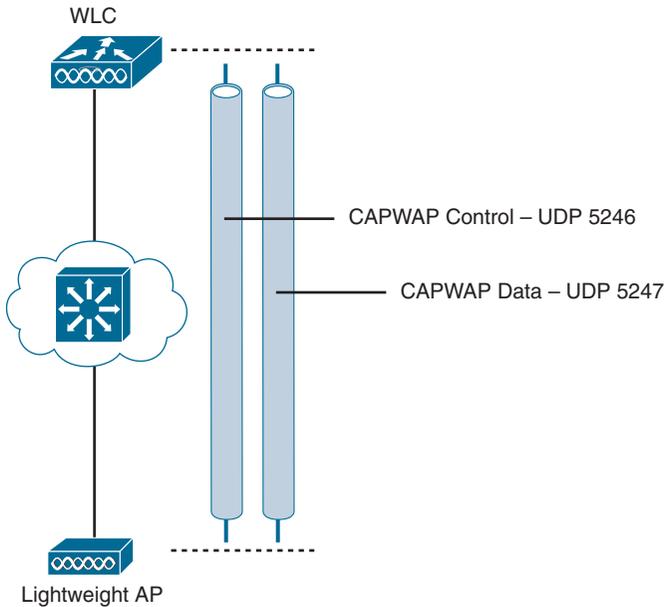
CAPWAP Operation

The division of labor between the WLC and LAPs is known as *split-MAC architecture*. The LAP must interact with wireless clients on some low level, known as the Media Access Control (MAC) layer. These functions must stay with the LAP hardware, closest to the clients. The management functions are not integral to handling frames but are things that should be centrally administered. Therefore, those functions can be moved to a centrally located platform away from the AP. Table 22-3 summarizes MAC functions of the LAP and WLC.

Table 22-3 Split-MAC Functions of the AP and WLC

AP MAC Functions	WLC MAC Functions
Beacons and probe responses	Authentication
Packet acknowledgments and retransmissions	Association and re-association of roaming clients
Frame queueing and packet prioritization	Frame translation to other protocols
MAC layer data encryption and decryption	Termination of 802.11 traffic on a wired interface

LWAPP has been replaced with the Control and Provisioning of Wireless Access Points (CAPWAP) tunneling protocol to implement these split-MAC functions. CAPWAP uses two tunnels—one for control and one for data—as shown in Figure 22-10 and described in the list that follows:

Figure 22-10 CAPWAP Control and Data Tunnels

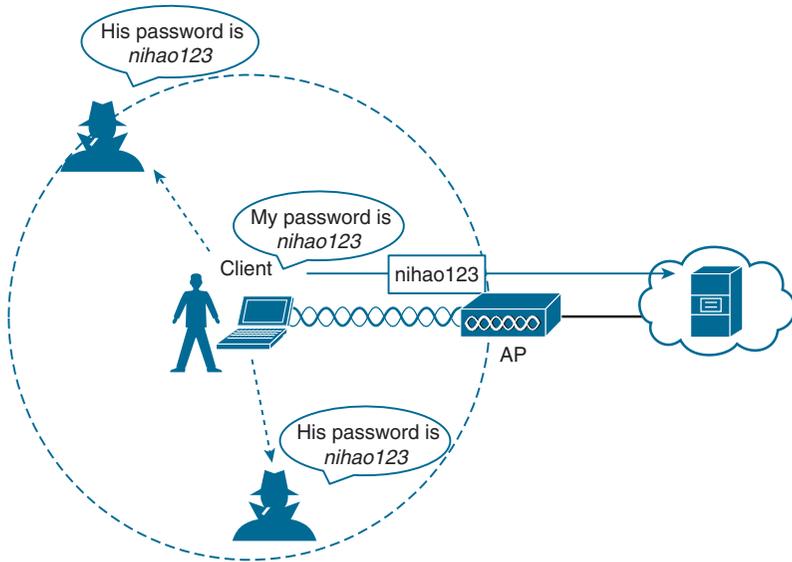
- **CAPWAP control message tunnel:** Carries exchanges that are used to configure the LAP and manage its operation. The control messages are authenticated and encrypted, so the LAP is securely controlled by only the appropriate WLC and then transported over the control tunnel using UDP port 5246.
- **CAPWAP data tunnel:** Used for packets traveling to and from wireless clients that are associated with the AP. Data packets are transported over the data tunnel using UDP port 5247 but are not encrypted by default. When data encryption is enabled for a LAP, packets are protected with Datagram Transport Layer Security (DTLS).

Wireless Security Protocols

Wireless traffic is inherently different from traffic traveling over a wired infrastructure. Any wireless device operating in the same frequency can hear the frames and potentially read them. Therefore, WLANs need to be secured to allow only authorized users and devices and to prevent eavesdropping and tampering of wireless traffic.

Wireless Authentication Methods

For wireless devices to communicate over a network, they must first associate with the AP. An important part of the 802.11 process is discovering a WLAN and subsequently connecting to it. During this process, transmitted frames can reach any device within range. If the wireless connection is not secured, then others can read the traffic, as shown in Figure 22-11.

Figure 22-11 Open Wireless Network

The best way to secure a wireless network is to use authentication and encryption systems.

Two types of authentication were introduced with the original 802.11 standard:

- **Open system authentication:** Should only be used in situations where security is of no concern. The wireless client is responsible for providing security such as by using a virtual private network (VPN) to connect securely.
- **Shared key authentication:** Provides mechanisms shown in Table 22-4 to authenticate and encrypt data between a wireless client and an AP. However, the password must be pre-shared between the parties to allow connection.

Table 22-4 Shared Key Authentication Methods

Authentication Method	Description
Wired Equivalent Privacy (WEP)	The original 802.11 specification designed to secure the data using the Rivest Cipher 4 (RC4) encryption method with a static key. However, the key never changes when exchanging packets. This makes WEP easy to hack. WEP is no longer recommended and should never be used.
Wi-Fi Protected Access (WPA)	A Wi-Fi Alliance standard that uses WEP but secures the data with the much stronger Temporal Key Integrity Protocol (TKIP) encryption algorithm. TKIP changes the key for each packet, making it much more difficult to hack.
WPA2	The current industry standard for securing wireless networks. It uses the Advanced Encryption Standard (AES) for encryption. AES is currently considered the strongest encryption protocol.
WPA3	The next generation of Wi-Fi security. All WPA3-enabled devices use the latest security methods, disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF). However, devices with WPA3 are not yet readily available.

WPA and WPA2

Home routers typically have two choices for authentication: WPA and WPA2. WPA2 is the stronger of the two. WPA2 authentication methods included the following:

- **Personal:** Intended for home or small office networks, users authenticate using a pre-shared key (PSK). Wireless clients authenticate with the wireless router using a pre-shared password. No special authentication server is required.
- **Enterprise:** Intended for enterprise networks but requires a Remote Authentication Dial-In User Service (RADIUS) authentication server. Although more complicated to set up, it provides additional security. The device must be authenticated by the RADIUS server, and then users must authenticate using the 802.1X standard, which uses Extensible Authentication Protocol (EAP) for authentication.

802.1X/EAP

With open and WEP authentication, wireless clients are authenticated locally at the AP without further intervention. The scenario changes with 802.1X: The client uses open authentication to associate with the AP, and then the client authentication process occurs at a dedicated authentication server. Figure 22-11 shows the three-party 802.1X arrangement, which consists of the following entities:

- **Supplicant:** The client device that is requesting access.
- **Authenticator:** The network device that provides access to the network. In Figure 22-11, the AP forwards the supplicant's message to the WLC.
- **Authentication server (AS):** The device that permits or denies network access based on a user database and policies (usually a RADIUS server).

