Companion Website and Pearson Test Prep Access Code

Access interactive study tools on this book’s companion website, including practice test software, review exercises, a Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the Registered Products tab.

When you register your book, your Pearson Test Prep practice test access code will automatically be populated in your account under the Registered Products tab. You will need this code to access the practice test that comes with this book. You can redeem the code at PearsonTestPrep.com. Simply choose Pearson IT Certification as your product group and log in to the site with the same credentials you used to register your book. Click the Activate New Product button and enter the access code. More detailed instructions on how to redeem your access code for both the online and desktop versions can be found on the companion website.

If you have any issues accessing the companion website or obtaining your Pearson Test Prep practice test access code, you can contact our support team by going to pearsonitp.echelp.org.
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.

Vice President, IT Professional: Mark Taub

Composition: codeMantra

Technical Editors: Richard Furr, Denise Fishburne, Dmitry Figol, Patrick Croak

Editorial Assistant: Cindy Teeters

Cover Designer: Chuti Prasertsith

Executive Editor: Malobika Chakraborty

Development Editor: Ellie Bru

Managing Editor: Sandra Schroeder

Indexer: Timothy Wright

Senior Project Editor: Tonya Simpson

Proofreader: Donna E. Mulder

Copy Editor: Chuck Hutchinson
About the Author(s)

Brad Edgeworth, CCIE No. 31574 (R&S and SP), is an SD-WAN technical solutions architect at Cisco Systems. Brad is a distinguished speaker at Cisco Live, where he has presented on various topics. Before joining Cisco, Brad worked as a network architect and consultant for various Fortune 500 companies. Brad's expertise is based on enterprise and service provider environments, with an emphasis on architectural and operational simplicity. Brad holds a bachelor of arts degree in computer systems management from St. Edward's University in Austin, Texas. Brad can be found on Twitter as @BradEdgeworth.

Ramiro Garza Rios, CCIE No. 15469 (R&S, SP, and Security), has over 20 years of experience in the networking industry and currently works as a solutions architect in the Cisco Customer Experience (CX) organization. His expertise is on enterprise and service provider network environments, with a focus on evolving architectures and next-generation technologies. He is also a Cisco Live distinguished speaker.

Before joining Cisco Systems in 2005, he was a network consulting and presales engineer for a Cisco Gold Partner in Mexico, where he planned, designed, and implemented both enterprise and service provider networks.

David Hucaby, CCIE No. 4594 (R&S), CWNE No. 292, is a technical education content engineer for Cisco Meraki, where he focuses on eLearning for the Meraki product lines. David holds bachelor's and master's degrees in electrical engineering from the University of Kentucky. He has been authoring Cisco Press titles for almost 25 years.

Jason Gooley, CCIEx2 (RS, SP) No. 38759, has over 30 years of experience in the industry and currently works as a technical evangelist for the Worldwide Enterprise Networking and Software Sales team at Cisco Systems. Jason is passionate about helping others in the industry succeed. In addition to being a public speaker, Jason is a published Cisco Press author, developer of CCIE exams, an online training instructor, and a blogger. Jason is also co-founder and organizer of the Chicago Network Operators Group (CHI-NOG). He is the founder and host of MetalDevOps, which is a YouTube video show about the intersection of metal music and technology.
About the Technical Reviewers

Richard Furr, CCIE No. 9173 (R&S and SP), is an technical leader in the Cisco Customer Experience (CX) organization, providing support for customers and TAC teams around the world. Richard has authored and acted as a technical editor for Cisco Press publications. During the past 19 years, Richard has provided support to service provider, enterprise, and data center environments, resolving complex problems with routing protocols, MPLS, IP Multicast, IPv6, and QoS.

Denise “Fish” Fishburne, CCDE No. 2009::0014, CCIE No. 2639 (R&S and SNA), is a solutions architect with Cisco Systems. Fish is a geek who absolutely adores learning and passing it on. Fish has been with Cisco since 1996 and has worn many varying “hats,” such as TAC engineer, advanced services engineer, CPOC engineer, and now solutions architect. Fish is heavily involved with Cisco Live, which is a huge passion of hers. Outside of Cisco, you will find her actively sharing and “passing it on” on her blog site, YouTube channel, and Twitter. Look for Fish swimming in the bits and bytes all around you or just go to www.NetworkingWithFish.com.

Dmitry Figol, CCIE No. 53592 (R&S), is a systems engineer in Cisco Systems Enterprise Sales. He is in charge of design and implementation of software applications and automation systems for Cisco. His main expertise is network programmability and automation. Before joining Cisco Sales, Dmitry worked on the Cisco Technical Assistance Center (TAC) Core Architecture and VPN teams. Dmitry maintains several open-source projects and is a regular speaker at conferences. He also does live streams on Twitch about network programmability and Python. Dmitry holds a bachelor of science degree in telecommunications. Dmitry can be found on Twitter as @dmfigol.

Patrick Croak, CCIE No. 34712 (Wireless), is a systems engineer with a focus on wireless and mobility. He is responsible for designing, implementing, and optimizing enterprise wireless networks. He also works closely with the business unit and account teams for product development and innovation. Prior to this role, he spent several years working on the TAC Support Escalation team, troubleshooting complex wireless network issues. Patrick has been with Cisco since 2006.
Dedications

Brad Edgeworth:

This book is dedicated to my wife, Tanya. The successes and achievements I have today are because of Tanya. Whenever I failed an exam, she provided the support and encouragement to dust myself off and try again. She sacrificed years' worth of weekends while I studied for my CCIE certifications. Her motivation has allowed me to overcome a variety of obstacles with great success.

Ramiro Garza:

I would like to dedicate this book to my wonderful and beautiful wife, Mariana, and to my four children, Ramiro, Frinee, Felix, and Lucia, for their love, patience, and support as I worked on this project. And to my parents, Ramiro and Blanca D., and my in-laws, Juan A. and Marisela, for their continued support and encouragement. And most important of all, I would like to thank God for all His blessings in my life.

David Hucaby:

As always, my work is dedicated to my wife and my daughters, for their love and support, and to God, who has blessed me with opportunities to learn, write, and work with so many friends.

Jason Gooley:

This book is dedicated to my wife, Jamie, and my children, Kaleigh and Jaxon. Without their support, these books would not be possible. To my father and brother, thank you for always supporting me.
Acknowledgments

Brad Edgeworth:
A debt of gratitude goes to my co-authors, Ramiro, Jason, and David. I’m privileged to be able to write a book with all of you.

To Brett Bartow, thank you for giving me the privilege to write on such an esteemed book. I’m thankful to work with Ellie Bru and Tonya Simpson again, along with the rest of the Pearson team.

To the technical editors—Richard, Denise, Dmitry, and Patrick—thank you for your attention to detail.

Many people within Cisco have provided feedback and suggestions to make this a great book. And to all of those who share knowledge (wherever you are located), keep doing it. That is how we make this world a better place.

To the readers of this text, never give up. Failure is an opportunity to learn and grow yourself. You probably will not like it, it does not taste good, but after you learn and overcome, you will learn to embrace it (or at least that is what I keep telling myself).

Ramiro Garza Rios:
I’d like to give a special thank you to Brett Bartow for giving us the opportunity to work on this project and for being our guiding light. I’m also really grateful and honored to have worked with Brad, Jason, and David; they are amazing and great to work with. I’d like to give special recognition to Brad for providing the leadership for this project. A big thank you to the Cisco Press team for all your support, especially to Ellie Bru. I would also like to thank our technical editors—Denise, Richard, Patrick, and Dmitry—for their valuable feedback to ensure that the technical content of this book is top-notch. And most important of all, I would like to thank God for all His blessings in my life.

David Hucaby:
I am very grateful to Brett Bartow for giving me the opportunity to work on this project. Brad, Ramiro, and Jason have been great to work with. Many thanks to Ellie Bru for her hard work editing our many chapters!

Jason Gooley:
Thank you to the rest of the author team for having me on this book. It has been a blast! Thanks to Brett and the whole Cisco Press team for all the support and always being available. This project is near and dear to my heart, as I am extremely passionate about helping others on their certification journey.
Contents at a Glance

Introduction  xli

Part I  Forwarding
Chapter 1  Packet Forwarding  2

Part II  Layer 2
Chapter 2  Spanning Tree Protocol  36
Chapter 3  Advanced STP Tuning  58
Chapter 4  Multiple Spanning Tree Protocol  80
Chapter 5  VLAN Trunks and EtherChannel Bundles  94

Part III  Routing
Chapter 6  IP Routing Essentials  124
Chapter 7  EIGRP  154
Chapter 8  OSPF  170
Chapter 9  Advanced OSPF  202
Chapter 10  OSPFv3  230
Chapter 11  BGP  244
Chapter 12  Advanced BGP  288
Chapter 13  Multicast  334

Part IV  Services
Chapter 14  Quality of Service (QoS)  370
Chapter 15  IP Services  418

Part V  Overlay
Chapter 16  Overlay Tunnels  466

Part VI  Wireless
Chapter 17  Wireless Signals and Modulation  510
Chapter 18  Wireless Infrastructure  542
Chapter 19  Understanding Wireless Roaming and Location Services  572  
Chapter 20  Authenticating Wireless Clients  590  
Chapter 21  Troubleshooting Wireless Connectivity  608  

**Part VII  Architecture**  
Chapter 22  Enterprise Network Architecture  622  
Chapter 23  Fabric Technologies  642  
Chapter 24  Network Assurance  672  

**Part VIII  Security**  
Chapter 25  Secure Network Access Control  736  
Chapter 26  Network Device Access Control and Infrastructure Security  778  

**Part IX  SDN**  
Chapter 27  Virtualization  826  
Chapter 28  Foundational Network Programmability Concepts  850  
Chapter 29  Introduction to Automation Tools  892  
Chapter 30  Final Preparation  926  
Chapter 31  ENCOR 350-401 Exam Updates  932  
Appendix A  Answers to the “Do I Know This Already?” Questions  936  
Glossary  956  
Index  978  

**Online Elements**  
Appendix B  Memory Tables  
Appendix C  Memory Tables Answer Key  
Appendix D  Study Planner  
Glossary
Reader Services

Register your copy at www.ciscopress.com/title/9780138216764 for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account. Enter the product ISBN 9780138216764 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

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

- Introduction  xli

## Part I  Forwarding

### Chapter 1  Packet Forwarding  2

- “Do I Know This Already?” Quiz  2
- Foundation Topics  3
  - Network Device Communication  3
    - Layer 2 Forwarding  4
    - Collision Domains  5
    - Virtual LANs  7
    - Access Ports  11
    - Trunk Ports  12
    - Layer 2 Diagnostic Commands  15
  - Layer 3 Forwarding  19
    - Local Network Forwarding  19
    - Packet Routing  20
    - IP Address Assignment  21
    - Verification of IP Addresses  24
- Forwarding Architectures  26
  - Process Switching  26
  - Cisco Express Forwarding  27
  - Ternary Content Addressable Memory  27
  - Centralized Forwarding  28
  - Distributed Forwarding  28
  - Software CEF  29
  - Hardware CEF  30
  - SDM Templates  30
- Exam Preparation Tasks  32
- Review All Key Topics  32
- Complete Tables and Lists from Memory  33
- Define Key Terms  33
- Use the Command Reference to Check Your Memory  33
- References in This Chapter  34
Part II  Layer 2

Chapter 2  Spanning Tree Protocol  36
“Do I Know This Already?” Quiz  36
Foundation Topics  38
Spanning Tree Protocol Fundamentals  38
IEEE 802.1D STP  38
802.1D Port States  39
802.1D Port Types  39
STP Key Terminology  39
Building the STP Topology  41
Spanning Tree Path Cost  41
Root Bridge Election  41
Locating Blocked Designated Switch Ports  45
Verification of VLANs on Trunk Links  48
STP Topology Changes  49
Converging with Direct Link Failures  50
Indirect Failures  52
Rapid Spanning Tree Protocol  53
RSTP (802.1W) Port States  54
RSTP (802.1W) Port Roles  54
RSTP (802.1W) Port Types  54
Building the RSTP Topology  55
RSTP Convergence  55
Exam Preparation Tasks  56
Review All Key Topics  56
Complete Tables and Lists from Memory  56
Define Key Terms  56
Use the Command Reference to Check Your Memory  56

Chapter 3  Advanced STP Tuning  58
“Do I Know This Already?” Quiz  58
Foundation Topics  59
STP Topology Tuning  59
Placing the Root Bridge  60
Modifying STP Root Port and Blocked Switch Port Locations  63
Modifying STP Port Priority  66
Additional STP Protection Mechanisms  67
Root Guard  68
Chapter 4  **Multiple Spanning Tree Protocol**  80

“Do I Know This Already?” Quiz  80

Foundation Topics  81

Multiple Spanning Tree Protocol  81

  MST Instances (MSTIs)  83
  MST Configuration  84
  MST Verification  85
  MST Tuning  87
  Common MST Misconfigurations  89

  **VLAN Assignment to the IST**  89
  **Trunk Link Pruning**  90
  **MST Region Boundary**  90
  **MST Region as the Root Bridge**  91
  **MST Region Not a Root Bridge for Any VLAN**  91

Exam Preparation Tasks  92

Review All Key Topics  92

Complete Tables and Lists from Memory  92

Define Key Terms  92

Use the Command Reference to Check Your Memory  92

Chapter 5  **VLAN Trunks and EtherChannel Bundles**  94

“Do I Know This Already?” Quiz  94

Foundation Topics  96

VLAN Trunking Protocol  96

  VTP Communication  97
  VTP Configuration  98
  VTP Verification  99

Dynamic Trunking Protocol  101
EtherChannel Bundle 104
  Dynamic Link Aggregation Protocols 106
  PAgP Port Modes 106
  LACP Port Modes 106
  EtherChannel Configuration 107
  Verifying EtherChannel Status 108
  Viewing EtherChannel Neighbors 110
  LACP 112
  PAgP 113
  Verifying EtherChannel Packets 113
  LACP 113
  PAgP 114
  Advanced LACP Configuration Options 114
  LACP Fast 115
  Minimum Number of EtherChannel Member Interfaces 115
  Maximum Number of EtherChannel Member Interfaces 116
  LACP System Priority 117
  LACP Interface Priority 118
  Troubleshooting EtherChannel Bundles 118
  Load Balancing Traffic with EtherChannel Bundles 119
Exam Preparation Tasks 121
  Review All Key Topics 121
  Complete Tables and Lists from Memory 121
  Define Key Terms 121
  Use the Command Reference to Check Your Memory 121

Part III  Routing

Chapter 6  IP Routing Essentials 124
  “Do I Know This Already?” Quiz 124
  Foundation Topics 126
  Routing Protocol Overview 126
    Distance Vector Algorithms 128
    Enhanced Distance Vector Algorithms 129
    Link-State Algorithms 130
    Path Vector Algorithm 131
  Path Selection 132
Prefix Length 133
Administrative Distance 133
Metrics 135
Equal-Cost Multipathing 135
Unequal-Cost Load Balancing 136

Static Routing 137
Static Route Types 138
Directly Attached Static Routes 138
Recursive Static Routes 139
Fully Specified Static Routes 141
Floating Static Routing 141
Static Routes to Null Interfaces 143
IPv6 Static Routes 145

Policy-based Routing 146
Virtual Routing and Forwarding 149

Exam Preparation Tasks 151
Review All Key Topics 152
Complete Tables and Lists from Memory 152
Define Key Terms 152
Use the Command Reference to Check Your Memory 153

Chapter 7  EIGRP 154
“Do I Know This Already?” Quiz 154
Foundation Topics 156
EIGRP Fundamentals 156
Autonomous Systems 157
EIGRP Terminology 157
Topology Table 159
EIGRP Neighbors 160
Path Metric Calculation 160
Wide Metrics 162
Metric Backward Compatibility 163
Load Balancing 163
Failure Detection and Timers 164
Convergence 164
Route Summarization 166
Chapter 9  **Advanced OSPF**  202

“Do I Know This Already?” Quiz  202

Foundation Topics  204

Areas  204

Area ID  207

OSPF Route Types  207

Link-State Advertisements  209

LSA Sequences  210

LSA Age and Flooding  210

LSA Types  210

**LSA Type 1: Router Link**  210

**LSA Type 2: Network Link**  213

**LSA Type 3: Summary Link**  213

Discontiguous Networks  217

OSPF Path Selection  218

Intra-Area Routes  218

Inter-Area Routes  219

Equal-Cost Multipathing  220

Summarization of Routes  220

Summarization Fundamentals  221

Inter-Area Summarization  222

Summarization Metrics  222

Configuration of Inter-Area Summarization  223

Route Filtering  224

Filtering with Summarization  225

Area Filtering  225
Chapter 10  OSPFv3  230

“Do I Know This Already?” Quiz  230
Foundation Topics  231
OSPFv3 Fundamentals  231
  OSPFv3 Link-State Advertisement  232
  OSPFv3 Communication  232
OSPFv3 Configuration  233
  OSPFv3 Verification  235
  Passive Interface  237
  Summarization  238
  Network Type  239
IPv4 Support in OSPFv3  240
Exam Preparation Tasks  242
Review All Key Topics  242
Complete Tables and Lists from Memory  242
Define Key Terms  243
Use the Command Reference to Check Your Memory  242
References in This Chapter  243

Chapter 11  BGP  244

“Do I Know This Already?” Quiz  244
Foundation Topics  246
BGP Fundamentals  246
  Autonomous System Numbers  246
  Path Attributes  247
  Loop Prevention  247
  Address Families  248
  Inter.Router Communication  248
  BGP Session Types  249
  BGP Messages  252
BGP Neighbor States  253
  Idle  254
  Connect  254
  Active  254
  OpenSent  254
  OpenConfirm  255
  Established  255

Basic BGP Configuration  255
  Verification of BGP Sessions  257
  Route Advertisement  260
  Receiving and Viewing Routes  262
  BGP Route Advertisements from Indirect Sources  265

IPv4 Route Summarization  268
  Aggregate Address  269
  Atomic Aggregate  274
  Route Aggregation with AS_SET  276

Multiprotocol BGP for IPv6  278
  IPv6 Configuration  279
  IPv6 Route Summarization  284

Exam Preparation Tasks  285
  Review All Key Topics  285
  Complete Tables and Lists from Memory  286
  Define Key Terms  286
  Use the Command Reference to Check Your Memory  286

References in This Chapter  287

Chapter 12  Advanced BGP  288

  “Do I Know This Already?” Quiz  288

Foundation Topics  290
  BGP Multihoming  291
    Resiliency in Service Providers  291
    Internet Transit Routing  292
    Branch Transit Routing  293

Conditional Matching  295
  Access Control Lists  295
  Standard ACLs  295
Extended ACLs 296
BGP Network Selection 296
Prefix Matching 297
Prefix Lists 299
IPv6 Prefix Lists 299
Regular Expressions (regex) 300
Route Maps 301
    Conditional Matching 302
Multiple Conditional Match Conditions 303
Complex Matching 304
Optional Actions 304
The continue Keyword 305
BGP Route Filtering and Manipulation 306
    Distribute List Filtering 307
    Prefix List Filtering 308
    AS_Path ACL Filtering 309
    Route Maps 311
    Clearing BGP Connections 313
BGP Communities 313
    Well-Known Communities 314
    Enabling BGP Community Support 314
    Conditionally Matching BGP Communities 315
    Setting Private BGP Communities 317
Understanding BGP Path Selection 318
    Routing Path Selection Using Longest Match 319
    BGP Best Path Overview 320
Weight 321
Local Preference 322
Locally Originated via Network or Aggregate Advertisement 323
Accumulated Interior Gateway Protocol Metric 323
Shortest AS Path 324
Origin Type 325
Multi-Exit Discriminator 326
eBGP over iBGP 327
Lowest IGP Metric 327
Prefer the Path from the Oldest eBGP Session 328
Chapter 13  Multicast  334

“Do I Know This Already?” Quiz  334
Foundation Topics  337
Multicast Fundamentals  337
Multicast Addressing  340
Internet Group Management Protocol  343
IGMPv2  344
IGMPv3  346
IGMP Snooping  346
Protocol Independent Multicast  349
PIM Distribution Trees  349
Source Trees  349
Shared Trees  350
PIM Terminology  352
PIM Dense Mode  354
PIM Sparse Mode  357
PIM Shared and Source Path Trees  357
Shared Tree Join  358
Source Registration  358
PIM SPT Switchover  358
Designated Routers  359
Reverse Path Forwarding  360
PIM Forwarder  361
Rendezvous Points  363
Part IV Services

