

# EXAM ✓ CRAM

## CCNP<sup>®</sup> and CCIE<sup>®</sup> Enterprise Core

ENCOR 350-401



Cram  
Sheet



Flash  
Cards



Practice  
Tests



DONALD BACHA

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



# CCNP<sup>®</sup> and CCIE<sup>®</sup> Enterprise Core

ENCOR 350-401

## Special Offers

### ENHANCE YOUR EXAM PREPARATION

#### **Save 70% on Complete Video Course**

The *CCNP and CCIE Enterprise Core ENCOR 350-401 Complete Video Course, Complete Video Course*, available for both streaming and download, provides you with hours of expert-level instruction mapped directly to exam objectives. Put your knowledge to the test with full practice exams powered by the Pearson Test Prep practice test software, module quizzes, and more.

#### **Save 80% on Premium Edition eBook and Practice Test**

The *CCNP and CCIE Enterprise Core ENCOR 350-401 Exam Cram Premium Edition eBook and Practice Test* provides three eBook files (PDF, EPUB, and MOBI/Kindle) to read on your preferred device and an enhanced edition of the Pearson Test Prep practice test software. You will also receive two additional practice exams with links for every question mapped to the PDF eBook.

---

#### **Pearson Test Prep online system requirements:**

**Browsers:** Browsers: Chrome version 73 and above, Safari version 12 and above, Microsoft Edge 44 and above.

**Devices:** Desktop and laptop computers, tablets running Android v8.0 and above or iPadOS v13 and above, smartphones running Android v8.0 and above or iOS v13 and above with a minimum screen size of 4.7". Internet access required.

#### **Pearson Test Prep offline system requirements:**

Windows 10, Windows 8.1; Microsoft .NET Framework 4.5 Client; Pentium-class 1 GHz processor (or equivalent); 512 MB RAM; 650 MB disk space plus 50 MB for each downloaded practice exam; access to the Internet to register and download exam databases

---

**See card insert in the back of the book**  
for your Pearson Test Prep activation code and special offers.



**EXAM ✓ CRAM**

**CCNP and CCIE  
Enterprise Core  
ENCOR 350-401  
Exam Cram**

**Donald Bacha**



Pearson

## CCNP and CCIE Enterprise Core ENCOR 350-401 Exam Cram

Copyright © 2022 by Pearson Education, Inc.

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

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

ISBN-13: 978-0-13-689193-2

ISBN-10: 0-13-689193-4

Library of Congress Control Number: 2021924388

ScoutAutomatedPrintCode

### Trademarks

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

### Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

### Special Sales

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

For government sales inquiries, please contact [governmentsales@pearsoned.com](mailto:governmentsales@pearsoned.com).

For questions about sales outside the U.S., please contact [intlcs@pearson.com](mailto:intlcs@pearson.com).

### Editor-in-Chief

Mark Taub

### Director, ITP Product Management

Brett Bartow

### Executive Acquisitions Editor

James Manly

### Development Editor

Ellie Bru

### Managing Editor

Sandra Schroeder

### Project Editor

Mandie Frank

### Copy Editor

Kitty Wilson

### Indexer

Erika Millen

### Proofreader

Gill Editorial  
Services

### Technical Editor

Raymond Lacoste

### Publishing Coordinator

Cindy Teeters

### Designer

Chuti Prasertsith

### Compositor codeMantra

# Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where

- ▶ Everyone has an equitable and lifelong opportunity to succeed through learning
- ▶ Our educational products and services are inclusive and represent the rich diversity of learners
- ▶ Our educational content accurately reflects the histories and experiences of the learners we serve
- ▶ Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview)

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

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

# Figure Credit

Figure 5-1; Figure 5-2 Figure 5-3; Figure 5-4 Figure 5-5 Figure 5-6	Courtesy of Cisco Systems, Inc.  Screenshot of Monitor Section for a Cisco WLC © Cisco Systems, Inc Courtesy of Cisco Systems, Inc.
Figure 5-7 Figure 9-1; Figure 9-2; Figure 9-3; Figure 9-4; Figure 9-5; Figure 9-6; Figure 9-7; Figure 9-8; Figure 9-9; Figure 9-10; Figure 9-11; Figure 9-12; Figure 9-13	Courtesy of Cisco Systems, Inc.  Screenshot of Monitor Section for a Cisco WLC © Cisco Systems, Inc Courtesy of Cisco Systems, Inc.
Figure 15-2; Figure 15-3; Figure 15-4 Figure 20-6 Figure 22-3	Courtesy of Cisco Systems, Inc.  Screenshot of The Cisco vManage Main Dashboard © Cisco Systems, Inc
Figure 23-1 Figure 24-2	Screenshot of Cisco DNA Center © Cisco Systems, Inc  Screenshot of Cisco WLC QoS profiles © Cisco Systems, Inc
Figure 26-2; Figure 26-3 Figure 26-5a; Figure 26-5b Figure 26-5c	© 2022 VMware, Inc Courtesy of Cisco Systems, Inc.
Figure 31-2; Figure 31-3; Figure 31-4	Courtesy of Cisco Systems, Inc.

# Contents at a Glance

Introduction	xxiii
<b>Part I: Infrastructure</b>	
CHAPTER 1 Understanding Layer 2	1
CHAPTER 2 Understanding Layer 3: IGP	59
CHAPTER 3 Understanding Layer 3: BGP	103
CHAPTER 4 IP Services	123
CHAPTER 5 Enterprise Wireless	167
<b>Part II: Security</b>	
CHAPTER 6 Device Access Control	193
CHAPTER 7 Infrastructure Security	219
CHAPTER 8 Securing REST APIs	239
CHAPTER 9 Wireless Security	247
CHAPTER 10 Network Security Design	265
CHAPTER 11 Network Access Control	287
<b>Part III: Automation</b>	
CHAPTER 12 Anatomy of Python	299
CHAPTER 13 Building JSON Files	315
CHAPTER 14 YANG Data Modeling	325
CHAPTER 15 DNA Center and vManage APIs	333
CHAPTER 16 Interpreting REST API Codes	345
CHAPTER 17 EEM Applets	351
CHAPTER 18 Configuration Management and Orchestration	363
<b>Part IV: Architecture</b>	
CHAPTER 19 Enterprise Network Design Principles	379
CHAPTER 20 Wireless LAN Deployments	409
CHAPTER 21 On-Premises vs. Cloud Infrastructure	433
CHAPTER 22 SD-WAN	451

CHAPTER 23	SD-Access	467
CHAPTER 24	QoS	487
CHAPTER 25	Switching	505
<b>Part V: Virtualization</b>		
CHAPTER 26	Basic Virtualization	525
CHAPTER 27	VRF Instances, GRE, and IPsec	545
CHAPTER 28	Extending the Network Virtually	573
<b>Part VI: Network Assurance</b>		
CHAPTER 29	Troubleshooting	587
CHAPTER 30	Monitoring	613
CHAPTER 31	IP SLA and DNA Center	641
CHAPTER 32	NETCONF and RESTCONF	661
	Glossary	673
	Index	695



# Table of Contents

Introduction . . . . .	xxiii
------------------------	-------

## Part I: Infrastructure

### CHAPTER 1

<b>Understanding Layer 2 . . . . .</b>	<b>1</b>
VLANs Overview . . . . .	3
VLAN Assignment . . . . .	4
802.1Q Trunking . . . . .	7
Dynamic Trunking Protocol (DTP) . . . . .	9
VLAN Trunking Protocol (VTP) . . . . .	11
Inter-VLAN Routing . . . . .	16
Spanning Tree Protocol Overview . . . . .	19
Root Bridge, Root Port, and Designated Port Elections . . . . .	20
Rapid Spanning Tree Protocol (RSTP) . . . . .	25
Spanning Tree Protocol Tuning and Protection Mechanisms . . . . .	28
Switch Priorities Overview . . . . .	28
Multiple Spanning Tree Protocol (MST) . . . . .	40
EtherChannels . . . . .	47
Review Questions . . . . .	57
Answers to Review Questions . . . . .	58
Further Reading . . . . .	58
What's Next? . . . . .	58

### CHAPTER 2

<b>Understanding Layer 3: IGPs . . . . .</b>	<b>59</b>
IP Routing Essentials . . . . .	60
Routing Algorithms . . . . .	61
Path Selection . . . . .	62
Static Routing . . . . .	65
Enhanced Interior Gateway Routing Protocol (EIGRP) . . . . .	68
Neighbor Table . . . . .	70
Topology Table . . . . .	72
Routing Tables . . . . .	75
EIGRP Authentication . . . . .	76
EIGRP Named Mode . . . . .	76
Route Summarization . . . . .	78

Open Shortest Path First (OSPF) . . . . .	80
OSPF Cost . . . . .	81
OSPF Authentication . . . . .	82
OSPF Areas . . . . .	83
Neighbors and Adjacencies . . . . .	85
OSPF Packet Types . . . . .	87
Basic OSPF Configuration . . . . .	87
Router ID (RID) . . . . .	91
Passive Interfaces . . . . .	91
Default Route Advertisements . . . . .	91
OSPF Optimizations . . . . .	92
Link-State Advertisements (LSAs) . . . . .	92
OSPF Path Selection . . . . .	93
Route Summarization . . . . .	95
OSPFv3 . . . . .	95
Review Questions . . . . .	100
Answers to Review Questions . . . . .	101
Further Reading . . . . .	101
What's Next? . . . . .	101

### CHAPTER 3

<b>Understanding Layer 3: BGP . . . . .</b>	<b>103</b>
BGP Fundamentals . . . . .	104
BGP Configuration and Verification . . . . .	112
Review Questions . . . . .	120
Answers to Review Questions . . . . .	120
Further Reading . . . . .	121
What's Next? . . . . .	121

### CHAPTER 4

<b>IP Services . . . . .</b>	<b>123</b>
Network Time Protocol (NTP) . . . . .	124
Network Address Translation (NAT) . . . . .	134
Static NAT . . . . .	136
Dynamic NAT . . . . .	137
Port Address Translation (PAT) . . . . .	138
First-Hop Redundancy Protocols (FHRPs) . . . . .	143
Virtual Router Redundancy Protocol (VRRP) . . . . .	147
Gateway Load Balancing Protocol (GLBP) . . . . .	150
Object Tracking with FHRPs . . . . .	154

Multicast . . . . .	156
Multicast Fundamentals . . . . .	156
Multicast Group Addressing . . . . .	157
Internet Group Management Protocol (IGMP) . . . . .	157
Protocol Independent Multicast (PIM) . . . . .	161
Review Questions . . . . .	165
Answers to Review Questions . . . . .	165
Further Reading . . . . .	166
What's Next? . . . . .	166

**CHAPTER 5**

**Enterprise Wireless . . . . . 167**

Wireless Basics . . . . .	168
Radio Frequency (RF). . . . .	168
Free Space Path Loss . . . . .	171
Received Signal Strength Indicator (RSSI). . . . .	171
Signal-to-Noise Ratio (SNR). . . . .	171
IEEE Wireless Standards . . . . .	172
Multiple Radios . . . . .	173
WLC and AP Operation and Pairing . . . . .	176
AP and WLC Interaction . . . . .	178
Wireless Roaming . . . . .	185
Troubleshooting WLAN Configuration and Client Connectivity Issues. . . . .	188
Review Questions . . . . .	191
Answers to Review Questions . . . . .	192
Further Reading . . . . .	192
What's Next? . . . . .	192

**Part II: Security**

**CHAPTER 6**

**Device Access Control . . . . . 193**

Cisco IOS CLI Session Overview . . . . .	194
Protection of Access to Cisco IOS EXEC Modes . . . . .	197
Secured Access with SSH . . . . .	203
Privilege Levels and Role-Based Access Control (RBAC). . . . .	206
Authentication, Authorization, and Accounting (AAA) Overview . . . . .	210
TACACS+ Overview. . . . .	211
RADIUS Overview. . . . .	211
AAA Configuration for Network Devices . . . . .	212

Review Questions . . . . .	217
Answers to Review Questions . . . . .	217
Further Reading . . . . .	218
What's Next? . . . . .	218

**CHAPTER 7**

<b>Infrastructure Security . . . . .</b>	<b>219</b>
Access Control Lists (ACLs) Overview . . . . .	220
Types of ACLs . . . . .	224
Port ACLs (PACLs) and VLAN ACLs (VACLs) . . . . .	229
Control Plane Policing (CoPP) . . . . .	233
Review Questions . . . . .	236
Answers to Review Questions . . . . .	236
Further Reading . . . . .	237
What's Next? . . . . .	237

**CHAPTER 8**

<b>Securing REST APIs . . . . .</b>	<b>239</b>
REST API Security . . . . .	240
Review Questions . . . . .	245
Answers to Review Questions . . . . .	245
Further Reading . . . . .	245
What's Next? . . . . .	245

**CHAPTER 9**

<b>Wireless Security . . . . .</b>	<b>247</b>
Wireless Authentication Overview . . . . .	248
Open Authentication . . . . .	249
Pre-Shared Key (PSK) Authentication . . . . .	251
Extensible Authentication Protocol (EAP) Authentication . . . . .	254
WebAuth . . . . .	257
Review Questions . . . . .	262
Answers to Review Questions . . . . .	262
Further Reading . . . . .	262
What's Next? . . . . .	263

**CHAPTER 10**

<b>Network Security Design . . . . .</b>	<b>265</b>
Threat Defense . . . . .	266
Network Security Components . . . . .	270

TrustSec, MACsec . . . . .	279
TrustSec . . . . .	279
MACsec . . . . .	281
Review Questions . . . . .	284
Answers to Review Questions . . . . .	284
Further Reading . . . . .	285
What's Next? . . . . .	285

## CHAPTER 11

<b>Network Access Control . . . . .</b>	<b>287</b>
Cisco Identity Services Engine (ISE) . . . . .	288
Network Access Control (NAC) . . . . .	290
Review Questions . . . . .	296
Answers to Review Questions . . . . .	296
Further Reading . . . . .	296
What's Next? . . . . .	297

## Part III: Automation

### CHAPTER 12

<b>Anatomy of Python . . . . .</b>	<b>299</b>
Interpreting Python Components and Scripts . . . . .	300
Python Overview . . . . .	300
Python Releases . . . . .	301
Setting Up Guest Shell . . . . .	301
Using Python . . . . .	302
Python Requirements . . . . .	309
Parsing Python Output to JSON . . . . .	310
Exception Handling . . . . .	311
Review Questions . . . . .	313
Answers to Review Questions . . . . .	313
Further Reading . . . . .	314
What's Next? . . . . .	314

### CHAPTER 13

<b>Building JSON Files . . . . .</b>	<b>315</b>
Data Formats (XML and JSON) . . . . .	316
Extensible Markup Language (XML) . . . . .	317
JavaScript Object Notation (JSON) . . . . .	319
XML and JSON Comparison . . . . .	321

Review Questions . . . . .	323
Answers to Review Questions . . . . .	323
Further Reading . . . . .	324
What's Next? . . . . .	324
<b>CHAPTER 14</b>	
<b>YANG Data Modeling . . . . .</b>	<b>325</b>
YANG Data Modeling . . . . .	326
Different YANG Models . . . . .	327
Review Questions . . . . .	332
Answers to Review Questions . . . . .	332
Further Reading . . . . .	332
What's Next? . . . . .	332
<b>CHAPTER 15</b>	
<b>DNA Center and vManage APIs . . . . .</b>	<b>333</b>
APIs for Cisco DNA Center and vManage . . . . .	334
DNA Center API Integrations . . . . .	334
vManage API Integrations . . . . .	338
Review Questions . . . . .	344
Answers to Review Questions . . . . .	344
Further Reading . . . . .	344
What's Next? . . . . .	344
<b>CHAPTER 16</b>	
<b>Interpreting REST API Codes . . . . .</b>	<b>345</b>
Interpreting REST API Response Codes . . . . .	346
HTTP Status Codes . . . . .	347
Review Questions . . . . .	349
Answers to Review Questions . . . . .	349
Further Reading . . . . .	349
What's Next? . . . . .	349
<b>CHAPTER 17</b>	
<b>EEM Applets . . . . .</b>	<b>351</b>
Embedded Event Manager (EEM) . . . . .	352
EEM Architecture . . . . .	354
EEM Policies . . . . .	355
Review Questions . . . . .	362
Answers to Review Questions . . . . .	362

Further Reading . . . . .	362
What's Next? . . . . .	362

**CHAPTER 18**

**Configuration Management and Orchestration . . . . . 363**

Agent-Based Orchestration Tools . . . . .	365
Puppet . . . . .	365
Chef . . . . .	367
SaltStack . . . . .	369
Agentless Orchestration Tools . . . . .	372
Ansible . . . . .	372
Bolt . . . . .	375
Configuration Management and Orchestration Tools Comparison . . . . .	376
Review Questions . . . . .	378
Answers to Review Questions . . . . .	378
Further Reading . . . . .	378
What's Next? . . . . .	378