WPA3

WPA3 includes four features:

- **WPA3-Personal:** In WPA2-Personal, threat actors can listen in on the “handshake” between a wireless client and the AP and use brute-force attacks to try to guess the PSK. WPA3-Personal thwarts such attacks by using Simultaneous Authentication of Equals (SAE), a feature specified in the IEEE 802.11-2016. The PSK is never exposed, making it impossible for the threat actor to guess.
- **WPA3-Enterprise:** WPA3-Enterprise still uses 802.1X/EAP authentication. However, it requires the use of a 192-bit cryptographic suite and eliminates the mixing of security protocols for previous 802.11 standards. WPA3-Enterprise adheres to the Commercial National Security Algorithm (CNSA) suite, which is commonly used in high-security Wi-Fi networks.
- **Open networks:** Open networks in WPA2 send user traffic in unauthenticated plaintext. In WPA3, open or public Wi-Fi networks still do not use any authentication. However, they do use Opportunistic Wireless Encryption (OWE) to encrypt all wireless traffic.

- **IoT onboarding:** Although WPA2 included Wi-Fi Protected Setup (WPS) to quickly onboard devices that were not previously configured, WPS is vulnerable to a variety of attacks and is not recommended. Furthermore, IoT devices are typically headless, meaning they have no built-in GUI for configuration and need an easy way to get connected to the wireless network. Device Provisioning Protocol (DPP) was designed to address this need. Each headless device has a hard-coded public key. The key is typically stamped on the outside of the device or its packaging as a Quick Response (QR) code. The network administrator can scan the QR code and quickly onboard the device. Although DPP is not strictly part of the WPA3 standard, it will replace WPS over time.

Wireless Encryption Methods

Encryption is used to protect data. An intruder may be able to capture encrypted data, but he or she would not be able to decipher it in any reasonable amount of time. The following encryption protocols are used with wireless authentication:

- **Temporal Key Integrity Protocol (TKIP):** TKIP is the encryption method used by WPA. It provides support for legacy WLAN equipment and addresses the original flaws associated with the 802.11 WEP encryption method. It makes use of WEP but encrypts the Layer 2 payload using TKIP and carries out a message integrity check (MIC) in the encrypted packet to ensure that the message has not been altered.
- **Advanced Encryption Standard (AES):** AES is the encryption method used by WPA2. It is the preferred method because it is a very strong method of encryption. It uses Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP), which allows destination hosts to recognize if the encrypted and nonencrypted bits have been altered.
- **Counter/CBC-MAC Protocol (CCMP):** CCMP is the encryption protocol used by WPA2. It provides enhanced data confidentiality and integrity by using AES. CCMP operates using Counter Mode for encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity, ensuring that both encrypted and non-encrypted parts of the packet have not been altered. This makes CCMP a highly secure and reliable protocol for protecting wireless communications.
- **The Galois/Counter Mode Protocol (GCMP):** GCMP is the encryption protocol used by WPA3. It enhances security and efficiency compared to CCMP. GCMP combines the Galois Message Authentication Code (GMAC) for data integrity and authenticity with the Counter Mode for encryption. This dual approach ensures that encrypted data remains confidential, and any tampering with the data can be detected. GCMP provides robust protection against attacks and improves performance, making it suitable for modern wireless networks that require higher security standards.

Table 22-5 summarizes the basic differences between WPA, WPA2, and WPA3. Each successive version is meant to replace prior versions and offer better security features. You should avoid using WPA and use WPA2 instead—at least until WPA3 becomes widely available on wireless client devices, APs, and WLCs.

Table 22-5 Wireless Authentication and Encryption Comparison

Feature	WPA	WPA2	WPA3
Authentication with pre-shared keys?	Yes	Yes	Yes
Authentication with 802.1X?	Yes	Yes	Yes
Encryption and MIC with TKIP?	Yes	No	No
Encryption and MIC with AES and CCMP?	Yes	Yes	No
Encryption and MIC with AES and GCMP?	No	No	Yes

Study Resources

For today's exam topics, refer to the following resources for more study.

Resource	Module or Chapter
Cisco Network Academy: Switching, Routing, and Wireless Essentials v7	12
CCNA 200-301 Official Cert Guide, Volume 2, 2nd edition	1–3
Portable Command Guide	23

This page intentionally left blank

Numerics

- 3-1-4 rule, 70
- 3DES (Triple DES), 351
- 10BASE-T, 36
- 100BASE-TX, 36-37
- 802.1X, 170, 187-189
- 802.11 standards, 161-162

A

- AAA, switch port hardening, 186-187
- access attack, 299-300
- access control
 - local authentication, 183-184
 - SSH (Secure Shell), 184-186, 230-231
- access layer, 14, 26
- access-list command, 314-317
- acknowledgment, 5
- ACL (access control list), 307, 415
 - adding comments, 318
 - comparing IPv4 and IPv6, 320-321
 - defining, 307
 - design guidelines, 311-312
 - extended named IPv4, 318
 - extended numbered IPv4, 315
 - command parameters, 316
 - deny FTP from subnets, 316
 - deny only Telnet from subnet, 316-317
 - identification, 311
 - interface processing, 308
 - IPv6
 - configuration, 321-322
 - extended, 323
 - standard, 322
 - verifying, 323-325
 - matching logic, 308-309
 - named IPv4, 317
 - deny a single host from a given subnet, 317-318
 - steps and syntax, 317
 - operation, 307
 - planning to use, 309
 - standard numbered IPv4, 313
 - deny a specified host, 314
 - deny a specified subnet, 315
 - deny Telnet or SSH to the router, 315
 - permit specific network, 314
 - troubleshooting, 326
 - types of, 310
- ad hoc mode, 164
- address spoofing attack, 302
- administrative distance, 209-211
- Advanced Summary page, WLC, 175
- adware, 298
- AES (Advanced Encryption Standard), 171, 351
- AF (Assured Forwarding), 360
- AI (artificial intelligence). *See* generative AI
- AIOps (artificial intelligence for IT operations), 435-436
- algorithm
 - Bellman-Ford, 207
 - CSMA/CD, 34-35
 - SPF (shortest path first), 213-214, 269-270
 - STP (Spanning Tree Protocol), 104
 - VPN encryption, 351-352
- AMP (Advanced Malware Protection), 18
- amplification and reflection attack, 301
- ANDing, 59-60
- Ansible, 420
 - inventory file, 421-422
 - playbook, 422
 - versus Terraform, 427
 - YAML playbook, 421
- anycast address, 77
- AP (access point), 19
 - autonomous, 165
 - BSA (basic service area), 164
 - BSS (basic service set), 164
 - cloud-based architecture, 166
 - lightweight architecture, 166-167
 - split-MAC architecture, 167-168
 - SSID (service set identifier), 164
- API, RESTful, 432, 434-435
- application layer, TCP/IP model, 5
- architecture, AP (access point)
 - autonomous, 165
 - cloud-based, 166
 - split-MAC, 167-168

ARP (Address Resolution Protocol), 4

- attacks, 198–199
- dynamic inspection. *See* DAI (dynamic ARP inspection)

assets, 295**assigned multicast address, 75–76****asymmetric switching, 32****attack/s, 295**

- ARP, 198–199
- compromised-key, 298
- data modification, 297
- DHCP, 196–198
- DoS (denial of service), 298, 301
- eavesdropping, 297
- IP, 301–302
- IP address spoofing, 297
- man-in-the-middle, 298
- network, 299–300
- password, 303
- password-based, 298
- reconnaissance, 299
- sniffer, 298
- social engineering, 300–301
- transport layer, 302
- vector, 296
- VLAN, 194–195

authentication

- local, 183–184
- multifactor, 304
- REST, 432–434
- VPN, 352
- wireless, 168–169, 172
 - 802.1X/EAP, 170*
 - shared key, 169*
 - WPA and WPA2, 170*
 - WPA3, 170–171*

auto-MDIX, 48–49**autonomous AP architecture, 165****AVC (Application Visibility and Control), 18****B****backing up Cisco IOS images, 390–391****baiting, 300****band, 159****bandwidth, 357****bandwidth command, 280****BDR (backup designated router), 269****Bellman-Ford algorithm, 207****BID (bridge ID), 104–105, 114****biometric credentials, 304****botnet, 301****BPDU (bridge protocol data unit), 104****BPDU Filter, configuration, 116–117****BPDU Guard, configuration, 116****bridge, 29****broadband**

