Contents

Introduction xxxi

Part I Wireless LANs 3

Chapter 1 Fundamentals of Wireless Networks 4

"Do I Know This Already?" Quiz 4

Foundation Topics 6

Comparing Wired and Wireless Networks 6

Wireless LAN Topologies 7

Basic Service Set 8

Distribution System 10

Extended Service Set 12

Independent Basic Service Set 13

Other Wireless Topologies 14

Repeater 14

Workgroup Bridge 15

Outdoor Bridge 16

Mesh Network 17

Wireless Bands and Channels 17

Chapter Review 20

Chapter 2 Analyzing Cisco Wireless Architectures 22

"Do I Know This Already?" Quiz 22

Foundation Topics 24

Autonomous AP Architecture 24

Cloud-based AP Architecture 26

Split-MAC Architectures 28

Comparing Cisco Wireless LAN Controller Deployments 32

Cisco AP Modes 35

FlexConnect Mode 36

Chapter Review 37

Chapter 3 Securing Wireless Networks 40

"Do I Know This Already?" Quiz 40

Foundation Topics 42

Anatomy of a Secure Connection 42

Authentication 43

Message Privacy 44

Message Integrity 45

Wireless Client Authentication Methods 46
Open Authentication 46
WEP 47
802.1x/EAP 47
LEAP 48
EAP-FAST 49
PEAP 49
EAP-TLS 50
Wireless Privacy and Integrity Methods 50
TKIP 50
CCMP 51
GCMP 51
WPA, WPA2, and WPA3 51
Chapter Review 53

Chapter 4 Building a Wireless LAN 56
"Do I Know This Already?" Quiz 56
Foundation Topics 58
Connecting a Cisco AP 58
Accessing a Cisco WLC 59
Connecting a Cisco WLC 63
WLC Physical Ports 63
Configuring a WLAN 65
Configuring a WLAN on an IOS-XE WLC 67
Step 1: Configure a WLAN Profile 69
Step 2: Configure a Policy Profile 74
Step 3: Map the WLAN and Policy Profiles to a Policy Tag 77
Step 4: Apply the Policy Tag to Some APs 78
Configuring a WLAN on an AireOS WLC 79
Step 1: Create a Dynamic Interface 79
Step 2: Create a New WLAN 80
Step 3: Configure the WLAN 81
Configuring WLAN Security 83
Configuring WLAN QoS 85
Configuring Advanced WLAN Settings 85
Finalizing WLAN Configuration 86
Chapter Review 87

Part I Review 88

Part II IP Access Control Lists 91

Chapter 5 Introduction to TCP/IP Transport and Applications 92

"Do I Know This Already?" Quiz 92

Foundation Topics 94

TCP/IP Layer 4 Protocols: TCP and UDP 94

Transmission Control Protocol 95

Multiplexing Using TCP Port Numbers 95

Popular TCP/IP Applications 98

Connection Establishment and Termination 100

Error Recovery and Reliability 101

Flow Control Using Windowing 102

User Datagram Protocol 103

TCP/IP Applications 104

Uniform Resource Identifiers 104

Finding the Web Server Using DNS 105

Transferring Files with HTTP 108

How the Receiving Host Identifies the Correct Receiving Application 109

HTTP Versions 110

HTTP 1.0 and 1.1 110

HTTP/2 and TLS 110

HTTP 3.0 111

Chapter Review 112

Chapter 6 Basic IPv4 Access Control Lists 114

"Do I Know This Already?" Quiz 114

Foundation Topics 116

IPv4 Access Control List Basics 116

ACL Location and Direction 116

Matching Packets 117

Taking Action When a Match Occurs 118

Types of IP ACLs 118

Standard Numbered IPv4 ACLs 119

List Logic with IP ACLs 119

Matching Logic and Command Syntax 121

Matching the Exact IP Address 121

Matching a Subset of the Address with Wildcard Masks 122

Binary Wildcard Masks 123

Finding the Right Wildcard Mask to Match a Subnet 124
Matching Any/All Addresses 124
Implementing Standard IP ACLs 125
Standard Numbered ACL Scenario 1 125
Standard Numbered ACL Scenario 2 127
Troubleshooting and Verification Tips 129
Practice Applying Standard IP ACLs 130
Practice Building access-list Commands 130
Reverse Engineering from ACL to Address Range 131
Chapter Review 133