**Part IV: Architecture**

**CHAPTER 19**

**Enterprise Network Design Principles . . . . . 379**

Hierarchical LAN Design Model . . . . .	380
Access Layer . . . . .	381
Distribution Layer . . . . .	382
Core Layer . . . . .	382
Enterprise Network Architecture Options . . . . .	383
First-Hop Redundancy Protocols (FHRPs) . . . . .	392
Host Standby Router Protocol (HSRP) . . . . .	392
Virtual Router Redundancy Protocol (VRRP) . . . . .	396
Gateway Load Balancing Protocol (GLBP) . . . . .	397
Hardware Redundancy Mechanisms . . . . .	400
Stateful Switchover (SSO) . . . . .	400
Nonstop Forwarding (NSF) . . . . .	405
Review Questions . . . . .	407
Answers to Review Questions . . . . .	408
Further Reading . . . . .	408
What's Next? . . . . .	408

**CHAPTER 20**

<b>Wireless LAN Deployments</b> . . . . .	<b>409</b>
Wireless Deployment Models . . . . .	410
Autonomous Wireless Deployments . . . . .	411
Centralized Wireless Deployments . . . . .	412
Cisco FlexConnect Wireless Deployments . . . . .	415
Cloud-Based Wireless Deployments . . . . .	418
Embedded Wireless Deployments . . . . .	422
Wireless Location Services . . . . .	427
Review Questions . . . . .	430
Answers to Review Questions . . . . .	431
Further Reading . . . . .	431
What's Next? . . . . .	431

**CHAPTER 21**

<b>On-Premises vs. Cloud Infrastructure</b> . . . . .	<b>433</b>
Cloud Infrastructure Basics . . . . .	434
Cloud Services Models . . . . .	438
Infrastructure as a Service (IaaS) . . . . .	438
Platform as a Service (PaaS) . . . . .	440
Software as a Service (SaaS) . . . . .	441
Anything as a Service (XaaS) . . . . .	442
Cloud Deployment Models . . . . .	444
On-Premises or Cloud Infrastructure . . . . .	447
Review Questions . . . . .	449
Answers to Review Questions . . . . .	449
Further Reading . . . . .	450
What's Next? . . . . .	450

**CHAPTER 22**

<b>SD-WAN</b> . . . . .	<b>451</b>
SD-WAN Overview . . . . .	452
The Need for SD-WAN . . . . .	453
Secure Automated WAN . . . . .	454
Application Performance Optimization . . . . .	455
Secure Direct Internet Access (DIA) . . . . .	456
Multicloud . . . . .	456
SD-WAN Architecture Components . . . . .	459
vSmart Controllers . . . . .	459
WAN Edge Routers . . . . .	460



vBond Orchestrators . . . . .	461
vManage . . . . .	461
SD-WAN Considerations . . . . .	463
Review Questions . . . . .	465
Answers to Review Questions . . . . .	465
Further Reading . . . . .	466
What's Next? . . . . .	466
<b>CHAPTER 23</b>	
<b>SD-Access . . . . .</b>	<b>467</b>
SD-Access Overview . . . . .	468
SD-Access Architecture . . . . .	471
SD-Access Operational Planes . . . . .	474
SD-Access Fabric Roles and Components . . . . .	477
Control Plane Nodes . . . . .	478
Edge Nodes . . . . .	479
Intermediate Nodes . . . . .	480
Border Nodes . . . . .	480
Fabric Wireless LAN Controllers (WLCs) . . . . .	481
Fabric-Mode Access Points . . . . .	481
SD-Access Embedded Wireless . . . . .	481
Fabric in a Box . . . . .	482
Shared Services . . . . .	482
Review Questions . . . . .	484
Answers to Review Questions . . . . .	484
Further Reading . . . . .	484
What's Next? . . . . .	485
<b>CHAPTER 24</b>	
<b>QoS . . . . .</b>	<b>487</b>
The Need for QoS . . . . .	488
Packet Loss . . . . .	489
Delay . . . . .	490
Jitter . . . . .	491
Lack of Bandwidth . . . . .	491
QoS Models and Components . . . . .	493
Classification and Marking . . . . .	495
DSCPs and Per-Hop Behaviors (PHBs) . . . . .	497
Policing and Shaping . . . . .	497

Congestion Management and Congestion Avoidance . . . . .	499
Congestion Management (Queuing) . . . . .	499
Congestion Avoidance . . . . .	500
Wireless QoS . . . . .	500
Review Questions . . . . .	503
Answers to Review Questions . . . . .	503
Further Reading . . . . .	503
What's Next? . . . . .	504

**CHAPTER 25**

<b>Switching</b> . . . . .	<b>505</b>
Traffic Forwarding Basics . . . . .	506
Forwarding Architectures . . . . .	511
Process Switching . . . . .	511
Fast Switching . . . . .	512
Cisco Express Forwarding (CEF) . . . . .	512
Tables Used in Switching . . . . .	515
Review Questions . . . . .	522
Answers to Review Questions . . . . .	522
Further Reading . . . . .	523
What's Next? . . . . .	523

**Part V: Virtualization****CHAPTER 26**

<b>Basic Virtualization</b> . . . . .	<b>525</b>
Virtualization Overview . . . . .	526
Hypervisors . . . . .	527
Virtual Machines (VMs) . . . . .	532
Virtual Switching . . . . .	535
Network Virtualization . . . . .	537
Cisco Enterprise Network Function Virtualization (NFV) . . . . .	537
Cisco Enterprise NFV Architecture . . . . .	538
VNFs Supported in Cisco Enterprise NFV . . . . .	539
Cisco NFV Hardware Options . . . . .	539
Review Questions . . . . .	542
Answers to Review Questions . . . . .	543
Further Reading . . . . .	543
What's Next? . . . . .	543

**CHAPTER 27**

**VRF Instances, GRE, and IPsec . . . . . 545**

- Virtual Routing and Forwarding (VRF) . . . . . 546
  - VRF-Lite . . . . . 547
- Generic Routing Encapsulation (GRE) . . . . . 552
- IPsec VPNs . . . . . 558
  - Site-to-Site VPNs . . . . . 558
  - Dynamic Multipoint VPN (DMVPN) . . . . . 559
  - Cisco IOS Virtual Tunnel Interfaces (VTIs) . . . . . 560
  - Cisco IOS FlexVPN . . . . . 561
  - IP Security (IPsec) . . . . . 562
  - GRE Tunneling over IPsec . . . . . 567
- Review Questions . . . . . 570
  - Answers to Review Questions . . . . . 570
- Further Reading . . . . . 571
- What's Next? . . . . . 571

**CHAPTER 28**

**Extending the Network Virtually . . . . . 573**

- Locator ID/Separation Protocol (LISP) . . . . . 574
  - LISP Architecture . . . . . 577
- Virtual Extensible LAN (VXLAN) . . . . . 580
- Review Questions . . . . . 585
  - Answers to Review Questions . . . . . 585
- Further Reading . . . . . 586
- What's Next? . . . . . 586

**Part VI: Network Assurance**

**CHAPTER 29**

**Troubleshooting . . . . . 587**

- Troubleshooting Overview . . . . . 588
  - Using debug to Analyze Traffic . . . . . 589
  - Troubleshooting with traceroute . . . . . 593
  - Troubleshooting with ping . . . . . 597
- Simple Network Management Protocol (SNMP) . . . . . 604
- Review Questions . . . . . 610
  - Answers to Review Questions . . . . . 610
- Further Reading . . . . . 611
- What's Next? . . . . . 611

**CHAPTER 30**

<b>Monitoring</b> . . . . .	<b>613</b>
Syslog . . . . .	614
NetFlow and Flexible NetFlow . . . . .	620
Switch Port Analyzer (SPAN), Remote SPAN (RSPAN), and Encapsulated Remote SPAN (ERSPAN) . . . . .	632
Remote SPAN (RSPAN) . . . . .	634
Encapsulated Remote SPAN (ERSPAN) . . . . .	635
Review Questions . . . . .	639
Answers to Review Questions . . . . .	640
Further Reading . . . . .	640
What's Next? . . . . .	640

**CHAPTER 31**

<b>IP SLA and DNA Center</b> . . . . .	<b>641</b>
IP SLA Overview . . . . .	642
Cisco DNA Center Assurance . . . . .	652
Review Questions . . . . .	660
Answers to Review Questions . . . . .	660
Further Reading . . . . .	660
What's Next? . . . . .	660

**CHAPTER 32**

<b>NETCONF and RESTCONF</b> . . . . .	<b>661</b>
NETCONF . . . . .	662
RESTCONF . . . . .	668
Review Questions . . . . .	671
Answers to Review Questions . . . . .	671
Further Reading . . . . .	671
What's Next? . . . . .	671

<b>Glossary</b> . . . . .	<b>673</b>
---------------------------	------------

<b>Index</b> . . . . .	<b>695</b>
------------------------	------------

# About the Author

**Donald Bacha** is a systems engineer with a health research organization. He's the technical lead responsible for the design and implementation of networking, compute, virtualization, storage, and disaster recovery systems. Over the past 18 years, Donald has supported cloud services provider, enterprise, and data center environments by contributing to complex routing and switching, data center, storage, and virtualization projects in both greenfield and brownfield deployments. His certifications include CCNP Enterprise, CCNP Data Center, and VCAP-DCV. He holds a master's of business administration. Donald can be found at [www.allthingsvirtual.net](http://www.allthingsvirtual.net) and on Twitter at [@donald\\_bacha](https://twitter.com/donald_bacha).

# Dedication

*First, I dedicate this book to our Lord and Savior Jesus Christ (I can do all things through Christ which strengthens me.—Philippians 4:13). He has blessed me with the opportunity to learn, write, and share my knowledge. To my father and mother, thank you for always supporting and encouraging me.*

# Acknowledgments

A debt of gratitude goes out to executive acquisitions editor James Manly for giving me the opportunity to author this book and for his guidance. A special thank you to my development editor, Ellie Bru, who did well working to get this title out and for making it as strong as it can be. Many thanks go out to Mandie Frank and Kitty Wilson for ensuring that this book looks good and reads easily. I would like to thank the entire Pearson team and those who contributed in one way or another to this project.

# About the Technical Reviewer

**Raymond Lacoste** has dedicated his career to developing the skills of those interested in IT. In 2001, he began to mentor hundreds of IT professionals pursuing their Cisco certification dreams. This role led to teaching Cisco courses full time. Raymond is currently master instructor for Cisco Enterprise Routing and Switching, AWS, and ITIL at StormWind Studios. Raymond treats all technologies as an escape room, working to uncover every mystery in the protocols he works with. Along this journey, Raymond has passed more than 110 exams, and his office wall includes certificates from Microsoft, Cisco, ISC2, ITIL, AWS, and CompTIA. If you were visualizing Raymond's office, you'd probably expect the usual network equipment, certifications, and awards. Those certainly take up space, but they aren't his pride and joy. Most impressive, at least to Raymond, is his gemstone and mineral collection; once he starts talking about it, he just can't stop. Who doesn't get excited by a wondrous barite specimen in a pyrite matrix? Raymond presently resides with his wife and two children in eastern Canada, where they experience many adventures together.

# We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

*Please note that we cannot help you with technical problems related to the topic of this book.*

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: [community@informit.com](mailto:community@informit.com)

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



# Introduction

Welcome to *CCNP and CCIE Enterprise Core ENCOR 350-401 Exam Cram*. This book is a late-stage preparation tool that covers the CCNP/CCIE ENCOR 350-401 certification exam. It provides the information you need to quickly and efficiently go over all the topics covered on the CCNP/CCIE ENCOR 350-401 exam. This *Exam Cram* provides concise and exam-focused coverage of all of the CCNP/CCIE ENCOR 350-401 exam domains and objectives. It allows you to assess your preparedness and helps you to practice through questions and examples of the exam topics. The information you find in this *Exam Cram* will aid you in your success as you build knowledge, gain experience, and review for the CCNP/CCIE ENCOR 350-401 exam.

## About CCNP ENCOR 350-401 Exam Cram

This *Exam Cram* follows a predefined structure that makes the book easy to study as it provides the material in a concise manner. It also allows for the testing of knowledge as you go through each chapter, covering the various ENCOR domains and objectives. This book includes the following helpful elements:

- ▶ **Cram Sheet:** This foldout tear card that appears inside the front cover of the book presents important information that you should go over just before taking the exam. It is the most important “cram” element of the book and, as such, is presented as concisely as possible.
- ▶ **Chapter Topics:** Each chapter begins with a list of the exam objectives that are covered in the chapter as well as a list of the main topics in the chapters. The chapter's topics are then covered in a concise manner, with brief examples and figures where needed.
- ▶ **CramSavers:** Each chapter contains a short-answer quiz that allows you to assess how knowledgeable you are about the topics covered in the chapter. It helps you figure out if you should skip the entire chapter or skim the material and skip ahead to the Exam Alerts and CramQuizzes for particular sections.
- ▶ **Exam Alerts:** These notes provide exam-specific information that is important for you to know before you take the exam. Pay attention to Exam Alerts because the material they cover is likely to appear on the exam.

- ▶ **Cram Quizzes:** Each section of a chapter ends with a handful of multiple-choice questions that test your knowledge of the topics covered in that section. You will find the answers and explanations following each quiz.
- ▶ **Review Questions:** End-of-chapter review questions help you solidify what you have learned related to the topics for a particular chapter.

Chances are you have picked up this book in the early stage of your studies. The *Exam Cram* series was designed for late-stage study. So, unless you are very familiar with the technologies covered in the CCNP/CCIE ENCOR 350-401 exam and have considerable experience configuring and troubleshooting Cisco networks, it is highly recommended that you not use this book as your sole study resource. This *Exam Cram* is recommended for use after core knowledge has been built.

Both Cisco Press and Pearson IT Certification offer a number of CCNP/CCIE study materials to help you learn the core networking technologies covered on the CCNP/CCIE ENCOR 350-401 exam. The following highly recommended resources will help you gain core knowledge of the topics covered on the CCNP/CCIE ENCOR 350-401 exam:

- ▶ ***CCNP and CCIE Enterprise Core 350-401 Official Cert Guide* by Jason Gooley, Ramiro Garza Rios, Bradley Edgeworth, and David Hucaby (ISBN 978-1-58714-523-0):** This official cert guide provides in-depth coverage of the domains and objectives of the CCNP/CCIE ENCOR 350-401 exam.
- ▶ ***CCNP and CCIE Enterprise Core & CCNP Advanced Routing Portable Command Guide* by Patrick Gargano and Scott Empson (ISBN: 978-0-13-576816-7):** This book includes lots of configuration and verification examples to aid you in understanding the IOS commands you will encounter on the ENCOR and ENARSI exams.
- ▶ ***CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide* by Raymond Lacoste and Brad Edgeworth (ISBN 978-1587145254):** I recommend that you read the routing-related chapters of this book (the first set of chapters, which covers EIGRP, OSPF, and BGP) to supplement your Layer 3 core knowledge.

The coauthor, Raymond Lacoste, is also the technical reviewer of this *Exam Cram*.

- ▶ **Cisco Modeling Labs (CML) Personal:** CML Personal (formerly Cisco VIRL) is a powerful network virtualization and orchestration platform you can use to study for Cisco certifications. CML Personal uses real Cisco IOS images and gives you the ability to simulate networks reliably. Both IOSv and IOSvL2 images are included. The majority of the topics that are covered in the CCNP/CCIE ENCOR 350-401 exam can be practiced using CML Personal. CML Personal allows up to 20 concurrent simulated nodes, and CML Personal Plus supports up to 40 concurrent simulated nodes. The majority of the examples in this *Exam Cram* were created using CML Personal. For more information on CML Personal, see <https://developer.cisco.com/docs/modeling-labs>. Cisco CML Personal can be purchased from the Cisco Learning Network Store at <https://learningnetworkstore.cisco.com/cisco-modeling-labs-personal/cisco-cml-personal>.

## About the ENCOR 350-401 Exam

The material in this *Exam Cram* closely follows the official exam domains and objectives to ensure your success on the CCNP/CCIE ENCOR 350-401 exam. To earn the CCNP Enterprise certification, there is no formal prerequisite, although Cisco recommends that you have a good understanding of the exam topics before taking the exams. In addition, Cisco recommends that CCNP candidates have three to five years of experience implementing enterprise networking solutions.

To earn the CCNP Enterprise certification, you have to pass two exams: one required exam that covers core enterprise technologies and one enterprise concentration exam of your choice, based on your technical area of focus. Passing any of these concentration exams also allows you to earn an individual Specialist certification that helps recognize your accomplishments along the way to earning your CCNP Enterprise certification. These are the requirements for earning the CCNP Enterprise certification:

- ▶ Required exam: 350-401: Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)
- ▶ One concentration exam:

- ▶ 300-410: Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)
- ▶ 300-415: Implementing Cisco SD-WAN Solutions (ENSDWI)
- ▶ 300-420: Designing Cisco Enterprise Networks (ENSLD)
- ▶ 300-425: Designing Cisco Enterprise Wireless Networks (ENWLSD)
- ▶ 300-430: Implementing Cisco Enterprise Wireless Networks (ENWLSI)
- ▶ 300-435: Implementing Automation for Cisco Enterprise Solutions (ENAU)

This book focuses on the required 350-401 (ENCOR) exam. It is a 120-minute exam that tests your knowledge of enterprise infrastructure, including dual-stack architecture, virtualization, infrastructure, network assurance, security, and automation. The CCNP/CCIE ENCOR 350-401 exam is also the qualifying exam for the CCIE Enterprise Infrastructure and CCIE Enterprise Wireless certifications. Once you pass the CCNP/CCIE ENCOR 350-401 exam, you are automatically qualified to schedule and take the CCIE lab exam in those tracks.