- cable modem, 344–345
- DSL, 344
- wireless, 345–346

broadcast, 29**broadcast address, IPv4 subnet, 62–63****broadcast domain, 31****broadcast storm, 103****BSA (basic service area), 164****BSS (basic service set), 164****buffer overflow attack, 300****bus topology, 25****C****cable. *See also* network/s, media**

- crossover, 22–23, 37
- EIA/TIA standard Ethernet, 36–37
- RJ-45 connector, 36
- straight-through, 22
- UTP (unshielded twisted-pair), 36–37

cable modem, 344–345**CAPWAP (Control and Provisioning of Wireless Access Points), 167–168****CBWFQ (Class-Based Weighted Fair Queueing), 361****CCMP (Counter/CBC-MAC Protocol), 171****cd command, 387–388****CDP (Cisco Discovery Protocol), 365, 366**

- configuration, 366–367
- defaults, 365
- disabling on an interface, 367–368
- verifying, 367, 368–371

cdp holdtime command, 368**cdp timer command, 368****channel-group command, 124–125****channels, 159–160**

ChatGPT

- as network simulator, 439–442
- prompting, 436
- troubleshooting, 438

CIR (Committed Information Rate), 362**Cisco ACI (Application Centric Infrastructure), 402–404****Cisco Catalyst Center, 414–415, 417–418****Cisco devices. See also PVST+ (Per-VLAN Spanning Tree Plus); router/s; switches/switching**

- auto-MDIX, 48–49
- IFS (Integrated File System)
 - command/s*, 385–388
 - URL prefixes for specifying file locations*, 388
- password recovery, 392–393
- WebUI
 - configuring access*, 42
 - dashboard*, 43

Cisco DevNet Learning Labs, 427**Cisco IOS, 41. See also CLI (command-line interface)**

- console error messages, 44
- images
 - backing up*, 390–391
 - restoring*, 391–392
- subconfiguration modes, 46

Cisco SD-Access, 407

- architecture, 407
- Cisco Catalyst Center, 414–415, 417–418
- overlay, 411
 - LISP*, 412–414
 - VXLAN tunnels*, 411–412
- scalable groups, 415
- underlay, 409–411
 - deploying on existing equipment*, 409
 - new deployments*, 409–411
- user groups, 416–417

classful addressing, 58–59**classful routing protocols, 208****classification, 358****classless routing protocols, 208****clear ip ospf process command, 291****CLI (command-line interface). See also**

- command/s**
 - accessing, 41
 - command history, 45
 - console password, 219

- EXEC sessions, 43
- navigation and editing shortcuts, 44–45
- privileged EXEC mode, 219
- using the help facility, 43–44

cloud/cloud computing, 395

- based AP architecture, 166
- models, 398
- server virtualization, 396–397
- services, 397–398
- virtual network infrastructure, 398–399

collision domain, 31, 37**command/s**

- access-list, 314–317
- bandwidth, 280
- cd, 387–388
- cdp holdtime, 368
- cdp timer, 368
- channel-group, 124–125
- clear ip ospf process, 291
- configuration file management, 388–390
- configure terminal, 46, 116
- copy, 388–390
- crypto key zeroize rsa, 185–186
- debug ip nat, 338
- dir, 386, 391
- getting help from ChatGPT, 436–442
- history, 45
- ifconfig, 156, 157
- IFS (Integrated File System), 385–388
- interface port-channel, 125
- interface range, 48, 124–125
- ip access-list, 317–318
- ip address dhcp, 143–144
- ip arp inspection validate, 201
- ip dhcp excluded address, 138–140
- ip dhcp snooping, 198, 200–201
- ip forward-protocol udp, 143
- ip helper-address, 142–143
- ip http access-class, 42
- ip nat inside source static, 334
- ip nat pool, 334–335
- ip ospf cost, 280
- ip ospf priority, 289
- ip route, 256
- ip routing, 249
- ipconfig, 50
- ipconfig/all, 141–142, 152
- ipv6 access-class, 322
- ipv6 access-list, 321–322, 323
- ipv6 address, 226–227
- ipv6 address autoconfig, 148

- ipv6 nd managed-config-flag, 146
- ipv6 nd other-config-flag, 146
- ipv6 route, 261–262
- ipv6 traffic-filter, 322
- ipv6 unicast-routing, 147, 226
- login local, 183–184
- name, 92
- network, 277–278
- no cdp enable, 367–368
- no cdp run, 367
- no shutdown, 186, 250
- no switchport, 250
- OSPF troubleshooting, 292–293
- passive-interface, 278
- ping, 49, 50–51, 229
- router configuration, syntax, 218
- router ospf, 276
- router-id, 276–277
- service-password encryption, 219
- show, 45
 - show access-lists, 319, 324–325
 - show cdp interface, 366, 368
 - show cdp neighbors, 367
 - show cdp neighbors detail, 369–371
 - show cdp traffic, 371–374
 - show etherchannel summary, 126
 - show file system, 385–386
 - show flash, 386–387
 - show interface, 222–225
 - show interface status, 53–54
 - show interfaces switchport, 94, 100, 126–127
 - show interfaces trunk, 99–100
 - show ip dhcp binding, 140
 - show ip dhcp conflict, 150
 - show ip dhcp server statistics, 140–141
 - show ip interface, 319–320
 - show ip interface brief, 221–222, 247–248, 281, 366–367
 - show ip nat statistics, 337
 - show ip nat translations, 336
 - show ip ospf, 282–283
 - show ip ospf interface brief, 283
 - show ip ospf neighbor, 281–282, 290
 - show ip protocols, 210–211, 281
 - show ip route, 209, 220–221, 237–238, 247, 249–250, 255, 256–257, 259, 281
 - show ip route ospf, 287
 - show ip ssh, 184, 185
 - show ipv6 access-list, 325
 - show ipv6 dhcp binding, 149
 - show ipv6 interface, 228, 325
 - show ipv6 interface command, 325
 - show ipv6 route, 238–239, 262, 263
 - show llpd, 373
 - show llpd interface, 373
 - show llpd neighbors, 373
 - show llpd neighbors detail, 373–374
 - show llpd traffic, 374
 - show logging, 382–384
 - show mac address-table, 97
 - show ntp associations, 385
 - show ntp status, 385
 - show port-security, 190–191
 - show port-security interface, 193
 - show run, 323–324
 - show running-config, 220, 320
 - show snmp, 378–379
 - show snmp community, 379
 - show spanning-tree, 115
 - show spanning-tree vlan, 117–118
 - show standby, 131–132
 - show standby brief, 131–132, 134
 - show vlan, 97, 247
 - show vlan brief, 91–93
 - shutdown, 186
 - snmp-server community, 378
 - spanning-tree bpdguard default, 116
 - spanning-tree guard root, 117–118
 - spanning-tree mode, 113–114
 - spanning-tree pathcost method, 105
 - spanning-tree portfast bpdudfilter default, 117
 - spanning-tree portfast default, 116
 - spanning-tree vlan, 114–115
 - ssh, 230–231
 - standby ip, 131
 - standby preempt, 131
 - standby priority, 131
 - switch configuration, 46–48
 - switchport access vlan, 186
 - switchport mode, 186
 - switchport mode access, 189
 - switchport mode trunk, 89–90
 - switchport negotiate, 90
 - switchport port-security, 189
 - switchport port-security aging, 191–192
 - switchport trunk native vlan, 186
 - terraform apply, 426
 - traceroute, 229–230
 - tracert, 51–52, 258, 259
 - username secret, 183–184
 - VLAN troubleshooting, 98