Chapter 14 Quality of Service (QoS) 370

“Do I Know This Already?” Quiz 371
Foundation Topics 374
The Need for QoS 374
  Lack of Bandwidth 374
  Latency and Jitter 374
  Propagation Delay 375
  Serialization Delay 375
  Processing Delay 376
  Delay Variation 376
  Packet Loss 376
QoS Models 377
Modular QoS CLI 379
Classification and Marking 381
  Classification 381
  Layer 7 Classification 382
  MQC Classification Configuration 382
  Marking 385
  Layer 2 Marking 385
  Priority Code Point (PCP) 386
  Layer 3 Marking 386
  DSCP Per-Hop Behaviors 387
  Class Selector (CS) PHB 388
  Default Forwarding (DF) PHB 388
  Assured Forwarding (AF) PHB 388
Hot Standby Router Protocol 432
Virtual Router Redundancy Protocol 438
VRRPv2 Configuration 438
VRRPv3 Configuration 440
Gateway Load Balancing Protocol 441
Network Address Translation 446
   NAT Topology 447
   Static NAT 449
      Inside Static NAT 449
      Outside Static NAT 452
   Pooled NAT 455
      Port Address Translation 458
Exam Preparation Tasks 461
Review All Key Topics 461
Complete Tables and Lists from Memory 462
Define Key Terms 462
Use the Command Reference to Check Your Memory 462

Part V Overlay

Chapter 16 Overlay Tunnels 466
   “Do I Know This Already?” Quiz 467
Foundation Topics 469
   Generic Routing Encapsulation (GRE) Tunnels 469
      GRE Tunnel Configuration 470
      GRE Configuration Example 472
      Problems with Overlay Networks: Recursive Routing 474
IPsec Fundamentals 475
   Authentication Header 476
   Encapsulating Security Payload 477
   Transform Sets 478
   Internet Key Exchange 480
   IKEv1 480
   IKEv2 482
IPsec VPNs 484
   Site-to-Site (LAN-to-LAN) IPsec VPNs 486
   Cisco Dynamic Multipoint VPN (DMVPN) 486
Cisco Group Encrypted Transport VPN (GET VPN)  486
Cisco FlexVPN  486
Remote VPN Access  486
Site-to-Site IPsec Configuration  486
Site-to-Site GRE over IPsec  487
Site-to-Site VTI over IPsec  493
Cisco Locator/ID Separation Protocol (LISP)  495
  LISP Architecture and Protocols  497
  LISP Routing Architecture  497
  LISP Control Plane  497
  LISP Data Plane  498
  LISP Operation  499
  Map Registration and Notification  499
  Map Request and Reply  500
  LISP Data Path  501
  Proxy ETR (PETR)  502
  Proxy ITR (PITR)  503
Virtual Extensible Local Area Network (VXLAN)  504
Exam Preparation Tasks  507
Review All Key Topics  507
Complete Tables and Lists from Memory  508
Define Key Terms  508
Use the Command Reference to Check Your Memory  509

Part VI   Wireless

Chapter 17   Wireless Signals and Modulation  510
  “Do I Know This Already?” Quiz  510
  Foundation Topics  512
  Understanding Basic Wireless Theory  512
    Understanding Frequency  514
    Understanding Phase  519
    Measuring Wavelength  519
    Understanding RF Power and dB  520
  Important dB Laws to Remember  522
  Comparing Power Against a Reference: dBm  524
  Measuring Power Changes Along the Signal Path  525
  Free Space Path Loss  527
Part VII  Architecture

Chapter 22  Enterprise Network Architecture  622

“Do I Know This Already?” Quiz  622

Foundation Topics  624

Hierarchical LAN Design Model  624

Access Layer  625
Distribution Layer  627
Core Layer  628

High Availability Network Design  629

High Availability Technologies  630

SSO and NSF  630
SSO/NSF with GR  631
SSO/NSF with NSR  631
SSO/NSF with NSR and GR  631

Enterprise Network Architecture Options  632

Two-Tier Design (Collapsed Core)  632
Three-Tier Design  634

Layer 2 Access Layer (STP Based)  634
Layer 3 Access Layer (Routed Access)  636

Simplified Campus Design  637
Software-Defined Access (SD-Access) Design  640

Exam Preparation Tasks  640

Review All Key Topics  640

Complete Tables and Lists from Memory  640

Define Key Terms  640
Chapter 23  Fabric Technologies  642

“Do I Know This Already?” Quiz  643
Foundation Topics  645
Software-Defined Access (SD-Access)  645
  What Is SD-Access?  646
  SD-Access Architecture  646
  Physical Layer  647
  Network Layer  647
  Underlay Network  648
  Overlay Network (SD-Access Fabric)  649
  SD-Access Fabric Roles and Components  652
  Fabric Control Plane Node  653
  Fabric Border Nodes  654
  Fabric Wireless Controller (WLC)  654
  SD-Access Fabric Concepts  655
  Controller Layer  656
  Management Layer  657
  Cisco DNA Design Workflow  658
  Cisco DNA Policy Workflow  658
  Cisco DNA Provision Workflow  659
  Cisco DNA Assurance Workflow  660
Software-Defined WAN (SD-WAN)  661
  Cisco SD-WAN Architecture  661
  vBond Orchestrator  662
  vManage NMS  663
  vSmart Controller  663
  Cisco SD-WAN Edge Devices  663
  vAnalytics  664
  Cisco SD-WAN Cloud OnRamp  664
  SD-WAN Policy  665
  Application-Aware Routing  665
  Cloud OnRamp for SaaS  666
  Cloud OnRamp for IaaS  668
Exam Preparation Tasks  669
Review All Key Topics  669
Complete Tables and Lists from Memory  670
Define Key Terms  670
Chapter 24  Network Assurance  672

“Do I Know This Already?” Quiz  672
Foundation Topics  674
Network Diagnostic Tools  675
  ping  675
  traceroute  680
Debugging  685
  Conditional Debugging  692
  Simple Network Management Protocol (SNMP)  695
  syslog  701
NetFlow and Flexible NetFlow  706
Switched Port Analyzer (SPAN) Technologies  716
  Local SPAN  717
  Specifying the Source Ports  717
  Specifying the Destination Ports  718
  Local SPAN Configuration Examples  719
Remote SPAN (RSPAN)  720
  Encapsulated Remote SPAN (ERSPAN)  722
  Specifying the Source Ports  722
  Specifying the Destination  723
IP SLA  724
Cisco DNA Center Assurance  728
Exam Preparation Tasks  734
Review All Key Topics  735
Complete Tables and Lists from Memory  735
Define Key Terms  735

Part VIII  Security

Chapter 25  Secure Network Access Control  736

“Do I Know This Already?” Quiz  736
Foundation Topics  738
Network Security Design for Threat Defense  738
Next-Generation Endpoint Security  741
  Cisco Talos  741
  Cisco Secure Malware Analytics (Threat Grid)  742
  Cisco Advanced Malware Protection (AMP)  742
Chapter 28  Foundational Network Programmability Concepts  850

“Do I Know This Already?” Quiz  850
Foundation Topics  854
Command-Line Interface  854
Application Programming Interface  855
  Northbound API  855
  Southbound API  856
  Representational State Transfer (REST) APIs  856
  API Tools and Resources  857
  Introduction to Postman  857
  Data Formats (XML and JSON)  860
Cisco DNA Center APIs  862
Cisco vManage APIs  867
Data Models and Supporting Protocols  870
  YANG Data Models  870
  NETCONF  872
  RESTCONF  876
Cisco DevNet  877
  Documentation  878
  Learn  878
  Technologies  878
  Community  879
  Events  879
GitHub  880
Basic Python Components and Scripts  882
Exam Preparation Tasks  889
Review All Key Topics  889
Complete Tables and Lists from Memory  890
Define Key Terms  890
References in This Chapter  890
Chapter 29  Introduction to Automation Tools  892

“Do I Know This Already?” Quiz  892
Foundation Topics  894
Embedded Event Manager  894
   EEM Applets  895
   EEM and Tcl Scripts  899
   EEM Summary  901
Agent-Based Automation Tools  902
   Puppet  902
   Chef  904
   SaltStack (Agent and Server Mode)  909
Agentless Automation Tools  912
   Ansible  912
   Puppet Bolt  922
   SaltStack SSH (Server-Only Mode)  923
Comparing Tools  924
Exam Preparation Tasks  925
Review All Key Topics  925
Complete Tables and Lists from Memory  925
Define Key Terms  925

Chapter 30  Final Preparation  926

Getting Ready  926
Tools for Final Preparation  927
   Pearson Test Prep Practice Test Software and Questions on the Website  927
   Accessing the Pearson Test Prep Software Online  927
   Accessing the Pearson Test Prep Software Offline  928
Customizing Your Exams  928
Updating Your Exams  929
Premium Edition  929
Chapter-Ending Review Tools  930
Suggested Plan for Final Review/Study  930
Summary  930

Chapter 31  ENCOR 350-401 Exam Updates  932

The Purpose of This Chapter  932
   About Possible Exam Updates  932
Impact on You and Your Study Plan  933
News About the Next Exam Release  934
Updated Technical Content  934

Appendix A  Answers to the “Do I Know This Already?” Questions  936
Glossary  956
Index  978

Online Elements
Appendix B  Memory Tables
Appendix C  Memory Tables Answer Key
Appendix D  Study Planner
Glossary
**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

Congratulations! If you are reading this Introduction, then you have probably decided to obtain a Cisco certification. Obtaining a Cisco certification will ensure that you have a solid understanding of common industry protocols along with Cisco's device architecture and configuration. Cisco has a high market share of routers and switches, with a global footprint.

Professional certifications have been an important part of the computing industry for many years and will continue to become more important. Many reasons exist for these certifications, but the most popularly cited reason is credibility. All other factors being equal, a certified employee/consultant/job candidate is considered more valuable than one who is not certified.

Cisco provides three primary certifications: Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP), and Cisco Certified Internetwork Expert (CCIE). Cisco made the following changes to all three certifications in 2020. The following are the most notable of the many changes:

- The exams will include additional topics, such as programming.
- The CCNA certification is not a prerequisite for obtaining the CCNP certification. CCNA specializations will not be offered anymore.
- The exams will test a candidate's ability to configure and troubleshoot network devices in addition to answering multiple-choice questions.
- The CCNP is obtained by taking and passing a Core exam and a Concentration exam.
- The CCIE certification requires candidates to pass the Core written exam before the CCIE lab can be scheduled.

CCNP Enterprise candidates need to take and pass the CCNP and CCIE Enterprise Core ENCOR 350-401 examination. Then they need to take and pass one of the following Concentration exams to obtain their CCNP Enterprise:

- 300-410 ENARSI: Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)
- 300-415 ENSDWI: Implementing Cisco SD-WAN Solutions (SDWAN300)
- 300-420 ENSLD: Designing Cisco Enterprise Networks (ENSLD)
- 300-425 ENWLSD: Designing Cisco Enterprise Wireless Networks (ENWLSD)
- 300-430 ENWLSI: Implementing Cisco Enterprise Wireless Networks (ENWLSI)
- 300-435 ENAUTO: Implementing Automation for Cisco Enterprise Solutions (ENAUTO)
- 300-440 ENCC: Designing and Implementing Cloud Connectivity (ENCC)
Be sure to visit www.cisco.com to find the latest information on CCNP Concentration requirements and to keep up to date on any new Concentration exams that are announced.

CCIE Enterprise candidates need to take and pass the CCNP and CCIE Enterprise Core ENCOR 350-401 examination. Then they need to take and pass the CCIE Enterprise Infrastructure or Enterprise Wireless lab exam.

Goals and Methods

The most important and somewhat obvious goal of this book is to help you pass the CCNP and CCIE Enterprise Core ENCOR 350-401 exam. In fact, if the primary objective of this book were different, then the book's title would be misleading; however, the methods used in this book to help you pass the exam are designed to also make you much more knowledgeable about how to do your job.

One key methodology used in this book is to help you discover the exam topics that you need to review in more depth, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. This book does not try to help you simply memorize; rather, it helps you truly learn and understand the topics. The CCNP and CCIE Enterprise Core exam is just one of the foundation topics in the CCNP certification, and the knowledge contained within is vitally important to being a truly skilled routing/switching engineer or specialist. This book would do you a disservice if it didn't attempt to help you learn the material. To that end, the book will help you pass the CCNP and CCIE Enterprise Core exam by using the following methods:

- Helping you discover which test topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises and scenarios that enhance your ability to recall and deduce the answers to test questions

Who Should Read This Book?

This book is not designed to be a general networking topics book, although it can be used for that purpose. This book is intended to tremendously increase your chances of passing the CCNP and CCIE Enterprise Core exam. Although other objectives can be achieved from using this book, the book is written with one goal in mind: to help you pass the exam.

So why should you want to pass the CCNP and CCIE Enterprise Core ENCOR 350-401 exam? Because it's one of the milestones toward getting the CCNP certification or to being able to schedule the CCIE lab—which is no small feat. What would getting the CCNP or CCIE mean to you? It might translate to a raise, a promotion, and recognition. It would certainly enhance your resume. It would demonstrate that you are serious about continuing the learning process and that you're not content to rest on your laurels. It might please your reseller-employer, who needs more certified employees for a higher discount from Cisco. Or you might have one of many other reasons.
Strategies for Exam Preparation

The strategy you use to prepare for the CCNP and CCIE Enterprise Core ENCOR 350-401 exam might be slightly different from strategies used by other readers, depending on the skills, knowledge, and experience you already have obtained. For instance, if you have attended the CCNP and CCIE Enterprise Core ENCOR 350-401 course, then you might take a different approach than someone who learned switching via on-the-job training.

Regardless of the strategy you use or the background you have, the book is designed to help you get to the point where you can pass the exam with the least amount of time required. For instance, there is no need for you to practice or read about IP addressing and subnetting if you fully understand it already. However, many people like to make sure that they truly know a topic and thus read over material that they already know. Several features of this book will help you gain the confidence that you need to be convinced that you know some material already and to also help you know what topics you need to study more.

The Companion Website for Online Content Review

All the electronic review elements, as well as other electronic components of the book, exist on this book's companion website.

How to Access the Companion Website

To access the companion website, which gives you access to the electronic content with this book, start by establishing a login at www.ciscopress.com and registering your book. To do so, simply go to www.ciscopress.com/register and enter the ISBN of the print book: 9780138216764. After you have registered your book, go to your account page and click the Registered Products tab. From there, click the Access Bonus Content link to get access to the book's companion website.

Note that if you buy the Premium Edition eBook and Practice Test version of this book from Cisco Press, your book will automatically be registered on your account page. Simply go to your account page, click the Registered Products tab, and select Access Bonus Content to access the book's companion website.

How to Access the Pearson Test Prep (PTP) App

You have two options for installing and using the Pearson Test Prep application: a web app and a desktop app. To use the Pearson Test Prep application, start by finding the registration code that comes with the book. You can find the code in these ways:

- **Print book or bookseller eBook versions:** You can get your access code by registering the print ISBN (9780138216764) on ciscopress.com/register. Make sure to use the print book ISBN regardless of whether you purchased an eBook or the print book. Once you register the book, your access code will be populated on your account page under the Registered Products tab. Instructions for how to redeem the code are available on the book's companion website by clicking the Access Bonus Content link.
Premium Edition: If you purchase the Premium Edition eBook and Practice Test
directly from the Cisco Press website, the code will be populated on your account
page after purchase. Just log in at www.ciscopress.com, click Account to see details
of your account, and click the digital purchases tab.

NOTE After you register your book, your code can always be found in your account
under the Registered Products tab.

Once you have the access code, to find instructions about both the PTP web app and the
desktop app, follow these steps:

Step 1. Open this book’s companion website, as shown earlier in this Introduction
under the heading “How to Access the Companion Website.”

Step 2. Click the Practice Exams button.

Step 3. Follow the instructions listed there both for installing the desktop app and for
using the web app.

Note that if you want to use the web app only at this point, just navigate to
www.pearsonatestprep.com, establish a free login if you do not already have one, and
register this book’s practice tests using the registration code you just found. The process
should take only a couple of minutes.

How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow
you to easily move between chapters and sections of chapters to cover just the material
that you need more work with. If you do intend to read them all, the order in the book is
an excellent sequence to use.

The book includes the following chapters:

- **Chapter 1, “Packet Forwarding”**: This chapter provides a review of basic network
  fundamentals and then dives deeper into technical concepts related to how network
  traffic is forwarded through a router or switch architecture.

- **Chapter 2, “Spanning Tree Protocol”**: This chapter explains how switches prevent
  forwarding loops while allowing for redundant links with the use of Spanning Tree
  Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

- **Chapter 3, “Advanced STP Tuning”**: This chapter reviews common techniques that
  are in Cisco Validated Design guides. Topics include root bridge placement and pro-
  tection.

- **Chapter 4, “Multiple Spanning Tree Protocol”**: This chapter completes the section
  of spanning tree by explaining Multiple Spanning Tree (MST) protocol.
Chapter 5, “VLAN Trunks and EtherChannel Bundles”: This chapter covers features such as VTP, DTP, and EtherChannel for switch-to-switch connectivity.

Chapter 6, “IP Routing Essentials”: This chapter revisits the fundamentals from Chapter 1 and examines some of the components of the operations of a router. It reinforces the logic of the programming of the Routing Information Base (RIB), reviews differences between common routing protocols, and explains common concepts related to static routes.

Chapter 7, “EIGRP”: This chapter explains the underlying mechanics of the EIGRP routing protocol, the path metric calculations, and the failure detection mechanisms and techniques for optimizing the operations of the routing protocol.

Chapter 8, “OSPF”: This chapter explains the core concepts of OSPF and the basics in establishing neighborships and exchanging routes with other OSPF routers.

Chapter 9, “Advanced OSPF”: This chapter expands on Chapter 8 and explains the functions and features found in larger enterprise networks. By the end of this chapter, you should have a solid understanding of the route advertisement within a multi-area OSPF domain, path selection, and techniques to optimize an OSPF environment.

Chapter 10, “OSPFv3”: This chapter explains how the OSPF protocol has changed to accommodate support of IPv6.

Chapter 11, “BGP”: This chapter explains the core concepts of BGP and its path attributes. This chapter explains configuration of BGP and advertisement and summarization of IPv4 and IPv6 network prefixes.

Chapter 12, “Advanced BGP”: This chapter expands on Chapter 11 and explains BGP’s advanced features and concepts, such as BGP multihoming, route filtering, BGP communities, and the logic for identifying the best path for a specific network prefix.

Chapter 13, “Multicast”: This chapter describes the fundamental concepts related to multicast and how it operates. It also describes the protocols that are required to understand its operation in more detail, such as Internet Group Messaging Protocol (IGMP), IGMP snooping, Protocol Independent Multicast (PIM) Dense Mode/Sparse Mode, and rendezvous points (RPs).

Chapter 14, “Quality of Service (QoS)”: This chapter describes the different QoS models available: best effort, Integrated Services (IntServ), and Differentiated Services (DiffServ). It also describes tools and mechanisms used to implement QoS such as classification and marking, policing and shaping, and congestion management and avoidance, and it also explains how to configure them.

Chapter 15, “IP Services”: In addition to routing and switching network packets, a router can perform additional functions to enhance the network. This chapter covers time synchronization, virtual gateway technologies, and network address translation.
Chapter 16, “Overlay Tunnels”: This chapter explains Generic Routing Encapsulation (GRE) and IP Security (IPsec) fundamentals and how to configure them. It also explains Locator ID/Separation Protocol (LISP) and Virtual Extensible Local Area Network (VXLAN).

Chapter 17, “Wireless Signals and Modulation”: This chapter covers the basic theory behind radio frequency (RF) signals, measuring and comparing the power of RF signals, and basic methods and standards involved in carrying data wirelessly.

Chapter 18, “Wireless Infrastructure”: This chapter describes autonomous, cloud-based, centralized, embedded, and Mobility Express wireless architectures. It also explains the process that lightweight APs must go through to discover and bind to a wireless LAN controller. Various AP modes and antennas are also described.

Chapter 19, “Understanding Wireless Roaming and Location Services”: This chapter discusses client mobility from the AP and controller perspectives so that you can design and configure a wireless network properly as it grows over time. It also explains how components of a wireless network can be used to compute the physical locations of wireless devices.

Chapter 20, “Authenticating Wireless Clients”: This chapter covers several methods you can use to authenticate users and devices in order to secure a wireless network.