Chapter 7 Named and Extended IP ACLs 136
"Do I Know This Already?" Quiz 136
Foundation Topics 138
Named ACLs and ACL Editing 138
Named IP Access Lists 138
Editing ACLs 140
Editing Named ACLs 140
Editing Numbered ACLs 143
Extended IP Access Control Lists 144
Matching the Protocol, Source IP, and Destination IP 145
Matching TCP and UDP Port Numbers 147
Extended IP ACL Configuration 150
Extended IP ACL Example 1: Packets to Web Servers 151
Extended IP ACL Example 2: Packets from Web Servers 153
Adjusting ACLs for HTTP/3 154
Practice Building access-list Commands 155
ACL Implementation Considerations 156
Chapter Review 157

Chapter 8 Applied IP ACLs 160
"Do I Know This Already?" Quiz 160
Foundation Topics 162
ACLs and Network Infrastructure Protocols 162
Filtering DNS 163
Filtering ICMP 164
Filtering OSPF 165
Filtering DHCP 167
Filtering SSH and Telnet 169

Filtering for End User SSH/Telnet 169
Filtering for Router VTY Access 171
Comparing ACLs in IOS and IOS XE 173
Configuration Syntax and Show Commands 173
Resequencing ACL Sequence Numbers 174
Using a Second (Common) Interface ACL 175
Matching Multiple Nonconsecutive Ports with eq 177
Chapter Review 177

Part II Review 180

Part III Security Services 183

Chapter 9 Security Architectures 184
"Do I Know This Already?" Quiz 184
Foundation Topics 186
Security Terminology 186
Common Security Threats 188
Attacks That Spoof Addresses 188
Denial-of-Service Attacks 189
Reflection and Amplification Attacks 191
Man-in-the-Middle Attacks 191
Address Spoofing Attack Summary 193
Reconnaissance Attacks 193
Buffer Overflow Attacks 194
Malware 194
Human Vulnerabilities 195
Password Vulnerabilities 196
Password Alternatives 196
Controlling and Monitoring User Access 198
Developing a Security Program to Educate Users 200
Chapter Review 201

Chapter 10 Securing Network Devices 202
"Do I Know This Already?" Quiz 202
Foundation Topics 204
Securing IOS Passwords 204
Encrypting Older IOS Passwords with service password-encryption 205
Encoding the Enable Passwords with Hashes 206
Interactions Between Enable Password and Enable Secret 206

Making the Enable Secret Truly Secret with a Hash 207
Improved Hashes for Cisco's Enable Secret 209
Encoding the Passwords for Local Usernames 210
Firewalls and Intrusion Prevention Systems 211
Traditional Firewalls 211
Security Zones 213
Intrusion Prevention Systems (IPS) 215
Cisco Next-Generation Firewalls 216
Cisco Next-Generation IPS 218
Chapter Review 219

Chapter 11 Implementing Switch Port Security 222
"Do I Know This Already?" Quiz 222
Foundation Topics 224
Port Security Concepts and Configuration 224
Configuring Port Security 225
Verifying Port Security 228
Port Security MAC Addresses 229
Port Security Violation Modes 230
Port Security Shutdown Mode 231
Port Security Protect and Restrict Modes 233
Chapter Review 235

Chapter 12 DHCP Snooping and ARP Inspection 238
"Do I Know This Already?" Quiz 238
Foundation Topics 240
DHCP Snooping 240
DHCP Snooping Concepts 240
A Sample Attack: A Spurious DHCP Server 241
DHCP Snooping Logic 242
Filtering DISCOVER Messages Based on MAC Address 243
Filtering Messages That Release IP Addresses 244
DHCP Snooping Configuration 245
Configuring DHCP Snooping on a Layer 2 Switch 246
Limiting DHCP Message Rates 248
DHCP Snooping Configuration Summary 249
Dynamic ARP Inspection 250
DAI Concepts 250
Review of Normal IP ARP 250

Gratuitous ARP as an Attack Vector 251
Dynamic ARP Inspection Logic 253
Dynamic ARP Inspection Configuration 254
Configuring ARP Inspection on a Layer 2 Switch 254
Limiting DAI Message Rates 257
Configuring Optional DAI Message Checks 258
IP ARP Inspection Configuration Summary 259
Chapter Review 260