comments, adding to an ACL, 318

community cloud, 398

compromised-key attack, 298

configuration

BPDU Filter, 116–117

BPDU Guard, 116

CDP (Cisco Discovery Protocol),
366–367

DHCPv4, 138

DHCPv4 server, 138–140

EtherChannel, 124–125

HSRP (Hot Standby Router Protocol),
131

LLDP (Link Layer Discovery Protocol),
371–372

Loop Guard, 118
manual, 418

NAT (Network Address Translation)
dynamic, 334–335
overload, 335–336
static, 334

OSPF network, 277–278, 286–287

port security, 189–190

PortFast, 116

provisioning, 419

Rapid PVST+, 113–114

Root Guard, 117–118

router interface, 219–220

SNMP (Simple Network Management
Protocol), 378

STP (Spanning Tree Protocol), 112–113

templates and variables, 419–420

trunking, 94–96

virtual interface, 176–178

configure terminal command, 46, 116

congestion management, 361–362

connectionless protocol, 9–10

connectivity

DHCP (Dynamic Host Configuration
Protocol), 150

IPv4/IPv6, 229–231

verifying, 49

VLAN, troubleshooting, 97–98

control plane, 166, 399–400

controller, 400–401

convergence

link-state routing protocol, 214–215

Rapid PVST+, 109

STP (Spanning Tree Protocol),
105–106

copy commands, 388–390

core layer, 26

core layer switch, 15

CoS (Class of Service), 360

cost

OSPFv2, 278–279

switch, 14

creating

VLAN (virtual local-area network), 92

WLAN (wireless LAN), 178–181

crossover cable, 22–23, 37

**crypto key zeroize rsa command,
185–186**

CSMA/CD, 34–35

cut-through switching, 32

D

DAD (duplicate address detection), 76

DAI (dynamic ARP inspection), 199–201

dashboard, WebUI, 43

data encapsulation. See encapsulation

data exfiltration, 296

data formats, 429–431

data link layer, OSI model, 32–33

data modification attack, 297

data plane, 166, 399

**DDoS (distributed denial of service)
attack, 301**

dead interval, OSPFv2, 288

debug ip nat command, 338

debuggers, 297

default gateway, 121, 233

default route, 237, 239

IPv4, 255–258

IPv6, 261–262

redistributing, 287

DES (Data Encryption Standard), 351

devices, 14. See also access control;

router/s; switches/switching

AP (access point), 19

bridge, 29

end, 22

firewall

next-generation, 18

software, 16

stateful, 16

- IDS (intrusion detection system), 16–18
 - IPS (intrusion prevention system), 18
 - NAT-enabled, 329
 - remote access using SSH, 230–231
 - routers, 15–16
 - configuring as a DHCPv4 client, 143–144*
 - configuring to relay DHCPv4 requests, 142–143*
 - SOHO, 24*
 - switches, 14, 29–30. *See also* switches/switching
 - access layer, 14*
 - broadcast domain, 31*
 - collision domain, 31*
 - cost, 14*
 - frame forwarding, 31*
 - interface, 14*
 - WLC (wireless LAN controller), 19
 - DHCP (Dynamic Host Configuration Protocol), 3**
 - attacks, 196–198
 - resolving address conflicts, 149–150
 - verifying switch port configuration, 150
 - DHCPv4, 137–138, 150**
 - configuration options, 138
 - configuring a router as a client, 143–144
 - configuring a router to relay requests, 142–143
 - server, configuring a router as, 138–140
 - verifying, 140–141
 - DHCPv6, 144**
 - configuring a router as a stateful server, 149
 - configuring a router as a stateless server, 147–148
 - configuring an interface as a client, 148
 - full operation, 146–147
 - SLAAC (stateless address autoconfiguration)
 - NDP messages, 144*
 - neighbor discovery, 145–146*
 - stateful, 146
 - stateless, 146
 - testing connectivity, 150
 - digital certificate, 304**
 - Dijkstra algorithm, 213–214**
 - dir command, 386, 391**
 - directly connected network, 237**
 - distance vector routing protocols, 207**
 - distribution layer, 26**
 - distribution layer switch, 14–15**
 - DLP (data loss prevention), 296**
 - DMVPN (Dynamic Multipoint VPN), 349**
 - DNS (Domain Name System), 3, 150**
 - resource records, 151
 - root servers, 151–152
 - troubleshooting, 152
 - URI (uniform resource identifier)
 - structure, 150–151
 - verifying host IP configuration
 - on Linux, 156–158*
 - on macOS, 155–156*
 - on Windows, 153–155*
 - DoS (denial of service) attack, 298, 301**
 - double-tagging attack, 194**
 - DR (designated router), 269**
 - DSCP (Differentiated Services Code Point), 359–360**
 - DSL (Digital Subscriber Line), 344**
 - DTP (Dynamic Trunking Protocol), 89–90, 194**
 - dual stacking, 82–83**
 - dumpster diving, 301**
 - dynamic NAT (Network Address Translation), 332, 334–335**
 - dynamic routing, 205–206**
- ## E
- EAP (Extensible Authentication Protocol), 170**
 - eavesdropping attack, 297**
 - edge ports, RSTP (Rapid STP), 111–112**
 - EF (Expedited Forwarding), 360**
 - EGP (exterior gateway protocol), 207**
 - email, spam, 300**
 - encapsulation, 4, 12–13, 33, 412**
 - encryption**
 - password, 219
 - tools, 297
 - VPN, 350
 - wireless, 171
 - end devices, 22**
 - error recovery, reliability, 7–8**
 - ESS (extended service set), 164**
 - EtherChannel, 121, 123**

benefits, 122
 configuration, 124–125
 implementation restrictions, 122–123
 LACP (Link Aggregation Control Protocol), 124
 PAgP (Port Aggregation Protocol), 123–124
 troubleshooting, 127
 verifying, 125–127

Ethernet, 4, 25. See also switches/

switching

10BASE-T, 36
 100BASE-TX, 36–37
 addressing, 37–38
 bridge, 29
 bus, 33
 CSMA/CD, 34–35
 framing, 38–39
 group addresses, 38
 legacy technologies, 33–34, 35
 OUI (organizationally unique identifier), 37
 standards, 22, 35
 UTP cabling, 36–37

EUI-64, 80–81

EXEC sessions, CLI, 43

exit-interface parameter, 254–255

exploit, 296

extended IPv6 ACL, 323

extended named IPv4 ACL, steps and syntax, 318

extended numbered IPv4 ACL, 315

command parameters, 316
 deny FTP from subnets, 316
 deny only Telnet from subnet, 316–317

extended System ID, PVST+, 108–109

F

FHRP (first-hop redundancy protocol), 121, 128–129

GLBP (Gateway Load Balancing Protocol), 136
 HSRP (Hot Standby Router Protocol), 130
configuration, 131
load balancing, 132–134
priority and preemption, 131
troubleshooting, 135
verifying, 131–132
versions, 130

VRRP (Virtual Router Redundancy Protocol), 135

FIN bit, 9

firewall

next-generation, 18
 software, 16
 stateful, 16

forensic tools, 297

fragment-free switching, 32

frame, 29

BPDU (bridge protocol data unit), 104
 Ethernet, 38–39

FTP (File Transfer Protocol), 3

full-duplex, 48

G

GCMP (Galois/Counter Mode Protocol), 171

generative AI, 436

ChatGPT
as network simulator, 439–442
prompting, 436
troubleshooting, 438

get messages, SNMP, 375–376

GLBP (Gateway Load Balancing Protocol), 136

global unicast address, 70–72

3–1–4 rule, 70
 configuration options, 72

gratuitous ARP message, 198

Graziani, Rick

3–1–4 rule, 70
IPv6 Fundamentals, 67

GRE (Generic Routing Encapsulation), 348

H

half-duplex, 48

HCL (HashiCorp Configuration Language), 423

header

IPv4, 57–58
 OSPF, 266–267
 TCP, 6
 UDP, 7

hello packet

- modifying, 288
- OSPF, 266–268

hextet, 70–71, 78**hierarchical campus design, 25–26****HMAC (hashed message authentication code), 352****hold-down timer, 212****host range, IPv4 subnet, 62–63****HSRP (Hot Standby Router Protocol), 130**