Chapter 21, “Troubleshooting Wireless Connectivity”: This chapter helps you get some perspective about problems wireless clients may have with their connections, develop a troubleshooting strategy, and become comfortable using a wireless LAN controller as a troubleshooting tool.

Chapter 22, “Enterprise Network Architecture”: This chapter provides a high-level overview of the enterprise campus architectures that can be used to scale from a small environment to a large campus-size network.

Chapter 23, “Fabric Technologies”: This chapter defines the benefits of Software-Defined Access (SD-Access) over traditional campus networks as well as the components and features of the Cisco SD-Access solution, including the nodes, fabric control plane, and data plane. It also defines the benefits of Software-Defined WAN (SD-WAN) over traditional WANs, as well as the components and features of the Cisco SD-WAN solution, including the orchestration plane, management plane, control plane, and data plane.

Chapter 24, “Network Assurance”: This chapter covers some of the tools most commonly used for operations and troubleshooting in the network environment. Cisco DNA Center with Assurance is also covered, to showcase how the tool can improve mean time to innocence (MTTI) and root cause analysis of issues.

Chapter 25, “Secure Network Access Control”: This chapter describes a Cisco security framework to protect networks from evolving cybersecurity threats as well as the security components that are part of the framework, such as next-generation firewalls, web security, email security, and much more. It also describes network access control (NAC) technologies such as 802.1x, Web Authentication (WebAuth), MAC Authentication Bypass (MAB), TrustSec, and MACsec.
Chapter 26, “Network Device Access Control and Infrastructure Security”: This chapter focuses on how to configure and verify network device access control through local authentication and authorization as well through AAA. It also explains how to configure and verify router security features, such as access control lists (ACLs), control plane policing (CoPP), and zone-based firewalls (ZBFWs), that are used to provide device and infrastructure security.

Chapter 27, “Virtualization”: This chapter describes server virtualization technologies such as virtual machines, containers, and virtual switching. It also describes the network functions virtualization (NFV) architecture and Cisco’s enterprise NFV solution.

Chapter 28, “Foundational Network Programmability Concepts”: This chapter covers current network management methods and tools as well as key network programmability methods. It also covers how to use software application programming interfaces (APIs) and common data formats.

Chapter 29, “Introduction to Automation Tools”: This chapter discusses some of the most common automation tools that are available. It covers on-box, agent-based, and agentless tools and examples.

Chapter 30, “Final Preparation”: This chapter details a set of tools and a study plan to help you complete your preparation for the CCNP and CCIE Enterprise Core ENCOR 350-401 exam.

Certification Exam Topics and This Book
The questions for each certification exam are a closely guarded secret. However, we do know which topics you must know to successfully complete the CCNP and CCIE Enterprise Core ENCOR 350-401 exam. Cisco publishes them as an exam blueprint. Table I-1 lists each exam topic listed in the blueprint along with a reference to the book chapter that covers the topic. These are the same topics you should be proficient in when working with enterprise technologies in the real world.

Table I-1  CCNP and CCIE Enterprise Core ENCOR 350-401 Topics and Chapter References

<table>
<thead>
<tr>
<th>CCNP and CCIE Enterprise Core ENCOR (350-401) Exam Topic</th>
<th>Chapter(s) in Which Topic Is Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Architecture</td>
<td></td>
</tr>
<tr>
<td>1.1 Explain the different design principles used in an enterprise network</td>
<td></td>
</tr>
<tr>
<td>1.1.a High-level enterprise network design such as 2-tier, 3-tier, fabric, and cloud</td>
<td>22</td>
</tr>
<tr>
<td>1.1.b High availability techniques such as redundancy, FHRP, and SSO</td>
<td>15, 22</td>
</tr>
<tr>
<td>1.2 Describe wireless network design principles</td>
<td></td>
</tr>
<tr>
<td>CCNP and CCIE Enterprise Core ENCOR (350-401) Exam Topic</td>
<td>Chapter(s) in Which Topic Is Covered</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>1.2.a Wireless deployment models (centralized, distributed, controller-less, controller-based, cloud, remote branch)</td>
<td>18</td>
</tr>
<tr>
<td>1.2.b Location services in a WLAN design</td>
<td>19</td>
</tr>
<tr>
<td>1.2.c Client density</td>
<td>18</td>
</tr>
<tr>
<td>1.3 Explain the working principles of the Cisco SD-WAN solution</td>
<td></td>
</tr>
<tr>
<td>1.3.a SD-WAN control and data planes elements</td>
<td>23</td>
</tr>
<tr>
<td>1.3.b Benefits and limitations of SD-WAN solutions</td>
<td>23</td>
</tr>
<tr>
<td>1.4 Explain the working principles of the Cisco SD-Access solution</td>
<td></td>
</tr>
<tr>
<td>1.4.a SD-Access control and data planes elements</td>
<td>23</td>
</tr>
<tr>
<td>1.4.b Traditional campus interoperating with SD-Access</td>
<td>23</td>
</tr>
<tr>
<td>1.5 Interpret wired and wireless QoS configurations</td>
<td></td>
</tr>
<tr>
<td>1.5.a QoS components</td>
<td>14</td>
</tr>
<tr>
<td>1.5.b QoS policy</td>
<td>14</td>
</tr>
<tr>
<td>1.6 Describe hardware and software switching mechanisms such as CEF, CAM, TCAM, FIB, RIB, and adjacency tables</td>
<td>1</td>
</tr>
<tr>
<td>2.0 Virtualization</td>
<td></td>
</tr>
<tr>
<td>2.1 Describe device virtualization technologies</td>
<td></td>
</tr>
<tr>
<td>2.1.a Hypervisor type 1 and 2</td>
<td>27</td>
</tr>
<tr>
<td>2.1.b Virtual machine</td>
<td>27</td>
</tr>
<tr>
<td>2.1.c Virtual switching</td>
<td>27</td>
</tr>
<tr>
<td>2.2 Configure and verify data path virtualization technologies</td>
<td></td>
</tr>
<tr>
<td>2.2.a VRF</td>
<td>6</td>
</tr>
<tr>
<td>2.2.b GRE and IPsec tunneling</td>
<td>16</td>
</tr>
<tr>
<td>2.3 Describe network virtualization concepts</td>
<td></td>
</tr>
<tr>
<td>2.3.a LISP</td>
<td>16</td>
</tr>
<tr>
<td>2.3.b VXLAN</td>
<td>16</td>
</tr>
<tr>
<td>3.0 Infrastructure</td>
<td></td>
</tr>
<tr>
<td>3.1 Layer 2</td>
<td></td>
</tr>
<tr>
<td>3.1.a Troubleshoot static and dynamic 802.1q trunking protocols</td>
<td>5</td>
</tr>
<tr>
<td>3.1.b Troubleshoot static and dynamic EtherChannels</td>
<td>5</td>
</tr>
<tr>
<td>3.1.c Configure and verify common Spanning Tree Protocols (RSTP, MST) and Spanning Tree enhancements such as root guard and BPDG guard</td>
<td>2, 3, 4</td>
</tr>
<tr>
<td>3.2 Layer 3</td>
<td></td>
</tr>
<tr>
<td>3.2.a Compare routing concepts of EIGRP and OSPF (advanced distance vector vs. linked state, load balancing, path selection, path operations, metrics, and area types)</td>
<td>6, 7, 8, 9</td>
</tr>
<tr>
<td>CCNP and CCIE Enterprise Core ENCOR (350-401) Exam Topic</td>
<td>Chapter(s) in Which Topic Is Covered</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>3.2.b Configure simple OSPFv2/v3 environments, including multiple normal areas, summarization, and filtering (neighbor adjacency, point-to-point, and broadcast network types, and passive-interface)</td>
<td>8, 9, 10</td>
</tr>
<tr>
<td>3.2.c Configure and verify eBGP between directly connected neighbors (best path selection algorithm and neighbor relationships)</td>
<td>11, 12</td>
</tr>
<tr>
<td>3.2.d Describe policy-based routing</td>
<td>6</td>
</tr>
<tr>
<td>3.3 Wireless</td>
<td></td>
</tr>
<tr>
<td>3.3.a Describe Layer 1 concepts, such as RF power, RSSI, SNR, interference, noise, bands, channels, and wireless client devices capabilities</td>
<td>17</td>
</tr>
<tr>
<td>3.3.b Describe AP modes and antenna types</td>
<td>18</td>
</tr>
<tr>
<td>3.3.c Describe access point discovery and join process (discovery algorithms, WLC selection process)</td>
<td>18</td>
</tr>
<tr>
<td>3.3.d Describe the main principles and use cases for Layer 2 and Layer 3 roaming</td>
<td>19</td>
</tr>
<tr>
<td>3.3.e Troubleshoot WLAN configuration and wireless client connectivity issues using GUI only</td>
<td>21</td>
</tr>
<tr>
<td>3.3.f Describe wireless segmentation with groups, profiles, and tags</td>
<td>18</td>
</tr>
<tr>
<td>3.4 IP Services</td>
<td></td>
</tr>
<tr>
<td>3.4.a Interpret network time protocol configurations such as NTP and PTP</td>
<td>15</td>
</tr>
<tr>
<td>3.4.b Configure NAT/PAT</td>
<td>15</td>
</tr>
<tr>
<td>3.4.c Configure first hop redundancy protocols, such as HSRP, VRRP</td>
<td>15</td>
</tr>
<tr>
<td>3.4.d Describe multicast protocols, such as RPF check, PIM, and IGMP v2/v3</td>
<td>13</td>
</tr>
<tr>
<td>4.0 Network Assurance</td>
<td></td>
</tr>
<tr>
<td>4.1 Diagnose network problems using tools such as debugs, conditional debugs, traceroute, ping, SNMP, and syslog</td>
<td>24</td>
</tr>
<tr>
<td>4.2 Configure Flexible NetFlow</td>
<td>24</td>
</tr>
<tr>
<td>4.3 Configure and verify SPAN/RSPAN/ERSPAN</td>
<td>24</td>
</tr>
<tr>
<td>4.4 Configure and verify IPSLA</td>
<td>24</td>
</tr>
<tr>
<td>4.5 Describe Cisco DNA Center workflows to apply network configuration, monitoring, and management</td>
<td>24</td>
</tr>
<tr>
<td>4.6 Configure and verify NETCONF and RESTCONF</td>
<td>28</td>
</tr>
<tr>
<td>5.0 Security</td>
<td></td>
</tr>
<tr>
<td>5.1 Configure and verify device access control</td>
<td>26</td>
</tr>
<tr>
<td>CCNP and CCIE Enterprise Core ENCOR (350-401) Exam Topic</td>
<td>Chapter(s) in Which Topic Is Covered</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td><strong>5.1.a Lines and local user authentication</strong></td>
<td>26</td>
</tr>
<tr>
<td><strong>5.1.b Authentication and authorization using AAA</strong></td>
<td>26</td>
</tr>
<tr>
<td>5.2 Configure and verify infrastructure security features</td>
<td>26</td>
</tr>
<tr>
<td><strong>5.2.a ACLs</strong></td>
<td>26</td>
</tr>
<tr>
<td><strong>5.2.b CoPP</strong></td>
<td>26</td>
</tr>
<tr>
<td>5.3 Describe REST API security</td>
<td>28</td>
</tr>
<tr>
<td>5.4 Configure and verify wireless security features</td>
<td>20, 25</td>
</tr>
<tr>
<td><strong>5.4.a 802.1X</strong></td>
<td>20</td>
</tr>
<tr>
<td><strong>5.4.b WebAuth</strong></td>
<td>20</td>
</tr>
<tr>
<td><strong>5.4.c PSK</strong></td>
<td>20</td>
</tr>
<tr>
<td><strong>5.4.d EAPOL (4-way handshake)</strong></td>
<td>20</td>
</tr>
<tr>
<td>5.5 Describe the components of network security design</td>
<td>25</td>
</tr>
<tr>
<td><strong>5.5.a Threat defense</strong></td>
<td>25</td>
</tr>
<tr>
<td><strong>5.5.b Endpoint security</strong></td>
<td>25</td>
</tr>
<tr>
<td><strong>5.5.c Next-generation firewall</strong></td>
<td>25</td>
</tr>
<tr>
<td><strong>5.5.d TrustSec and MACsec</strong></td>
<td>25</td>
</tr>
<tr>
<td><strong>5.5.e Network access control with 802.1X, MAB, and WebAuth</strong></td>
<td>20, 25</td>
</tr>
<tr>
<td><strong>6.0 Automation</strong></td>
<td></td>
</tr>
<tr>
<td>6.1 Interpret basic Python components and scripts</td>
<td>29</td>
</tr>
<tr>
<td>6.2 Construct valid JSON-encoded file</td>
<td>28</td>
</tr>
<tr>
<td>6.3 Describe the high-level principles and benefits of a data modeling language, such as YANG</td>
<td>28</td>
</tr>
<tr>
<td>6.4 Describe APIs for Cisco DNA Center and vManage</td>
<td>28</td>
</tr>
<tr>
<td>6.5 Interpret REST API response codes and results in payload using Cisco DNA Center and RESTCONF</td>
<td>28</td>
</tr>
<tr>
<td>6.6 Construct EEM applet to automate configuration, troubleshooting, or data collection</td>
<td>29</td>
</tr>
<tr>
<td>6.7 Compare agent vs. agentless orchestration tools, such as Chef, Puppet, Ansible, and SaltStack</td>
<td>29</td>
</tr>
</tbody>
</table>

Each version of the exam may emphasize different functions or features, and some topics are rather broad and generalized. The goal of this book is to provide the most comprehensive coverage to ensure that you are well prepared for the exam. Although some chapters might not address specific exam topics, they provide a foundation that is necessary for a clear understanding of important topics.

It is also important to understand that this book is a static reference, whereas the exam topics are dynamic. Cisco can and does change the topics covered on certification exams often.
This exam guide should not be your only reference when preparing for the certification exam. You can find a wealth of information available at Cisco.com that covers each topic in great detail. If you think that you need more detailed information on a specific topic, read the Cisco documentation that focuses on your chosen topic.

Note that as technologies continue to evolve, Cisco reserves the right to change the exam topics without notice. Although you can refer to the list of exam topics in Table I-1, always check Cisco.com to verify the actual list of topics to ensure that you are prepared before taking the exam. You can view the current exam topics on any current Cisco certification exam by visiting the Cisco.com website, hovering over Training & Events, and selecting from the Certifications list. Note also that, if needed, Cisco Press might post additional preparatory content on the web page associated with this book: http://www.ciscopress.com/title/9780138216764. It's a good idea to check the website a couple weeks before taking the exam to be sure that you have up-to-date content.
Figure Credits

Figure 28-2 through Figure 28-14: Postman, Inc
Figure 28-20 through Figure 28-23: GitHub, Inc
Figure 29-2, Figure 29-3: Perforce Software, Inc
Figure 29-4: Chef Software, Inc
Figure 29-5, Figure 29-6, Figure 29-7: VMware, Inc
Figure 29-14: Puppet
Figure 29-10 through Figure 29-13: YAML Lint
OSPFv3

This chapter covers the following subjects:

- **OSPFv3 Fundamentals**: This section provides an overview of the OSPFv3 routing protocol and the similarities to OSPFv2.
- **OSPFv3 Configuration**: This section demonstrates the configuration and verification of an OSPFv3 environment.
- **IPv4 Support in OSPFv3**: This section explains and demonstrates how OSPFv3 can be used for exchanging IPv4 routes.

OSPF Version 3 (OSPFv3), which is the latest version of the OSPF protocol, includes support for both the IPv4 and IPv6 address families. The OSPFv3 protocol is not backward compatible with OSPFv2, but the protocol mechanisms described in Chapters 8, “OSPF,” and 9, “Advanced OSPF,” are essentially the same for OSPFv3. This chapter expands on Chapter 9 and discusses OSPFv3 and its support of IPv6.

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz enables you to assess whether you should read the entire chapter. If you miss no more than one of these self-assessment questions, you might want to move ahead to the “Exam Preparation Tasks” section. Table 10-1 lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in Appendix A, “Answers to the ‘Do I Know This Already?’ Questions.”

| Table 10-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping |
|---------------------------------|------------------|
| **Foundation Topics Section**  | **Questions**    |
| OSPFv3 Fundamentals            | 1–2              |
| OSPFv3 Configuration           | 3–4              |
| IPv4 Support in OSPFv3         | 5                |

1. OSPFv3 uses _________ packet types for inter-router communication.
   a. three
   b. four
   c. five
   d. six
   e. seven
2. The OSPFv3 hello packet uses the ___________ for the destination address.
   a. MAC address 00:C1:00:5C:00:FF
   b. MAC address E0:00:00:06:00:AA
   c. IP address 224.0.0.8
   d. IP address 224.0.0.10
   e. IPv6 address FF02::A
   f. IPv6 address FF02::5

3. How do you enable OSPFv3 on an interface?
   a. Use the command network prefix/prefix-length under the OSPF process.
   b. Use the command network interface-id under the OSPF process.
   c. Use the command ospfv3 process-id ipv6 area area-id under the interface.
   d. Nothing. OSPFv3 is enabled on all IPv6 interfaces upon initialization of the OSPF process.

4. True or false: On a brand-new router installation, OSPFv3 requires only that an IPv6 link-local address be configured and that OSPFv3 be enabled on that interface to form an OSPFv3 neighborship with another router.
   a. True
   b. False

5. True or false: OSPFv3 support for IPv4 networks only requires that an IPv4 address be assigned to the interface and that the OSPFv3 process be initialized for IPv4.
   a. True
   b. False

Foundation Topics

**OSPFv3 Fundamentals**

OSPFv3 is different from OSPFv2 in the following ways:

- **Support for multiple address families**: OSPFv3 supports IPv4 and IPv6 address families.
- **New LSA types**: New LSA types have been created to carry IPv6 prefixes.
- **Removal of addressing semantics**: The IP prefix information is no longer present in the OSPF packet headers. Instead, it is carried as LSA payload information, making the protocol essentially address family independent, much like IS-IS. OSPFv3 uses the term *link* instead of *network* because the SPT calculations are per link instead of per subnet.
- **LSA flooding**: OSPFv3 includes a new link-state type field that is used to determine the flooding scope of LSA, as well as the handling of unknown LSA types.
- **Packet format**: OSPFv3 runs directly over IPv6, and the number of fields in the packet header has been reduced.
- **Router ID:** The router ID is used to identify neighbors, regardless of the network type in OSPFv3. When you're configuring OSPFv3 on IOS routers, the ID must always be manually assigned in the routing process.

- **Authentication:** Neighbor authentication has been removed from the OSPF protocol and is now performed through IPsec extension headers in the IPv6 packet.

- **Neighbor adjacencies:** OSPFv3 inter-router communication is handled by IPv6 link-local addressing. Neighbors are not automatically detected over non-broadcast multiple access (NBMA) interfaces. A neighbor must be manually specified using the link-local address. IPv6 allows for multiple subnets to be assigned to a single interface, and OSPFv3 allows for neighbor adjacency to form even if the two routers do not share a common subnet.

- **Multiple instances:** OSPFv3 packets include an instance ID field that may be used to manipulate which routers on a network segment are allowed to form adjacencies.

**NOTE**  
RFC 5340 provides in-depth coverage of all the differences between OSPFv2 and OSPFv3.

**OSPFv3 Link-State Advertisement**

The OSPF link-state database information is organized and advertised differently in Version 3 than in Version 2. OSPFv3 modifies the structure of the router LSA (type 1), renames the network summary LSA to inter-area prefix LSA, and renames the ASBR summary LSA to inter-area router LSA. The principal difference is that the router LSA is only responsible for announcing interface parameters such as the interface type (point-to-point, broadcast, NBMA, point-to-multipoint, and virtual links) and metric (cost).

IP address information is advertised independently by two new LSA types:

- Intra-area prefix LSA
- Link LSA

The OSPF Dijkstra calculation used to determine the shortest path tree (SPT) only examines the router and network LSAs. Advertising the IP prefix information using new LSA types eliminates the need for OSPF to perform full shortest path first (SPF) tree calculations every time a new IP address (prefix) is added or changed on an interface. The OSPFv3 link-state database (LSDB) creates a shortest path topology tree based on links instead of networks.