Part III Review 264

Part IV IP Services 267

Chapter 13 Device Management Protocols 268
"Do I Know This Already?" Quiz 268
Foundation Topics 270
System Message Logging (Syslog) 270
Sending Messages in Real Time to Current Users 270
Storing Log Messages for Later Review 271
Log Message Format 272
Log Message Severity Levels 272
Configuring and Verifying System Logging 273
The debug Command and Log Messages 276
Network Time Protocol (NTP) 277
Setting the Time and Time Zone 278
Basic NTP Configuration 279
NTP Reference Clock and Stratum 281
Analyzing Topology Using CDP and LLDP 283
Examining Information Learned by CDP 283
Configuring and Verifying CDP 286
Examining Information Learned by LLDP 287
Configuring and Verifying LLDP 290
LLDP-MED and TLVs 292
Chapter Review 293

Chapter 14 Network Address Translation 298
"Do I Know This Already?" Quiz 298
Foundation Topics 300
Network Address Translation Concepts 300
IPv4 Address Conservation with NAT 300

Inside Source NAT 302
Static NAT 303
Inside Local and Inside Global Addresses 303
Dynamic NAT 304
Overloading NAT with Port Address Translation 306
NAT Configuration and Troubleshooting 307
Static NAT Configuration 308
Dynamic NAT Configuration 310
Dynamic NAT Verification 312
NAT Overload (PAT) Configuration 314
NAT Troubleshooting 317
Chapter Review 318

Chapter 15 Quality of Service (QoS) 322
"Do I Know This Already?" Quiz 322
Foundation Topics 324
Introduction to QoS 324
QoS: Managing Bandwidth, Delay, Jitter, and Loss 324
Types of Traffic 325
Data Applications 325
Voice and Video Applications 327
QoS as Mentioned in This Book 328
QoS on Switches and Routers 329
Classification and Marking 329
Classification Basics 329
Matching (Classification) Basics 330
Classification on Routers with ACLs and NBAR 331
Marking IP DSCP and Ethernet CoS 332
Marking the IP Header 333
Marking the Ethernet 802.1Q Header 333
Other Marking Fields 334
Defining Trust Boundaries 334
DiffServ Suggested Marking Values 335
Expedited Forwarding (EF) 336
Assured Forwarding (AF) 336
Class Selector (CS) 336
Guidelines for DSCP Marking Values 337

Queuing 337
Round-Robin Scheduling (Prioritization) 338
Low Latency Queuing 339
A Prioritization Strategy for Data, Voice, and Video 341
Shaping and Policing 341
Policing 342
Where to Use Policing 342
Shaping 344
Setting a Good Shaping Time Interval for Voice and Video 345
Congestion Avoidance 346
TCP Windowing Basics 346
Congestion Avoidance Tools 347
Chapter Review 348

Chapter 16 First Hop Redundancy Protocols 350
"Do I Know This Already?" Quiz 350
Foundation Topics 352
First Hop Redundancy Protocols 352
The Need for Redundancy in Networks 353
The Need for a First Hop Redundancy Protocol 354
The Three Solutions for First-Hop Redundancy 356
Hot Standby Router Protocol 356
HSRP Virtual IP and MAC Addresses 357
HSRP Failover 357
HSRP Load Balancing 359
HSRP Interface Tracking 359
HSRP Recovery and Preemption 360
HSRP Versions 361
VRRP and GLBP Concepts 362
Virtual Router Redundancy Protocol (VRRP) 362
GLBP Concepts 363
Similarities of GLBP, HSRP, and VRRP 363
GLBP Active/Active Load Balancing 364
Chapter Review 366

Chapter 17 SNMP, FTP, and TFTP 368
"Do I Know This Already?" Quiz 368
Foundation Topics 370
Simple Network Management Protocol 370