- configuration, 131
- load balancing, 132–134
- priority and preemption, 131
- troubleshooting, 135
- verifying, 131–132
- versions, 130

HTTP (Hypertext Transfer Protocol), 3, 5, 11–12**hybrid cloud, 398****I****IaaS (infrastructure as a service), 398****IaC (Infrastructure as Code) tools**

- Ansible, 420–422
- Terraform, 422–427

IANA (Internet Assigned Numbers Authority), 71**IBSS (Independent Basic Service Set), 164****ICMP (Internet Control Message Protocol), 4****icons, networking, 13****IDS (intrusion detection system), 16–18****IEEE standards**

- Ethernet, 35
- native VLAN, 193–194
- STP (Spanning Tree Protocol), 104
- wireless, 161–162

IETF (Internet Engineering Task Force), 67**ifconfig command, 156, 157****IFS (Integrated File System)**

- command/s, 385–388
- URL prefixes for specifying file locations, 388

IGP (interior gateway protocol), 207, 211**IMAP (Internet Message Access Protocol), 3****impersonation, 300****infrastructure mode, 163–164****inside network, 330****interface port-channel command, 125****interface range command, 48, 124–125****interface/s. *See also* port/s**

- ACLs, 308
- auto-MDIX, 48–49
- configuring a description, 220
- configuring as a DHCPv6 client, 148
- disabling CDP, 367–368
- Layer 1 problems, troubleshooting, 55
- northbound, 401
- passive, 278
- router, configuration, 219–220
- RSTP behavior, 110
- status codes, 53
- switch, 14
- virtual, creating, 176–178
- VLAN assignment, 93–95

internal threat, 296**Internet, 23****Internet layer, TCP/IP model, 10****internetwork, 23****inter-VLAN routing, 243**

- legacy, 243–244
- multilayer switching, 245, 248
 - configuring a Layer 3 routed port, 250*
 - creating additional SVIs, 248–250*
- router on a stick, 244, 245–248

intranet, 23**IP (Internet Protocol), 4****ip access-list command, 317–318****ip address dhcp command, 143–144****ip arp inspection validate command, 201****IP attacks, 301–302****ip dhcp excluded address command, 138–140****ip dhcp snooping command, 198, 200–201****ip forward-protocol udp command, 143****ip helper-address command, 142–143****ip http access-class command, 42****ip nat inside source static command, 334****ip nat pool command, 334–335**

ip ospf cost command, 280

ip ospf priority command, 289

ip route command, 256

ip routing command, 249

IP settings, verifying

on Linux, 156–158

on macOS, 155–156

on Windows, 153–155

ipconfig command, 50

ipconfig/all command, 141–142, 152

IPP (IP Precedence), 359–360

IPS (intrusion prevention system), 18

IPsec, 352–355

IPv4, 57

address classes, 58–59

default route configuration, 255–258

duplicate IP addresses,
troubleshooting, 234

enabling on a router, 217–225

header format, 57–58

longest match, 235–236

migration to IPv6, 82–83

private addressing, 60

public addresses, 60

routing table, 237–238

static routing, 252–253

summary route configuration, 258–259

using next-hop parameter, 254

using the exit-interface parameter, 254–255

subnet mask, 59–60

ANDing, 59–60

binary values, 60

subnetting, 60–61, 63–64

*determining how many bits to borrow,
61–62*

determining the new subnet mask, 62

determining the subnet multiplier, 62

host range and broadcast address, 62–63

verifying connectivity, 229–231

VLSM (variable-length subnet masking),
64–66

IPv6, 67–68

ACL (access control list)

configuration, 321–322

extended, 323

standard, 322

verifying, 323–325

anycast address, 77

comparing with IPv4, 68–69

conventions for hexadecimal numbers, 78

default gateway, troubleshooting, 233

DHCPv6, 81

duplicate IP addresses, troubleshooting, 234

enabling on a router, 225–231

EUI-64, 80–81

global unicast address, 70–72

3-1-4 rule, 70

configuration options, 72

hextet, 70–71

interface ID, 70, 80

IPv4 embedded address, 74–75

link-local address, 73

longest match, 236

loopback address, 73

multicast address, 75

assigned, 75–76

solicited-node, 76–77

overview and benefits, 67–68

prefix, writing, 78–79

routing table, 238–239

SLAAC (stateless address

autoconfiguration), 81

static routing, 259–261

default route, 261–262

summary route, 262–263

subnetting, 79–80

unicast address, 69

unique local address, 74

unspecified unicast address, 73–74

verifying connectivity, 229–231

ipv6 access-class command, 322

ipv6 access-list command, 321–322, 323

ipv6 address autoconfig command, 148

ipv6 address command, 226–227

**ipv6 nd managed-config-flag
command, 146**

ipv6 nd other-config-flag command, 146

ipv6 route command, 261–262

ipv6 traffic-filter command, 322

ipv6 unicast-routing command, 147, 226

J-K-L

jitter, 357

**JSON (JavaScript Object Notation),
430–431**

**LACP (Link Aggregation Control
Protocol), 124**

LAN (local-area network), 23, 29–30

- collision domain, 31, 37
- device connection guidelines, 22–23
- switches, 37

LAP (lightweight AP), 166**latency, 357****Layer 2 switch, 32****Layer 3 switch, 32****leased lines, 341–342****lightweight AP architecture, 166–167****link-local address, 73****link-state routing protocols, 207–215.**

See also OSPF (Open Shortest Path First)

- building the LSDB, 212–213
- calculating the Dijkstra algorithm, 213–214
- convergence, 214–215

Linux, verifying IP settings, 156–158**LISP (Locator/ID Separation Protocol), 412–414****LLC (Logical Link Control)**

- sublayer, 33

LLDP (Link Layer Discovery Protocol), 371

- configuration, 371–372
- verifying, 372–374

LLQ (Low Latency Queueing), 361–362**load balancing, HSRP (Hot Standby Router Protocol), 132–134****local authentication, 183–184****local link address, 11****logical topology, 25****login, WLC (wireless LAN controller), 173–174****login local command, 183–184****longest match**

- IPv4, 235–236
- IPv6, 236

Loop Guard, configuration, 118**loopback address, 73****loss, 357****LSA (link-state advertisement), 268****LWAPP (Lightweight Access Point Protocol), 166****M****MAC (Media Access Control) address, 11, 30, 33, 37****MAC (Media Access Control) sublayer, 33****MAC address table, instability, 103****macOS, verifying IP settings, 155–156****malware**

- adware, 298
- ransomware, 298
- rootkit, 299
- spyware, 299
- Trojan horse, 298
- virus, 298
- worm, 298

management plane, 400**management VLAN, 193–194****man-in-the-middle attack, 298, 300, 302****manual configuration management, 418****marking, 360****media. *See* network, media****mesh, 164****message/s**

- of-the-day banner, 219
- OSPF (Open Shortest Path First), format, 265–266
- SNMP (Simple Network Management Protocol), 375–376
- syslog, 380–382

metric

- cost, 278–279, 280
- routing protocol, 208

Metro Ethernet, 343**MFA (multifactor authentication), 304****MIB (Management Information Base), 376–378****migration to IPv6, 82–83****MIMO (multiple input, multiple output), 161****ML (machine learning), 435****MPLS (Multiprotocol Label Switching), 343–344****MST (Multiple Spanning Tree), 107****MSTP (Multiple Spanning Tree Protocol), 107**

multiarea OSPF, 272

design, 272–274
performance, 274

multicast address, 75

assigned, 75–76
solicited-node, 76–77

multilayer switching, 245, 248

configuring a Layer 3 routed port, 250
creating additional SVIs, 248–250

N**name command, 92****named IPv4 ACL, 317**

deny a single host from a given subnet,
317–318
steps and syntax, 317

NAT (Network Address Translation), 60, 329, 331

benefits, 333
dynamic, 332, 334–335
inside network, 330
limitations, 333
outside network, 330
overload, 332–333, 335–336
static, 332, 334
topology, 329–330
troubleshooting, 337–338
verifying, 336–337

native VLAN, 193–194**navigation and editing shortcuts, CLI, 44–45****NBI (northbound interface), 401****neighbor discovery, SLAAC (stateless address autoconfiguration), 145–146****network access layer, TCP/IP model, 11–12****network command, 277–278****Network Summary page, WLC, 174****network/s. See also LAN (local-area network); VPN (virtual private network); WAN (wide-area network)**

access attack, 299–300
connectivity, verifying, 49
directly connected, 237
hierarchical campus design, 25–26
inside, 330
local-area, 23
media, 21

advantages and disadvantages, 21–22
standards, 22
troubleshooting, 52
UTP (unshielded twisted-pair), 34