**OSPFv3 Communication**

OSPFv3 packets use protocol number 89 in the IPv6 header, and routers communicate with each other using the local interface's IPv6 link-local address as the source. It also uses the

Answers to the “Do I Know This Already?” quiz:

1. C  
2. F  
3. C  
4. B  
5. B
same five packet types and logic as OSPFv2. Depending on the packet type, the destination address is either a unicast link-local address or a multicast link-local scoped address:

- FF02::05: OSPFv3 AllSPFRouters
- FF02::06: OSPFv3 AllDRouters

Every router uses the AllSPFRouters multicast address FF02::5 to send OSPF hello messages to routers on the same link. The hello messages are used for neighbor discovery and detecting whether a neighbor relationship is down. The DR and BDR routers also use this address to send link-state update and flooding acknowledgment messages to all routers.

Non-DR/BDR routers send an update or link-state acknowledgment message to the DR and BDR by using the AllDRouters address FF02::6.

**OSPFv3 Configuration**

The process of configuring OSPFv3 involves the following steps:

**Step 1.** Initialize the routing process. As a prerequisite, `ipv6 unicast-routing` must be enabled on the router. Afterward, the OSPFv3 process is configured with the command `router ospfv3 [process-id].`

**Step 2.** Define the router ID. The command `router-id router-id` assigns a router ID to the OSPF process. The router ID is a 32-bit value that does not need to match an IPv4 address. It may be any number in IPv4 address format (for example, 0.1.2.3), as long as the value is unique within the OSPF domain.

OSPFv3 uses the same algorithm as OSPFv2 for dynamically locating the RID. If there are not any IPv4 interfaces available, the RID is set to 0.0.0.0 and does not allow adjacencies to form.

**Step 3.** (Optional) Initialize the address family. The address family is initialized within the routing process with the command `address-family {ipv6 | ipv4} unicast`. The appropriate address family is enabled automatically when OSPFv3 is enabled on an interface.

**Step 4.** Enable OSPFv3 on an interface. The interface command `ospfv3 process-id ipv6 area area-id` enables the protocol and assigns the interface to an area.

**NOTE** OSPFv3 does not use the network statement for initializing interfaces.

Figure 10-1 displays a simple four-router topology to demonstrate OSPFv3 configuration. Area 0 consists of R1, R2, and R3, and Area 34 contains R3 and R4. R3 is the ABR.
Example 10-1 provides the OSPFv3 and IPv6 address configurations for R1, R2, R3, and R4. IPv6 link-local addressing has been configured so that all router interfaces reflect their local numbers (for example, R1’s interfaces are set to FE80::1) in addition to traditional IPv6 addressing. The link-local addressing is statically configured to assist with any diagnostic output in this chapter. The OSPFv3 configuration has been highlighted in this example.

**Example 10-1  IPv6 Addressing and OSPFv3 Configuration**

### R1

```plaintext
interface Loopback0
  ipv6 address 2001:DB8::1/128
  ospfv3 1 ipv6 area 0

interface GigabitEthernet0/1
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:0:1::1/64
  ospfv3 1 ipv6 area 0

interface GigabitEthernet0/2
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:0:12::1/64
  ospfv3 1 ipv6 area 0

router ospfv3 1
  router-id 192.168.1.1
```

### R2

```plaintext
interface Loopback0
  ipv6 address 2001:DB8::2/128
  ospfv3 1 ipv6 area 0

interface GigabitEthernet0/1
  ipv6 address FE80::2 link-local
  ipv6 address 2001:DB8:0:12::2/64
  ospfv3 1 ipv6 area 0

interface GigabitEthernet0/3
  ipv6 address FE80::2 link-local
  ospfv3 1 ipv6 area 0

router ospfv3 1
  router-id 192.168.2.2
```

### R3

```plaintext
interface Loopback0
  ipv6 address 2001:DB8::3/128
```
**NOTE** Earlier versions of IOS used the commands `ipv6 router ospf` for initialization of the OSPF process and `ipv6 ospf process-id area area-id` for identification of the interface. These commands are considered legacy and should be migrated to the ones used in this book.

**OSPFv3 Verification**

The commands for viewing OSPFv3 settings and statuses are similar to those used in OSPFv2; they essentially replace `ip ospf` with `ospfv3 ipv6`. Supporting OSPFv3 requires verifying the OSPFV3 interfaces, neighborship, and the routing table.

For example, to view the neighbor adjacency for OSPFv2, the command `show ip ospf neighbor` is executed, and for OSPFv3, the command `show ospfv3 ipv6 neighbor` is used. Example 10-2 shows this command executed on R3.
Example 10-2  Identifying R3’s OSPFv3 Neighbors

R3# show ospfv3 ipv6 neighbor

OSPFv3 1 address-family ipv6 (router-id 192.168.3.3)

<table>
<thead>
<tr>
<th>Neighbor ID</th>
<th>Pri</th>
<th>State</th>
<th>Dead Time</th>
<th>Interface ID</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.2.2</td>
<td>1</td>
<td>FULL/DR</td>
<td>00:00:32</td>
<td>5</td>
<td>GigabitEthernet0/2</td>
</tr>
<tr>
<td>192.168.4.4</td>
<td>1</td>
<td>FULL/BDR</td>
<td>00:00:33</td>
<td>5</td>
<td>GigabitEthernet0/4</td>
</tr>
</tbody>
</table>

Example 10-3 shows R1's GigabitEthernet0/2 OSPFv3-enabled interface status with the command `show ospfv3 interface [interface-id]`. Notice that address semantics have been removed compared to OSPFv2. The interface maps to the interface ID value 3 rather than an IP address value, as in OSPFv2. In addition, some helpful topology information describes the link. The local router is the DR (192.168.1.1), and the adjacent neighbor router is the BDR (192.168.2.2).

Example 10-3  Viewing the OSPFv3 Interface Configuration

R1# show ospfv3 interface GigabitEthernet0/2

GigabitEthernet0/2 is up, line protocol is up

Link Local Address FE80::1, Interface ID 3
Area 0, Process ID 1, Instance ID 0, Router ID 192.168.1.1
Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.1.1, local address FE80::1
Backup Designated router (ID) 192.168.2.2, local address FE80::2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
Graceful restart helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 4
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1

A brief version of the OSPFv3 interface settings can be viewed with the command `show ospfv3 interface brief`. The associated process ID, area, address family (IPv4 or IPv6), interface state, and neighbor count are provided in the output.

Example 10-4 demonstrates this command being executed on the ABR, R3. Notice that some interfaces reside in Area 0, and others reside in Area 34.

Example 10-4  Viewing a Brief Version of OSPFv3 Interfaces

R3# show ospfv3 interface brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>PID</th>
<th>Area</th>
<th>AF</th>
<th>Cost</th>
<th>State</th>
<th>Nbrs</th>
<th>F/C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lo0</td>
<td>1</td>
<td>0</td>
<td>ipv6</td>
<td>1</td>
<td>LOOP</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>Gi0/2</td>
<td>1</td>
<td>0</td>
<td>ipv6</td>
<td>1</td>
<td>BDR</td>
<td>1/1</td>
<td></td>
</tr>
<tr>
<td>Gi0/4</td>
<td>1</td>
<td>34</td>
<td>ipv6</td>
<td>1</td>
<td>DR</td>
<td>1/1</td>
<td></td>
</tr>
</tbody>
</table>
The OSPFv3 IPv6 routing table is viewed with the command `show ipv6 route ospf`. Intra-area routes are indicated with `O`, and inter-area routes are indicated with `OI`.

Example 10-5 shows this command being executed on R1. The forwarding address for the routes is the link-local address of the neighboring router.

**Example 10-5  Viewing the OSPFv3 Routes in the IPv6 Routing Table**

```
R1# show ipv6 route ospf
! Output omitted for brevity
IPv6 Routing Table - default - 11 entries
    RL - RPL, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
    OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
    
    O  2001:DB8::2/128 [110/1]
        via FE80::2, GigabitEthernet0/2
    O  2001:DB8::3/128 [110/2]
        via FE80::2, GigabitEthernet0/2
    OI 2001:DB8::4/128 [110/3]
        via FE80::2, GigabitEthernet0/2
    OI 2001:DB8:0:4::/64 [110/4]
        via FE80::2, GigabitEthernet0/2
    O  2001:DB8:0:23::/64 [110/2]
        via FE80::2, GigabitEthernet0/2
    OI 2001:DB8:0:34::/64 [110/3]
        via FE80::2, GigabitEthernet0/2
```

**Passive Interface**

OSPFv3 supports the ability to mark an interface as passive. The command is placed under the OSPFv3 process or under the specific address family. Placing the command under the global process cascades the setting to both address families. An interface is marked as being passive with the command `passive-interface interface-id` or globally with `passive-interface default`, and then the interface is marked as active with the command `no passive-interface interface-id`.

Example 10-6 shows how to make the LAN interface on R1 explicitly passive and how to make all interfaces passive on R4 while marking the Gi0/3 interface as active.

**Example 10-6  Configuring OSPFv3 Passive Interfaces**

```
R1(config)# router ospfv3 1
R1(config-router)# passive-interface GigabitEthernet0/1

R4(config)# router ospfv3 1
R4(config-router)# passive-interface default

22:10:46.838: %OSPFv3-5-ADJCHG: Process 1, IPv6, Nbr 192.168.3.3 on
GigabitEthernet0/3 from FULL to DOWN, Neighbor Down: Interface down or detached
R4(config-router)# no passive-interface GigabitEthernet 0/3
```

The active/passive state of an interface is verified by examining the OSPFv3 interface status using the command `show ospfv3 interface [interface-id]` and searching for the *Passive* keyword. In Example 10-7, R1 confirms that the Gi0/3 interface is passive.
Example 10-7  Viewing an OSPFv3 Interface State

R1# show ospfv3 interface GigabitEthernet 0/1 | include Passive
   No Hellos (Passive interface)

Summarization

The ability to summarize IPv6 networks is as important as summarizing routes in IPv4 (and it may even be more important, due to hardware scale limitations). Example 10-8 shows the IPv6 routing table on R4 before summarization is applied on R3.

Example 10-8  R4’s IPv6 Routing Table Before Summarization

R4# show ipv6 route ospf | begin Application
  1A - LISP away, a - Application
  OI  2001:DB8::1/128 [110/3]
      via FE80::3, GigabitEthernet0/3
  OI  2001:DB8::2/128 [110/2]
      via FE80::3, GigabitEthernet0/3
  OI  2001:DB8::3/128 [110/1]
      via FE80::3, GigabitEthernet0/3
  OI  2001:DB8:0:1::/64 [110/4]
      via FE80::3, GigabitEthernet0/3
  OI  2001:DB8:0:12::/64 [110/3]
      via FE80::3, GigabitEthernet0/3
  OI  2001:DB8:0:23::/64 [110/2]
      via FE80::3, GigabitEthernet0/3


NOTE  A common mistake with summarization of IPv6 addresses is to confuse hex with decimal. We typically perform summarization logic in decimal, and the first and third digits in a hextet should not be confused as decimal values. For example, the first hextet of the IPv6 address 2001::1/128 is 2001. When we separate those values further, it is not 20 and 1 in decimal format. The decimal values in that hextet are 32 (20 in hex) and 1 (1 in hex).

Summarization of internal OSPFv3 routes follows the same rules as in OSPFv2 and must occur on ABRs. In our topology, R3 summarizes the three loopback addresses into the 2001:db8:0:0::/65 network. Summarization involves the command area area-id range prefix/ prefix-length, which resides under the address family in the OSPFv3 process.

Example 10-9 shows R3’s configuration for summarizing these prefixes.

Example 10-9  IPv6 Summarization

R3# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)# router ospfv3 1
R3(config-router)# address-family ipv6 unicast
R3(config-router-af)# area 0 range 2001:db8:0:0::/65
Example 10-10 shows R4’s IPv6 routing table after configuring R3 to summarize the Area 0 loopback interfaces. The summary route is highlighted in this example.

**Example 10-10  R4’s IPv6 Routing Table After Summarization**

```plaintext
R4# show ipv6 route ospf | begin Application
   IA - LISP away, a - Application
OI  2001:DB8::/65 [110/4]  
   via FE80::3, GigabitEthernet0/3
OI  2001:DB8::1::/64 [110/4]  
   via FE80::3, GigabitEthernet0/3
OI  2001:DB8::12::/64 [110/3]  
   via FE80::3, GigabitEthernet0/3
OI  2001:DB8::23::/64 [110/2]  
   via FE80::3, GigabitEthernet0/3
```

**Network Type**

OSPFv3 supports the same OSPF network types as OSPFv2. Example 10-11 shows that R2’s Gi0/3 interface is set as a broadcast OSPF network type and is confirmed as being in a DR state.

**Example 10-11  Viewing the Dynamic Configured OSPFv3 Network Type**

```plaintext
R2# show ospfv3 interface GigabitEthernet 0/3 | include Network
   Network Type BROADCAST, Cost: 1
R2# show ospfv3 interface brief
   Interface    PID   Area         AF     Cost  State Nbrs F/C
   Lo0           1     0              ipv6   1      LOOP  0/0
   Gi0/3         1     0              ipv6   1      DR    1/1
   Gi0/1         1     0              ipv6   1      BDR   1/1
```

The OSPFv3 network type is changed with the interface parameter command `ospfv3 network` [point-to-point | broadcast]. Example 10-12 shows the interfaces associated with the 2001:DB8:0:23::/64 network being changed to point-to-point.

**Example 10-12  Changing the OSPFv3 Network Type**

```plaintext
R2# configure terminal
   Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# interface GigabitEthernet 0/3
R2(config-if)# ospfv3 network point-to-point
R3(config)# interface GigabitEthernet 0/2
R3(config-if)# ospfv3 network point-to-point
```

After the changes are typed in, the new settings are verified in Example 10-13. The network is now a point-to-point link, and the interface state shows as P2P for confirmation.
Example 10-13  Viewing the Statically Configured OSPFv3 Network Type

| R2# show ospfv3 interface GigabitEthernet 0/3 | include Network |
|------------------------------------------------|
| Network Type POINT_TO_POINT, Cost: 1 |

<table>
<thead>
<tr>
<th>R2# show ospfv3 interface brief</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
</tr>
<tr>
<td>Lo0</td>
</tr>
<tr>
<td>Gi0/3</td>
</tr>
<tr>
<td>Gi0/1</td>
</tr>
</tbody>
</table>

IPv4 Support in OSPFv3

RFC 5838 specifies that OSPFv3 should support multiple address families by setting the instance ID value from the IPv6 reserved range to the IPv4 reserved range (64 to 95) in the link LSAs.

Enabling IPv4 support for OSPFv3 is straightforward:

**Step 1.** Ensure that the IPv4 interface has an IPv6 address (global or link local) configured. Remember that configuring a global address also places a link-local address; alternatively, a link-local address can statically be configured.

**Step 2.** Enable the OSPFv3 process for IPv4 on the interface with the command `ospfv3 process-id ipv4 area area-id`.

Using the topology shown in Figure 10-1, IPv4 addressing has been placed onto R1, R2, R3, and R4 using the conventions outlined earlier. Example 10-14 demonstrates the deployment of IPv4 using the existing OSPFv3 deployment.

Example 10-14  Configuration Changes for IPv4 Support

<table>
<thead>
<tr>
<th>R1(config)# interface Loopback 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1(config-if)# ospfv3 1 ipv4 area 0</td>
</tr>
<tr>
<td>R1(config-if)# interface GigabitEthernet0/1</td>
</tr>
<tr>
<td>R1(config-if)# ospfv3 1 ipv4 area 0</td>
</tr>
<tr>
<td>R1(config-if)# interface GigabitEthernet0/2</td>
</tr>
<tr>
<td>R1(config-if)# ospfv3 1 ipv4 area 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>R2(config)# interface Loopback 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>R2(config-if)# ospfv3 1 ipv4 area 0</td>
</tr>
<tr>
<td>R2(config-if)# interface GigabitEthernet0/1</td>
</tr>
<tr>
<td>R2(config-if)# ospfv3 1 ipv4 area 0</td>
</tr>
<tr>
<td>R2(config-if)# interface GigabitEthernet0/3</td>
</tr>
<tr>
<td>R2(config-if)# ospfv3 1 ipv4 area 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>R3(config)# interface Loopback 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>R3(config-if)# ospfv3 1 ipv4 area 0</td>
</tr>
<tr>
<td>R3(config-if)# interface GigabitEthernet0/2</td>
</tr>
<tr>
<td>R3(config-if)# ospfv3 1 ipv4 area 0</td>
</tr>
</tbody>
</table>
Example 10-15 verifies that the routes were exchanged and installed into the IPv4 RIB.

**Example 10-15**  Verifying IPv4 Route Exchange with OSPFv3

```
R4# show ip route ospfv3 | begin Gateway
Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O IA  10.1.1.24 [110/4] via 10.34.1.3, 00:00:39, GigabitEthernet0/3
O IA  10.12.0/24 [110/3] via 10.34.1.3, 00:00:39, GigabitEthernet0/3
O IA  10.23.1.0/24 [110/2] via 10.34.1.3, 00:00:39, GigabitEthernet0/3
192.168.1.0/32 is subnetted, 1 subnets
O IA  192.168.1.1 [110/3] via 10.34.1.3, 00:00:39, GigabitEthernet0/3
192.168.2.0/32 is subnetted, 1 subnets
O IA  192.168.2.2 [110/2] via 10.34.1.3, 00:00:39, GigabitEthernet0/3
192.168.3.0/32 is subnetted, 1 subnets
O IA  192.168.3.3 [110/1] via 10.34.1.3, 00:00:39, GigabitEthernet0/3
```

The command `show ospfv3 interface [brief]` displays the address families enabled on an interface. When IPv4 and IPv6 are both configured on an interface, an entry appears for each address family. Example 10-16 lists the interfaces and associated address families.

**Example 10-16**  Listing of OSPFv3 Interfaces and Their Address Families

```
R4# show ospfv3 interface brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>PID</th>
<th>Area</th>
<th>AF</th>
<th>Cost</th>
<th>State</th>
<th>Nbrs</th>
<th>F/C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lo0</td>
<td>1</td>
<td>34</td>
<td>ipv4</td>
<td>1</td>
<td>LOOP</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>G10/1</td>
<td>1</td>
<td>34</td>
<td>ipv4</td>
<td>1</td>
<td>DR</td>
<td>1/1</td>
<td></td>
</tr>
<tr>
<td>G10/3</td>
<td>1</td>
<td>34</td>
<td>ipv4</td>
<td>1</td>
<td>DR</td>
<td>1/1</td>
<td></td>
</tr>
<tr>
<td>Lo0</td>
<td>1</td>
<td>34</td>
<td>ipv6</td>
<td>1</td>
<td>LOOP</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>G10/1</td>
<td>1</td>
<td>34</td>
<td>ipv6</td>
<td>1</td>
<td>DR</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>G10/3</td>
<td>1</td>
<td>34</td>
<td>ipv6</td>
<td>1</td>
<td>BDR</td>
<td>1/1</td>
<td></td>
</tr>
</tbody>
</table>
```

Example 10-17 shows how to view the OSPFv3 neighbors to display the neighbors enabled for IPv4 and IPv6 as separate entities.
Example 10-17  Verifying OSPFv3 IPv4 Neighbors

R4# show ospfv3 neighbor

OSPFv3 1 address-family ipv4 (router-id 192.168.4.4)
Neighbor ID   Pri   State           Dead Time   Interface ID    Interface
192.168.3.3   1   FULL/BDR        00:00:30    6               GigabitEthernet0/3

OSPFv3 1 address-family ipv6 (router-id 192.168.4.4)
Neighbor ID   Pri   State           Dead Time   Interface ID    Interface
192.168.3.3   1   FULL/DR         00:00:31    6               GigabitEthernet0/3
192.168.3.3  1 FULL/DR 00:00:31 6 GigabitEthernet0/3

Exam Preparation Tasks

You have a couple of choices for exam preparation: the exercises here, Chapter 30, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. Table 10-2 lists these key topics and the page number on which each is found.

<table>
<thead>
<tr>
<th>Key Topic Element</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section</td>
<td>OSPFv3 Fundamentals</td>
<td>231</td>
</tr>
<tr>
<td>Section</td>
<td>OSPFv3 Verification</td>
<td>235</td>
</tr>
<tr>
<td>Paragraph</td>
<td>OSPFv3 summarization</td>
<td>238</td>
</tr>
<tr>
<td>List</td>
<td>IPv4 support on OSPFv3</td>
<td>240</td>
</tr>
</tbody>
</table>

Complete Tables and Lists from Memory

There are no memory tables in this chapter.

Define Key Terms

There are no key terms in this chapter.