SNMP Variable Reading and Writing: SNMP Get and Set 371
SNMP Notifications: Traps and Informs 372
The Management Information Base 372
Securing SNMP 374
FTP and TFTP 376
Managing Cisco IOS Images with FTP/TFTP 376
The IOS File System 376
Upgrading IOS Images 378
Copying a New IOS Image to a Local IOS File System Using TFTP 378
Listing the Files in the IOS File System 379
Verifying IOS Code Integrity with MD5 or SHA512 381
Copying Images with FTP 382
The FTP and TFTP Protocols 384
FTP Protocol Basics 384
FTP Active and Passive Modes 385
TFTP Protocol Basics 387
Chapter Review 388

Part IV Review 392

Part V Network Architecture 395

Chapter 18 LAN Architecture 396
"Do I Know This Already?" Quiz 396
Foundation Topics 398
Analyzing Campus LAN Topologies 398
Two-Tier Campus Design (Collapsed Core) 399
Three-Tier Campus Design (Core) 400
Topology Design Terminology 402
Ethernet Physical Media and Standards 403
Ethernet UTP Links at the Access Layer 403
Multigig Ethernet on CAT 5E Cabling 405
Fiber Uplinks 406
Small Office/Home Office 407
Power over Ethernet (PoE) 408
PoE Basics 409
PoE Operation 409
PoE and LAN Design 411
Chapter Review 412

Chapter 19 WAN Architecture 414

"Do I Know This Already?" Quiz 414

Foundation Topics 416

Metro Ethernet 416

Metro Ethernet Physical Design and Topology 416

Ethernet WAN Services and Topologies 418

Ethernet Line Service (Point-to-Point) 418

Ethernet LAN Service (Full Mesh) 419

Layer 3 Design Using Metro Ethernet 420

Layer 3 Design with E-Line Service 420

Layer 3 Design with E-LAN Service 421

Multiprotocol Label Switching (MPLS) 422

MPLS VPN Physical Design and Topology 423

Layer 3 with MPLS VPN 424

Internet VPNs 425

Internet Access 426

Digital Subscriber Line 426

Cable Internet 427

Wireless WAN (4G, 5G) 428

Fiber (Ethernet) Internet Access 429

Internet VPN Fundamentals 430

Site-to-Site VPNs with IPsec 431

Remote Access VPNs with IPsec 433

Remote Access VPNs with TLS 434

Chapter Review 435

Chapter 20 Cloud Architecture 438

"Do I Know This Already?" Quiz 438

Foundation Topics 440

Server Virtualization 440

Cisco Server Hardware 440

Server Virtualization and Virtual Machine Basics 441

Networking with Virtual Switches on a Virtualized Host 443

Software Containers 444

The Physical Data Center Network 446

Workflow with a Virtualized Data Center 446

Cloud Computing Services 448

Private Cloud (On-Premise) 449

Public Cloud 450
Cloud and the "As a Service" Model 451
Infrastructure as a Service 451
Software as a Service 452
(Development) Platform as a Service 453
Virtual Routing and Forwarding (VRF) Instances 454
WAN Traffic Paths to Reach Cloud Services 456
Enterprise WAN Connections to Public Cloud 456
Accessing Public Cloud Services Using the Internet 456
Pros and Cons with Connecting to Public Cloud with Internet 457
Private WAN and Internet VPN Access to Public Cloud 458
Pros and Cons of Connecting to Cloud with Private WANs 459
Intercloud Exchanges 459
Summarizing the Pros and Cons of Public Cloud WAN Options 460
Understanding Cloud Management 460
Chapter Review 465

Part V Review 466

Part VI Network Automation 469

Chapter 21 Introduction to Controller-Based Networking 470
"Do I Know This Already?" Quiz 471
Foundation Topics 472
SDN and Controller-Based Networks 472
The Data, Control, and Management Planes 472
The Data Plane 473
The Control Plane 474
The Management Plane 475
Cisco Switch Data Plane Internals 475
Controllers and Software Defined Architecture 477
Controllers and Centralized Control 477
The Southbound Interface 478
The Northbound Interface 479
Software Defined Architecture Summary 481
Examples of Network Programmability and SDN 481
OpenDaylight and OpenFlow 481
The OpenDaylight Controller 482
The Cisco Open SDN Controller (OSC) 483

Cisco Application Centric Infrastructure (ACI) 484
ACI Physical Design: Spine and Leaf 484
ACI Operating Model with Intent-Based Networking 486
Summary of the SDN Examples 488
Comparing Traditional Versus Controller-Based Networks 488
How Automation Impacts Network Management 489
Comparing Traditional Networks with Controller-Based Networks 491
Chapter Review 492