OSPF, 288–289

outside, 330
reconnaissance attack, 299
remote, 237
resiliency, 103
scanning and hacking tools, 297
SOHO (small office/home office), 23–24
traffic types, 86
wide-area, 23

next-generation firewall, 18**next-hop parameter, 254****no cdp enable command, 367–368****no cdp run command, 367****no shutdown command, 186, 250****no switchport command, 250****NTP (Network Time Protocol), 384–385****O****Odom, Wendell, 82****OpenDaylight, 401–402****OpenFlow, 401–402****OSI (Open Systems Interconnection) model, 1–2**

communication process, 4–5
data link layer, 32–33
encapsulation, 4
layers and functions, 2
PDUs (protocol data units), 4
physical layer, 33, 39–40

OSPF (Open Shortest Path First)

BDR (backup designated router), 269
DR (designated router), 269
hello packet, 266–268
link-state routing process, 270–271
LSA (link-state advertisement), 268
message format, 265–266
multiarea, 272
design, 272–274
performance, 274
neighbor establishment, 266–268
packet types, 266
single-area, 265
SPF (shortest path first) algorithm, 269–270
versions, 265, 271–272

OSPFv2, 275

- addressing scheme, 275–276
- changing the reference bandwidth, 279–280
- cost values, 278–279
- dead interval, 288
- DR/BDR election, 289–291
- enabling on a router, 276
- hello packet, modifying, 288
- modifying the metric, 280
- network configuration, 277–278, 286–287
- network types, 288–289
- passive interfaces, 278
- redistributing a default route, 287
- router ID, 276–277
- troubleshooting, 291–293
- verifying, 280–283

OUI (organizationally unique identifier), 37**outside network, 330****overlay, Cisco SD-Access, 411–414****P****PaaS (platform as a service), 398****packet/s**

- crafting tools, 297
- forwarding, 203–204, 236
- OSPF (Open Shortest Path First), 266
- sniffers, 297
- switching, 342
 - Metro Ethernet, 343*
 - MPLS, 343–344*

PAgP (Port Aggregation Protocol), 123–124**PAR (positive acknowledgment with retransmission), 8****passive interfaces, 278****passive-interface command, 278****password/s**

- alternatives, 304–305
- attacks, 298, 300, 303
- best practices, 305–306
- console, 219
- crackers, 297
- encryption, 219
- guidelines, 303–304
- policies, 303
- recovering on Cisco devices, 392–393

- router, 219
- vulnerabilities, 303

PDU (protocol data units), 4**penetration testing, tools, 296–297****performance, multiarea OSPF, 274****phishing, 300****physical layer**

- OSI model, 33, 39–40
- TCP/IP model, 20

ping command, 49, 50–51, 229**poison reverse, 212****policies**

- Cisco SD-Access, 417
- password, 303

policing, 362**POP3 (Post Office Protocol), 3****PortFast, configuration, 116****port/s**

- assigning to a black hole VLAN, 186
- bandwidth, 105
- edge, 111–112
- hardening
 - 802.1X, 187–189*
 - AAA, 186–187*
- numbers, 7
- redirection, 300
- routed, 248
- security, 189
 - aging, 191–192*
 - configuration, 189–190*
 - port restoration after a violation, 192–193*
 - verifying, 190–191*
- states
 - PVST+, 108*
 - RSTP, 110*
 - STP, 105, 106*
- WLC (wireless LAN controller), 176

prefix, IPv6, writing, 78–79**pretexting, 300****private addressing, 60****private cloud, 398****privileged EXEC mode, CLI, 219****prompting generative AI, 436****public cloud, 398****PVST+ (Per-VLAN Spanning Tree Plus), 107**

- configuring and verifying the BID, 114
- extended System ID, 108–109
- port states, 108

Q

QoS (quality of service), 357–358

- AF (Assured Forwarding), 360
- CBWFQ (Class-Based Weighted Fair Queuing), 361
- CIR (Committed Information Rate), 362
- classification, 358
- congestion management, 361–362
- DSCP (Differentiated Services Code Point), 359–360
- EF (Expedited Forwarding), 360
- IPP (IP Precedence), 359–360
- LLQ (Low Latency Queuing), 361–362
- marking, 359, 360
- policing, 362
- shaping, 362–363
- TCP and, 363–364

quad-zero route. *See* **default route**

R

RADIUS, 187

ransomware, 298

Rapid PVST+, 107, 109

- configuration, 113–114
- convergence, 109

RCA (root cause analysis), 436

reconnaissance attack, 299

remote networks, 237

remote-access VPN, 347–348

resiliency, 103

REST

- API, 432, 434–435
- authentication types, 432–434
- web service, 432

restoring Cisco IOS images, 391–392

RF spectrum, 159–160

RFC 1918 “Address Allocation for Private Internets”, 60

RIR (Regional Internet Registry), 71

risk, 296

RJ-45 connector, 36

rogue switch, 194

root bridge, STP (Spanning Tree Protocol), 105

Root Guard, configuration, 117–118

root servers, 151–152

rootkit, 299

rootkit detector, 297

routed port, 248

router ospf command, 276

router-id command, 276–277

router/s, 15–16

- configuring as a DHCPv4 client, 143–144
- configuring as a DHCPv6 stateful server, 149
- configuring as a stateless server, 147–148
- configuring SSH, 219
- configuring the interfaces, 219–220
- configuring to relay DHCPv4 requests, 142–143
- dynamic, 205–206
- enabling IPv6, 225–231
- learned routes, 205
- message-of-the-day banner,
 - configuring, 219
- naming, 219
- packet forwarding, 203–204, 236
- password, 219
 - best practices, 305–306*
 - encryption, 219*
- path determination, 204–205, 235–236
- SOHO, 24
 - connection options, 232*
 - internal functions, 232–233*
- on a stick, 244, 245–248
- switching functions, 204–205
- verifying your configuration
 - show interface command, 222–225*
 - show ip interface brief command, 221–222*
 - show ip route command, 220–221*
 - show running-config command, 220*

routing

- inter-VLAN, 243
 - legacy, 243–244*
 - multilayer switching, 245, 248–250*
 - router on a stick, 244, 245–248*
- loop prevention, 211–212
- static, 205–206, 251–252. *See also* static routing

routing protocol

- administrative distance, 209–211
- classful, 208
- classless, 208
- distance vector, 207
- dynamic, 205–206
- EGP (exterior gateway protocol), 207

IGP (interior gateway protocol), 207, 211
 link-state, 207–215
 building the LSDB, 212–213
 calculating the Dijkstra algorithm, 213–214
 convergence, 214–215
 metric, 208

routing table

components, 236–237
 default route, 237, 239
 IPv4, 237–238
 IPv6, 238–239
 longest match, 235
 IPv4, 235–236
 IPv6, 236
 principles, 239–240
 route entries, 239, 240

RSA (Rivest, Shamir, and Adleman), 351

RSTP (Rapid STP), 107

edge ports, 111–112
 interface behavior, 110
 port roles, 110–111
 port states, 110