## Cisco ENCOR 350-401 Exam Topics

Table I-1 lists general exam topics (that is, objectives) and specific topics under each general topic (that is, subobjectives) for the CCNP/CCIE ENCOR 350-401 exam. This table also lists the chapter in which each exam topic is covered.

This *Exam Cram* covers every domain and objective of the CCNP/CCIE ENCOR 350-401 exam. It follows the official exam objectives closely to ensure your success on the CCNP/CCIE ENCOR 350-401 exam. As such, all of the contents, including CramSaver, Cram Quizzes, and Review Questions, map to specific objectives of the CCNP/CCIE ENCOR 350-401 exam. The latest CCNP/CCIE ENCOR 350-401 exam objectives can be found on the Cisco Learning Network at <https://learningnetwork.cisco.com/s/encor-exam-topics>.

TABLE I-1 **ENCOR 350-401 Exam Topics**

Chapter	ENCOR Exam Objectives
	<i>1.0 Architecture</i>
	1.1 Explain the different design principles used in an enterprise network
19: Enterprise Network Design Principles	1.1.a Enterprise network design such as Tier 2, Tier 3, and Fabric Capacity planning
19: Enterprise Network Design Principles	1.1.b High availability techniques such as redundancy, FHRP, and SSO
	1.2 Analyze design principles of a WLAN deployment
20: Wireless LAN Deployments	1.2.1 Wireless deployment models (centralized, distributed, controller-less, controller based, cloud, remote branch)
20: Wireless LAN Deployments	1.2.b Location services in a WLAN design
21: On-Premises vs. Cloud Infrastructure	1.3 Differentiate between on-premises and cloud infrastructure deployments
	1.4 Explain the working principles of the Cisco SD-WAN solution
22: SD-WAN	1.4.a SD-WAN control and data planes elements
22: SD-WAN	1.4.b Traditional WAN and SD-WAN solutions
	1.5 Explain the working principles of the Cisco SD-Access solution
23: SD-Access	1.5.a SD-Access control and data planes elements
23: SD-Access	1.5.b Traditional campus interoperating with SD-Access
	1.6 Describe concepts of wired and wireless QoS
24: QoS	1.6.a QoS components
24: QoS	1.6.b QoS policy
	1.7 Differentiate hardware and software switching mechanisms
25: Switching	1.7.a Process and CEF
25: Switching	1.7.b MAC address table and TCAM
25: Switching	1.7.c FIB vs. RIB
	<i>2.0 Virtualization</i>
	2.1 Describe device virtualization technologies
26: Basic Virtualization	2.1.a Hypervisor type 1 and 2
26: Basic Virtualization	2.1.b Virtual machine
26: Basic Virtualization	2.1.c Virtual switching

<b>Chapter</b>	<b>ENCOR Exam Objectives</b>
	2.2 Configure and verify data path virtualization technologies
27: VRF Instances, GRE, and IPsec	2.2.a VRF
27: VRF Instances, GRE, and IPsec	2.2.b GRE and IPsec tunneling
	2.3 Describe network virtualization concepts
28: Extending the Network Virtually	2.3.a LISP
28: Extending the Network Virtually	2.3.b VXLAN
	<i>3.0 Infrastructure</i>
	3.1 Layer 2
1: Understanding Layer 2	3.1.a Troubleshoot static and dynamic 802.1q trunking protocols
1: Understanding Layer 2	3.1.b Troubleshoot static and dynamic EtherChannels
1: Understanding Layer 2	3.1.c Configure and verify common Spanning Tree Protocols (RSTP and MST)
	3.2 Layer 3
2: Understanding Layer 3: IGPs	3.2.a Compare routing concepts of EIGRP and OSPF (advanced distance vector vs. link state, load balancing, path selection, path operations, metrics)
2: Understanding Layer 3: IGPs	3.2.b Configure and verify simple OSPF environments, including multiple normal areas, summarization, and filtering (neighbor adjacency, point-to-point and broadcast network types, and passive interface)
3: Understanding Layer 3: BGP	3.2.c Configure and verify eBGP between directly connected neighbors (best path selection algorithm and neighbor relationships)
	3.3 Wireless
5: Enterprise Wireless	3.3.a Describe Layer 1 concepts, such as RF power, RSSI, SNR, interference noise, band and channels, wireless client devices capabilities
5: Enterprise Wireless	3.3.b Describe AP modes and antenna types
5: Enterprise Wireless	3.3.c Describe access point discovery and join process (discovery algorithms, WLC selection process)
5: Enterprise Wireless	3.3.d Describe the main principles and use cases for Layer 2 and Layer 3 roaming

<b>Chapter</b>	<b>ENCOR Exam Objectives</b>
5: Enterprise Wireless	3.3.e Troubleshoot WLAN configuration and wireless client connectivity issues
	3.4 IP Services
4: IP Services	3.4.a Describe Network Time Protocol (NTP)
4: IP Services	3.4.b Configure and verify NAT/PAT
4: IP Services	2.4.c Configure first hop redundancy protocols, such as HSRP and VRRP
4: IP Services	3.4.d Describe multicast protocols, such as PIM and IGMP v2/v3
	<i>4.0 Network Assurance</i>
29: Troubleshooting	4.1 Diagnose network problems using tools such as debugs, conditional debugs, trace route, ping, SNMP, and syslog
30: Monitoring	4.2 Configure and verify device monitoring using syslog for remote logging
30: Monitoring	4.3 Configure and verify NetFlow and Flexible NetFlow
30: Monitoring	4.4 Configure and verify SPAN/RSPAN/ERSPAN
31: IP SLA and DNA Center	4.5 Configure and verify IPSLA
31: IP SLA and DNA Center	4.6 Describe Cisco DNA Center workflows to apply network configuration, monitoring, and management
32: NETCONF and RESTCONF	4.7 Configure and verify NETCONF and RESTCONF
	<i>5.0 Security</i>
	5.1 Configure and verify device access control
6: Device Access Control	5.1.a Lines and password protection
6: Device Access Control	5.1.b Authentication and authorization using AAA
	5.2 Configure and verify infrastructure security features
7: Infrastructure Security	5.2.a ACLs
7: Infrastructure Security	5.2.b CoPP
8: Securing REST APIs	5.3 Describe REST API security
	5.4 Configure and verify wireless security features
9: Wireless Security	5.4.a EAP
9: Wireless Security	5.4.b WebAuth
9: Wireless Security	5.4.c PSK
	5.5 Describe the components of network security design

Chapter	ENCOR Exam Objectives
10: Network Security Design	5.5.a Threat defense
10: Network Security Design	5.5.b Endpoint security
10: Network Security Design	5.5.c Next-generation firewall
10: Network Security Design	5.5.d TrustSec, MACsec
11: Network Access Control	5.5.e Network access control with 802.1X, MAB, and WebAuth
	6.0 Automation
12: Anatomy of Python	6.1 Interpret basic Python components and scripts
13: Building JSON Files	6.2 Construct valid JSON encoded file
14: YANG Data Modeling	6.3 Describe the high-level principles and benefits of a data modeling language, such as YANG
15: DNA Center and vManage APIs	6.4 Describe APIs for Cisco DNA Center and vManage
16: Interpreting REST API Codes	6.5 Interpret REST API response codes and results in payload using Cisco DNA Center and RESTCONF
17: EEM Applets	6.6 Construct EEM applet to automate configuration, troubleshoot, or data collection
18: Configuration Management and Orchestration	6.7 Compare agent vs. agentless orchestration tools, such as Chef, Puppet, Ansible, and SaltStack

## Booking and Taking the ENCOR 350-401 Exam

Because this *Exam Cram* is a late-stage study material, by the time you are reading it, you have probably already registered to take the CCNP/CCIE ENCOR 350-401 exam. If not, my recommendation is that you go ahead and register and use that registration as motivation to prepare for the exam. If you find yourself not feeling fully prepared, or if some other circumstance comes up before the exam, you can cancel your registration. Pearson Vue allows you to cancel your registration up until 24 hours before you are scheduled to take the exam without a penalty.

At this writing, Pearson Vue allows you to take the exam at one of its testing sites or from home using the OnVUE online proctoring system, where a live proctor monitors you through the webcam of your computer. If you are using the online



proctoring system, you should run the system test and exam simulation before registering. You can register online at <https://home.pearsonvue.com/cisco>, over the phone, or as a Pearson Vue walk-in, where available. In the United States and Canada, you can schedule your exam up to six weeks in advance, and you must wait five calendar days from the end of your first attempt before retaking the same exam. Hopefully, with the help of this *Exam Cram* and the other recommended resources, you will not have to worry about that!

To register for the exam, you need the following information:

- ▶ Legal name (from a government-issued ID)
- ▶ Cisco certification ID (for example, CSC000000001) or test ID number
- ▶ Valid email address
- ▶ Method of payment

At this writing, the cost of the CCNP/CCIE ENCOR 350-401 exam is US\$400.

## What to Expect from the Exam

If you haven't taken a certification test, the process can be a little unnerving. Even if you've taken numerous tests, it is not much better. Mastering the inner mental game often can be as much of a battle as knowing the material. Knowing what to expect before heading in can make the process a little more comfortable.

Certification tests are administered on a computer system at a VUE authorized testing center. The format of the exams is straightforward: Each question has several possible answers to choose from. The questions in this book provide a good example of the types of questions you can expect on the exam. If you are comfortable with them, the test should hold few surprises.

As you take the CCNP/CCIE ENCOR 350-401 exam, be sure to review each answer before moving on to the next question. After you answer a question, you cannot go back at a later time to make changes.

You can expect to see several types of questions on the ENCOR exam:

- ▶ **Multiple-choice, single answer:** This type of question requires you to choose only one answer for a question. Once you select the radio button for your answer, click Next to move on to another question.
- ▶ **Multiple-choice, multiple answers:** This type of question shows you how many answers you need to select. To select the answers, you click the

small squares next to the answers of your choice to insert checkmarks. Once you choose the correct number of questions, you can click Next to move on to the next question.

- ▶ **Drag and drop:** This type of question requires you to select an option on the left and drag and drop it to its appropriate drop zone on the right. Sometimes only some of the options on the left are used.
- ▶ **Fill-in-the-blank:** This type of question requires you to insert your answer in a text box. Sometimes you may have to fill in multiple text boxes.
- ▶ **Testlet:** This type of question is scenario based. It involves reading a scenario and then answering the question(s) related to the scenario. Testlet questions are typically some variation of multiple-choice questions.

Cisco has published two exam tutorial videos that provide a walk-through demonstration on the various exam question types and how they function. You can find these short videos at <https://learningnetwork.cisco.com/s/certification-exam-tutorials>.

## A Few Exam-Day Details

It is recommended that you arrive at the examination room at least 15 minutes early, although a few minutes earlier certainly would not hurt. This will give you time to prepare and will give the test administrator time to answer any questions you might have before the test begins. Many people suggest that you review the most critical information about the test you're taking just before the test. (Exam Cram books provide a reference—the Cram Sheet, located inside the front of this book—that lists the essential information from the book in distilled form.) Arriving a few minutes early will give you some time to compose yourself and mentally review this critical information.

You will be asked to provide two forms of ID, one of which must be a photo ID. Both of the forms of ID you choose should have signatures. You also might need to sign in when you arrive and sign out when you leave.

Be warned: The rules are clear about what you can and cannot take into the examination room. Books, laptops, note sheets, and so on are not allowed in the examination room. The test administrator will hold these items, to be returned after you complete the exam. You might receive either a wipe board or a pen and a single piece of paper for making notes during the exam. The test administrator will ensure that no paper is removed from the examination room.

## After the Test

Whether you want it or not, as soon as you finish your test, your score displays on the computer screen. In addition to the results appearing on the computer screen, a hard copy of the report prints for you. Like the onscreen report, the hard copy displays the results of your exam and provides a summary of how you did on each section and on each technology. If you were unsuccessful, this summary can help you determine the areas you need to brush up on. After you have taken the CCNP/CCIE ENCOR 350-401 exam, please note the following:

- ▶ Every written proctored exam passed equals a Specialist certification.
- ▶ Within 24 hours of passing your certifying exam, you will receive an email advising you on the next steps. You must complete the steps to trigger the fulfillment process.
- ▶ The Cisco Certification Tracking System records exam and certification status. Be sure to keep your contact information up to date if you want to receive notifications.
- ▶ After you're certified, you will be authorized to use the Cisco Certification logo that identifies your status, provided that you read and acknowledge the Cisco Certifications Logo Agreement. You can download logos through the Certifications Tracking System.
- ▶ Visit the Certification and Fulfillment Benefits page to learn more about the certification fulfillment process and the benefits you'll receive.

## Last-Minute Exam Tips

Studying for a certification exam is no different than studying for any other exam, but a few hints and tips can give you the edge on exam day:

- ▶ **Read all the material:** Read each question carefully and entirely before answering.
- ▶ **Watch for the Exam Alerts:** The CCNP/CCIE ENCOR 350-401 exam objectives include a wide range of technologies. Exam Alerts found throughout each chapter of this book are designed to highlight exam-related hot spots. Skim the book for Exam Alerts when preparing for the exam.
- ▶ **Use the questions to assess your knowledge:** Don't just read the chapter content; use the CramSaver questions to find out what you know and what you don't. If you struggle to answer any of these questions, read the entire chapter, including Exam Alerts, and complete the Cram Quiz

at the end of each section and the Review Questions at the end of the chapter.

- ▶ **Review the exam objectives:** Develop your own questions and examples for each topic listed. If you can develop and answer several questions for each topic, you should not find it difficult to pass the exam.

Good luck with your CCNP/CCIE ENCOR 350-401 exam studies, and thank you for selecting the *CCNP and CCIE Enterprise Core ENCOR 350-401 Exam Cram*.

## Companion Website

Register this book to get access to the Pearson Test Prep practice test software and other study materials plus additional bonus content. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exams. Be sure to check the box that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access this companion website, follow these steps:

1. Go to **[www.pearsonITcertification.com/register](http://www.pearsonITcertification.com/register)** and log in or create a new account.
2. Enter the ISBN **9780136891932**.
3. Answer the challenge question as proof of purchase.
4. Click the **Access Bonus Content** link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

Please note that many of our companion content files, especially image and video files, can be very large.

If you are unable to locate the files for this title by following these steps, please visit [www.pearsonITcertification.com/contact](http://www.pearsonITcertification.com/contact) and select the Site Problems/Comments option. Our customer service representatives will assist you.

## Pearson Test Prep Practice Test Software

This book comes complete with the Pearson Test Prep practice test software, containing two full exams. These practice tests are available to you either online or in an offline Windows application. To access the practice exams that

were developed with this book, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep practice test software.

### Note

The cardboard sleeve in the back of this book includes a piece of paper. The paper lists the activation code for the practice exams associated with this book. Do not lose the activation code. On the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

## Accessing the Pearson Test Prep Software Online

The online version of this software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, simply follow these steps:

1. Go to <http://www.PearsonTestPrep.com>.
2. Select **Pearson IT Certification** as your product group.
3. Enter your email and password for your account. If you don't have an account on [PearsonITCertification.com](http://PearsonITCertification.com) or [CiscoPress.com](http://CiscoPress.com), you need to establish one by going to [PearsonITCertification.com/join](http://PearsonITCertification.com/join).
4. In the **My Products** tab, click the **Activate New Product** button.
5. Enter the access code printed on the insert card in the back of your book to activate your product. The product is then listed in your My Products page.
6. Click the Exams button to launch the exam settings screen and start the exam.

## Accessing the Pearson Test Prep Software Offline

If you wish to study offline, you can download and install the Windows version of the Pearson Test Prep software. You can find a download link for this software on the book's companion website, or you can just enter this link in your browser:

<http://www.pearsonitcertification.com/content/downloads/pcpt/engine.zip>

To access the book's companion website and the software, simply follow these steps:

1. Register your book by going to [PearsonITCertification.com/register](http://PearsonITCertification.com/register) and entering the ISBN **9780136891932**.
2. Respond to the challenge questions.
3. Go to your account page and select the **Registered Products** tab.
4. Click on the **Access Bonus Content** link under the product listing.
5. Click the **Install Pearson Test Prep Desktop Version** link in the Practice Exams section of the page to download the software.
6. When the software finishes downloading, unzip all the files onto your computer.
7. Double-click the application file to start the installation, and follow the onscreen instructions to complete the registration.
8. When the installation is complete, launch the application and click the **Activate Exam** button on the My Products tab.
9. Click the **Activate a Product** button in the Activate Product Wizard.
10. Enter the unique access code from the card in the sleeve in the back of your book and click the **Activate** button.
11. Click **Next** and then click the **Finish** button to download the exam data to your application.
12. You can now start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam.