Chapter 22 Cisco Software-Defined Access (Cisco SD-Access) 494
"Do I Know This Already?" Quiz 495
Foundation Topics 496
Cisco SD-Access Fabric, Underlay, and Overlay 496
The Cisco SD-Access Underlay 499
Using Existing Gear for the Cisco SD-Access Underlay 499
Using New Gear for the Cisco SD-Access Underlay 501
The Cisco SD-Access Overlay 503
VXLAN Tunnels in the Overlay (Data Plane) 504
LISP for Overlay Discovery and Location (Control Plane) 505
Cisco Catalyst Center and Cisco SD-Access Operation 509
Cisco Catalyst Center 509
Cisco Catalyst Center and Scalable Groups 510
Issues with Traditional IP-Based Security 511
Cisco SD-Access Security Is Based on User Groups 512
Cisco Catalyst Center as a Network Management Platform 514
Cisco Catalyst Center Similarities to Traditional Management 515
Cisco Catalyst Center and Differences with Traditional Management 516
Artificial Intelligence (AI), Machine Learning (ML), and Operational Management 517
Chapter Review 524

Chapter 23 Understanding REST and JSON 526
"Do I Know This Already?" Quiz 526
Foundation Topics 528
REST-Based APIs 528
REST-Based (RESTful) APIs 528
Client/Server Architecture 529
Stateless Operation 530
Cacheable (or Not) 530

Background: Data and Variables 530
Simple Variables 530
List and Dictionary Variables 531
REST APIs and HTTP 533
Software CRUD Actions and HTTP Verbs 533
Using URIs with HTTP to Specify the Resource 534
Example of REST API Call to Cisco Catalyst Center 536
Data Serialization and JSON 541
The Need for a Data Model with APIs 542
Data Serialization Languages 544
JSON 544
XML 544
YAML 545
Summary of Data Serialization 546
Recognizing the Components of JSON 546
Interpreting JSON Key:Value Pairs 547
Interpreting JSON Objects and Arrays 547
Minified and Beautified JSON 550
Chapter Review 550

Chapter 24 Understanding Ansible and Terraform 552
"Do I Know This Already?" Quiz 552
Foundation Topics 554
Device Configuration Challenges and Solutions 554
Configuration Drift 554
Centralized Configuration Files and Version Control 555
Configuration Monitoring and Enforcement 557
Configuration Provisioning 558
Configuration Templates and Variables 559
Files That Control Configuration Automation 561
Ansible and Terraform Basics 562
Ansible 562
Terraform 563
Summary of Configuration Management Tools 565
Chapter Review 566

Part VI Review 568

Part VII **Exam Updates and Final Review 571**

Chapter 25 ***CCNA 200-301 Official Cert Guide, Volume 2*, Second Edition, Exam Updates 572**

The Purpose of This Chapter 572
Additional Technical Content 573
Official Blueprint Changes 573
Impact on You and Your Study Plan 575
News About the Next CCNA Exam Release 576
Updated Technical Content 576

Chapter 26 **Final Review 578**

Advice About the Exam Event 578
Learn About Question Types 578
Think About Your Time Budget 581
An Example Time-Check Method 581
One Week Before Your Exam 582
24 Hours Before Your Exam 582
30 Minutes Before Your Exam 583
The Hour After Your Exam 583
Exam Review 584
Using Practice Questions 585
Hold Practice Exam Events 586
Exam Scoring on the Real Exam 587
Self-Assessment Suggestions 587
Gap Analysis Using Q&A 589
Advice on How to Answer Exam Questions 590
Additional Exams with the Premium Edition 592
Practicing CLI Skills 593
Adjustments for Your Second Attempt 595
Other Study Tasks 596
Final Thoughts 596

Part VIII **Print Appendixes 599**

Appendix A **Numeric Reference Tables 601**

Appendix B **Exam Topics Cross-Reference 607**

Appendix C **Answers to the "Do I Know This Already?" Quizzes 619**

Glossary 641

Index 668

Online Appendixes

Appendix D Topics from Previous Editions

Appendix E Practice for Chapter 6: Basic IPv4 Access Control Lists

Appendix F Study Planner

Glossary