Use the Command Reference to Check Your Memory

Table 10-3 lists the important commands from this chapter. To test your memory, cover the right side of the table with a piece of paper, read the description on the left side, and see how much of the command you can remember.
Table 10-3  Command Reference

<table>
<thead>
<tr>
<th>Task</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure OSPFv3 on a router and enable it on an interface</td>
<td>router ospfv3 [process-id] interface interface-id ospfv3 process-id [ipv4</td>
</tr>
<tr>
<td>Configure a specific OSPFv3 interface as passive</td>
<td>passive-interface interface-id</td>
</tr>
<tr>
<td>Configure all OSPFv3 interfaces as passive</td>
<td>passive-interface default</td>
</tr>
<tr>
<td>Summarize an IPv6 network range on an ABR</td>
<td>area area-id range prefix/prefix-length</td>
</tr>
<tr>
<td>Configure an OSPFv3 interface as a point-to-point or broadcast network type</td>
<td>ospfv3 network [point-to-point</td>
</tr>
<tr>
<td>Display OSPFv3 interface settings</td>
<td>show ospfv3 interface [interface-id]</td>
</tr>
<tr>
<td>Display OSPFv3 IPv6 neighbors</td>
<td>show ospfv3 ipv6 neighbor</td>
</tr>
</tbody>
</table>

References in This Chapter


Index

Numbers

0MQ, 909
2.4 GHz band, 516
5 GHz band, 516
6 GHz band, 516
802.1p, 957
802.1q, 957
802.1x, 595, 758, 957
  authentication process flow, 759–760
  components, 758
  EAP methods, 760–762
  roles, 758–760
802.11, 533–535. See also wireless networks and theory

A

AAA (authentication, authorization, and accounting), 796, 803, 958
configuring for network device access control, 805–809
RADIUS, 804–805
TACACS+, 803–804
use cases, 803
verification, 809
AAR (Application-Aware Routing), 665–666
ABR (area border router), 205–206, 957
absolute timeout command, 802–803
access layer, 625–627, 957
access ports, 11–12, 957
access-list command, 782–784
ACL (access control list), 295, 781–782, 957
AS_Path filtering, 309–311
conditional debugging, 692–693
configuring for CoPP, 817–818
controlling access to vty line, 796–797
downloadable, 788
extended, 296
named, 784–785
numbered, 782–783
numbered extended, 783–784
port, 785–786
standard, 295–296
VLAN, 786–788
wildcard mask, 782
Active state, BGP, 254
AD (administrative distance), 132, 133–135, 957
address family, 248, 957
adjacency table, 29
advertisements
  BGP, 260–261
  OSPF, default route, 187–188
  VTP (VLAN Trunking Protocol), 97
AF (Assured Forwarding) PHB, 388–390
agent-based automation tools. See automation tools
agentless automation tools. See
automation tools
aggregate-address command, 267–274
as _set keyword, 276–277
summary-only keyword, 272
AIGP (Accumulated Interior Gateway
Protocol), 323–324
algorithm
distance vector, 128–129
enhanced distance vector, 129–130
link-state, 130–131
path vector, 131–132
queuing, 406–408
transform sets, 478–480
allowed VLAN, 14–15
AMP (Advanced Malware Protection),
742–744, 957, 959
amplitude, 520, 957
anchor controller, 957
Ansible, 912–913
CLI commands, 916
inventory file, 917
playbooks, 913–914, 917–930
workflow, 913
YAML files, 915–916
antenna/s, 309–311
beamwidth, 563
directional, 567–570
EIRP (effective isotropic radiated
power), 526, 538
free space path loss, 527–529
gain, 525–526, 562
isotropic, 526
link budget, 526–527
omnidirectional, 564–566
parabolic dish, 569–570
patch, 567–568
polarization, 563–564
radiation pattern, 560–562
RSSI (received signal strength indicator),
530–531
spatial multiplexing, 535–536
wave propagation, 513–514
Yagi, 565–569
anycast gateway, 656
API (application programming
interface), 850–855, 857, 957. See
also Postman
Cisco DNA Center
  Network Device, 864–867
  Token, 862–864
Cisco vManage, 867–868
  Authentication, 868
  Fabric Device, 869–870
HTTP status codes, 862
JSON (JavaScript Object Notation),
861–862
northbound, 855–856
REST (Representational State Transfer),
856
southbound, 856
XML (Extensible Markup Language),
860–861
applets, EEM, 895
debugging, 896–898
manually executing, 899–901
syslog, 896
WR MEM, 898
AP (access point). See also antenna/s;
Cisco lightweight APs; roaming
autonomous, 545–546
Cisco lightweight, 547
customization, 558–559
discovering a WLC, 554–555
integrated antennas, 565–566
maintaining WLC availability,
556–557
pairing with a WLC, 552
policy tag, 558
RF tag, 558
segmenting wireless configurations, 557–559
selecting a WLC, 555–556
site tag, 558
special-purpose modes, 547–548
split-MAC architecture, 547
state machine, 552–554
client density, 559–560
Probe Requests, 587
troubleshooting connectivity issues, 617–620
architecture. See also hierarchical LAN design
AMP (Advanced Malware Protection), 743–744
Chef, 905
Cisco ENFV (Enterprise Network Functions Virtualization), 843
Cisco SD-WAN, 661–662
LISP (Cisco Locator/ID Separation Protocol), 497
central plane, 497–498
data plane, 498–499
SD-Access, 646–647
network layer, 647–648
physical layer, 647
underlay network, 648–649
area range command, 223
area/s, 173–174, 204–207, 217
filtering, 225–227
ID, 207
ARP (Address Resolution Protocol), 19–20, 957
AS (autonomous systems), 127, 157, 958
ASICs (application-specific integrated circuits), 4, 30
ASNs (autonomous system numbers), 246
AS_Path, 957
as_set keyword. See also keywords
atomic aggregate attribute, 274–276, 958
authentication, 603
Enhanced FlexAuth, 766
password, 790–793
WebAuth, 764
Central, 765
Local, 764–765
wireless, 593
EAP, 597–602
Open Authentication, 593–594
pre-shared key, 595–597
WebAuth, 603–606
Authentication API, 868
auto-cost reference bandwidth command, 189
automation tools
Ansible, 912–913
CLI commands, 916
inventory file, 917
playbooks, 913–914, 917–930
workflow, 913
YAML files, 915–916
Chef, 904
architecture, 905
comparison with Puppet, 906
cookbooks, 906
demo_install.rb, 906–908
kitchen, 906
recipe, 906
server, 906
server deployments, 906
comparing, 924–925
Puppet, 902
   agent/server communication, 902
   components, 902
   installation modes, 903
   manifests, 903–904
   modules, 903
Puppet Bolt, 922
   command line, 922–923
   tasks, 922, 923
Salt SSH, 923–924
autonomous APs, 545–546, 574–576, 958
Auto-RP, 364
auxiliary port, 802
AVG (active virtual gateway), 441

B

backbone area, 958
bare-metal server, 828
Bc (committed burst size), 395
BDR (backup designated router), 177–178, 958
   election, 190–192
   placement, 192–194
beacon, 909
beamwidth, 563, 958
BGP (Border Gateway Protocol), 244, 290–291
   address family, 248
   Adj-RIB-In table, 262
   Adj-RIB-Out table, 262, 265
   ASNs (autonomous system numbers), 246
   best path selection, 318–319
Accumulated Interior Gateway Protocol metric, 323–324
eBGP over iBGP, 327
local preference attribute, 322–323
locally originated via network or aggregate advertisement, 323
lowest IGP metric, 327–328
lowest neighbor address, 329
minimum cluster list length, 329
multi-exit discriminator, 326–327
origin type, 325–326
overview, 320–321
prefer path from the oldest eBGP session, 328
router ID, 328–329
shortest AS path, 324–325
using longest match, 319–320
weight attribute, 321–322
community, 313, 958
   conditionally matching, 315–317
   enabling support, 314–315
   extended, 314
   private, 314, 317–318
   well-known, 314
conditional matching, 295
   ACL, 295–296
   IPv6 prefix list, 299–300
   prefix list, 299
   prefix matching, 297–299
   regex, 300–301
configuration, 256–257
   network advertisement, 261
   requirements, 255
deterministic routing, 293–294
inter-router communication, 248–249
IPv6
configuring, 277–282
route summarization, 282–285
Loc-RIB table, 262, 263–264
loop prevention, 247–248
messages, 252
multihoming, 291, 958
branch transit routing, 293–295
Internet transit routing, 292–293
resiliency in service providers, 291–292
multiprotocol, 277
neighbor state, 253
Active, 254
Connect, 254
Established, 255
Idle, 254
OpenConfirm, 255
OpenSent, 254–255
neighbors, 249
network statements, 260–261
NLRI (Network Layer Reachability Information), 248
PA (path attribute), 247
packets, 252
peering, 279
receiving and viewing routes, 262–265
redistributing routes into an IGP, 267
route advertisement/s, 260–261
from indirect sources, 265–268
route aggregation, 267–268
with AS_SET, 276–277
aggregate-address command, 267–274
atomic aggregate attribute, 274–276
route filtering, 306–307
AS_Path ACL filtering, 309–311
distribute lists, 307
prefix lists, 308
route maps, 311–313
route maps, 301–302
command syntax, 301
complex matching, 304
components, 301
conditional match options, 302–303
continue keyword, 305–306
multiple conditional match conditions, 303–304
optional actions, 304–305
sessions, 249–250
clearing, 313
eBGP, 251
iBGP, 250–251
verification, 257–260
bootstrap router, 366–367
border nodes, SD-Access, 654
BPDU (bridge protocol data unit), 40, 958
BPDU filter, 72–73, 958
BPDU guard, 70–72, 958
broadcast domain, 6, 959
broadcast networks, OSPF, 194–195
broadcast traffic, 339
BSS (basic service set), 592
BSS (business support system), 836

C

CAM (content addressable memory), 17, 960
campus network
Layer 2 access layer, 634–636
Layer 3 access layer, 636–637
SD-Access design, 640
simplified campus design, 637–639
three-tier design, 634
two-tier design, 632
candidate RP (rendezvous point), 364–365, 366–367
capabilities, NETCONF, 874
CAPWAP (Control and Provisioning of Wireless Access Points), 552, 959
carrier signal, 531, 959
CBWFQ (class-based weighted fair queuing), 407–408
commands, 410–411
configuring, 410–414
CEF (Cisco Express Forwarding), 27, 959
    hardware, 30
    software, 29–30
Central Web Authentication, 765
centralized forwarding, 28
centralized wireless deployment, 548–550
channel, 517, 959
Chef, 904
    architecture, 905
    comparison with Puppet, 906
    cookbooks, 906
demo_install.rb, 906–908
    kitchen, 906
    recipe, 906
    server, 906
    server deployments, 906
CIR (committed information rate), 395
Cisco Advanced Malware Protection, 742–744
Cisco DevNet. See DevNet
Cisco DNA Center, 642
    assurance, 728, 733–734
        Assurance tab, 729
        main page, 728–729
management, 657
    Network Time Travel, 728–729
Path Trace, 731
    search capabilities, 730–731
Token API, 862–864
    workflow, 660
design workflow, 658
management layer, 657
policy workflow, 658–659
provision workflow, 659–660
Cisco ENFV (Enterprise Network Functions Virtualization), 842–843
    architecture, 843
    management and orchestration, 843–844
    NFVIS (network function virtualization infrastructure software), 846–847
    virtual network functions and applications, 845
Cisco FlexVPN, 486
Cisco FMC (Firewall Management Center), 753
Cisco IBNS (Identity-Based Networking Services) 2.0, 766
Cisco ISE (Identity Services Engine), 657, 756–758, 959
Cisco lightweight AP, 547, 966. See also antenna/s; roaming
customization, 558–559
discovering a WLC, 554–555
integrated antennas, 565–566
intercontroller roaming, 579
intracontroller roaming, 577–579
maintaining WLC availability, 556–557
Network Device API, 864–867
pairing with a WLC, 552
policy tag, 558
RF tag, 558
segmenting wireless configurations, 557–559
selecting a WLC, 555–556
site tag, 558
special-purpose modes, 547–548
split-MAC architecture, 547
state machine, 552–554
Cisco NCP (Network Control Platform), 656
Cisco SAFE (Secure Architectural Framework), 959
advanced threat defense protection, 740–741
AMP (Advanced Malware Protection), 742–744
Cisco FMC (Firewall Management Center), 753
Cisco ISE (Identity Services Engine), 756–758
Cisco Secure Client, 744
Cisco Secure Cloud Analytics, 755–756
Cisco Secure Email, 748–749
Cisco Secure Firewall, 751–752
Cisco Secure IPS, 749–751
Cisco Secure Network Analytics, 753–755
Cisco Secure Web Appliance, 746–748
key, 740
Malware Analytics, 742
next-generation endpoint security, 737–741
PINs (places in the network), 738–739
security concepts, 739–740
Talos, 741–742
Umbrella, 744–745
Cisco SD-WAN
AAR (Application-Aware Routing), 665–666
architecture, 661–662
Cloud OnRamp, 664–665
for IaaS, 668–669
for SaaS, 666–668
edge devices, 663–664
SD-WAN policy, 665
vAnalytics, 664
vBond orchestrator, 662–663
vManage NMS, 663
vSmart controllers, 663
Cisco Secure Client, 744
Cisco Secure Cloud Analytics, 755
Network Analytics SaaS, 755–756
Public Cloud Monitoring, 755
Cisco Secure Email, 748–749
Cisco Secure Firewall, 751–752, 959
Cisco Secure Malware Analytics, 742, 959
Cisco Secure Network Analytics, 753–755
Cisco Secure Web Appliance, 746–748
Cisco Talos, 741–742, 960
Cisco TrustSec, 766–767, 960
egress enforcement, 770–771
ingress classification, 767–768
propagation, 768–770
Cisco Umbrella, 744–745, 960
Cisco vManage APIs, 867–868
Authentication, 868
Fabric Device, 869–870
Cisco wireless deployments, 548
centralized, 548–550
cloud-based, 550
controller-less, 551
distributed, 551
class-based policing, 398
classification, 381–382
ingress, 767–768
Layer 7, 382
clear ip bgp command, 313
clear ip ospf process command, 193–194
clear mac address-table dynamic command, 17
clear ospf process command, 181
clearing BGP sessions, 313
CLI (command-line interface), 960. See also IOS XE
pros and cons, 854–855
terminal lines, 788–789
client density, 559–560
Cloud OnRamp, 664–665
for IaaS, 668–669
for SaaS, 666–668
cloud-based wireless deployment, 550
code. See also Python
editing, 881–882
functions, 888
manifest, 903–904
recipe, 906
collections, Postman, 858–859
collision domains, 5–6, 960
command/s. See also keywords
absolute timeout, 802–803
access-list, 782–784
aggregate-address, 267–274
Ansible, 916
area range, 223
auto-cost reference bandwidth, 189
CBWFQ, 410–411
clear ip bgp, 313
clear ip ospf process, 193–194
clear mac address-table dynamic, 17
clear ospf process, 181
default-information originate, 187
device hardening, 822–823
do show ip ospf neighbor, 691–692
do show logging, 702–703
clearing BGP sessions, 313
CLI (command-line interface), 960. See also IOS XE
pros and cons, 854–855
terminal lines, 788–789
client density, 559–560
Cloud OnRamp, 664–665
for IaaS, 668–669
for SaaS, 666–668
cloud-based wireless deployment, 550
code. See also Python
editing, 881–882
functions, 888
manifest, 903–904
recipe, 906
collections, Postman, 858–859
collision domains, 5–6, 960
command/s. See also keywords
absolute timeout, 802–803
access-list, 782–784
aggregate-address, 267–274
Ansible, 916
area range, 223
auto-cost reference bandwidth, 189
CBWFQ, 410–411
clear ip bgp, 313
clear ip ospf process, 193–194
clear mac address-table dynamic, 17
clear ospf process, 181
default-information originate, 187
device hardening, 822–823
do show ip ospf neighbor, 691–692
do show logging, 702–703
clearing BGP sessions, 313
CLI (command-line interface), 960. See also IOS XE
pros and cons, 854–855
terminal lines, 788–789
client density, 559–560
Cloud OnRamp, 664–665
for IaaS, 668–669
for SaaS, 666–668
cloud-based wireless deployment, 550
code. See also Python
editing, 881–882
functions, 888
manifest, 903–904
recipe, 906
collections, Postman, 858–859
collision domains, 5–6, 960
command/s. See also keywords
absolute timeout, 802–803
access-list, 782–784
aggregate-address, 267–274
Ansible, 916
area range, 223
auto-cost reference bandwidth, 189
CBWFQ, 410–411
clear ip bgp, 313
clear ip ospf process, 193–194
clear mac address-table dynamic, 17
clear ospf process, 181
default-information originate, 187
device hardening, 822–823
do show ip ospf neighbor, 691–692
do show logging, 702–703
encapsulation dot1q, 22
erreable recovery cause bpduguard, 71–72
event manager run, 899
fhrp version vrrp v3, 440–441=file prompt quiet, 899
interface vlan, 23
ip access-list, 784–785
ip address, 21
ip address secondary, 21
ip flow monitor, 715
ip ospf area, 180
ip ospf network broadcast, 689–690
ip route, 138
ip sla, 725–727
ipv6 address, 21
lacp max-bundle, 116–117
lacp rate fast, 115
logging buffered ?, 702
logout-warning, 802–803
mac address-table static vlan, 16
match, 382–384
monitor session destination interface, 718
name, 8
neighbor distribute-list, 307
network area, 178
no switchport, 23
passive-interface, 237–238
ping, 675–676
  extended, 677–680
  repeat option, 676–677
port-channel min-links, 115
privilege levels, 793–796
Puppet Bolt, 922–923
remote-span, 721
route-map, 301
router ospf, 178
SaltStack, 910–911
sdm prefer, 30
service-policy, 380
show bgp ipv4 unicast, 263–265, 267–268
show bgp ipv4 unicast neighbors, 258–260
show bgp ipv4 unicast summary, 257
show bgp ipv6 unicast neighbors, 281
show bgp ipv6 unicast summary, 281–282
show bgp summary, 257
show etherchannel load-balance, 120
show etherchannel port, 110–112
show etherchannel summary, 108–109
show flow record, 710–711
show glbp, 443–444
show interface port-channel, 110
show interfaces status, 18–19, 71
show interfaces switchport, 17–18
show interfaces trunk, 13–14, 103
show ip arp, 20
show ip flow export, 707–708
show ip interface brief, 23–24
show ip nat translations, 450–452
show ip ospf database summary, 215
show ip ospf interface, 184–185, 689
show ip ospf neighbor, 186, 686
show ip route, 137, 139, 266–267
show ip route bgp, 265
show ip route ospf, 187
show ipv6 interface brief, 24–25
show ipv6 route, 146
show ipv6 route ospf, 237, 238, 239
show lacp counters, 113–114
show lacp neighbor, 112–113
show lacp sys-id, 117–118
show logging, 703–704
show mac address-table dynamic, 15–16
show monitor session erspan-source session, 723–724
show ntp associations, 423–424
show ntp status, 422–423
show ospfv3 interface, 236, 240
show ospfv3 ipv6 neighbor, 236
show pagp counters, 114
show pagp neighbor, 113
show running-config, 270–271
show sdm prefer, 31–32
show spanning-tree, 85–86
show spanning-tree inconsistentports, 74
show spanning-tree interface, 48–49, 70–71, 73
show spanning-tree mst, 86–87, 88
show spanning-tree mst configuration, 84–85
show spanning-tree mst interface, 87
show spanning-tree root, 42–45
show spanning-tree vlan, 45–47, 61–62, 64–66
show spanning-tree vlan detail, 49–50
show standby, 435–438
show track, 431–432
show udld neighbors, 75–76
show vlan, 9–10
show vrrp, 439
show vrrp brief, 441
show vtp status, 99–101
spanning-tree bpdufilter enable, 72
spanning-tree guard root, 68
spanning-tree mode mst, 84
spanning-tree pathcost method long, 41
spanning-tree portfast, 68–70
spanning-tree portfast bpduguard default, 70
spanning-tree vlan forward-time, 40
spanning-tree vlan hello-time, 40
spanning-tree vlan max-age, 40
spanning-tree vlan priority, 60
spanning-tree vlan root, 60
switchport access vlan, 12
switchport mode access, 12
switchport mode trunk, 12
switchport trunk allowed vlan, 14–15
switchport trunk native vlan, 14
traceroute, 448, 680–683
  extended, 684–685
  options, 683
transport input, 797–800
tunnel mode ipsec, 493
udld enable, 75
undebug interface loopback0, 695
vlan, 8
vtp domain, 98–99
vtp mode, 98–99
vtp password, 98–99
vtp version, 98–99
communication, OSPFv3, 232–233
community, BGP, 313
  conditionally matching, 315–317
  enabling support, 314–315
  extended, 314
  private, 314, 317–318
  well-known, 314
Community page, DevNet, 879
conditional debugging
  on a specific interface, 693–695
  using ACLs, 692–693
conditional matching, 295. See also route maps
ACL, 295
  extended, 296
  standard, 295–296
BGP communities, 315–317
prefix matching, 297–299
  IPv6 prefix lists, 299–300
  prefix lists, 299
regex, 300–301
configuration
BGP (Border Gateway Protocol), 255–257, 261
DTP (Dynamic Trunking Protocol), 102
EtherChannel, 107–108
HSRP (Hot Standby Router Protocol), 434–435
MQC classification, 382–385
MST (Multiple Spanning Tree Protocol), 84
NTP (Network Time Protocol), 421–422
OSPF (Open Shortest Path First), 181–183
  for all interfaces, 178–180
  with explicit IP addresses, 179
  with explicit subnet, 179
  interface-specific, 180–181
  network statement, 178
OSPFv3, 233–235
PTP (Precision Time Protocol), 427–429
QoS (Quality of Service)
  CBWFQ, 410–414
  class-based policing, 398
SNMP (Simple Network Management Protocol), 699–700
trunk port, 13
VRRP (Virtual Router Redundancy Protocol), 438–441
VTP (VLAN Trunking Protocol), 98–99
ZBFW (Zone-Based Firewall), 811–815
configuration BPDU, 40
congestion avoidance, 408–410
congestion management, 406–408
Connect state, BGP, 254
containers, 830–831, 960
control plane
  LISP (Cisco Locator/ID Separation Protocol), 497–498
  nodes, SD-Access, 653–654
  SD-Access, 649–650
  VXLAN (Virtual eXtensible Local Area Network), 506
controller layer, SD-Access, 656–657
controller-less wireless deployment, 551
convergence
  EIGRP (Enhanced Interior Gateway Routing Protocol), 164–166
  RSTP (Rapid Spanning Tree Protocol), 55
  STP (Spanning Tree Protocol)
    with direct link failures, 50–52
    with indirect failures, 52–53
cookbook, 906
CoPP (Control Plane Policing), 817, 960
ACL configuration, 817–818
  applying the policy map, 819–820
  class map configuration, 818
  policy map configuration, 819
  verification, 820–822
core layer, 628–629, 960
CQ (custom queuing), 407
creating
  username, 790
  VLANs, 8
  VRF instance, 150
CRUD functions, 856
CS (Class Selector) PHB, 388
CSMA/CD (Carrier Sense Multiple Access/Collision Detect), 5
CST (Common Spanning Tree), 81–82, 960