S

SaaS (software as a service), 398

scalable groups, 415

SDN (software-defined networking), 399

Cisco ACI (Application Centric Infrastructure), 402–404
 control plane, 399–400
 controllers, 400–401
 data plane, 399
 management plane, 400
 Open, 401–402

security. See also access control;

attack/s; authentication

assets, 295
 Cisco SD-Access, 416–417
 exploit, 296
 penetration testing, tools, 296–297
 port, 189
 aging, 191–192
 configuration, 189–190
 port restoration after a violation, 192–193
 verifying, 190–191
 program, 302–303
 risk/s, 296

switch port hardening, 186
 802.1X, 187–189
 AAA, 186–187
 threat, 296
 vulnerability, 295

server

DHCPv4, configuring a router as a,
 138–140
 root, 151–152
 stateless, configuring a router as, 147–148
 virtualization, 396–397

service-password encryption

command, 219

session hijacking, 302

set messages, SNMP, 375–376

shaping, 362–363

shared key authentication, 169

shoulder surfing, 301

show access-lists command, 319,
324–325

show cdp interface command, 366, 368

show cdp neighbors command, 367

show cdp neighbors detail command,
369–371

show cdp traffic command, 371–374

show etherchannel summary
command, 126

show file system command, 385–386

show flash command, 386–387

show interface command, 222–225

show interface status command, 53–54

show interfaces switchport command,
94, 100, 126–127

show interfaces trunk command, 99–100

show ip dhcp binding command, 140

show ip dhcp conflict command, 150

show ip dhcp server statistics
command, 140–141

show ip interface brief command,
221–222, 247–248, 281, 366–367

show ip interface command, 319–320

show ip nat statistics command, 337

show ip nat translations command, 336

show ip ospf command, 282–283

show ip ospf interface brief
command, 283

- show ip ospf neighbor command, 281–282, 290
- show ip protocols command, 210–211, 281
- show ip route command, 209, 220–221, 237–238, 247, 249–250, 255, 256–257, 259, 281
- show ip route ospf command, 287
- show ip ssh command, 184, 185
- show ipv6 access-list command, 325
- show ipv6 dhcp binding command, 149
- show ipv6 interface command, 228
- show ipv6 route command, 238–239, 262, 263
- show lldp command, 373
- show lldp interface command, 373
- show lldp neighbors command, 373
- show lldp neighbors detail command, 373–374
- show lldp traffic command, 374
- show logging command, 382–384
- show mac address-table command, 97
- show ntp associations command, 385
- show ntp status command, 385
- show port-security command, 190–191
- show port-security interface command, 193
- show run command, 184, 323–324
- show running-config command, 220, 320
- show snmp command, 378–379
- show snmp community command, 379
- show spanning-tree command, 115
- show spanning-tree vlan command, 117–118
- show standby brief command, 131–132, 134
- show standby command, 131–132
- show vlan brief command, 91–93
- show vlan command, 97
- show vlans command, 247
- shutdown command, 186
- single-area OSPF, 265
- site-to-site VPN, 347
- SLAAC (stateless address autoconfiguration), 81
 - NDP messages, 144
 - neighbor discovery, 145–146
- SMTP (Simple Mail Transfer Protocol), 3**
- sniffer attack, 298**
- SNMP (Simple Network Management Protocol), 3, 375, 375**
 - components, 375
 - configuration, 378
 - messages, 375–376
 - MIB (Management Information Base), 376–378
 - verifying, 378–379
 - versions, 376
- snmp-server community command, 378**
- social engineering attack**
 - baiting, 300
 - dumpster diving, 301
 - impersonation, 300
 - phishing, 300
 - pretexting, 300
 - shoulder surfing, 301
 - something for something, 300
 - spam, 300
 - spear phishing, 300
 - tailgating, 301
- software, firewall, 16**
- SOHO (small office/home office), 23–24**
 - routers, 24
 - connection options, 232
 - internal functions, 232–233
- solicited-node multicast address, 76–77**
- something for something, 300**
- spam, 300**
- spanning-tree bpduguard default command, 116**
- spanning-tree guard root command, 117–118**
- spanning-tree mode command, 113–114**
- spanning-tree pathcost method command, 105**
- spanning-tree portfast bpduguard default command, 117**
- spanning-tree portfast default command, 116**
- spanning-tree vlan command, 114–115**
- spear phishing, 300**

- SPF (shortest path first) algorithm,**
 - 213–214, 269–270
- spine-and-leaf switch,** 403
- split horizon,** 212
- split-MAC architecture,** 167–168
- spoofing attack,** 300
- spyware,** 299
- SSH (Secure Shell),** 3
 - configuration, 184–185
 - remote access using, 230–231
 - verifying, 185
- ssh command,** 230–231
- SSID (service set identifier),** 164
- standard IPv6 ACL,** 322
- standard numbered IPv4 ACL,** 313
 - deny a specified host, 314
 - deny a specified subnet, 315
 - deny Telnet or SSH to the router, 315
 - permit specific network, 314
- standards**
 - Ethernet, 22, 35, 36–37
 - wireless, 159, 161–162
- standby ip command,** 131
- standby preempt command,** 131
- standby priority command,** 131
- stateful DHCPv6,** 146
- stateful firewall,** 16
- stateless DHCPv6,** 146
- static NAT (Network Address Translation),** 332, 334
- static routing,** 205–206, 251–252
 - IPv4, 252–253
 - default route configuration, 255–258*
 - using next-hop parameter, 254*
 - using the exit-interface parameter, 254–255*
 - IPv6, 259–261
 - default route, 261–262*
 - summary route configuration, 262–263*
 - summary route configuration, 258–259
- store-and-forward switching,** 31–32
- STP (Spanning Tree Protocol),** 103–104.
 - See also EtherChannel; PVST+ (Per-VLAN Spanning TreePlus); RSTP (Rapid STP)*
 - algorithm, 104
 - BID (bridge ID), 104–105
 - BPDU (bridge protocol data unit), 104
 - configuration, 112–113
 - convergence, 105–106
 - default IEEE port costs, 106
 - root bridge, 105
 - topology, 114
 - varieties, 106–107
 - verifying, 115, 118–119
- straight-through cable,** 22
- subconfiguration modes, Cisco IOS,** 46
- subnet mask,** 59–60
 - ANDing, 59–60
 - binary values, 60
 - variable-length, 64–66
- subnetting,** 60–61, 63–64
 - determining how many bits to borrow, 61–62
 - determining the new subnet mask, 62
 - determining the subnet multiplier, 62
 - host range and broadcast address, 62–63
 - IPv6, 79–80
- summary route**
 - IPv4, 258–259
 - IPv6, 262–263
- SVI (switch virtual interface),** 248
- switches/switching,** 39–40. *See also port/s; STP (Spanning Tree Protocol)*
 - access layer, 14
 - asymmetric, 32
 - benefits of using, 37
 - broadcast domain, 31
 - collision domain, 31
 - configuration commands, 46–48
 - core layer, 15
 - cost, 14
 - cut-through, 32
 - distribution layer, 14–15
 - duplex mode, 48
 - enabling/disabling VLAN, 98
 - forwarding, 30
 - fragment-free, 32
 - frame forwarding, 31
 - interface, 14
 - Layer 2, 32
 - Layer 3, 32
 - logic, 30–31
 - memory buffering, 32
 - multilayer, 245, 248
 - configuring a Layer 3 routed port, 250*
 - creating additional SVIs, 248–250*
 - rogue, 194
 - spine-and-leaf, 403

store-and-forward, 31–32
 symmetric, 32
 troubleshooting, 52–53
 duplex and speed mismatches, 53–55
 interface status codes, 53
 Layer 1 problems, 55

switchport access vlan command, 186

switchport mode access command, 189

switchport mode command, 186

switchport mode trunk command, 89–90

switchport negotiate command, 90

switchport port-security aging command, 191–192

switchport port-security command, 189

switchport trunk native vlan command, 186

symmetric switching, 32

syntax

 extended named IPv4 ACL, 318
 JSON (JavaScript Object Notation), 431
 named IPv4 ACL, 317
 router configuration command, 218

syslog, 380

 messages, 380–382
 severity levels, 380–381
 verifying, 382–384

T

TACACS+, 187

tail drop, 363–364

tailgating, 301

TCP (Transmission Control Protocol), 4, 6

 connection establishment and termination, 9
 error recovery, 7–8
 flow control, 8
 header, 6
 PAR (positive acknowledgment with retransmission), 8
 QoS and, 363–364
 reset attack, 302
 session hijacking, 302
 SYN flood attack, 302