Note that the offline and online versions sync together, so saved exams and grade results recorded on one version will be available to you in the other version as well.

## Customizing Your Exams

When you are in the exam settings screen, you can choose to take exams in one of three modes:

- ▶ Study mode
- ▶ Practice Exam mode
- ▶ Flash Card mode

Study mode allows you to fully customize an exam and review answers as you are taking the exam. This is typically the mode you use first to assess your knowledge and identify information gaps. Practice Exam mode locks certain customization options in order to present a realistic exam experience. Use this mode when you are preparing to test your exam readiness. Flash Card mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation, when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes provide, so it is not the best mode for helping you identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The two exams printed in the book are available to you, as are two additional exams of unique questions. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

You can make several other customizations to your exam from the exam settings screen, such as the time of the exam, the number of questions, whether to randomize questions and answers, whether to show the number of correct answers for multiple answer questions, or whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

## Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if there are any updates to your exam data and automatically download any changes made since the last time you used the software. This requires you to be connected to the Internet at the time you launch the software.

Sometimes, due to a number of factors, the exam data might not fully download when you activate your exam. If you find that figures or exhibits are missing, you might need to manually update your exams.

To update a particular exam you have already activated and downloaded, simply select the **Tools** tab and click the **Update Products** button. Again, this is only an issue with the desktop Windows application.

If you want to check for updates to the Windows desktop version of the Pearson Test Prep exam engine software, simply select the **Tools** tab and click the **Update Application** button. Doing so allows you to ensure that you are running the latest version of the software engine.

## Assessing Exam Readiness

Exam candidates never really know whether they are adequately prepared for the exam until they have completed about 30% of the questions. At that point, if you are not prepared, it is too late. The best way to determine your readiness is to work through the CramSaver quiz at the beginning of each chapter and review the topics presented in each chapter. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

## Premium Edition eBook and Practice Tests

This book includes an exclusive offer for 70% off the Premium Edition eBook and Practice Tests edition of this title. Please see the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.



## CHAPTER 6

# Device Access Control

**This chapter covers the following official ENCOR 350-401 exam objectives:**

- ▶ 5.1 Configure and verify devices access control
- ▶ 5.1.a Lines and password protection
- ▶ 5.1.b Authentication and authorization using AAA

This chapter is divided into two sections. The first section looks at the configuration and verification of network device access control with usernames and passwords. It also covers the configuration and verification of role-based access control (RBAC) using privilege levels. The second section covers authentication, authorization, and accounting (AAA). It looks at the configuration and verification of network device access control on Cisco IOS devices using TACACS+ and RADIUS.

**This chapter covers the following technology topics:**

- ▶ Cisco IOS CLI Session Overview
  - ▶ Protection of Access to Cisco IOS EXEC Modes
  - ▶ Secured Access with SSH
  - ▶ Privilege Levels and Role-Based Access Control (RBAC)
- ▶ Authentication, Authorization, and Accounting (AAA) Overview
  - ▶ TACACS+ Overview
  - ▶ RADIUS Overview
  - ▶ AAA Configuration for Network Devices

## CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the CramQuiz at the end of each section and the Review Questions at the end of the chapter. If you are in doubt at all, read everything in this chapter!

1. What are the first steps in securing user EXEC access to allow for secure network device access?
2. Which command option on remote CLI sessions is used to limit the session to use only a secure connection method?
3. What protocol does TACACS+ use for communication between a TACACS+ client (network device) and a TACACS+ server?
4. What are two of the high-level benefits of using a remote AAA server over local AAA services on each network device individually?

## Answers

1. Configure passwords for local and remote CLI sessions.
2. **transport input ssh**
3. TCP port 49
4. Scalability and standardized authentication methods using RADIUS and TACACS+

# Cisco IOS CLI Session Overview

Cisco IOS software provides several features that you can use to implement basic security for network devices' command-line sessions. These features include:

- ▶ Using different levels of authorization for CLI sessions to control access to commands that can modify the status of the networking device and for commands that are used to monitor the device
- ▶ Assigning passwords to CLI sessions
- ▶ Requiring users to log in to a networking device with a username
- ▶ Changing the privilege levels of commands to create new authorization levels for CLI sessions

You can establish IOS CLI sessions on Cisco IOS devices in two ways:

- ▶ **Local CLI sessions:** Local CLI sessions require direct access to the console port of the networking device. Local CLI sessions start in user EXEC mode. All of the tasks needed to configure and manage a networking device can be done using a local CLI session. The most common method for establishing a local CLI session is to connect a laptop to the console port of the networking device and then launch a terminal emulation application, like Putty, on the computer. The type of cable and connectors required and the settings for the terminal emulation application depend on the type of networking device that you are configuring. Some devices have an auxiliary (aux) port for remote administration through a dial-up modem. In most cases, this should be disabled with the **no exec** command under **line aux 0**.
- ▶ **Terminal lines and remote CLI sessions:** A remote CLI session is created between a host and a networking device by using a remote terminal access application, such as Telnet or SSH. Most of the tasks required to configure and manage a networking device can be done using a remote CLI session. The exceptions are tasks that interact directly with the console port (such as recovering from a corrupted operating system by uploading a new OS image over the console port) and interacting with the networking device when it is in ROMMON mode. SSH is a more secure alternative to Telnet. SSH provides encryption for the session traffic between the local management device and the networking device you are managing. Encrypting the session traffic with SSH prevents anyone who may have intercepted the traffic from decoding it.

With Cisco IOS networking devices, the word “lines” is used to refer to the software components that manage local and remote CLI sessions. You use the **line console 0** global configuration command to enter line configuration mode to configure options such as a password for the console port. Remote CLI sessions use lines that are referred to as vty lines. You use the **line vty *line-number* [*ending-line-number*]** global configuration command to enter line configuration mode to configure options such as a password for remote CLI sessions. Once you are in the line configuration mode, you can set the protocol you will be connecting over (for example, SSH).

Example 6.1 shows the console, auxiliary, and vty lines in the running configuration that are available on R1.

**EXAMPLE 6.1 Console, Auxiliary, and vty Lines in the Running Configuration**

```
R1#  
R1# show running-config | section line  
line con 0  
line aux 0  
line vty 0 4  
R1#
```

---

Before we look at how to protect access to Cisco IOS EXEC modes, let's take a look at the five different types of passwords available in Cisco IOS:

- ▶ **Type 0 passwords:** Type 0 passwords are not encrypted and are stored in plaintext in the device configuration. The **enable password** command uses type 0 passwords. Type 0 passwords should not be used in a production environment.
- ▶ **Type 5 passwords:** Type 5 passwords use an MD5 hashing algorithm. These passwords are easily reversible with tools available on the Internet. The **enable secret** and **username *username* secret** commands use type 5 passwords.
- ▶ **Type 7 passwords:** Type 7 passwords uses the Vigenère cipher encryption algorithm, which is known to be weak. These passwords are easily reversible (in under 1 second) with tools available on the Internet. Type 7 password encryption is enabled with the **service password encryption** command.
- ▶ **Type 8 passwords:** Type 8 passwords use a Password-Based Key Derivation Function 2 (PBKDF2) with a SHA-256 hashed secret. Type 8 password security is considered good.
- ▶ **Type 9 passwords:** Type 9 passwords use the SCRYPT hashing algorithm. Type 9 passwords are considered the best passwords and should be used when supported.

Type 4 passwords were deprecated in IOS 15.3(3). The type 4 password hash was weaker than the type 5 (MD5) hash. Therefore, type 4 passwords should never be used. IOS 15.3(3) introduced support for type 8 and type 9 passwords, and these password types should always be used when supported.

# Protection of Access to Cisco IOS EXEC Modes

This section looks at the steps you can take to secure both user and privileged EXEC modes.

The first step in creating secure network device access is to protect the user EXEC mode by configuring passwords for local and remote CLI sessions. You start by entering line configuration mode by selecting the line number for the console port (for example, **line console 0**). Once you are in that mode, you use the **password** command to assign a password to **line console 0**. You use the **login** command at **line console 0** to enable password checking at login.

Next, let's look at configuring a password for remote CLI sessions. After a password is configured for remote CLI sessions, the IOS device prompts for a password the next time you establish a remote CLI session with that device. Cisco IOS networking devices require that a password be configured for remote CLI sessions. If you attempt to start a remote CLI session with a device that does not have a password configured for remote CLI sessions, you get a message indicating that a password is required and that the password is not set. The remote CLI session will be terminated by the remote host.

To configure a password for remote CLI sessions, you start by entering the line configuration mode and selecting the vty line (for example, **line vty 0 4**). When you are in that mode, you use the **password** command as you do for the console line. You use the **login** command at the vty line to enable password checking at login.

Example 6.2 shows how to assign a password to the console, auxiliary, and vty lines and verify it in the running configuration.

---

## EXAMPLE 6.2 Configuring and Verifying Line Passwords

```
R1#  
R1# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)# line con 0  
R1(config-line)# password Cisco123  
R1(config-line)# login  
R1(config-line)# line aux 0  
R1(config-line)# password Cisco123  
R1(config-line)# login  
R1(config-line)# line vty 0 4
```

```
R1 (config-line)# password Cisco123
R1 (config-line)# login
R1 (config-line)# end
R1#
R1# show running-config | section line
line con 0
  password Cisco123
  login
line aux 0
  password Cisco123
  login
line vty 0 4
  password Cisco123
  login
R1#
```

---

The previous section covers protection of access to both local and remote CLI sessions in user EXEC mode using line passwords. Now let's look at how to protect access to privileged EXEC mode. To add an additional layer of security, particularly for passwords that cross a network or that are stored with the configuration on a TFTP server, you can use the **enable secret** global configuration command.

Cisco recommends the use of the **enable secret** command over the **enable password** command because it uses an improved encryption algorithm. When you configure the **enable secret** command, it takes precedence over the **enable password** command. The two commands cannot be in effect simultaneously.

Let's look at the use of the **enable password** command to configure a password for privileged EXEC mode. The password you enter with the **enable password** command is stored as plaintext in the device's running configuration. You can encrypt the password for the **enable password** command in the configuration file of the networking device by using the **service password-encryption** command. However, the type 7 encryption level used by the **service password-encryption** command can be decrypted using tools available on the Internet, so it is not recommended for production deployments. The recommendation is to use the **enable secret** command because it provides strong encryption by hashing the password using type 5 passwords by default. However, on modern platforms, you can use type 8 or 9 passwords as well. You configure a password in privileged EXEC mode by using the command **enable secret [level level] unencrypted-password | encryption-type encrypted-password**. You can use the **show privilege** command to display the current level of privilege.

Example 6.3 shows the configuration and verification of protection of privileged EXEC mode using the **enable password** command. Note in the

verification that the password is stored in the running configuration in plaintext. This is because the default password, of type 0, was used. You can also set a type 7 password or set the EXEC level here. The command **service password-encryption** would make the password unreadable in the running configuration.

---

#### EXAMPLE 6.3 Protecting Privileged EXEC with enable password

---

```
R1#
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# enable password ?
  0 Specifies an UNENCRYPTED password will follow
  7 Specifies a HIDDEN password will follow
  LINE The UNENCRYPTED (cleartext) 'enable' password
  level Set exec level password

R1(config)# enable password ExamCram123
WARNING: Command has been added to the configuration using a type 0
password. However, type 0 passwords will soon be deprecated. Migrate
to a supported password type
R1(config)#
*Oct 28 23:00:00.922: %AAAA-4-CLI_DEPRECATED: WARNING: Command has
been added to the configuration using a type 0 password. However, type
0 passwords will soon be deprecated. Migrate to a supported password
type

R1(config)# do show run | include password
enable password ExamCram123
R1(config)#
R1(config)# service password-encryption
R1(config)# do show run | include password
enable password 7 106B11180834000A01557878
R1(config)# end
R1#
```

---

Example 6.4 shows the configuration and verification of protection of privileged EXEC mode using the **enable secret** command. This provides stronger encryption and is the recommended method to use. This example uses type 9 encryption. When using type 9, you need to type in the encrypted password or use the **algorithm-type** command to hash a plaintext **enable** secret. Note that the verification output shows the encrypted type 9 password.

---

#### EXAMPLE 6.4 Protecting Privileged EXEC with enable secret

---

```
R1#
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```

R1(config)# enable ?
  algorithm-type  Algorithm to use for hashing the plaintext 'enable'
secret
  password       Assign the privileged level password (MAX of 25
                  characters)
  secret         Assign the privileged level secret (MAX of 25
                  characters)

R1(config)# enable algorithm-type scrypt secret ?
  LINE          The UNENCRYPTED (cleartext) 'enable' secret
  level        Set exec level password

R1(config)# enable algorithm-type scrypt secret ExamCram123
R1(config)# do sho run | include secret
enable secret 9 $9$QlfhhreZrBM56f$VX4YG.yR/jHO/3gLFfTPqAw.
cdraNRDSKJoEotCrC3Q
R1(config)# end
R1#

```

---

After you have protected access to user EXEC mode and privileged EXEC mode by configuring passwords for them, you can further increase the level of security on the device by creating usernames. You configure usernames to limit access to CLI sessions to a networking device to specific users. This is especially important if you are configuring a device to allow first-line technical support user access. These users typically would not need to run all commands available in privileged EXEC mode. For example, suppose you want technical support staff to be able to view the configuration on a device that will help them to troubleshoot network problems without being able to modify the configuration. In this case, you can create a username, configure it with privilege level 15, and configure it to run the **show running-config** command automatically. When a user logs in with the username, the running configuration will be displayed automatically.

There are three ways you can configure a username on a Cisco IOS device:

- ▶ Using the command **username *username* password *password*** configures a plaintext password (type 0).
- ▶ Using the command **username *username* secret *password*** provides type 5 encryption.
- ▶ Using the command **username *username* algorithm-type [md5 | sha256 | scrypt] secret *password*** provides type 5, type 8, or type 9 encryption, respectively.



The last option provides the highest level of security since it allows for the highest level of password encryption (type 8 or type 9). If the final option is not supported on a network device, then the second option should be used since it provides MD5 encryption. The first option should be avoided because it configures a plaintext password.

When you enable password authentication on a line by using the **password** command, you need to enable password checking. You do so by using the **login** command. This is what allows password use on the line. Once you have an alternate connection to the device, you can test the login. It is a good idea to have an alternate connection to a device if there is a problem logging in again using the line you made the changes on. The **login local** command allows for username/password pairs stored locally on the router to be used for the lines. By using the command **login local**, you can disable any password configured on lines.

To enable username and password authentication on a line, you need to do the following configuration:

- ▶ Create the user with the **username** command in global configuration mode, using one of the three options listed earlier in this section.
- ▶ Use the **login local** command in line configuration mode.

For remote CLI sessions, you can further protect the lines by using the **transport input** command. This command controls what protocols are allowed to access the vty lines. This can be configured with the command **transport input {all | none | telnet | ssh}**. The **all** option allows both Telnet and SSH access; **none** blocks Telnet and SSH; **telnet** allows only Telnet; and **ssh** allows only SSH access. Using **telnet ssh** allows both Telnet and SSH access. For the most secure access, the vty lines should be limited to SSH.

Example 6.5 shows the configuration and verification of usernames. The user **user1** is configured with a type 0 password, **admin1** is configured with a type 9 password, **tier1admin** is configured with a type 9 password (scrypt in this case), and **tier2admin** is configured with a type 8 password (sha256 in this case). The **login local** command is configured under the vty lines to tell it to use the router local user account database for authentication.

In this example, take note of the configured user accounts and the password types. **user1** with the type 0 password is shown in running configuration in plaintext. Privilege level 15 gives access to all commands, such as the **reload** command, and allows a user to make configuration changes on the device.

**EXAMPLE 6.5 Configuring Usernames and Passwords**


---

```

R1#
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# username user1 password weakpassword
WARNING: Command has been added to the configuration using a type 0
password. However, type 0 passwords will soon be deprecated. Migrate
to a supported password type
R1(config)# username admin1 privilege 15 secret admin1secret
R1(config)# username tier1admin algorithm-type scrypt secret
tier1adminsecret
R1(config)# username tier2admin algorithm-type sha256 secret
tier2adminsecret
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# end
R1#
R1# show running-config | include username
username user1 password 0 weakpassword
username admin1 privilege 15 secret 9 $9$iVS2wE3FxxTvDv$6k.
NoCSCi2af4T8HpWeO11BaTUnJze1T8S6xEETp7AI
username tier1admin secret 9 $9$bIFEJkC8eW9Xyf$vXBZD.8ZSiHTcjpNVfuMWwX
vveegKfHCfNXgLZUYA9w
username tier2admin secret 8 $8$PLF4/9DTLkfoTf$820AEmeaZA2mNh1oNJjAYk6
bYKSlLhUn9pULnifodyo
R1#

```

---

Example 6.6 shows how to establish a Telnet session from R2 to R1 by using username-based authentication with the **tier1admin** username and type 9 password created earlier. You can see here that you can successfully connect and authenticate by using the **tier1admin** account.