D

dACL (downloadable ACL), 788
data link layer, 4
data model, YANG, 870–872
data plane
  LISP (Cisco Locator/ID Separation Protocol), 498–499
  SD-Access, 650–651
datastore, NETCONF, 875
dB (decibel), 522, 523–524, 961
  Law of 3s, 522–523
  Law of 10s, 523
  Law of Zero, 522
dBm (dB-milliwatt), 525, 961
dead interval timer, 961
  OSPF, 190
  OSPF (Open Shortest Path First), 689
debug event manager action cli command, 898
debug ip ospf adj command, 687, 690–691
debug ip ospf hello command, 687–689, 690–691
debugging, 685–686. See also diagnostic tools; troubleshooting conditional
  on a specific interface, 693–695
  using ACLs, 692–693
EEM actions, 896–898
OSPF (Open Shortest Path First)
  debug ip ospf adj command, 687, 690–691
  debug ip ospf hello command, 687–689, 690–691
  ip ospf network broadcast command, 689–690
  show ip ospf interface command, 689
  show ip ospf neighbor command, 686
default-information originate command, 187
delay variation, 376
demodulation, 961
deterministic routing, 293–294
device driver, 837
device hardening, 822–823
DevNet, 877–878, 961
  Community page, 879
  Documentation page, 878
  Events page, 879
  Learn page, 878
  Technologies page, 878
DF (Default Forwarding) PHB, 388
diagnostic tools. See also Cisco DNA Center Assurance
  IP SLA, 724
    HTTP GET operation, 726–728
    ICMP echo operation, 724–726
  ping command, 675–676
    extended, 677–680
    repeat option, 676–677
  traceroute command, 680–683
    extended, 684–685
    options, 683
dictionary
  Python, 885
  YAML, 915–916
DiffServ, 379, 961
dipole antenna, 564–565, 961
directional antenna, 567–570, 961
directly attached static routes, 138–139, 961
discontiguous networks, OSPF, 217–218
displaying, trunk port information, 13
distance vector algorithms, 128–129, 962
distribute lists, 307, 962
distributed forwarding, 28
distributed wireless deployment, 551
distribution layer, 627–628, 962
distribution tree, 349
  shared tree, 350–352
  source tree, 349–350
DMA (direct memory access), 837
DMVPN (Cisco Dynamic Multipoint VPN), 486
do show ip ospf neighbor command, 691–692
do show logging command, 702–703
Docker, 831, 832–833
Documentation page, DevNet, 878
donlink MACsec, 774
downstream interface, 962
DP (designated port), 961
DR (designated router), 176–178, 961
election, 190–192
placement, 192–194
drop precedence, 390
DRS (dynamic rate shifting), 538–540, 962
DSCP per-hop behaviors. See PHB
(per-hop behavior), 387
DSSS (direct sequence spread spectrum), 533, 961
DTLS (Datagram Transport Layer Security), 961
DTP (Dynamic Trunking Protocol), 101, 962
configuring, 102
disabling trunk port negotiation, 103
matrix for establishing a dynamic trunk link, 102
modes, 102
DUAL (diffusing update algorithm), 129
dynamic routing protocol, 126–128

E
plane, 962
EAP (Extensible Authentication Protocol), 597–599, 760–762, 963
configuring with external RADIUS servers, 600–602
verification, 602
eBGP, 962
eBGP (external BGP) sessions, 251
edge node, SD-Access, 652–653
editing, code in GitHub, 881–882
EEM (Embedded Event Manager), 901, 962
applets, 895
debbuging, 896–898
syslog, 896
WR MEM, 898
email variables, 899
event detectors, 894–895
Tcl scripts, 899–901
EF (Expedited Forwarding) PHB, 390
EGP (Exterior Gateway Protocol), 127–128. See also BGP (Border Gateway Protocol)
EIGRP (Enhanced Interior Gateway Routing Protocol), 129–130
AS (autonomous system), 157
convergence, 164–166
failure detection and timers, 164
FD (feasible distance), 158
feasibility condition, 158
feasible successor, 158
k value, 160–161
load balancing, 163
metric backward compatibility, 163
neighbors, 160
packets, 160
path metric calculation, 160–162
RD (reported distance), 158
route summarization, 166–167
successor/successor route, 158
topology table, 159–160
variance value, 163
wide metric, 162
EIRP (effective isotropic radiated power), 526, 538, 962
email variables, EEM (Embedded Event Manager), 899
EMs (element managers), 835
encapsulation dot1q command, 22
ENCOR 350–401 exam
getting ready, 926–927
suggested plan for final review/study, 930
tools for final preparation, 927–930
updates, 932–934
encryption
MACsec, 772–773
downlink, 774
frame format, 773–774
uplink, 774
password, 789–790
endpoint, 962
enhanced distance vector algorithms, 129–130, 962. See also EIGRP (Enhanced Interior Gateway Routing Protocol)
Enhanced FlexAuth, 766
enterprise network architecture, 632
Layer 2 access layer, 634–636
Layer 3 access layer, 636–637
SD-Access design, 640
simplified campus design, 637–639
three-tier design, 634
two-tier design, 632
Env_Lab.py script, 882–885
equal-cost multipath, 135–136, 163, 220, 962
errdisable recovery cause bpdu guard command, 71–72
ERSPAN (Encapsulated Remote SPAN), 722, 963
specifying the destination port, 723–724
specifying the source port, 722–723
ESP (Encapsulating Security Payload), 477–478
Established state, BGP, 255
EtherChannel bundle, 104, 105, 963
components, 104–105
configuring, 107–108
link-state propagation and detection, 105–106
load balancing traffic, 119–120
logical interface status fields, 109
member interface status fields, 109
multiple links with STP, 104
troubleshooting, 118–119
verifying the status, 108–110
viewing show etherchannel port command output, 110–112
Ethernet, collision domains, 5–6
ETR (egress tunnel router), 962
event manager run command, 899
Events page, DevNet, 879
EXEC timeout, 802
extended ACLs, 296
extended communities, BGP, 314
extended ping command, 677–680
extended traceroute command, 684–685
fabric
SD-Access, 649
border nodes, 654
control plane, 649–650
control plane nodes, 653–654
data plane, 650–651
device roles, 652
edge nodes, 652–653
policy plane, 651–652
WLC (wireless LAN controller), 654
Fabric Device API, 869–870
fabric network, 642. See also SD-Access
failure detection, EIGRP, 164
FD (feasible distance), 158
feasibility condition, 158
feasible successor, 158
FHRP (first-hop redundancy protocol), 429–430, 963
configuration, 442–443
GLBP (Gateway Load Balancing Protocol), 441
   AVF (active virtual forwarder), 442
   AVG (active virtual gateway), 441
   changing the load-balancing method, 444–446
   viewing the status, 443–444
HSRP (Hot Standby Router Protocol), 432–433
   configuration, 434–435
   object tracking, 436–438
   versions, 433
   viewing the status, 435–436
VRRP (Virtual Router Redundancy Protocol), 438
   legacy configuration, 439
   version 2 configuration, 438
   version 3 configuration, 440–441
   viewing the status, 439
fhrp version vrrp v3 command, 440–441
FIB (Forwarding Information Base), 29, 132, 963
FIFO (first-in, first-out), 406
file prompt quiet command, 899
firewall
   next-generation, 751
zone-based. See ZFW (Zone-Based Firewall)
Flexible NetFlow, 709
   applying the flow monitor to the interfaces, 715–716
   creating a custom flow record, 709–711
   creating a flow exporter, 711–712
   creating a flow monitor, 713–714
   mapping the flow exporter to the flow monitor, 714
floating static route, 141–143, 963
flows, 706
forward delay, 40, 963
forwarding architecture, 25–26
   CEF (Cisco Express Forwarding), 27
      hardware, 30
      software, 29–30
   centralized forwarding, 28
   distributed forwarding, 28
   process switching, 26–27
SDM (Switching Database Manager) templates, 30–32
TCAM (ternary content addressable memory), 27–28
free space path loss, 527–529
frequency, 514–515, 963
   2.4 GHz band, 516
   5 GHz band, 516
   6 GHz band, 516
   channels, 517
   non-overlapping channel spacing, 518–519
   radio, 516
   signal bandwidth, 517–518
FTD (Firepower Threat Defense)
   software image, 963
fully specified static route, 141
functions. See also VNF (virtual network function)
CRUD, 856
HTTP, 856
Python, 888

G

gain, 525–526, 562, 964
general-purpose CPU, 27
GET (Cisco Group Encrypted Transport) VPN, 486
get_dnac_devices.py script, 885–889
GitHub, 880, 964
  code editing, 881–882
  projects, 880–881
GLBP (Gateway Load Balancing Protocol), 441
  AVF (active virtual forwarder), 442
  AVG (active virtual gateway), 441
  changing the load-balancing method, 444–446
  configuration, 442–443
  viewing the status, 443–444
grain, 909–910, 964
GRE (Generic Routing Encapsulation), 469
  encapsulation, 469
  encrypting traffic using IPsec profiles, 487–493
  tunnel configuration, 470–474
  verification, 474

H

H plane, 964
hard reset, BGP, 313
hardware, CEF (Cisco Express Forwarding), 30
header, VLAN, 8
hello packet, OSPF, 175
hello time, 40, 190, 689, 964
hierarchical LAN design, 624–625
  access layer, 625–627
  core layer, 628–629
  distribution layer, 627–628
high availability
  network design, 629
  technologies, 630
    SSO and NSF, 623–630
    SSO/NSF with GR, 631
    SSO/NSF with NSR, 631
    SSO/NSF with NSR and GR, 631
host pool, 655, 964
HSRP (Hot Standby Router Protocol), 432–433
  configuration, 434–435
  object tracking, 436–438
  versions, 433
  viewing the status, 435–436
  VIP (virtual IP) instance, 433–434
HTTP
  functions, 856
  status codes, 862
hubs, collision domain, 5–6
hypervisor, 828–829, 964

I

IaaS (infrastructure as a service), Cloud OnRamp, 668–669
IANA (Internet Assigned Numbers Authority), 247
iBGP (internal BGP) sessions, 250–251, 964
Idle state, BGP, 254
IDS (intrusion detection system), 749
IEEE (Institute of Electrical and Electronic Engineers) standards, 5
802.1D STP. See STP (Spanning Tree Protocol)
802.1p, 386
802.1Q, 7, 385
802.11, 533–535. See also wireless networks and theory
IGMP (Internet Group Management Protocol), 337, 343–344, 965
message format, 344–345
snooping, 346–348, 964
version 2, 344
version 3, 346
IGP (Interior Gateway Protocol), 127, 249
IKE (Internet Key Exchange), 480, 965
version 1, 480–482
version 2, 482–484
ingress classification, 767–768
inside static NAT, 449–452
installation modes, Puppet, 903
integrated antennas, 565–566, 964
inter-area routes, 207, 219, 222, 223–224, 965
intercontroller roaming, 579, 965
interface cost, OSPF, 189
interface priority, LACP (Link Aggregation Control Protocol), 118
interface vlan command, 23
Internet, transit routing, 292–293
intra-area routes, 207, 218–219, 965
intracontroller roaming, 577–579, 965
IntServ, 377–378
inventory file, Ansible, 917
I/O (input/output), 836
IOS XE, 796–797
creating a username, 790
EXEC timeout, 802
hash options, 119–120
ip_input process, 26
passwords
encryption, 789–790
types of, 789
privilege levels, 793–796
ip access-list command, 784–785
ip address command, 21
ip address secondary command, 21
IP addressing, 21–22. See also MAC (Media Access Control) address;
NAT (Network Address Translation); PAT (Port Address Translation)
ESP (Encapsulating Security Payload), 477–478
multicast, 340
GLOP block, 342
IANA-assigned addresses, 340–341
internetwork control block, 341
local network control block, 341
organization-local scope addresses, 342
Source Specific Multicast block, 342
well-known reserved address, 341
routed subinterface, 22
routed switch port, 23
SVI (switched virtual interface), 23
verification, 23–25
ip flow monitor command, 715
ip flow-top-talkers command, 708–709
ip ospf area command, 180
ip ospf network broadcast command, 689–690
ip route command, 138
IP SLA, 724, 965
  HTTP GET operation, 726–728
  ICMP echo operation, 724–726
ip sla command, 725–727
ip_input process, 26
IPS (intrusion prevention system), 749
IPsec, 475–476, 965
  authentication header, 476
  DMVPN (Cisco Dynamic Multipoint VPN), 486
  encryption, hashing, and keying methods, 478
  IKE (Internet Key Exchange), 480
    version 1, 480–482
    version 2, 482–484
  site-to-site configuration, 486–487
  site-to-site GRE over, 487–493
  site-to-site VTI over, 493–495
  transform set, 478–480
  VPN, 484–486
    Cisco Dynamic Multipoint, 486
    Cisco FlexVPN, 486
    GET, 486
    remote access, 486
    site-to-site, 486
IPv6, 21
  BGP configuration, 277–285
  OSPFv3 configuration, 234–235
  static routes, 145–146
ipv6 address command, 21
IRQ (interrupt request), 836
ISAKMP (Internet Security Association and Key Management Protocol), 480, 965
isotropic antenna, 526, 560–561, 965
IST (internal spanning tree), 83, 965

J

jitter, 374, 376
jobs, SaltStack, 909
JSON (JavaScript Object Notation), 861–862, 965

K

k value, 160–161, 965
kernel, 837
keyword/s
  access-list command, 782, 783
  aggregate-address command, 272, 276–277
  continue, 305–306
  show mac address-table dynamic command, 15
  show vlan command, 10–11
  switchport trunk allowed vlan command, 15
kitchen, 906
knife, 906

L

LACP (Link Aggregation Control Protocol), 106–107
  fast, 115
  interface priority, 118
  maximum number of EtherChannel member interfaces, 116–117
  minimum number of EtherChannel member interfaces, 115
  system priority, 117–118, 966
  viewing neighbor information, 112–113
  viewing packet counters, 113–114
lacp max-bundle command, 116–117
lacp rate fast command, 115
latency, 162, 374
jitter, 376
processing delay, 376
propagation delay, 375
satellite communication, 375
serialization delay, 375
Law of 3s, 522–523
Law of 10s, 523
Law of Zero, 522
Layer 2 forwarding, 4–5, 966. See also switches
MAC address table, 15–17
troubleshooting, 16
Layer 2 roaming, 579–580
Layer 3 forwarding, 19, 966
ARP (Address Resolution Protocol), 19–20
IP address assignment, 21–22
routed subinterfaces, 22
routed switch ports, 23
SVI (switched virtual interface), 23
verification, 23–25
packet routing, 20–21
on the same subnet, 19–20
Layer 3 roaming, 581–583, 966
Layer 7 classification, 382
Learn page, DevNet, 878
LHR (last-hop router), 966
link aggregation protocols, 106. See also EtherChannel bundle
EtherChannel configuration, 107–108
LACP (Link Aggregation Control Protocol), 106–107
fast, 115
interface priority, 118
maximum number of Ether-Channel member interfaces, 116–117
minimum number of EtherChannel member interfaces, 115
system priority, 117–118
viewing neighbor information, 112–113
viewing packet counters, 113–114
PAgP (Port Aggregation Protocol), 106, 113
link budget, 526–527
link-state algorithm, 130–131, 966. See also OSPF (Open Shortest Path First)
LISP (Cisco Locator/ID Separation Protocol), 495–496, 649, 966
architecture
control plane, 497–498
data plane, 498–499
components, 496–497
data path, 501–502
map registration and notification, 499–500
map request and reply, 500–501
proxy ETR, 502–503
proxy ITR, 503–504
routing architecture, 497
LLQ (low-latency queuing), 407–408
load balancing, 966
EIGRP, 163
EtherChannel, 119–120
unequal-cost, 136–137
local bridge identifier, 40, 966
Local SPAN (Switched Port Analyzer), 717
configuration examples, 719–720
specifying the destination port, 718–719
specifying the source port, 717–718
Local Web Authentication, 764–765
locating devices in a wireless network, 584–587
logarithm, 521–522
logging buffered ? command, 702
logout-warning command, 802–803
looking glasses, 301
loop guard, 74
loop prevention, BGP, 247–248
loopback networks, OSPF, 196–198
LSA/s (link-state advertisement/s), 172, 209–210
age and flooding, 210
OSPFv3, 232
sequence, 210
type 1, 210–212
type 2, 213–214
type 3, 213–217
LSDB (link-state database), 172

M

MAB (MAC Authentication Bypass), 762–764, 967
MAC (Media Access Control) address, 4–5, 967
multicast, 342–343
table, 15–17
mac address-table static vlan command, 16
MACsec, 772–773, 967
downlink, 774
frame format, 773–774
uplink, 774
Malware Analytics, 742
manifest, Puppet, 903–904
MANO (management and orchestration), 836
marking, 385
class-based, 392–393
Layer 2, 385–386
Layer 3, 386–387
PCP (Priority Code Point), 386
match command, 382–384
max age, 40, 967
MED (multi-exit discriminator), 326–327
member links, 967
message/s
BGP, 252
PIM, 354
PTP (Precision Time Protocol), 426
RPC, 875–876
syslog, 701
logging buffer, 701–704
sending to a host, 704–706
severity levels, 701
method list, 806
metric/s, 132
EIGRP, 160–162
backward compatibility, 163
wide, 162
equal-cost multipathing, 135–136
OSPF, inter-area summarization, 222–223
unequal-cost load balancing, 136–137
MFIB (Multicast Forwarding Information Base), 968
MIB (Management Information Base), 695, 697–699
migration, VM (virtual machine), 829–830
MIMO (multiple-input, multiple-output) system, 535

minions, 909

misconfiguration, MST (Multiple Spanning Tree Protocol)
  trunk link pruning, 90–91
  VLAN assignment to the IST, 89–90