TCP/IP model, 1–2

 application layer, 5
 encapsulation, 12–13

 Internet layer, 10
 layers and protocols, 3–4
 network access layer, 11–12
 physical layer, 20
 transport layer, 5–6

Telnet, 3

Terraform, 422–423

 versus Ansible, 427
 apply command, 426
 enabling on a Cisco router, 424–425
 HCL configuration file, 424
 workflow, 423

threats, 296. *See also* attack/s

three-tier campus network, 26

TIA (Telecommunications Industry Association)/EIA (Electronics Industry Alliance), 36–37

TKIP (Temporal Key Integrity Protocol), 171

tools

 Ansible, 420
 inventory file, 421–422
 playbook, 422
 YAML playbook, 421
 ChatGPT, prompting, 436
 configuration management, 419
 penetration testing, 296–297
 policers, 362
 shapers, 362–363

topology/ies, 25

 bus, 25
 logical, 25
 NAT, 329–330
 physical, 25
 redundancy, 103
 STP (Spanning Tree Protocol), 114
 VLSM, 65
 WAN, 339–340
 wireless
 ad hoc mode, 164
 infrastructure mode, 163–164
 mesh, 164

traceroute command, 229–230

tracert command, 51–52, 258, 259

transport layer

 attacks, 302
 TCP/IP model, 5–6

triggered updates, 212

Trojan horse, 298

troubleshooting

- ACLs, 326
- ChatGPT, 438
- DHCP (Dynamic Host Configuration Protocol)
 - connectivity*, 150
 - resolving address conflicts*, 149–150
 - verifying switch port configuration*, 150
- DNS (Domain Name System), 152
- EtherChannel, 127
- HSRP (Hot Standby Router Protocol), 135
- IP addressing
 - default gateway*, 233
 - duplicate IP addresses*, 234
- media issues, 52
- NAT (Network Address Translation), 337–338
- OSPF (Open Shortest Path First), 291–293
- switches/switching
 - duplex and speed mismatches*, 53–55
 - interface status codes*, 53
 - Layer 1 problems*, 55
- VLAN, 97–98, 99
 - check both ends of a trunk*, 99–100
 - connectivity*, 97–98
 - trunking*, 100
- trunking, 88–89**
 - configuration, 94–96
 - troubleshooting, 99, 100
 - verifying, 96–97
- trust exploitation, 300**
- TTL (Time To Live), 212**
- tunneling, 82. See also VPN (virtual private network)**
 - CAPWAP (Control and Provisioning of Wireless Access Points), 167–168
 - VPN, 351

U

- UDP (User Datagram Protocol), 4, 6, 9–10**
 - flood attack, 302
 - header, 7
- underlay, Cisco SD-Access, 409–411**
- unicast address, IPv6, 69**
- unique local address, 74**

URI (uniform resource identifier), 150–151, 434

URL (uniform resource locator) filtering, 18, 434

user groups, 416–417

username secret command, 183–184

UTP (unshielded twisted-pair), 34, 36–37

V**verifying**

- CDP (Cisco Discovery Protocol), 367, 368–371
- DHCPv4, 140–141
- EtherChannel, 125–127
- HSRP (Hot Standby Router Protocol), 131–132
- IP settings
 - on Linux*, 156–158
 - on macOS*, 155–156
 - on Windows*, 153–155
- IPv4 ACLs, 319–320
- IPv4/IPv6 connectivity, 229–231
- IPv6 ACLs, 323–325
- LLDP (Link Layer Discovery Protocol), 372–374
- NAT (Network Address Translation), 336–337
- network connectivity, 49
- OSPFv2, 280–283
- router configuration
 - show interface command*, 222–225
 - show ip interface brief command*, 221–222
 - show ip route command*, 220–221
 - show running-config command*, 220
- SNMP (Simple Network Management Protocol), 378–379
- SSH (Secure Shell), 185
- STP (Spanning Tree Protocol), 118–119
- VLAN, 90–93

versions

- HSRP (Hot Standby Router Protocol), 130
- OSPF (Open Shortest Path First), 265, 271–272
- SNMP (Simple Network Management Protocol), 376

virtual interface, configuration, 176–178

virus, 298

VLAN (virtual local-area network), 85–86

- assigning to interfaces, 93–95
- attacks, 194–195
- configuration and verification, 90–93
- connectivity, troubleshooting, 97–98
- creating, 92
- creating a virtual interface, 176–178
- DTP (Dynamic Trunking Protocol), 89–90
- enabling/disabling on a switch, 98
- management, 193–194
- native, 193–194
- trunking, 88–89
 - configuration, 94–96*
 - troubleshooting, 100*
 - verifying, 96–97*
- types of, 86–87
- voice, 87

VLSM (variable-length subnet masking), 64–66**VM (virtual machine), 396–397****VNFs (virtual network functions), 398–399****voice VLAN, 87****VPN (virtual private network), 346**

- authentication, 352
- benefits, 347
- components, 350
- DMVPN (Dynamic Multipoint VPN), 349
- encapsulation and encryption, 350
- encryption, 351–352
- GRE (Generic Routing Encapsulation), 348
- HMAC (hashed message authentication code), 352
- IPsec, 352–355
- remote-access, 347–348
- site-to-site, 347
- tunneling, 351

VRRP (Virtual Router Redundancy Protocol), 135**vulnerability/ies, 295**

- exploitation tools, 297
- password, 303
- scanner, 297

W**WAN (wide-area network), 23**

- choosing a link option, 346
- circuit-switched connection options, 342–343

Internet connection options

- cable modem, 344–345*
- DSL, 344*
- wireless, 345–346*

leased lines, 341–342**packet-switched connection options, 342**

- Metro Ethernet, 343*
- MPLS, 343–344*

topologies, 339–340**web service, REST, 432****WebUI**

- configuring access, 42
- dashboard, 43

well-known port numbers, 7**WEP (Wired Equivalent Privacy), 169****Wi-Fi Alliance generational names, 162–163****Windows, verifying IP settings, 153–155****wireless**

- 802.11 standards, 159
- ad hoc mode, 164
- AP (access point), 19
 - autonomous architecture, 165*
 - cloud-based architecture, 166*
 - lightweight architecture, 166–167*
 - split-MAC architecture, 167–168*
- authentication, 168–169, 172
 - 802.1X/EAP, 170*
 - shared key, 169*
 - WPA and WPA2, 170*
 - WPA3, 170–171*
- band, 159
- BSA (basic service area), 164
- BSS (basic service set), 164
- encryption, 171
- ESS (extended service set), 164
- hacking tools, 297
- infrastructure mode, 163–164
- Internet connection options, 345–346
- mesh topology, 164
- RF spectrum, 159–160
- SSID (service set identifier), 164
- Wi-Fi Alliance generational names, 162–163
- WLC (wireless LAN controller), 19

WLAN, creating, 178–181

WLC (wireless LAN controller), 19

- Advanced Summary page, 175
- configuring a new interface, 176–178
- configuring a RADIUS server, 176
- creating a WLAN, 178–181
- logging into, 173–174
- LWAPP (Lightweight Access Point Protocol), 166
- Network Summary page, 174

worm, 298

WPA (Wi-Fi Protected Access), 170

WPA2, 169, 170

WPA3, 170–171

X-Y-Z

zombie, 301