**EXAMPLE 6.6 Verifying Username-Based Authentication for vty Lines**


---

```

R2#
R2# telnet 100.1.1.1
Trying 100.1.1.1 ... Open

User Access Verification

Username: tier1admin
Password:

! Password entered is not displayed by the router
R1>
R1#

```

```
R1# show line
```

Tty	Typ	Tx/Rx	A	Modem	Roty	AccO	AccI	Uses	Noise	Overruns	Int
*	0	CTY	-	-	-	-	-	0	0	0/0	-
	1	AUX	9600/9600	-	-	-	-	0	0	0/0	-
*	578	VTY	-	-	-	-	-	2	0	0/0	-
	579	VTY	-	-	-	-	-	0	0	0/0	-
	580	VTY	-	-	-	-	-	0	0	0/0	-
	581	VTY	-	-	-	-	-	0	0	0/0	-
	582	VTY	-	-	-	-	-	0	0	0/0	-

```
Line(s) not in async mode -or- with no hardware support:
```

```
2-577
```

```
! the * in the output of the showline command indicates that the first vty (0) is in use
```

```
! vty 0 is mapped to vty 578 automatically
```

```
R1#
```

### ExamAlert

For the ENCOR exam, it is important to know the differences between the two SSH versions as well as the high-level steps for SSH configuration on Cisco devices.

## Secured Access with SSH

SSH is a far more secure option than Telnet. Although Telnet is the most popular protocol used to access Cisco IOS devices, it is an insecure protocol. Its session packets are carried in plaintext, making it easy for someone to sniff and capture session information as it traverses the network. SSH provides encryption for session traffic between a device and a terminal access application. This prevents others from being able to intercept and decode the traffic.

SSH is available in two versions:

- ▶ **SSH Version 1 (SSHv1):** SSHv1 should be avoided because there are some flaws in its implementation, including its weak CRC-32 integrity check.
- ▶ **SSH Version 2 (SSHv2):** SSHv2 should be used when it is supported. The SSHv2 enhancement for RSA supports RSA-based public key authentication for a client and a network device. SSHv2 is not compatible with SSHv1.

Let us now take a look at the steps that are needed to set up a Cisco IOS device to run SSH:

1. Configure a hostname for the device, using the **hostname** *hostname* command.
2. Configure a domain name for the device, using the **ip domain-name** *domain-name* command.
3. Generate an RSA crypto key. Generating a key pair on the IOS device automatically enables SSH. When you generate an RSA key, you are prompted to enter a modulus length. A longer modulus length takes longer to generate, but it is more secure. You generate an RSA key with the **crypto key generate rsa** command.

Those three steps are mandatory. After you have taken those steps, you may need to set SSH to Version 2 because it is at SSHv1 by default on some platforms. You do this with the **ip ssh version 2** command. The other settings you can configure for the SSH service running on a device are the SSH timeout value and the authentication retries number. You do so with the command **ip ssh timeout** *seconds* **authentication-retries** *number*. Next, you set the transport input at the vty lines by using the **transport input ssh** command. Finally, also at the vty lines, you use the **login local** command to cause the local username and password on the router to be used for authentication.

For verification, you can use the **show ip ssh** command to view the version and configuration information for the SSH server. We can also use the **show ssh** command to show the status of the SSH server.

Example 6.7 demonstrates how to configure SSH, secure the vty lines to allow only SSH access, and verify connectivity from R2 to R1.

#### EXAMPLE 6.7 Configuring and Verifying vty Access with SSH

---

```
R1#  
R1# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)# username admin2 secret Cisco123  
R1(config)# ip domain-name cisco.com  
R1(config)# crypto key generate rsa  
The name for the keys will be: R1.cisco.com  
Choose the size of the key modulus in the range of 360 to 4096 for  
your General Purpose Keys. Choosing a key modulus greater than 512 may  
take a few minutes.
```

```
How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)
```

```
R1(config)# ip ssh version 2
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# end
R1#
```

```
R2# ssh ?
-c      Select encryption algorithm
-l      Log in using this user name
-m      Select HMAC algorithm
-o      Specify options
-p      Connect to this port
-v      Specify SSH Protocol Version
-vrf    Specify vrf name
WORD    IP address or hostname of a remote system
```

```
R2# ssh -l admin2 -v 2 100.1.1.1
```

```
Password:
! Password entered is not displayed by the router
```

```
R1>
```

---

Finally, you can set a timeout for EXEC sessions that are left idle, which may pose a security risk. Under the line confirmation mode, you can use the **exec-timeout** *minutes seconds* command to set the timeout. The default setting is 10 minutes. Using **exec-timeout 0 0** and **no exec-timeout** disables the EXEC timeout. You should not use these commands this way in a production environment.

The **absolute-timeout** *minutes* command in the line configuration mode sets the interval for closing the EXEC session after a specified time has elapsed. This session is closed even if it is being used at the time of termination. You can use the **logout-warning** *seconds* command with the **absolute-timeout** command to notify users of an impending logout. By default, the user is given 20 seconds' notice before the session is terminated.

Example 6.8 shows how to configure EXEC and absolute timeouts and logout warning. For **line con 0**, a timeout value of 4 minutes is configured. For the vty lines, a value of 3 minutes and 30 seconds is configured. For the vty lines,

an absolute timeout of 10 minutes is configured, with a 120-second logout warning.

#### EXAMPLE 6.8 Configuring EXEC and Absolute Timeouts

---

```
R1#
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# line con 0
R1(config-line)# exec-timeout 4 0
R1(config-line)# line vty 0 4
R1(config-line)# exec-timeout 3 30
!next we configure absolute timeout and logout warning
R1(config-line)# absolute-timeout 10
!logout warning is configured in seconds
R1(config-line)# logout-warning 120
R1(config-line)# end
R1#
```

---

## Privilege Levels and Role-Based Access Control (RBAC)

Now that we have examined the various ways of securing user and privileged EXEC modes, let's take a look at the use of privilege levels and RBAC. By default, Cisco IOS devices have three privilege levels:

- ▶ **Privilege level 0:** Privilege level 0 allows for the use of five commands: **enable**, **disable**, **help**, **logout**, and **exit**.
- ▶ **Privilege level 1:** Privilege level 1 is the user EXEC mode that you saw configured earlier in this chapter, in the section “Protection of Access to Cisco IOS EXEC Modes.” In this mode, it is not possible to make configuration changes.
- ▶ **Privilege level 15:** Privilege level 15 is the privileged EXEC mode you saw configured earlier in this chapter, in Example 6.5. (It is also configured in the next example.) In this mode, all of the IOS CLI commands are available.

The commands that you can run in user EXEC mode at privilege level 1 are a subset of the commands that you can run in privileged EXEC mode at privilege 15. You can configure additional privilege levels from 2 through 14 to provide customized access control. For example, you might want to allow a group of

technical support staff to configure only a specific set of interface-level commands on interfaces while preventing device-wide configuration privileges. You could configure this in global configuration mode by using the command **privilege mode level level [command string]**. After you create that technical support user and assign this privilege, the user will be allowed to enter the interface and execute the commands specified in the command string. You can verify the configuration with the **show privilege** command.

Example 6.9 shows how to set up privileges to allow a network operation staff member to do basic manipulation of an interface. This example shows how to create the user **user1noc** with a type 9 password and privilege level 5 configured. In this particular case, a user with the **user1noc** username will be allowed to shut, unshut, and assign an IP address on the interface because these are the only commands this configuration allows in privilege level 5 in interface configuration mode. A user who tries to type a command that is not allowed (such as the **description** command) gets the message “Invalid input detected.”

#### EXAMPLE 6.9 Configuring and Verifying a Username and a Privilege Level

```
R1#
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# username user1noc privilege 5 algorithm-type scrypt secret
Cisco123
R1(config)# privilege exec level 5 configure terminal
R1(config)# privilege configure level 5 interface
R1(config)# privilege interface level 5 shutdown
R1(config)# privilege interface level 5 no shutdown
R1(config)# privilege interface level 5 ip address
R1(config)# end
R1#

R2# telnet 100.1.1.1
Trying 100.1.1.1 ... Open

User Access Verification

Username: user1noc
Password:

R1# show privilege
Current privilege level is 5
R1#
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R1(config)# interface GigabitEthernet 0/0
```

```
!The options to configure on the interface are limited
```

```
R1(config-if)# ?
```

```
Interface configuration commands:
```

```
default  Set a command to its defaults
exit     Exit from interface configuration mode
help     Description of the interactive help system
ip       Interface Internet Protocol config commands
no       Negate a command or set its defaults
shutdown Shutdown the selected interface
```

```
R1(config-if)# description test
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
R1(config-if)# end
```

```
R1#
```

---

## CramQuiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which of these commands can you use to force the vty lines to only allow remote connections via a protocol that supports encryption?
  - A. transport input telnet
  - B. transport input ssh
  - C. crypto key generate rsa
  - D. ip ssh version 2
2. What type of encryption does the **service password encryption** command provide?
  - A. Type 0
  - B. Type 5
  - C. Type 7
  - D. Type 9
3. True or false: SSH Version 1 implementation is compatible with SSH Version 2 implementation.
  - A. True
  - B. False



## Answers

1. **B** is correct. You can restrict the terminal line for SSH only by using the **transport input ssh** command in line configuration mode.
  2. **C** is correct. Type 7 password encryption is enabled with the **service password encryption** command.
  3. **B** is correct. SSHv2 is not compatible with SSHv1.
-

# Authentication, Authorization, and Accounting (AAA) Overview

Using line and local authentication as well as privilege levels works fine for controlling access on a small number of devices. However, this solution does not scale well as the number of devices grows. It becomes cumbersome and introduces the risk of inconsistent access control configurations across devices. To help simplify configuration and maintain consistency as the number of Cisco IOS devices grows, you can use an authentication, authorization, and accounting (AAA) solution.

There are many AAA protocol implementations, but this chapter focuses on the two most popular of them: RADIUS and TACACS+.

With AAA, network devices use a centralized RADIUS or TACACS+ server to authenticate users, authorize the commands users can run on a device, and provide accounting information. As a fallback mechanism, it is recommended that you still use local authentication in case the AAA server becomes unavailable at some point.

Let's briefly examine the AAA framework and how each part of it provides security functions:

- ▶ **Authentication:** Authentication provides identity verification before access to a network device is granted. It is the process of verifying the identity of the person or device accessing a network device, and it is based on the username and password combination provided by the entity trying to gain access.
- ▶ **Authorization:** Authorization provides access control. It is the process of assembling a set of attributes that describes what the user is authorized to perform. RADIUS and TACACS+ authorize users for specific rights by associating attribute/value (AV) pairs, which define the rights and the appropriate users.
- ▶ **Accounting:** Accounting provides a method for collecting information, logging the information locally on a network device, and sending the information to an AAA server for billing, auditing, and reporting. The accounting feature tracks and maintains a log of every management session used for access. You can use this information to generate reports for troubleshooting and auditing purposes.

Some of the high-level benefits of using a remote AAA server over local AAA services on each network device individually are highlighted next:

- ▶ Increased flexibility and control of access configuration
- ▶ Scalability
- ▶ Standardized authentication methods using RADIUS and TACACS+
- ▶ Ease of setup, since RADIUS and TACACS+ may have already been deployed across the enterprise
- ▶ More efficiency, since you can create user attributes once centrally and use them across multiple devices

Next, let's touch on the high points of TACACS+ and RADIUS before looking at their configuration.

## TACACS+ Overview

TACACS+ implementation provides for separate and modular authentication, authorization, and accounting facilities. It allows for a single access control server (referred to as the TACACS+ daemon) to provide authentication, authorization, and accounting to the network access server (NAS) independently. Typically, a client of a TACACS+ server is referred to as a NAS. A NAS may be a router, a switch, or an access point.

The TACACS+ protocol uses TCP port 49 for communication between the TACACS+ client (network device) and the TACACS+ server. A network administrator typically uses a workstation using Telnet, SSH, or the console to connect to a Cisco IOS device that needs to be managed. In this process, the TACACS+ client communicates with the TACACS+ server using the TACACS+ protocol. The TACACS+ protocol ensures confidentiality because all protocol exchanges between a TACACS+ client and a TACACS+ server are encrypted.

## RADIUS Overview

The Cisco implementation of RADIUS provides for a RADIUS client that runs on a Cisco IOS device to send an authentication request to a central RADIUS server that contains all user authentication and network service access information. RADIUS can be used with other AAA security protocols, such as local username lookup and TACACS+.

There are two implementations of RADIUS: Cisco's implementation and the industry-standard implementation. Cisco's implementation uses UDP port

1645 for authentication and authorization and UDP port 1646 for accounting. The industry-standard implementation uses UDP port 1812 for authentication and authorization and UDP port 1813 for accounting. The industry-standard implementation of the RADIUS protocol provides the distinction of working in a multi-vendor environment. Network devices from different vendors can connect to the same RADIUS server for AAA services. RADIUS can also be more convenient for AAA than TACACS+ since some organizations may already have it deployed.

As it relates to the privilege levels examined earlier in the chapter, TACACS+ and RADIUS can also be implemented when using AAA. For example, TACACS+ provides two ways to control the authorization of the network device commands on a per-user or per-group basis. One way is to assign privilege levels to commands and have the router verify with the TACACS+ server whether the user is authorized at the specified privilege level. Another way is to explicitly specify in the TACACS+ server, on a per-user or per-group basis, the allowed commands.

Cisco's TACACS+ and RADIUS implementations used to occur through the implementation of Cisco Secure Access Control Server (ACS), where RADIUS was used for network access control and TACACS+ was used for network devices access control. However, Cisco Identity Services Engine (ISE) is now the preferred implementation for AAA servers to support both TACACS+ and RADIUS protocols.

## AAA Configuration for Network Devices

In this section, you will see how both TACACS+ and RADIUS are configured from a Cisco IOS device. This section does not cover the configuration of a TACACS+ or RADIUS server because that is beyond the scope of this chapter.

There are two parts to configuring TACACS+ support: a TACACS+ server (for example, Cisco ISE) and a Cisco IOS device. At a high level, to configure a Cisco IOS device to support TACACS+, the following steps are involved:

1. Create a local user that will serve as the fallback if the TACACS+ server is not available or if you accidentally lock yourself out after enabling the AAA command. As highlighted previously, this is done with the command **username *username* privilege 15 algorithm-type {md5 | sha256 | scrypt} secret *password***.
2. Enable the AAA function with the **aaa new-model** global configuration command.

3. Add a TACACS+ server.
4. Define the method lists for TACACS+ authentication by using the **aaa authentication** global configuration command.
5. Use the **line** and **interface** commands to apply the defined method lists to various interfaces.
6. If needed, use the **aaa authorization** global command to configure authorization for the device. Unlike with authentication, which can be configured per line or per interface, authorization is configured globally for an entire device.
7. If needed, use the **aaa accounting** command to enable accounting for TACACS+ connections.

Example 6.10 shows how to configure an IOS device with TACACS+ for device access control based on these steps. This example demonstrates basic authentication, authorization, and accounting configuration. Once the command **aaa-new model** is configured, there is no line authentication anymore on the vty lines as the default login method becomes AAA. The console port defaults to no authentication. If you were to disable this with the **no aaa new-model** command afterward, the login method would switch back to line authentication. However, you would not see **login local** under vty line; you would see just **login** (meaning just the line password will be checked, and not the local user database that is configured locally on the router).