MLS (multilayer switch), 4

mobility domain, 967

mobility group, 583–584, 967

modulation, 532–533, 967
  DRS (dynamic rate shifting), 538–540
  spread spectrum, 532–533

module, 967
  Puppet, 903
  Python, 886–887

monitor session destination interface command, 718

MP-BGP (multiprotocol BGP), 277

MQC (Modular QoS CLI), 379–381
  class-based marking, 392–393
  classification configuration, 382–385

MR (map resolver), 967

MRC (maximal-ratio combining), 538, 967

MRIB (Multicast Routing Information Base), 968

MS (map server), 967

MST (Multiple Spanning Tree Protocol), 80, 967
  configuring, 84
  instance, 82
  IST (internal spanning tree), 83
  misconfigurations
    trunk link pruning, 90–91
    VLAN assignment to the IST, 89–90
  region boundary, 90–91
  MST region as the root bridge, 91
  MST region not a root bridge for any VLAN, 91
  topologies, 82–83
  tuning, 87
    changing the interface cost, 88
    changing the interface priority, 88–89
  verification, 84–87

multi-area topology, OSPF, 206–207

multicast, 337, 342–343
  addressing, 340
    GLOB block, 342
    IANA-assigned addresses, 340–341
    internetwork control block, 341
    local network control block, 341
    organization-local scope addresses, 342
    Source Specific Multicast block, 342
    well-known reserved addresses, 341
  architecture, 338
  group address, 339
  IGMP, 343–344
    message format, 344–345
    snooping, 346–348
    version 2, 344
    version 3, 346
  Layer 2 addresses, 342–343
  PIM, 349
    bootstrap router, 366–367
    dense mode, 354–356
    designated routers, 359–360
    distribution trees, 349
    forwarder, 361–363
messages, 354
RP, 350–351, 363–365
RPF, 360–361
shared and source path trees, 357–358
shared tree join, 358
shared trees, 350–352
source registration, 358
source trees, 349–350
sparse mode, 357
SPT switchover, 358–359
terminology, 352–354
state, 968
stream, 339

N

NAC (network access control), 758
802.1x, 758
authentication process flow, 759–760
components, 758
EAP methods, 760–762
roles, 758–760
Cisco IBNS 2.0, 766
Cisco TrustSec, 766–767
egress enforcement, 770–771
ingress classification, 767–768
propagation, 768–770
Enhanced FlexAuth, 766
MAB (MAC Authentication Bypass), 762–764
Web Authentication, 764
Central, 765
Local, 764–765
name command, 8
named ACL, 784–785
narrowband transmission, 532, 968

NAT (Network Address Translation), 446–447, 968
pooled, 447–455
static
inside, 449–452
outside, 452–455
topology, 447–449
types of, 447
native VLANs, 14, 968
NBAR2 (Next-Generation Network-Based Application Recognition), 382
NDP (Cisco Network Data Platform), 657
neighbor distribute-list command, 307
neighbor state, BGP, 253
Active, 254
Connect, 254
Established, 255
Idle, 254
OpenConfirm, 255
OpenSent, 254–255
neighbors
BGP, 249
EIGRP, 160
OSPF, 175–185
adjacency requirements, 181
state fields, 186
verifying, 185–186
NETCONF, 872, 968
capabilities, 874
comparison with SNMP, 873
datastores, 875
element, 873
operations, 874
RPC message, 875–876
save configuration, 876
shopping list analogy, 873–874
transactions, 873
NetFlow, 706, 968
  collected traffic types, 706
  configuring and verifying talkers, 708–709
  enabling on a device, 706–707
  Flexible, 709
    applying the flow monitor to the interfaces, 715–716
    creating a custom flow record, 709–711
    creating a flow exporter, 711–712
    creating a flow monitor, 713–714
    mapping the flow exporter to the flow monitor, 714
  flows, 706
  verification, 707–708
network area command, 178
Network Device API, 864–867
network/s. See also enterprise network architecture; QoS (quality of service); routing and routing protocols; VLANs (virtual LANs)
campus
  Layer 2 access layer, 634–636
  Layer 3 access layer, 636–637
  SD-Access design, 640
  simplified campus design, 637–639
  three-tier design, 634
  two-tier design, 632
fabric, 642. See also SD-Access
hierarchical LAN design, 624–625
  access layer, 625–627
  core layer, 628–629
  distribution layer, 627–628
high availability, 629
latency, 374
  jitter, 376
  processing delay, 376
  propagation delay, 375
  serialization delay, 375
layer, SD-Access, 647–648
OSPF, 194
  broadcast, 194–195
  discontiguous, 217–218
  loopback, 196–198
  point-to-point, 195–196
OSPFv3, 239–240
outages, 854
overlay, 466. See also overlay tunnels
virtual private. See VPN (virtual private network)
next-generation firewall, 751
NFV (network functions virtualization), 833–834, 968. See also Cisco ENFV (Enterprise Network Functions Virtualization)
NFVIS (network function virtualization infrastructure software), 846–847
NLRI (Network Layer Reachability Information), 248
no switchport command, 23
noise/noise floor, 530, 968
nonce, 968
non-overlapping channel spacing, 518–519
northbound API, 855–856
NSSA (Not-So-Stubby Area), 217
NTP (Network Time Protocol), 420–421, 968–969
  configuration, 421–422
  peers, 424–425
  stratum preference, 424
  verification, 422–423
  viewing associations, 423–424
numbered ACL, 782–783
numbered extended ACL, 783–784
object tracking, 430, 436–438
OFDM (orthogonal frequency division multiplexing), 533, 969
OHAI, 906
OIF (outgoing interface), 969
omnidirectional antennas, 564–566, 969
Open Authentication, 593–594, 969
OpenConfirm state, BGP, 255
OpenSent state, BGP, 254–255
optimization, OSPF, link-cost, 189
orchestrator, NFV, 836
OSI (Open Systems Interconnection) model, 3–4
OSPF (Open Shortest Path First)
  ABR (area border router), 205–206
  area, 173–174, 204–207
  area ID, 207
  BDR (backup designated router), 177–178
    election, 190–192
    placement, 192–194
  configuration
    for all interfaces, 178–180
    with explicit IP addresses, 179
    with explicit subnet, 179
    interface-specific, 180–181
  OSPF network statement, 178
  dead interval timer, 190, 689
debugging
  debug ip ospf adj command, 687, 690–691
  debug ip ospf bellow command, 687–689, 690–691
  ip ospf network broadcast command, 689–690

  show ip ospf interface command, 689
  show ip ospf neighbor command, 686
default route advertisement, 187–188
DR (designated router), 176–178
  election, 190–192
  placement, 192–194
equal-cost multipathing, 220
hello packets, 175
hello time, 190, 689
inter-area routes, 207, 219
inter-router communication, 174
intra-area routes, 207, 218–219
LSA/s (link-state advertisement/s), 172, 209–210
  age and flooding, 210
  sequences, 210
  type 1, 210–212
  type 2, 213–214
  type 3, 213–217
LSDB (link-state database), 172, 204–205
multi-area topology, 206–207
neighbors, 175–185
  adjacency requirements, 181
  state fields, 186
network, 194
  broadcast, 194–195
  discontiguous, 217–218
  loopback, 196–198
  point-to-point, 195–196
optimization, link-cost, 189
packet types, 174
passive interfaces, 181
RID (router ID), 175, 180–181
route filtering, 224–225
  area, 225–227
with summarization, 225
routing table, 208–209
sample topology and configuration, 181–183
SPT (shortest path tree), 172–173
summarization, 220–222
inter-area, 222, 223–224
metrics, 222–223
timers, 190
verification
interface, 184–185
neighbor adjacency, 185–186
routes installed on the RIB, 186–187
versions, 170
OSPFv3, 230
communication, 232–233
configuration, 233–235
differences with OSPFv2, 231–232
IPv4 support, 240–242
IPv6 summarization, 238–239
LSAs (link-state advertisements), 232
network types, 239–240
passive interface, 237–238
verification, 235–237
OSS (operations support system), 836
OUI (organizationally unique identifier), 5
outside static NAT, 452–455
overlay network/tunnels, 466, 969
GRE (Generic Routing Encapsulation), 469
capsulation, 469
encapsulation, 469
tunnel configuration, 470–474
verification, 474
IPsec, 475–476
authentication header, 476
Cisco FlexVPN, 486
DMVPN, 486
encryption, hashing, and keying methods, 478
ESP (Encapsulating Security Payload), 477–478
GET VPN, 486
IKE (Internet Key Exchange), 480
IKEv1, 480–482
IKEv2, 482–484
remote access VPN, 486
site-to-site GRE over, 487–493
site-to-site VPN, 486
site-to-site VTI over, 493–495
transform set, 478–480
VPN solutions, 484–486
LISP (Cisco Locator/ID Separation Protocol), 495–496
components, 496–497
control plane, 497–498
data path, 501–502
data plane, 498–499
map registration and notification, 499–500
map request and reply, 500–501
proxy ETR, 502–503
proxy ITR, 503–504
routing architecture, 497
recursive routing, 474–475
VXLAN (Virtual eXtensible Local Area Network), 504–505, 507
control plane, 506
VTEP, 505–506
OVS (Open vSwitch), 837
OVS-DPDK, 839–840
<table>
<thead>
<tr>
<th><strong>P</strong></th>
<th><strong>PIM (Protocol Independent Multicast)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>PA (path attribute), 247</td>
<td></td>
</tr>
<tr>
<td>packet/s</td>
<td></td>
</tr>
<tr>
<td>BGP, 252</td>
<td></td>
</tr>
<tr>
<td>EIGRP, 160</td>
<td></td>
</tr>
<tr>
<td>flow for virtualized systems, 837–839</td>
<td></td>
</tr>
<tr>
<td>loss, 376–377</td>
<td></td>
</tr>
<tr>
<td>OSPF, 174</td>
<td></td>
</tr>
<tr>
<td>OSPFv3, 232–233</td>
<td></td>
</tr>
<tr>
<td>routing, 20–21</td>
<td></td>
</tr>
<tr>
<td>VXLAN-GPO, 651</td>
<td></td>
</tr>
<tr>
<td>PACL (port ACL), 785–786</td>
<td></td>
</tr>
<tr>
<td>PAgP (Port Aggregation Protocol), 106</td>
<td></td>
</tr>
<tr>
<td>viewing neighbor information, 113</td>
<td></td>
</tr>
<tr>
<td>viewing packet counters, 114</td>
<td></td>
</tr>
<tr>
<td>parabolic dish antenna, 569–570, 969</td>
<td></td>
</tr>
<tr>
<td>passive interface, 969</td>
<td></td>
</tr>
<tr>
<td>OSPF, 181</td>
<td></td>
</tr>
<tr>
<td>OSPFv3, 237–238</td>
<td></td>
</tr>
<tr>
<td>passive-interface command, 237–238</td>
<td></td>
</tr>
<tr>
<td>password/s</td>
<td></td>
</tr>
<tr>
<td>encryption, 789–790</td>
<td></td>
</tr>
<tr>
<td>terminal line, 788–789, 790–793</td>
<td></td>
</tr>
<tr>
<td>types of, 789</td>
<td></td>
</tr>
<tr>
<td>PAT (Port Address Translation), 458–461, 970</td>
<td></td>
</tr>
<tr>
<td>patch antennas, 567–568, 970</td>
<td></td>
</tr>
<tr>
<td>path, 127</td>
<td></td>
</tr>
<tr>
<td>metrics</td>
<td></td>
</tr>
<tr>
<td>EIGRP (Enhanced Interior Gateway Routing Protocol), 160–163</td>
<td></td>
</tr>
<tr>
<td>equal-cost multipathing, 135–136</td>
<td></td>
</tr>
<tr>
<td>unequal-cost load balancing, 136–137</td>
<td></td>
</tr>
<tr>
<td>selection, 132</td>
<td></td>
</tr>
<tr>
<td>Path Trace, 970</td>
<td></td>
</tr>
<tr>
<td>path vector algorithm, 131–132, 970</td>
<td></td>
</tr>
<tr>
<td>PBR (policy-based routing), 146–149</td>
<td></td>
</tr>
<tr>
<td>PCI passthrough, 840–841</td>
<td></td>
</tr>
<tr>
<td>Pearson Test Prep practice test, 927</td>
<td></td>
</tr>
<tr>
<td>accessing, 927–928</td>
<td></td>
</tr>
<tr>
<td>customizing your exams, 928–929</td>
<td></td>
</tr>
<tr>
<td>updating your exams, 929</td>
<td></td>
</tr>
<tr>
<td>peers, NTP (Network Time Protocol), 424–425</td>
<td></td>
</tr>
<tr>
<td>performance, VNF (virtual network function), 836</td>
<td></td>
</tr>
<tr>
<td>PFS (Perfect Forward Secrecy), 482</td>
<td></td>
</tr>
<tr>
<td>phase, 519, 970</td>
<td></td>
</tr>
<tr>
<td>PHB (per-hop behavior), 387, 390–391, 970</td>
<td></td>
</tr>
<tr>
<td>Assured Forwarding, 388–390</td>
<td></td>
</tr>
<tr>
<td>Class Selector, 388</td>
<td></td>
</tr>
<tr>
<td>Default Forwarding, 388</td>
<td></td>
</tr>
<tr>
<td>Expedited Forwarding, 390</td>
<td></td>
</tr>
<tr>
<td>physical layer, SD-Access, 647</td>
<td></td>
</tr>
<tr>
<td>pillar, SaltStack, 909–910, 970</td>
<td></td>
</tr>
<tr>
<td>PIM (Protocol Independent Multicast), 337, 349</td>
<td></td>
</tr>
<tr>
<td>bootstrap router, 366–367</td>
<td></td>
</tr>
<tr>
<td>dense mode, 354–356</td>
<td></td>
</tr>
<tr>
<td>designated routers, 359–360</td>
<td></td>
</tr>
<tr>
<td>distribution tree, 349</td>
<td></td>
</tr>
<tr>
<td>shared tree, 350–352</td>
<td></td>
</tr>
<tr>
<td>source tree, 349–350</td>
<td></td>
</tr>
<tr>
<td>forwarder, 361–363</td>
<td></td>
</tr>
<tr>
<td>messages, 354</td>
<td></td>
</tr>
<tr>
<td>RP (rendezvous point), 350–351, 363–364</td>
<td></td>
</tr>
<tr>
<td>Auto-, 364</td>
<td></td>
</tr>
<tr>
<td>candidate, 364–365, 366–367</td>
<td></td>
</tr>
<tr>
<td>mapping agent, 365</td>
<td></td>
</tr>
<tr>
<td>static, 364</td>
<td></td>
</tr>
</tbody>
</table>
RPF (Reverse Path Forwarding), 360–361
shared and source path trees, 357–358
shared tree join, 358
source registration, 358
sparse mode, 357
SPT switchover, 358–359
terminology, 352–354

**ping command**, 675–676
  - extended, 677–680
  - repeat option, 676–677

**playbooks**, 913–914, 917–930, 970
point-to-point networks, OSPF, 195–196

**polar plot**, 970
polarization, 563–564, 970

**policer**
  - class-based, 398
  - markdown, 395
  - placing in the network, 395
  - single-rate three-color, 399–400
  - single-rate two-color, 399–400
token bucket algorithm, 395–397
two-rate three-color, 403–405

**policy/ies**
  - based routing, 147, 970
  - CoPP. See CoPP (Control Plane Policing)
maps, 379–381
MQC (Modular QoS CLI), 379–381
plane, SD-Access, 651–652
SD-WAN, 665
service, 379
tag, 558
workflow, Cisco DNA, 658–659

**pooled NAT**, 447–455, 970
port-channel min-links command, 115
portfast, 68–70

**port/s**
  - access, 11–12
  - auxiliary, 802
  - switch, viewing the status, 17–19
  - trunk, 12
    - displaying information about, 13
    - verifying status, 13–14

**Postman**, 857, 858
collections, 858–859
dashboard, 857
History tab, 858
URL bar, 859–860

**power**
  - comparing against a reference, 524–525
dB (decibel), 522, 523–524
  - Law of 3s, 522–523
  - Law of 10s, 523
  - Law of Zero, 522
dBm (dB-milliwatt), 525
effective isotropic radiated, 526
measuring changes along a signal path, 525–527
RF signal, 521
RSSI (received signal strength indicator), 530–531

**PPDIOO** (Prepare, Plan, Design, Implement, Operate, Optimize)
lifecycle, 913

**PQ** (priority queuing), 407
prefix length, 132, 133, 970
prefix list, 299, 308, 970
prefix matching, 297–299
  - IPv6 prefix list, 299–300
prefix list, 299
pre-shared key authentication, 595–597
private community, BGP, 314, 317–318
privilege level, IOS XE, 793–796, 971
Probe Request, 587
process switching, 26–27
processing delay, 376
propagation delay, 375
protocol, network, 3
proxy ETR, 971
proxy ITR, 971
PTK (Pairwise Transient Key), 598
PTP (Precision Time Protocol), 425–426, 970
configuration, 427–429
Event message types, 426
General message types, 426
Puppet, 902
agent/server communication, 902
comparison with Chef, 906
components, 902
Forge, 904
installation modes, 903
manifest, 903–904
module, 903
Puppet Bolt, 922
command line, 922–923
tasks, 922, 923
push model, 904
PVST (Per-VLAN Spanning Tree), 81–82, 971
Python, 911, 971
functions, 888
module, 886–887
scripts
  conditions, 885
dictionary, 885
  Env_Lab.py script, 882–885
get_dnac_devices.py, 885–889
quotation marks, 884
strings, 884
Q
QAM (quadrature amplitude modulation), 533, 971
QoS (quality of service)
  CBWFQ (class-based weighted fair queuing), configuring, 410–414
classification, 381–382
    configuring, 382–385
      Layer 7, 382
  congestion avoidance, 408–410
  congestion management, 406–408
  CoPP (Control Plane Policing), 817–818
  DiffServ, 379
  IntServ, 377–378
  marking, 385
    class-based, 392–393
      Layer 2, 385–386
      Layer 3, 386–387
  PHB (per-hop behavior), 387
    Assured Forwarding, 388–390
    Class Selector, 388
    Default Forwarding, 388
    Expedited Forwarding, 390
  need for, 374
    jitter, 376
    lack of bandwidth, 374
    latency, 374–375
    packet loss, 376–377
    processing delay, 376
    propagation delay, 375
    serialization delay, 375
  policers and shapers
    class-based, 398
markdown, 395
placing in the network, 395
single-rate three-color, 399–400
single-rate two-color, 399–400
token bucket algorithm, 395–397
two-rate three-color, 403–405
scavenger class, 391
trust boundary, 391–392
wireless, 393–394
queuing algorithm, 406–408