#### EXAMPLE 6.10 **Configuring TACACS+**

```
R1#
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
!Authentication setup
!First we create a fallback user account
R1(config)# username fallback privilege 15 algorithm-type scrypt
secret Cisco123
R1(config)# aaa new-model
R1(config)# tacacs server TACACSSERVER1
R1(config-server-tacacs)# address ipv4 100.1.1.2
R1(config-server-tacacs)# key Cisco123
R1(config-server-tacacs)# exit
R1(config)# aaa group server tacacs+ TACACSGROUP1
R1(config-sg-tacacs+)# server name TACACSSERVER1
R1(config)# aaa authentication login default group TACACSGROUP1 local
!the default method list automatically applies to all lines, except
!the ones that have a named method list explicitly define or in other
!words, it gets applied unless a more specific named method list is
!defined.
```

```

!We can also specify on the vty lines the login authentication METH-
ODLIST1 command then tacacs+ TACACSGROUP1 will be used as the primary
authentication method and the local user database is set as the backup
R1(config)# line vty 0 4
R1(config-line)# login authentication methodlist1
!Authorization setup
!Next, for authorization we create a method list TACACSAUTH1
!if-authentication option allows a user who is authenticated to be
placed in EXEC mode
R1(config)# aaa authorization exec TACACSAUTH1 group TACACSGROUP1
local if-authenticated
R1(config)# aaa authorization commands 15 TACACSAUTH1 group TACACS-
GROUP1 local
!The config-commands command indicates that the server must return
permission to use any router configuration command
R1(config)# aaa authorization config-commands
R1(config)# aaa authorization console
!The TACACSAUTH1 method list is applied to the vty lines for both EXEC
and level 15 command access
R1(config)# line vty 0 4
R1(config-line)# authorization exec TACACSAUTH1
R1(config-line)# authorization commands 15 TACACSAUTH1
R1(config-line)# exit
R1(config)#
!Accounting setup
!Next, for accounting we create a method list TACACSACC1
!User EXEC sessions will be recorded as they start and stop, along
with user information
R1(config)# aaa accounting exec TACACSACC1 start-stop group
TACACSGROUP1
!commands that are entered while a user is in privilege level 15
(enable mode) will be recorded
R1(config)# aaa accounting commands 15 TACACSACC1 start-stop group
TACASRVGROUP1
!The TACACSACC1 method list is applied to the vty lines for EXEC and
level 15 commands
R1(config)# line vty 0 4
R1(config-line)# accounting exec TACACSACC1
R1(config-line)# accounting commands 15 TACACSACC1
R1(config-line)# end
R1#

```

---

The AAA server also needs to be configured with the AAA client information (that is, the hostname, IP address, and key), the login credentials for the users, and the commands the users are authorized to execute on the device.

At a high level, to configure a Cisco IOS device to support RADIUS, the following steps are involved:

1. Enable AAA with the **aaa new-model** global configuration command.
2. Define the RADIUS server and specify the IP address and key.
3. Add the RADIUS server to a server group.
4. Define method lists for RADIUS authentication by using the **aaa authentication login *method-list*** global configuration command.
5. Create a named method list and add a RADIUS server group as the primary and local database as backup by using the **aaa authentication login** command.
6. Use the **line** and **interface** commands to enable the defined method lists to be used. For example, Example 6.11 specifies the **login authentication *method-list*** command on the vty lines, and then the RADIUS server group will be used as the primary authentication method, and the local user database is set as the backup.

Example 6.11 shows the configuration of an IOS device with RADIUS for device access control based on these steps (which are nearly identical to the steps for TACACS+ configuration). This example demonstrates basic authentication configuration.

#### EXAMPLE 6.11 **Configuring RADIUS**

```
R1#
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# aaa new-model
R1(config)# radius server RADIUSSERVER1
R1(config-radius-server)# address ipv4 100.1.1.2
R1(config-radius-server)# key Cisco123
R1(config-radius-server)# exit
R1(config)# aaa group server radius RADIUSGROUP1
R1(config-sg-radius)# server name RADIUSSERVER1
R1(config-sg-radius)# exit
R1(config)# aaa authentication login METHODLIST2 group RADIUSGROUP1
local
```

!the default method list automatically applies to all lines, except the ones that have a named method list explicitly define or in other words, it gets applied unless a more specific named method list is defined.

!we can also specify on the vty lines the **login authentication METHOD-LIST2** command then **RADIUSGROUP1** will be used as the primary authentication method and the local user database is set as the backup

```
R1 (config-line)# line vty 0 4
R1 (config-line)# login authentication METHODLIST2
R1 (config-line)# end
R1#
```

---

## CramQuiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. Which of the following is not one of the benefits of AAA?
  - A. Increased flexibility and control of access configuration
  - B. Scalability
  - C. Standardized authentication methods using RADIUS and TACACS+
  - D. Complete removal of the need for local user creation on IOS devices
2. In the industry-standard implementation of the RADIUS protocol, which port is used for accounting?
  - A. UDP port 1645
  - B. UDP port 1646
  - C. UDP port 1812
  - D. UDP port 1813
3. Which command is entered to enable AAA on a Cisco IOS device?
  - A. **aaa authentication**
  - B. **aaa authorization**
  - C. **aaa new-model**
  - D. **aaa accounting**

## Answers

1. **D** is correct. As a fallback mechanism, it is recommended that you use local authentication in case the AAA server becomes unavailable at some point.
  2. **D** is correct. The industry-standard implementation of RADIUS uses UDP port 1813 for accounting.
  3. **C** is correct. When configuring both TACACS+ and RADIUS, you enable AAA functionality by using the **aaa new-model** global configuration command.
-



## Review Questions

1. In implementing the TACACS+ protocol, which port is used for communication between a network device and a TACACS+ server?
  - A. UDP port 1645
  - B. TCP port 49
  - C. TCP port 389
  - D. UDP port 1813
2. In TACACS+ implementation, which of the following can serve as network access servers?
  - A. Routers
  - B. Switches
  - C. Access points
  - D. All of the above
3. Which of the following commands is used for configuring a vty line to use the method list name **list1**?
  - A. **aaa authentication**
  - B. **aaa authorization**
  - C. **login authentication list1**
  - D. **aaa new-model**
4. To add a TACACS+ server in IOS 15.x, what command follows **tacacs server name** if the IP address is 10.10.10.10?
  - A. **aaa tacacs 10.10.10.10**
  - B. **server 10.10.10.10**
  - C. **address ipv4 10.10.10.10**
  - D. **aaa server 10.10.10.10**

## Answers to Review Questions

1. **B** is correct. The TACACS+ protocol uses TCP port 49 for communication between a TACACS+ client (network device) and a TACACS+ server.
2. **D** is correct. The clients of a TACACS+ server is referred to as a network access server (NAS). A NAS may be a router, a switch, or an access point.
3. **C** is correct. A method list enables logic authentication. To apply a custom list to a line, you use **login authentication custom-list name** in line configuration mode.

4. **C** is correct. To add a TACACS+ server in IOS 15.x, you need to specify the TACACS+ server name, specify the server IP address with the **address ipv4 ip address** command (**address ipv4 10.10.10.10** in this case), and then specify the key string.

## Further Reading

- ▶ *CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide*

## What's Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the CramQuiz questions on the book's web page. The next chapter covers infrastructure security.

# Index

## Symbols

---

- :** (colon), 308–309
- %** (percent sign), 615
- #!** (shebang), 310
- 200 (OK)** status code, 347, 348
- 201 (Created)** status code, 348
- 202 (Accepted)** status code, 347
- 400 (Bad request)** status code, 348
- 401 (Unauthorized)** status code, 348
- 403 (Forbidden)** status code, 348
- 404 (Not Found)** status code, 348
- 429 (Too Many Request)** status code, 348
- 500 (Internal Server Error)** status code, 348
- 503 (Service Unavailable)** status code, 348
- 802.1AE**, 282
- 802.1AX**, 48. *See also* LACP (Link Aggregation Control Protocol)
- 802.1D**. *See* STP (Spanning Tree Protocol)
- 802.1Q**, 7–9, 495, 496, 547–548
- 802.11 wireless standards**, 172–173, 290–292
  - 802.11, 172
  - 802.11a, 172
  - 802.11ac, 173, 424, 481
  - 802.11ax, 481
  - 802.11b, 172
  - 802.11e, 500
  - 802.11g, 172
  - 802.11n, 172–173
  - 802.11r, 186
  - 802.12ax, 173
  - authentication initiation and message exchange, 292

- configuration, 291–292
- device roles, 291
- EAP (Extensible Authentication Protocol) authentication, 254–257

## A

### **AAA (authentication, authorization, and accounting). See also authentication**

- Cisco ISE (Identity Services Engine) support for, 289
- configuration, 212–216
- overview of, 210–211
- QoS profiles, 501
- RADIUS, 211–212, 215–216, 254–257, 289
- TACACS+
  - configuration, 213–214
  - overview of, 211

### **ABGs (active virtual gateways), 398**

### **absolute timeouts, 205–206**

### **absolute-timeout command, 205**

### **absolute-timeout minutes command, 205**

### **AC (access categories), 500**

### **access control, 193**

- with AAA (authentication, authorization, and accounting)
  - Cisco ISE (Identity Services Engine) support for, 289
  - configuration, 212–216
  - overview of, 210–211
  - QoS profiles, 501
  - RADIUS, 211–212, 215–216
  - TACACS+211, 213–214
- with ACLs (access control lists), 219, 507–508, 538
  - benefits of, 220–221
  - with debug, 589–590
  - definition of, 220
  - extended, 225–226
  - named, 226–228
  - port, 229

- rules for implementation of, 221–222
- standard, 224–225
- VLAN, 230–231
  - wildcard masking, 222–224
- to Cisco IOS CLI sessions, 194–196
- to Cisco IOS EXEC modes, 197–203
  - enable password command, 198–199
  - enable secret command, 199–200
  - line passwords, 197–198
  - usernames, 200–203
- further reading, 218
- with passwords
  - configuration, 197–198
  - enable password command, 198–199
  - enable secret command, 199–200
  - line, 197–198
  - in OSPF (open shortest path first), 82
  - types of, 196
- with privilege levels, 206–208
- with RBAC (role-based access control), 206–208
- with SSH (Secure Shell), 195, 203–206
  - configuration, 204–206
  - versions of, 203
- with usernames, 200–203

### **Access Control Server (ACS), 212**

### **access layer, hierarchical LAN design model, 381–382**

### **access points. See APs (access points)**

### **access-list access-list-number command, 224–225**

### **access-list access-list-number remark remark command, 226**

### **accounting. See AAA (authentication, authorization, and accounting)**

### **ACI Virtual Edge, 536**

### **ACK packets, 258–259**

**ACLs (access control lists), 219, 507–508, 538**

- benefits of, 220–221
- creating, 131–132
- with debug, 589–590
- definition of, 220
- extended, 225–226
- named, 226–228
- NTP (Network Time Protocol), 132
- port, 229
- rules for implementation of, 221–222
- standard, 224–225
- VLAN, 230–231
- wildcard masking, 222–224

**ACS (Access Control Server), 212****action cli (EEM applets), 357****action counter (EEM applets), 357****action decrement (EEM applets), 357****action forward command, 230****action mail (EEM applets), 357****action put (EEM applets), 357****action reload (EEM applets), 357****action SNMP-trap (EEM applets), 357****action statement, 230****action syslog (EEM applets), 357****actions**

- EEM (Embedded Event Manager) applets, 355–357, 359–360
- HTTP (Hypertext Transfer Protocol), 346
  - DELETE, 346
  - GET, 336, 346
  - POST, 346
  - PUT, 346

**Active Directory (AD), 289, 482****active mode (LACP), 48****Active state**

- BGP (Border Gateway Protocol), 107
- HSRP (Host Standby Router Protocol), 144, 393

**active virtual forwarders (AVFs), 398****active virtual gateways (AVGs), 398****AD (Active Directory), 482****AD (administrative distance), 62–64****Adaptive Security Virtual Appliance (ASA), 539****addresses, IP (Internet Protocol). See IP (Internet Protocol) routing; IP (Internet Protocol) services****addresses, multicast. See multicast****address-family [ipv6 | ipv4] unicast command, 98****adjacencies**

- adjacency tables, 513
- OSPF (open shortest path first), 85–87

**administrative and management APIs, Cisco vManage, 339****administrative distance (AD), 62–64****advanced distance vector algorithms, 61****Advanced Encryption Standard (AES), 252****Advanced Malware Protection (AMP), 271–272, 456****advertisements, VTP (VLAN Trunking Protocol), 13–14****AES (Advanced Encryption Standard), 252, 420****agent-based orchestration tools**

- Chef, 367–369
- comparison of, 376
- definition of, 365
- Puppet, 365–367
- SaltStack, 369–371

**agentless orchestration tools**

- Ansible, 372–375
- Bolt, 375–376
- comparison of, 376

**agents, SNMP (Simple Network Management Protocol), 604****aggregate command, 109****Aggregator attribute (BGP), 108****aggressive mode (UDLD), 39****AH (Authentication Header), 564**

- Aironet APs, 424**
- algorithms, routing, 61–62**
- AllDRouters, 86**
- AllSPFRouters, 86**
- alternate ports, 27**
- Amazon Web Services (AWS), 421, 439, 452**
- AMP (Advanced Malware Protection), 271–272**
- amplitude, radio frequency wave, 169–170**
- AND operator, 308**
- Ansible, 372–375**
- antennas, 181–183**
- AnyConnect Secure Mobility Client, 272**
- Anything as a Service (XaaS), 442**
- APIs (application programming interfaces)**
  - Cisco DNA Center API integrations, 334–338
    - further reading, 344
    - Intent API, 335, 344, 346
    - Know Your Network request paths, 336
    - site management APIs, 336–337
  - Cisco vManage API integrations, 338–342
    - administrative and management APIs, 339
    - configuration APIs, 339
    - connecting to, 339–340
    - device real-time monitoring APIs, 339
    - device state statistics bulk API, 339
    - Postman development tool, 340
    - REST operations on vManage web server, 341–342
    - troubleshooting and utility APIs, 339
  - NETCONF (Network Configuration Protocol), 241, 326
    - benefits of, 663
    - configuration, 664–666
      - configuration datastores, 663–664
      - definition of, 328–329, 662
      - further reading, 671
      - operations, 662–663
    - northbound, 241
    - OpenFlow, 241
    - REST (representational state transfer)
      - definition of, 242
      - response codes, 345–349
      - security, 240–245
    - RESTCONF (Representational State Transfer Configuration Protocol), 242, 326
      - configuration, 669–670
      - CRUD (create, read, update, and delete) mapping with, 668–669
      - definition of, 328–329, 668
      - further reading, 671
      - southbound, 241–242
- applets, EEM (Embedded Event Manager), 355–360**
  - actions, 355–357, 359–360
  - creating, 357–359
- application performance optimization, 455**
- application plane, SDN (software-defined networking), 240**
- application programming interfaces. See APIs (application programming interfaces)**
- application-aware firewalls, 456**
- application-aware routing, 455**
- application-specific integrated circuits (ASICs), 281, 471, 512**
- APs (access points), 248**
  - autonomous mode, 176
  - bridge mode, 177
  - CAPWAP (Control and Provisioning of Wireless Access Points), 481
  - Cisco Aironet APs, 424
  - EWC-AP (Cisco Embedded Wireless Controller on Catalyst Access Points), 422–424

- fabric-mode, 481
- Flex+Bridge mode, 177
- FlexConnect mode, 177
- lightweight mode, 176
- local mode, 177
- monitor mode, 177
- rogue detector mode, 177
- SE-Connect mode, 177
- sniffer mode, 177
- WLC (Wireless LAN Controller)
  - interaction, 178–183
    - antenna types, 181–183
    - discovery, 178–180
    - plane patterns, 180–181
- area *area-id* authentication message-digest command, 82**
- area *area-id* range ipv6-prefix/prefix-length command, 98**
- area *area-id* range network subnet-mask [advertise | not-advertise] [cost *metric*] command, 95**
- areas, OSPF (open shortest path first), 83–84**
- AS external LSA (link-state advertisement), 93**
- AS\_PATH (autonomous system path), 62, 107, 108**
- ASAv (Adaptive Security Virtual Appliance), 539**
- ASBR summary LSA (link-state advertisement), 93**
- ASICs (application-specific integrated circuits), 281, 471, 512**
- ASNs (autonomous system numbers), 104–105**
- assignment of VLANs (virtual LANs), 4–6**
- Assurance section, DNA Center, 654–658**
- assured forwarding (AFxy), 497**
- Atomic aggregate attribute (BGP), 108**
- Attempt states (OSPF), 86**
- augment statement, 328**
- authentication**
  - 802.1X, 290–292
  - Cisco ISE (Identity Services Engine) support for, 289
  - configuration, 212–216
  - definition of, 210
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 76
  - MAB (MAC Authentication Bypass), 292–293
  - MD5, 76, 80, 82, 395
  - NTP (Network Time Protocol), 131–132
  - OSPF (open shortest path first), 82–83
  - overview of, 210–211
  - plaintext, 80, 394–395
  - QoS profiles, 501
  - RADIUS, 211–212, 215–216
  - TACACS+
    - configuration, 213–214
    - overview of, 211
  - WebAuth, 293–295
  - wireless
    - AES (Advanced Encryption Standard), 252
    - APs (access points), 248
    - EAP (Extensible Authentication Protocol) authentication, 254–257
    - further reading, 262
    - GCM (Galois/Counter Mode), 252
    - Open Authentication, 249–251
    - overview of, 247–249
    - PSK (pre-shared key) authentication, 251–253
    - SSIDs (service set identifiers), 248–249
    - TKIP (Temporal Key Integrity Protocol), 251–252
    - WebAuth, 257–260
    - WEP (Wired Equivalent Privacy), 251
    - WPA (Wi-Fi Protected Access), 251–253

**Authentication Header (AH), 564****authentication servers**

802.1X, 291

EAP (Extensible Authentication Protocol), 254

**authenticators**

802.1X, 291

EAP (Extensible Authentication Protocol), 254

**authNoPriv, 606–608****authorization. See AAA**  
(authentication, authorization,  
and accounting)**authPriv, 606–608****auto mode (PAGP), 53****auto-anchor mobility, 188****auto-cost reference-bandwidth**  
**command, 81, 92****automation. See also cloud**  
**computing**automated WANs (wide area  
networks), 454–455automated zero-touch provisioning,  
454**autonomous mode (APs), 176****autonomous system external LSAs**  
**(link-state advertisements), 97****autonomous system numbers (ASNs),**  
**104–105****autonomous system path**  
**(AS\_Path), 62****autonomous wireless deployments,**  
**410, 411–412****AutoQoS, 500****Auto-RP, 163****auxiliary lines, 195–196****AVFs (active virtual forwarders),**  
**398****AWS (Amazon Web Services), 421,**  
**439, 452****AWS Elastic Beanstalk, 440****Azimuth plane pattern, 180****Azure, 439, 452****B****backup as a service (BaaS), 442****backup DRs (BDRs), 85–86****backup ports, 27****band of frequency, 169****bandwidth**

lack of, 491

SD-WAN (Software-Defined Wide  
Area Network), 454**banners, MOTD (message-of-the-day),**  
**367, 374–375****bare-metal (type 1) hypervisors,**  
**528, 533****basic service sets (BSSs), 411****BDRs (backup DRs), 85–86****beacons, SaltStack, 370****Bellman-Ford algorithms, 61****best-effort service, 487, 493****BFD (Bidirectional Forwarding**  
**Detection) probes, 455****BGP (Border Gateway Protocol), 460**ASNs (autonomous system numbers),  
104–105

configuration, 112–118

basic steps for, 112–113

BGP route verification, 118

BGP session state, 115–116

eBGP configuration on service  
provider and customer routers,  
113–114

neighbor verification, 116–117

reference topology, 113

router verification, 117–118

definition of, 103, 104

further reading, 121

message types, 106

MPLS (Multiprotocol Label  
Switching), 104–105

neighbors, 112

path vector routing algorithm,  
107–111

purpose of, 104–105



states, 106–107  
 tables, 105–106

**bgp default local-preference command**, 111

**bgp router-id command**, 113

**BID (bridge ID)**, 21

**Bidirectional Forwarding Detection (BFD) probes**, 455

**Bidirectional PIM (Bidir-PIM)**, 162

**Blocking state (Layer 2 ports)**, 24, 26

**blocks, finally**, 311

**Bolt**, 375–376

**Boolean data type**, 307

**Boolean operators**, 308

**Border Gateway Protocol. See BGP (Border Gateway Protocol)**

**border nodes, SD-Access**, 480

**botnets**, 267, 268

**BPDU Filter**, 35–36

**BPDU Guard**, 33–34, 386

**BDPUs (bridge protocol data units)**  
   BPDU Filter, 35–36  
   BPDU Guard, 33–34, 386  
   configuration BPDUs, 20, 25, 31, 35  
   messages, 19–20

**branches, security threats to**, 266–267

**Bridge Assurance**, 37–38

**bridge ID (BID)**, 21

**bridge mode (APs)**, 177

**bridge protocol data units. See BPDUs (bridge protocol data units)**

**bring-your-own-device (BYOD)**, 267, 279, 290

**broadcast**, 156

**BSR (Bootstrap Router)**, 164

**BSSs (basic service sets)**, 411

**buffering debug messages**, 590–591

**buffers, internal**, 614

**business policy**, 288

**BYOD (bring-your-own-device)**, 267, 279, 290

## C

**CAM (Content-Addressable Memory) tables**, 507–508, 515–517

**campuses, security threats to**, 267

**candidate configuration datastore (NETCONF)**, 664

**Candidate RPs**, 163

**CAPWAP (Control and Provisioning of Wireless Access Points)**, 176, 412–415, 481

**CAR (committed access rate)**, 494

**catalogs, Puppet**, 367

**Catalyst 9800 Embedded Wireless controller**, 481

**CBWFQ (class-based weighted fair queueing)**, 221, 499

**CCKM (Cisco Centralized Key Management)**, 186

**CDP (Cisco Discovery Protocol)**, 189

**CDP (Cisco Domain Protection)**, 274

**cEdge**, 460

**CEF (Cisco Express Forwarding)**, 400, 495, 512–515  
   benefits of, 512  
   components of, 513–514  
   modes of operation, 514–515

**Central Web Authentication**, 294

**centralized CEF mode**, 514

**centralized wireless deployments**, 410, 412–415

**certification, Cisco ISE (Identity Services Engine) support for**, 289

**Challenge Handshake Authentication Protocol (CHAP)**, 289

**change of authorization (CoA)**, 294

**channel-group command**, 49–51

**channels, RF**, 169

**CHAP (Challenge Handshake Authentication Protocol)**, 289

**Chef**, 367–369

**CIDR (classless interdomain routing)**, 80, 134

**Cisco ACI Virtual Edge**, 536

**Cisco Adaptive Security Virtual Appliance (ASAv), 539****Cisco Advanced Malware Protection (AMP), 271–272****Cisco Advanced Phishing Protection (CAPP), 274****Cisco Aironet APs, 424****Cisco AnyConnect Secure Mobility Client, 272****Cisco Centralized Key Management (CCKM), 186****Cisco Cloud OnRamp, 456–457****Cisco Discovery Protocol (CDP), 189****Cisco DNA Center, 652–658. See also REST (representational state transfer) APIs; SD-Access**

API integrations, 334–338

connectivity methods, 337

events and notifications, 338

further reading, 344

Integration API, 338

Intent API, 335, 346

Know Your Network request paths, 336

multivendor support, 338

operational tools, 337

RESTful API, 335–336

site management APIs, 336–337

Token API, 243

Assurance section, 654–658

benefits of, 652–653

definition of, 652

Design section, 653

further reading, 660

goal of, 334

HTTP status codes, 347–348

LAN Automation, 471

multivendor SDK, 335

Overall Health dashboard, 657–658

overview of, 475

Policy section, 654

Provision section, 654

SD-WAN architecture, 334

**Cisco Domain Protection (CDP), 274****Cisco Email Security Appliance (ESA), 272, 274****Cisco Embedded Event Manager (EEM), 351–362**

applets, 355–360

actions, 355–357, 359–360

creating, 357–359

architecture, 354–355

benefits of, 352–353

definition of, 352

event detectors, 354–355

further reading, 362

policies, 355–360

scripts, 353, 358–360

server, 354

Tcl (Tool Command Language), 351, 352, 358–359

**Cisco Embedded Wireless Controller (EWC), 422–424****Cisco Embedded Wireless Controller on Catalyst Access Points (EWC-AP), 422–424****Cisco ENCS (Enterprise Network Compute Systems), 540****Cisco Enterprise Network Function Virtualization (NFV)**

architecture, 538–539

benefits of, 537–538

hardware options, 539–540

**Cisco E-Series servers, 539–540****Cisco Express Forwarding (CEF), 400, 495, 512–515**

benefits of, 512

components of, 513–514

modes of operation, 513–514

**Cisco Firepower**

Management Center, 275

Next-Generation Firewall Virtual (NGFWv), 539

NGFWs (Next-Generation Firewalls), 276–277

NGIPSs (Next-Generation IPSs), 275–276

- Cisco FlexConnect, 410, 415–418**
- Cisco Identity Services Engine (ISE), 468–469, 472. See also SD-Access**
  - benefits of, 288–289
  - features of, 288–289
- Cisco Integrated Services Virtual Router (ISRv), 539**
- Cisco IOS CLI sessions, access control to, 194–196**
- Cisco IOS EXEC modes, access control to, 197–203**
  - enable password command, 198–199
  - enable secret command, 199–200
  - line passwords, 197–198
  - usernames, 200–203
- Cisco IOS Virtual Tunnel Interfaces (VTIs), 560–561**
- Cisco ISE (Identity Services Engine), 212, 272–273. See also REST (representational state transfer) APIs**
- Cisco ISR 4000 routers, 539–540**
- Cisco Locator/ID Separation Protocol (LISP)**
  - architecture, 577–578
  - benefits of, 574–575
  - components of, 574–576
  - definition of, 573
  - deployment environment, 576–577
  - limitations of, 573
- Cisco Meraki, cloud-based wireless deployments, 418–422**
- Cisco Mobile Experience (CMX), 427–428**
  - CMX Analytics, 428
  - CMX Connect, 428
- Cisco Mobility Express, 423–424**
- Cisco Multicloud, 456–457**
- Cisco Network Control Platform (NCP), 472**
- Cisco Network Data Platform (NDP), 472**
- Cisco Nexus 1000VE, 536**
- Cisco Python module, 304–305**
- Cisco SD-WAN. See SD-WAN (Software-Defined Wide Area Network)**
- Cisco Secure Access Control Server (ACS), 212**
- Cisco Secure Network Analytics, 273**
- Cisco Secure Web Appliance, 273–274**
- Cisco Software-Defined Access. See SD-Access**
- Cisco Software-Defined Wide Area Network (SD-WAN)**
  - architecture, 334–335
  - common use cases, 454–457
    - application performance optimization, 455
    - Cisco Multicloud, 456–457
    - secure automated WAN, 454–455
    - secure DIA (Direct Internet Access), 456
  - components of, 459–464
    - planes of operation, 459
    - vBond orchestrators, 461
    - vManage, 461–462
    - vSmart controllers, 459–460
    - WAN edge routers, 460–461
  - definition of, 451
  - delivery, 452
  - deployment considerations, 463–464
  - further reading, 466
  - need for, 453–454
  - overview of, 452–453
- Cisco StackWise, 388–389**
- Cisco Talos Security Intelligence and Research Group, 271**
- Cisco Technical Assistance Center (TAC), 655–656**
- Cisco Threat Grid, 271, 272**
- Cisco TrustSec, 288–289, 468–469, 475**
- Cisco UCS C-Series servers, 539**
- Cisco Umbrella, 272–273, 456**
- Cisco Unified Wireless Network, 412**
- Cisco vAnalytics, 462**

**Cisco virtual Wide Area Application Services (vWAAS), 539****Cisco virtual Wireless LAN Controllers (vWLCs), 539****Cisco vManage**

- API integrations, 338–342
  - administrative and management APIs, 339
  - configuration APIs, 339
  - connecting to, 339–340
  - device real-time monitoring APIs, 339
  - device state statistics bulk API, 339
  - further reading, 344
  - Postman development tool, 340
  - REST operations on vManage web server, 341–342
  - troubleshooting and utility APIs, 339
  - use cases, 339
- HTTP status codes, 347–348

**Cisco WebEx, 441****CIST (common and internal spanning tree), 41****Citrix Hypervisor (Citrix XenServer), 528****class of service (CoS), 495, 496, 621****class selectors, 497****class-based weighted fair queueing (CBWFQ), 221, 499****classes, Puppet, 367****classification, QoS (quality of service), 495–497****Classification phase (TrustSec), 279–280****classless interdomain routing (CIDR), 80, 134****class-map command, 234****Clean Air section, 189****clear ip bgp \* command, 111****clear ip nat translation command, 138****clear ip ospf process command, 91****CLI (command-line interface). See also commands**

- access control to, 194–196
- CLI event detector, 354
- in Python, 305–306

**cli.cli() function, 305****cli.clip() function, 305****cli.configure() function, 306****cli.configurep() function, 306****Client Health dashboard, 656, 658****client mode (VTP), 13****clients**

- 802.1X, 291
- Chef, 368
- EAP (Extensible Authentication Protocol) authentication, 254
- returning information about, 336
- wireless connectivity, troubleshooting, 188–189

**cli.execute() function, 305****cli.executep() function, 305****CLNS (Connectionless Network Services), 104****cloud computing**

- BaaS (backup as a service), 442
- characteristics of, 434–436
- cloud-based wireless deployments, 411, 418–422
- definition of, 434
- deployment models, 444–445
- DRaaS (disaster recovery as a service), 442
- further reading, 450
- IaaS (Infrastructure as a Service), 421, 438–439, 452, 456
- infrastructure basics, 433–436
- PaaS (Platform as a Service), 440
- SaaS (Software as a Service), 441, 452, 457
- security threats to, 268
- when to use, 447
- XaaS (Anything as a Service), 442

**Cloud OnRamp, 456–457**

**CMX (Cisco Mobile Experience),  
427–428**

CMX Analytics, 428

CMX Connect, 428

**collapsed core network design,  
384–385****collect command, 627****colon (:), 308–309****command icmp-echo command, 645****Command Runner, 337****command-and-control (C and C)  
attacks, 273****command-line interface. See CLI  
(command-line interface)****commands, 32, 74–75, 592–593, 669.  
See also functions and methods;  
statements**

absolute-timeout, 205

absolute-timeout minutes, 205

access-list access-list-number,  
224–225access-list access-list-number remark  
remark, 226

action forward, 230

address-family [ipv6 | ipv4]  
unicast, 98

aggregate, 109

area *area-id* authentication  
message-digest, 82area *area-id* range ipv6-prefix/  
prefix-length, 98area *area-id* range *network*  
*subnet-mask* [advertise |  
not-advertise] [cost *metric*], 95auto-cost reference-bandwidth,  
81, 92

bgp default local-preference, 111

bgp router-id, 113

channel-group *number*, 49–50

class-map, 234

clear ip bgp \*111

clear ip nat translation, 138

clear ip ospf process, 91

collect, 627

command icmp-echo, 645

debug, 589–593

ACLs (access control lists) with,  
589–590

conditional debugging, 592–593

debug message buffering, 590–591

output format, 589

debug ip packet, 589

debug tunnel, 556

debug tunnel packet, 556

default-information originate  
[always] [metric *metric value*]  
metric-type *type-value*, 91

default-metric, 111

destination, 636

dir(), 306

enable password, 198–199

enable secret, 199–200

encapsulation dot1q, 16

errdisable recovery cause  
bpduguard, 33

errdisable recovery internal, 33

erspan-id, 636

exec-timeout, 205

exec-timeout minutes seconds, 205

exit(), 303

extended traceroute, 595–597

frequency seconds, 645, 647

glbp, 150–153

guestshell run python, 302–303

help(), 304–305, 306

import cli, 305

instance, 40–41

interface vlan, 16

iox, 302

ip access-group access-list name, 227

ip access-group access-list  
number, 226

ip access-list extended name, 227

ip access-list log-update, 228

ip flow, 623

ip flow-top-talker, 624

ip flow-top-talkers, 625

- ip http authentication local, 669
- ip http secure-server, 669
- ip nat inside, 136, 138
- ip nat inside source list acl, 138
- ip nat inside source list acl pool nat-pool-name, 138
- ip nat inside source static inside-local-ip inside-global-ip, 136
- ip nat inside static, 136
- ip nat outside, 136, 138
- ip nat pool nat-pool-name starting-ip ending-ip prefix-length prefix-length, 138, 140
- ip nat translations, 136, 139
- ip ospf authentication key-chain, 83
- ip ospf authentication message-digest, 82
- ip ospf cost, 81, 92
- ip ospf dead-interval, 92
- ip ospf hello-interval, 92
- ip ospf message-digest-key *key-id* md5 *key*, 82
- ip ospf priority, 92
- ip ospf *process-id* area *area-id*, 87–88
- ip route, 65–66
- ip sla operation-number, 645, 647
- ip sla responder, 648–649
- ip sla schedule operation-number, 647
- ip ssh timeout seconds authentication-retries number, 204
- ip ssh version 2, 204
- ip summary-address eigrp, 78
- ipv6 unicast-routing, 97, 98
- logging rate-limit, 617
- login local, 204
- match, 230, 627
- maximum-paths, 94, 109
- metric rib-scale, 74
- name, 40–41
- neighbor *ip-address* remote-as, 112, 114
- netconf ssh, 664–665
- netconf-yang, 664–665
- netconf-yang feature candidate-datastore, 664
- network, 69, 87–88, 109, 112, 114, 117
- no auto-summary, 78
- no exec-timeout, 205
- no switchport, 51
- ntp access-group, 132
- ntp association, 126
- ntp authenticate, 131
- ntp authentication-key key-id md5 key-string, 131
- ntp master stratum-number, 126–127
- ntp peer ip-address, 126
- ntp server ip-address, 126–127
- ntp server server-ip-address key key-id, 131
- ntp status, 126
- ntp trusted-key key-id, 131
- ospfv3 *process-id* ipv6 area *area-id*, 98
- passive interface default, 91
- passive *interface-id*, 91
- ping, 375–376, 597–602
  - extended ping command, 601–602
  - extended ping fields, 599–601
  - output characters, 598
  - ping command to repeat count, 599
  - ping command with size specified, 599
  - simple example, 598–599
- policy-map, 234–235
- port-channel load-balance, 54
- privilege mode level level, 206–207
- remote-span, 634
- restconf, 669
- revision, 40–41
- root primary, 29, 30–31
- router bgp, 112, 114
- router eigrp, 69, 76–78
- router ospfv3, 97, 98
- router-id, 91, 98
- sdm prefer, 518–520

service-policy, 234–235  
show, 622  
show adjacency, 513–514  
show crypto isakmp sa, 565–567  
show etherchannel load-balance, 54  
show etherchannel summary, 50–52  
show flow record CUSTOM, 627  
show glbp, 151  
show interface *interface* switchport,  
6, 11  
show interface port-channel 1, 50–51  
show interface trunk, 11  
show iox-service, 302  
show ip bgp, 109–110, 113, 115–116,  
117–118  
show ip bgp neighbors, 113, 116–117  
show ip bgp summary, 113  
show ip cache flow, 623  
show ip cef, 513–514  
show ip eigrp interfaces, 70  
show ip eigrp neighbors, 71  
show ip eigrp topology  
[all-links], 72–73  
show ip flow export, 623  
show ip flow interface, 623  
show ip flow top-talkers, 625  
show ip interface brief, 16  
show ip nat translations, 138  
show ip ospf interface, 87–89, 92  
show ip ospf interface brief, 88–89  
show ip ospf neighbor, 87–89  
show ip protocol, 90  
show ip route bgp, 118  
show ip route eigrp, 75–76  
show ip route ospf, 87–90  
show ip sla configuration, 647  
show ip ssh, 204  
show ip statistics, 649  
show ip summary, 649  
show ipv6 route ospf, 98  
show logging, 590–591  
show mac address-table, 516–517  
show monitor session 1, 633  
show monitor session 2, 634  
show monitor session erspan-source  
session, 636  
show netconf-yang datastores,  
664–666  
show netconf-yang statistics, 664–666  
show ntp status, 131  
show ospfv3 interface, 98  
show ospfv3 ipv6 neighbor, 98  
show platform software  
yang-management process,  
664–666, 669  
show redundancy clients, 403–405  
show snmp host, 607  
show spanning-tree, 21, 25  
show spanning-tree mst, 43–45  
show spanning-tree mst  
configuration, 41–43  
show spanning-tree summary, 22–23  
show spanning-tree vlan 1, 22–23,  
29–30  
show standby, 144  
show vlan brief, 4, 5–6  
show vrrp, 148  
show vtp status, 15  
sort-by bytes, 625  
spanning-tree bpdudfilter enable, 35  
spanning-tree bpduguard disable,  
33–34  
spanning-tree bpduguard enable,  
33–34  
spanning-tree guard loop, 36  
spanning-tree loopguard default, 36  
spanning-tree mode mst, 41–43  
spanning-tree mode rapid-pvst, 25  
spanning-tree mst configuration,  
40–41  
spanning-tree mst forward-time, 45  
spanning-tree mst *instance-id*  
cost *cost*, 43  
spanning-tree mst *instance-id*  
port-priority *priority*, 43  
spanning-tree mst max-age, 45