R

radiation pattern, 560–562, 971
radio chain, 535
Radioactive Trace, 615–616
RADIUS, 971
RD (reported distance), 158
reactor, 909
receiver. See also antenna/s
  power level, 530–531
  sensitivity level, 530
recipe, 906, 971
recursive static route, 139–140, 474–475, 971
regex (regular expressions), 300–301, 972
Remote SPAN (Switched Port Analyzer), 720–722
remote VPN access, 486
remote-span command, 721
reported distance, 972
REST (Representational State Transfer) API, 856
RESTCONF, 876–877, 972
RF (radio frequency), 516, 971. See also antenna/s
  2.4 GHz band, 516
  5 GHz band, 516
  6 GHz band, 516
amplitude, 520
carrier signal, 531
channels, 517
fingerprinting, 586, 972
modulation, 532–533
  DRS (dynamic rate shifting), 538–540
  spread spectrum, 532–533
MRC (maximal-ratio combining), 538
narrowband transmissions, 532
noise/noise floor, 530
non-overlapping channel spacing, 518–519
phase, 519
power, 521
signal bandwidth, 517–518
SNR (signal-to-noise ratio), 530–531
spatial multiplexing, 535–536
tag, 558
TBF (transmit beamforming), 536–538
W (watts), 521
wavelength, 519–520
RFID tag, 587
RIB (Routing Information Base), 132, 134–135, 972
BGP, 262
  verifying installed routes, 186–187
RID (router ID), 175, 180–181, 972
roaming
  between autonomous APs, 574–576
  intercontroller, 579
  intracontroller, 577–579
  Layer 2, 579–580
  Layer 3, 581–583
rogue device, locating, 587
root bridge, 39, 60–63, 972
root bridge identifier, 40, 972
root guard, 68, 972
root path cost, 40, 972
root port, 972
round robin, 406
route aggregation, BGP
  with AS_SET, 276–277
aggregate-address command, 267–274
route filtering, 306–307
  AS_Path ACL filtering, 309–311
distribute lists, 307
  area, 225–227
  with summarization, 225
prefix lists, 308
route maps, 311–313
route map, 301–302, 972
  command syntax, 301
complex matching, 304
  components, 301
conditional match options, 302–303
continue keyword, 305–306
multiple conditional match conditions, 303–304
optional actions, 304–305
route filtering, 311–313
route summarization
  BGP, 274–276, 282–285
  EIGRP, 166–167
  OSPF, 220–222
    inter-area, 222, 223–224
    metrics, 222–223
router ospf command, 178
routing and routing protocols. See also
distance vector algorithm; enhanced
distance vector algorithm; link-state
algorithm; VRF (virtual routing and forwarding)
AD (administrative distance), 132,
  133–135
deterministic, 293–294
distance vector algorithm, 128–129
dynamic, 126–128
enhanced distance vector algorithm,
  129–130
FIB (Forwarding Information Base), 132
hybrid, 129
link-state algorithm, 130–131
metric, 132
path selection, 132
path vector algorithm, 131–132
policy-based, 146–149
prefix length, 132, 133
recursive, 474–475
RIB (Routing Information Base), 132,
  134–135
static, 137
  directly attached, 138–139
  floating, 141–143
  fully specified, 141
  IPv6, 145–146
  to null interfaces, 143–145
  recursive, 139–140
table, 133, 208–209
RP (rendezvous point), 350–351,
  363–364, 972
Auto-, 364
candidate, 364–365, 366–367
mapping agents, 365
static, 364
RP (route processor) engine, 28
RPF (Reverse Path Forwarding), 360–361
RSSI (received signal strength
  indicator), 530–531, 585, 971
RSTP (Rapid Spanning Tree Protocol), 36, 53–54
  building the topology, 55
  convergence, 55
  port roles, 54
  port states, 54
  port types, 54–55
RSVP (Resource Reservation Protocol), 377–378
RTLS (real-time location services), 585–587
Ruby, 906. See also Chef

S

SaaS (software as a service), Cloud OnRamp, 666–668
SAE (Simultaneous Authentication of Equals), 595
Salt SSH, 923–924
SaltStack, 909
  0MQ, 909
  beacon, 909
  commands, 910–911
  grain, 909–910
  jobs, 909
  minion, 909
  pillar, 909–910
  reactor, 909
  remote execution system, 909
  scaling, 910
  satellite communication, latency, 375
  save configuration, NETCONF, 876
  scalable group, 655–656
  scaling, SaltStack, 910
  scavenger class, 391
script
  Python
  conditions, 885
  dictionary, 885
  Env_Lab.py, 882–885
  get_dnac_devices.py, 885–889
  quotation marks, 884
  strings, 884
Tcl, 899–901
SD-Access, 506–507, 643–646
  anycast gateway, 656
  architecture, 646–647
    network layer, 647–648
    physical layer, 647
    underlay network, 648–649
  campus fabric, 646
  components, 646
  controller layer, 656–657
  fabric, 649
    control plane, 649–650
    control plane nodes, 653–654
    data plane, 650–651
    device roles, 652
    edge nodes, 652–653
    policy plane, 651–652
    WLC (wireless LAN controller), 654
  host pool, 655
  scalable group, 655–656
  VN (virtual network), 655
SDM (Switching Database Manager) templates, 30–32
sdm prefer command, 30
SD-WAN, 661. See also Cisco SD-WAN
  segmentation, 973
  sensitivity level, 530, 973
  serialization delay, 375
server/s
  bare-metal, 828
<table>
<thead>
<tr>
<th>Command</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ntp status command</td>
<td>1009</td>
</tr>
<tr>
<td>show interfaces switchport command</td>
<td>17–18</td>
</tr>
<tr>
<td>show interfaces trunk command</td>
<td>13–14, 103</td>
</tr>
<tr>
<td>show ip arp command</td>
<td>20</td>
</tr>
<tr>
<td>show ip flow export command</td>
<td>707–708</td>
</tr>
<tr>
<td>show ip interface brief command</td>
<td>23–24</td>
</tr>
<tr>
<td>show ip nat translations command</td>
<td>450–452</td>
</tr>
<tr>
<td>show ip ospf database summary command</td>
<td>215</td>
</tr>
<tr>
<td>show ip ospf interface command</td>
<td>184–185, 689</td>
</tr>
<tr>
<td>show ip ospf neighbor command</td>
<td>186, 686</td>
</tr>
<tr>
<td>show ip route bgp command</td>
<td>265</td>
</tr>
<tr>
<td>show ip route command</td>
<td>137, 139, 266–267, 448</td>
</tr>
<tr>
<td>show ip route ospf command</td>
<td>187</td>
</tr>
<tr>
<td>show ipv6 interface brief command</td>
<td>24–25</td>
</tr>
<tr>
<td>show ipv6 route command</td>
<td>146</td>
</tr>
<tr>
<td>show ipv6 route ospf command</td>
<td>237, 238, 239</td>
</tr>
<tr>
<td>show lacp counters command</td>
<td>113–114</td>
</tr>
<tr>
<td>show lacp neighbor command</td>
<td>112–113</td>
</tr>
<tr>
<td>show lacp sys-id command</td>
<td>117–118</td>
</tr>
<tr>
<td>show logging command</td>
<td>703–704</td>
</tr>
<tr>
<td>show mac address-table dynamic command</td>
<td>15–16</td>
</tr>
<tr>
<td>show monitor session erspan-source session command</td>
<td>723–724</td>
</tr>
<tr>
<td>show ntp associations command</td>
<td>423–424</td>
</tr>
<tr>
<td>show ntp status command</td>
<td>422–423</td>
</tr>
</tbody>
</table>
show ospfv3 interface command, 236, 240
show ospfv3 ipv6 neighbor command, 236
show pagp counters command, 114
show pagp neighbor command, 113
show running-config command, 270–271
show sdm prefer command, 31–32
show spanning-tree command, 85–86
show spanning-tree inconsistentports command, 74
show spanning-tree interface command, 48–49, 70–71, 73
show spanning-tree mst command, 86–87, 88
show spanning-tree mst configuration command, 84–85
show spanning-tree mst interface command, 87
show spanning-tree root command, 42–45
show spanning-tree vlan command, 45–47, 61–62, 64–66
show spanning-tree vlan detail command, 49–50
show standby command, 435–438
show track command, 431–432
show udld neighbors command, 75–76
show vlan command, 9–11
show vrrp brief command, 441
show vrrp command, 439
show vtp status command, 99–101
signal bandwidth, 517–518
single-rate three-color policer, 399–400
single-rate two-color policer, 399–400
SISO (single-in, single-out) system, 535
site tag, 558
site-to-site VPN, 486
GRE over IPsec, 487–493
VTI over IPsec, 493–495
SLA (service-level agreement), 375. See also IP SLA
SNMP (Simple Network Management Protocol), 695, 973
collection with NETCONF, 873
configuration, 699–700
MIB (Management Information Base), 695, 697–699
operations, 696
trap, 695
version comparison, 695–696
snmp-server enable traps command, 700
SNR (signal-to-noise ratio), 530–531, 973
soft reset, BGP, 313
software, CEF (Cisco Express Forwarding), 29–30
source tree, 349–350
southbound API, 856
SP (service provider), BGP
multihoming, 291–292
SPAN (Switched Port Analyzer), 716–717, 973
Encapsulated Remote, 722
specifying the destination ports, 723–724
specifying the source ports, 722–723
Local, 717
configuration examples, 719–720
specifying the destination ports, 718–719
specifying the source ports, 717–718
Remote, 720–722, 973
spanning-tree bpdufilter enable command, 72
spanning-tree guard root command, 68
spanning-tree mode mst command, 84
spanning-tree pathcost method long command, 41
spanning-tree portfast bpduguard default command, 70
spanning-tree portfast command, 68–70
spanning-tree vlan forward-time command, 40
spanning-tree vlan hello-time command, 40
spanning-tree vlan max-age command, 40
spanning-tree vlan priority command, 60
spanning-tree vlan root command, 60
spanning-tree vlan root command, 60
spatial multiplexing, 535–536, 973
split-MAC architecture, 547, 974
spread spectrum, 532–533, 974
SPT (shortest path tree), 973
SR-IOV, 841–842
SSH (Secure Shell), 800–802, 973
standard ACL, 295–296
state machine, Cisco lightweight AP, 552–554
static NAT, 974
inside, 449–452
outside, 452–455
static null route, 974
static route, 137
directly attached, 138–139
floating, 141–143
fully specified, 141
IPv6, 145–146
to null interfaces, 143–145
recursive, 139–140
static RP (rendezvous point), 364
STP (Spanning Tree Protocol), 36, 67–68. See also MST (Multiple Spanning Tree Protocol); RSTP (Rapid Spanning Tree Protocol)
802.1D, 38
  BPDU (bridge protocol data unit), 40
  configuration BPDU, 40
  forward delay, 40
  hello time, 40
  local bridge identifier, 40
  max age, 40
  path cost, 41
  port states, 39
  port types, 39
  root bridge, 39
  root bridge identifier, 40
  root path cost, 40
  system ID extension, 40
  system priority, 40
  TCN (topology change notification) BPDU, 40
BPDU filter, 72–73
BPDU guard, 70–72
building the topology, 41
  locating blocked designated switch ports, 45–47
  locating root ports, 44–45
  root bridge election, 41–44
  verification of VLANs on trunk links, 48–49
Error Recovery Service, 71–72
loop guard, 74
modifying port priority, 66–67
modifying root port and blocked switch port locations, 63–66
placing the root bridge, 60–63
portfast, 68–70
problems with unidirectional links, 73
root guard, 68

topology changes, 49–50
  converging with direct link failures, 50–52
  indirect failures, 52–53
UDLD (Unidirectional Link Detection), 75–76

stratum, 421, 974
streaming, 339
string, 884
Stubby area, OSPF, 217
subnet, 127
successor/successor route, 158
summarization, 974. See also route summarization
IPv6, 238–239
OSPF, 220–222
  inter-area, 222, 223–224
  metrics, 222–223
supplicant, 974
SVI (switched virtual interface), IP addressing, 23
switch, 5. See also VLANs (virtual LANs)
collision domain, 5–6
multilayer, 4
port, viewing the status, 17–19
TCAM (ternary content addressable memory), 27–28
virtual, 831–833
switchport access vlan command, 12
switchport mode access command, 12
switchport mode trunk command, 12
switchport trunk allowed vlan command, 14–15
switchport trunk native vlan command, 14
syslog, 701, 974

applet, 896
logging buffer, 701–704
message severity levels, 701
sending messages to a host or collector, 704–706
system ID extension, 40
system priority, 974
  LACP, 117–118
  STP, 40

TACACS+, 803–804, 805, 974
Talos, 741–742
tasks, Puppet Bolt, 922, 923
TBF (transmit beamforming), 536–538, 975
Tc (committed time interval), 395
TCAM (ternary content addressable memory), 27–28, 975
 Tcl, 899–901, 974
TCN (topology change notification)
BPDUs, 40, 975
TCP (Transmission Control Protocol), 249
TCP/IP (Transmission Control Protocol/Internet Protocol), 3
Technologies page, DevNet, 878
Telnet, 974
template, SDM (Switching Database Manager), 30–32
terminal line
  controlling access
    using ACLs, 796–797
    using transport input command, 797–800
line local username and password authentication, 790–793
password protection, 788–789
time synchronization, 420
  NTP (Network Time Protocol), 420–421
    configuration, 421–422
    peers, 424–425
    stratum preference, 424
    verification, 422–423
    viewing associations, 423–424
  PTP (Precision Time Protocol), 425–426
    configuration, 427–429
  Event message types, 426
  General message types, 426

timer
  EIGRP, 164
  OSPF, 190
Token API, 862–864
  token bucket algorithm, 395–397
tools. See also automation tools; commands
diagnostic
  IP SLA, 724–726
  ping command, 675–680
  traceroute command, 680–685
EEM (Embedded Event Manager), 901
  applets, 895
  debugging, 896–898
  email variables, 899
  event detector, 894–895
  syslog applet, 896
  WR MEM applet, 898
Postman, 857, 858
  collections, 858–859
  dashboard, 857
  History tab, 850–858
  URL bar, 859–860
Puppet, 902
  agent/server communication, 902
  components, 902
  installation modes, 903
  manifest, 903–904
  module, 903
SaltStack, 909
  0MQ, 909
  beacon, 909
  commands, 910–911
  grain, 909–910
  jobs, 909
  minion, 909
  pillar, 909–910
  reactor, 909
  remote execution system, 909
  scaling, 910
topology/ies. See also convergence
MST (Multiple Spanning Tree Protocol), 82–83
NAT (Network Address Translation), 447–449
OSPF (Open Shortest Path First), 181–183
  area, 204–207
  multi-area, 206–207
OSPFv3, 233
  table, 159–160, 975
ToS (Type of Service), 975
Totally Stubby area, 217
transit routing, 975
  branch, 293–295
  Internet, 292–293
transport input command, 797–800
troubleshooting. See also Cisco DNA Center Assurance; diagnostic tools
EtherChannel bundle, 118–119
Layer 2 forwarding, 16
tools. See diagnostic tools
wireless, 610–611
wireless connectivity, 610–611
at the AP, 617–620
from the WLC, 611–616
trunk port, 12, 975
  configuring, 13
  displaying information about, 13
  verifying status, 13–14
trust boundary, 391–392
tuning, MST (Multiple Spanning Tree Protocol), 87
  changing the interface cost, 88
  changing the interface priority, 88–89
tunnel mode ipsec command, 493
tunnels. See overlay tunnels
two-rate three-color policers, 403–405
type 1 LSA, 210–212
type 2 LSA, 213–214
type 3 LSA, 213–217

U

UDLD (Unidirectional Link Detection), 75–76, 975
udld enable command, 75
Umbrella, 744–745
undebug interface loopback0 command, 695
underlay network, 648–649, 975
unequal-cost load balancing, 136–137, 975
unicast, 338
unknown unicast flooding, 6
uplink MACsec, 774
upstream, 975
user space, 975
username, creating, 790

V

VACL (VLAN ACL), 786–788
vAnalytics, 664
variables, EEM email, 899
variance value, 163, 976
vBond orchestrator, 662–663
verifying
  AAA (authentication, authorization, and accounting), 809
  BGP session, 257–260
  CoPP (Control Plane Policing), 820–822
  EAP-based authentication, 602
  EtherChannel status, 108–110
  GLBP (Gateway Load Balancing Protocol), 443–444
  GRE tunnels, 474
  IP address, 23–25
  line local username and password authentication, 792–793
  MST (Multiple Spanning Tree Protocol), 84–87
  NetFlow, 707–708
  NTP (Network Time Protocol), 422–423
  OSPF (Open Shortest Path First)
    interfaces, 184–185
    neighbor adjacencies, 185–186
    routes installed on the RIB, 186–187
  OSPFv3, 235–237
  trunk port status, 13–14
  VLAN on trunk links, 48–49
VRRP (Virtual Router Redundancy Protocol), 439

VTP (VLAN Trunking Protocol), 99–100

creating VLANs on the VTP domain server, 100

with a transparent switch, 101

ZBFW (Zone-Based Firewall), 816–817

viewing

NTP associations, 423–424

VLAN port assignments, 9–10

VIM (Virtualized Infrastructure Manager), 834–835

virtualization, 826, 828. See also NFV (network functions virtualization)

vlan command, 8

VLAN (virtual LAN), 7, 976

access port, 11–12

allowed, 14–15

creating, 8

loop prevention, 634–636

native, 14

packet structure, 8

viewing port assignments, 9–10

vManage NMS, 663

VM (virtual machine), 828, 976

comparison with containers, 830–831

guest OS, 830

hypervisor, 828–829

migration, 829–830

packet flow, 837–839

VN (virtual network), 655, 976

VNFs (virtual network functions), 834–836, 840–847

EM (element manager), 835

performance, 836

VIM (Virtualized Infrastructure Manager), 834–835

VPN (virtual private network), 466, 976. See also overlay tunnels

Cisco Dynamic Multipoint, 486

Cisco Group Encrypted Transport, 486

IPsec, 484

remote access, 486

site-to-site, 486

VRF (virtual routing and forwarding), 149–151

VRRP (Virtual Router Redundancy Protocol), 438

configuration

legacy, 439

version 2, 438

version 3, 440–441

viewing the status, 439

vSmart controllers, 663

vSwitch, 831–833, 976

VTEP (virtual tunnel endpoint), 505–506, 976

VTP (VLAN Trunking Protocol), 96–97, 976

communication, 97

configuring, 98–99

servers, 97

verification, 99–100

creating VLANs on the VTP domain server, 100

with a transparent switch, 101

versions, 97

vtp domain command, 98–99

vtp mode command, 98–99

vtp password command, 98–99

vtp version command, 98–99

vty line. See also terminal line

controlling access

using ACLs, 796–797
using transport input command, 797–800
SSH (Secure Shell), 800–802
VXLAN (Virtual eXtensible Local Area Network), 504–505, 507, 650, 976
color plane, 506
VTEP, 505–506

W

W (watt), 521
WAN, 642
wave propagation, 513–514
wavelength, 519–520, 977
Web Authentication, 603, 764, 976
  Central, 765
  Local, 764–765
  wireless authentication, 603–606
well-known communities, BGP, 314
WFQ (weighted fair queuing), 407
wide metric, 162, 977
Wi-Fi, 533, 534
wildcard mask, 782
wireless networks and theory. See also Cisco lightweight APs; Cisco wireless deployments; power
antenna/s, 309–311
  beamwidth, 563
directional, 567–570
  EIRP (effective isotropic radiated power), 526
free space path loss, 527–529
gain, 525–526, 562
isotropic, 526
link budget, 526–527
omnidirectional, 564–566
parabolic dish, 569–570
patch, 567–568
polarization, 563–564
RSSI (received signal strength indicator), 530–531
wave propagation, 513–514
Yagi, 565–569
AP
  autonomous, 545–546
  Cisco, 547–548
  client density, 559–560
  authentication, 593
    EAP, 597–602
    Open Authentication, 593–594
    pre-shared key, 595–597
    WebAuth, 603–606
BSS (basic service set), 592
device location, 584–587
frequency, 514–515
power
  comparing against a reference, 524–525
dB (decibel), 522–524
dBm (dB-milliwatt), 525
measuring changes along a signal path, 525–527
RF signal, 521
QoS (quality of service), 393–394
radio chain, 535
RF (radio frequency), 516
  2.4 GHz band, 516
  5 GHz band, 516
  6 GHz band, 516
amplitude, 520
carrier signal, 531–532
channels, 517
modulation, 532–533
MRC (maximal-ratio combining), 538
narrowband transmissions, 532
noise/noise floor, 530
non-overlapping channel spacing, 518–519
phase, 519
power, 521
signal bandwidth, 517–518
SNR (signal-to-noise ratio), 530–531
spread spectrum, 532–533
TBF (transmit beamforming), 536–538
W (watts), 521
roaming
  between autonomous APs, 574–576
  intercontroller, 579
  intracontroller, 577–579
Layer 2, 579–580
Layer 3, 581–583
rope analogy, 512–513
spatial multiplexing, 535–536
troubleshooting connectivity issues, 610–611
  at the AP, 617–620
  from the WLC, 611–616
wavelength, 519–520
WLC (wireless LAN controller), 276–277, 545, 977.
See also Cisco lightweight APs
fabric, 654
mobility groups, 583–584
pairing with a lightweight AP, 552
split-MAC architecture, 547
troubleshooting client connectivity issues, 611–613
  checking the AP properties, 614–615
  checking the client's association and signal status, 613
  checking the client's properties, 614
Radioactive Trace, 615–616
WPA (Wi-Fi Protected Access), 595–597, 977
WR MEM applet, 898
WRED (weighted random early detection), 390
WRR (weighted round robin), 406

X-Y

XML (Extensible Markup Language), 860–861, 963
Yagi antenna, 568–569, 977
YAML (Yet Another Markup Language), 915
dictionary, 915–916
Lint, 916
lists, 915
YANG model, 870–871, 977. See also NETCONF; RESTCONF
  in NETCONF, 873–874
tree structure, 871–872

Z

ZBFW (Zone-Based Firewall), 809–810, 977
  configuration, 811–815
default zone, 810
self zone, 810
verification, 816–817