## commands

- spanning-tree pathcost method, 22
- spanning-tree pathcost method long, 22–23
- spanning-tree portfast, 33
- spanning-tree portfast bpdupfilter default, 35
- spanning-tree portfast bpduguard default, 33–34
- spanning-tree portfast default, 33
- spanning-tree portfast disable, 33
- spanning-tree portfast trunk, 33
- spanning-tree vlan, 29
- standby, 143–144
- summary-address, 78, 95
- switchport, 6
- switchport access vlan, 5
- switchport mode access, 5
- switchport mode dynamic auto, 9
- switchport mode dynamic desirable, 9
- switchport mode trunk, 10
- switchport non negotiate, 10
- traceroute, 593–597
  - extended traceroute, 595–597
  - messages, 596
  - output characters, 594
  - simple example, 594–595
- transport input ssh, 204
- type(), 306
- udld {aggressive | enable | message time *interval*}, 39
- udld {enable | aggressive | disable}, 39
- vlan, 4
- vlan access-map name sequence, 230
- vlan filter vlan-access-map-name vlan-list, 230
- vrrp, 147–148
- vtp domain, 14
- vtp mode, 14
- vtp password, 14
- vtp primary, 14
- committed access rate (CAR), 494**
- common and internal spanning tree (CIST), 41**
- Common Criteria, Unified Capabilities Approved Product List, 289**
- common spanning tree (CST), 41**
- Community attribute (BGP), 108**
- community cloud, 445**
- conditional debug command, 592–593**
- conditional debugging, 592–593**
- conditional statements, 308–309**
- configuration, 549–550. See also configuration management and orchestration tools**
  - 802.1X, 291–292
  - AAA (authentication, authorization, and accounting), 212–216
    - RADIUS, 215–216
    - TACACS+213–214
  - BGP (Border Gateway Protocol), 112–118
    - basic steps for, 112–113
    - BGP route verification, 118
    - BGP session state, 115–116
  - eBGP configuration on service provider and customer routers, 113–114
  - neighbor verification, 116–117
  - reference topology, 113
  - router verification, 117–118
- EAP (Extensible Authentication Protocol) authentication, 254–257
- EIGRP (Enhanced Interior Gateway Routing Protocol), 68–78
  - authentication, 76
  - configuration, 69–70
  - FD (feasible distance), 69
  - feasibility conditions, 69
  - feasible successors, 69
  - metrics, 73–75
  - named mode, 76–78
  - neighbor tables, 70–72
  - RD (reported distance), 69
  - route summarization, 78



- routing tables, 75–76
  - successor routes, 68
  - successors, 68
  - topology tables, 72–75
  - verifying, 70
- ERSPAN (Encapsulated Remote SPAN), 635–637
- EtherChannels, 47–54
  - LACP (Link Aggregation Control Protocol), 48–52
  - overview of, 47–48
  - PAgP (Port Aggregation Protocol), 52–54
- EXEC and absolute timeouts, 205–206
- Flexible NetFlow
  - flow exporter mapping to flow monitor, 629–630
  - flow exporters, 627, 628
  - flow monitor, 627, 628–629
  - flow monitor configuration on interface, 630–631
  - flow records, 627–628
  - flow samplers, 627
- GLBP (Gateway Load Balancing Protocol), 150–153
- GRE (Generic Routing Encapsulation), 552–556
- Guest Shell environment, 301–302
- HSRP (Host Standby Router Protocol), 143–147
- IP (Internet Protocol) routing
  - overview of, 60–61
  - path selection, 62–64
  - routing algorithms, 61–62
  - static routing, 65–66
- IP Security (IPsec), 564–567
- MOTD (message-of-the-day)
  - banner, 367
- NAT (Network Address Translation), 134–135
  - configuration topology, 135
  - dynamic NAT, 137–138
  - overview of, 134–135
  - static NAT, 136–137
- NETCONF (Network Configuration Protocol), 664–666
- NetFlow, 623
- NTP (Network Time Protocol)
  - access lists, 132
  - authentication, 131–132
  - peers, 130
  - router configuration, 125–130
- Open Authentication, 249–251
- OSPF (open shortest path first), 87–90, 460
  - areas, 83–84
  - authentication, 82–83
  - basic configuration, 87–90
  - costs, 81
  - definition of, 80
  - Dijkstra shortest path first algorithm, 80–81
  - neighbors and adjacencies, 85–87
  - packet types, 87
  - states, 86
  - versions of, 80
- passwords, 197–198
  - enable password command, 198–199
  - enable secret command, 199–200
  - line passwords, 197–198
- PAT (Port Address Translation), 138–141
- privilege levels, 206–208
- RBAC (role-based access control), 206–208
- RESTCONF (Representational State Transfer Configuration Protocol), 669–670
- RSPAN (Remote Switch Port Analyzer), 634–635
- RSTP (Rapid Spanning Tree Protocol), 25–28
- SNMP (Simple Network Management Protocol), 607–608
- SPAN (Switch Port Analyzer), 632–633

## configuration

- SSH (Secure Shell), 204–206
  - SSO (Stateful Switchover), 401–402
  - STP (Spanning Tree Protocol), 19–45
    - BPDU (bridge protocol data unit) messages, 19–20
    - BPDU Filter, 35–36
    - BPDU Guard, 33–34
    - Bridge Assurance, 37–38
    - designated port elections, 20–25
    - Loop Guard, 36–37
    - MST (Multiple Spanning Tree), 40–45
    - overview of, 19–20
    - PortFast, 32–33
    - root bridges, 20–25
    - Root Guard, 31–32
    - root ports, 20–25
    - RSTP (Rapid Spanning Tree Protocol), 25–28
    - switch priorities, 28–31
    - timers, 24–25
    - UDLD (Unidirectional Link Detection), 38–40
  - syslog, 614–618
    - basic configuration, 617–618
    - definition of, 614
    - message elements, 615–616
    - severity levels, 616–617
  - top talkers, 625
  - usernames, 200–203
  - VLANs (virtual LANs), 3–17
    - 802.1Q trunking, 7–9
    - assignment of, 4–6
    - creating, 4–5
    - DTP (Dynamic Trunking Protocol), 9–11
    - inter-VLAN routing, 16–17
    - overview of, 3
    - VLAN assignment, 4–6
    - VTP (VLAN Trunking Protocol), 11–15
  - VRF-Lite, 547–550
  - VRRP (Virtual Router Redundancy Protocol), 147–150
  - WebAuth, 257–260
  - WLANs (wireless LANs), 410–411
    - autonomous, 410, 411–412
    - centralized, 410, 412–415
    - Cisco FlexConnect, 410, 415–418
    - cloud-based, 411, 418–422
    - embedded, 411, 422–424
    - overview of, 409, 410–411
    - SD-Access. *See* SD-Access
    - troubleshooting, 188–189
  - WPA (Wi-Fi Protected Access), 251–253
- configuration APIs, Cisco vManage, 339**
- configuration BPDUs, 19, 20, 25, 31, 35**
- configuration management and orchestration tools, 363–364**
- agent-based
    - Chef, 367–369
    - definition of, 365
    - Puppet, 365–367
    - SaltStack, 369–371
  - agentless
    - Ansible, 372–375
    - Bolt, 375–376
  - comparison of, 376
  - further reading, 378
- configuration templates, 337**
- congestion avoidance, 500**
- congestion management, 499**
- Connect state (BGP), 107**
- connected mode, Cisco FlexConnect, 416–418**
- Connectionless Network Services (CLNS), 104**
- connectivity methods, Cisco DNA Center, 337**
- console lines, 195–196**
- container nodes, 329**

**content security, 273–274**

**Content-Addressable Memory (CAM) tables, 507–508, 515–517**

**Control and Provisioning of Wireless Access Points (CAPWAP), 176, 412–415, 481**

**control plane**

- CoPP (control plane policing), 233–235
- definition of, 400
- LISP (Cisco Locator/ID Separation Protocol), 577
- SD-Access, 474, 478–479
- SDN (software-defined networking) architecture, 240
- SD-WAN (Software-Defined Wide Area Network), 459
- VRF-Lite, 548

**control plane policing (CoPP), 233–235**

**controlled load service, 494**

**controller appliances, 471**

**controller layer, SD-Access, 472**

**cookbooks, Chef, 368–369**

**CoPP (control plane policing), 233–235**

**copy-config operation (NETCONF), 663**

**core layer, hierarchical LAN design model, 382–383**

**CoS (class of service), 495, 496, 621**

**costs**

- OSPF (open shortest path first), 81
- TCO (total cost of ownership), 335, 526–527

**counter event detector, 354**

**Coup messages (HSRP), 393**

**CPU load, 490**

**CPU speed, 490**

**CRUD (create, read, update, and delete) mapping, 668–669**

**cryptographic keys, 186–187**

**cryptomining, 273**

## D

**dACLs (downloadable access control lists), 288**

**dashboards, DNA Center, 655–658**

**data centers, security threats to, 268**

**data models**

- benefits of, 327
- definition of, 317
- NETCONF (Network Configuration Protocol), 241, 326
  - benefits of, 663
  - configuration, 664–666
  - configuration datastores, 663–664
  - definition of, 328–329, 662
  - further reading, 671
  - operations, 662–663
- RESTCONF (Representational State Transfer Configuration Protocol), 242, 326
  - configuration, 669–670
  - CRUD (create, read, update, and delete) mapping with, 668–669
  - definition of, 328–329, 668
  - further reading, 671
- YANG (Yet Another Next Generation), 325–332
  - characteristics of, 326–327
  - further reading, 332
  - nodes in, 329
  - tree structure of, 329–330
  - types of, 327–329

**data path virtualization. See virtualization, network**

**Data pattern field (ping command), 600**

**data plane**

- definition of, 400
- LISP (Cisco Locator/ID Separation Protocol), 577
- SD-Access, 474

## data plane

SDN (software-defined networking) architecture, 240

SD-WAN (Software-Defined Wide Area Network), 459

VRF-Lite, 548

**data reporting, NetFlow, 622****data types**

JSON (JavaScript Object Notation), 320

Python, 306–307

**database descriptor (DBD) packets, 87****databases**

LSDB (link-state database), 80–81

Puppet, 366

**data-encoding formats**

definition of, 317

JSON (JavaScript Object Notation)

characteristics of, 319–321

data types, 320

file structure, 319–320

formatting, 320–321

further reading, 324

XML (Extensible Markup Language)

characteristics of, 317–319

documents, 318–319

further reading, 324

syntax for, 318

**Datagram size field (ping command), 600****Datagram Transport Layer Security (DTLS), 412, 414****dastores, NETCONF (Network Configuration Protocol), 663–664****DBD (database descriptor) packets, 87****dCEF (distributed CEF) mode, 514****DDoS (distributed denial-of-service) attacks, 273, 386****debug command, 589–593**

ACLs (access control lists) with, 589–590

conditional debugging, 592–593

debug message buffering, 590–591  
output format, 589

**debug ip packet command, 589****debug tunnel command, 556****debug tunnel packet command, 556****decapsulation, VXLAN (Virtual Extensible LAN), 480****decibel (dB), 169–170****decibel isotropic (dBi), 169–170****decibel milliwatts (dBm), 169–170****default route advertisements, 91****default-free zone (DFZ), 574****default-information originate [always] [metric *metric value*] metric-type *type-value* command, 91****default-metric command, 111****delay, 490****delay variation, 491****DELETE action (HTTP), 346****delete-config operation (NETCONF), 663****denial-of-service (DoS) attacks, 386, 620****deployment**

Cisco SD-WAN (Software-Defined Wide Area Network), 463–464

cloud computing, 444–445

LISP (Cisco Locator/ID Separation Protocol), 576–577

NGIPSS (Next-Generation IPSs), 275–276

TrustSec, 279–280

WLANs (wireless LANs)

autonomous, 410, 411–412

centralized, 410, 412–415

Cisco FlexConnect, 410, 415–418

cloud-based, 411, 418–422

embedded, 411, 422–424

further reading, 431

overview of, 409, 410–411

SD-Access. *See* SD-Access

wireless location services, 418–422

- description element (syslog), 615
- design, network. *See* network design
- Design section, DNA Center, 653
- designated port elections (STP), 20–25
- designated ports, 27
- designated routers (DRs), 85–86
- desirable mode (PAgP), 53
- destination command, 636
- destination ports (SPAN), 632
- destination unreachable error message, 596
- Device 360/Client 360, 656
- device management, 336. *See also* access control
  - BYOD (bring-your-own-device), 290
  - NFV (Network Functions Virtualization) devices, 336
  - onboarding, 289
  - profiling, 289
- Device Onboarding API (PnP), 336
- device real-time monitoring APIs, 339
- device state statistics bulk API, 339
- DFZ (default-free zone), 574
- DIA (Direct Internet Access), 456
- dictionary data type, 307
- differentiated services code points (DSCPs), 220–221, 495, 497, 626
- differentiated services (DiffServ), 487, 494
- diffusing update algorithm (DUAL), 61
- Digital Network Architecture. *See* DNA (Digital Network Architecture) Center
- DigitalOcean, 439
- Dijkstra shortest path first algorithm, 61, 80–81
- dipole antennas, 181–182
- dir() command, 306
- Direct Internet Access (DIA), 456
- directional antennas, 182–183
- directly attached static routes, 65
- Disabled port state, 24, 26–27, 144, 393
- disaster recovery as a service (DRaaS), 442
- discovery, WLCs (Wireless LAN Controllers), 178–180
- distance vector algorithms, 61
- distributed CEF (dCEF) mode, 514
- distributed denial-of-service (DDoS) attacks, 273, 386
- Distributed Switches (vDSs), 536
- distribution layer, hierarchical LAN design model, 382
- dmiauthd, 664–665
- DMVPN (Dynamic Multipoint VPN), 559–560
- DNA (Digital Network Architecture) Center, 468, 652–658. *See also* REST (representational state transfer) APIs; SD-Access
  - API integrations, 334–338
    - connectivity methods, 337
    - events and notifications, 338
    - further reading, 344
    - Integration API, 338
    - Intent API, 335, 346
    - Know Your Network request paths, 336
    - multivendor support, 338
    - operational tools, 337
    - RESTful API, 335–336
    - site management APIs, 336–337
    - Token API, 243
  - Assurance section, 654–658
  - benefits of, 652–653
  - definition of, 652
  - Design section, 653
  - further reading, 660
  - goal of, 334
  - HTTP status codes, 347–348
  - IT Service Management (ITSM), 334
  - multivendor SDK, 335
  - Overall Health dashboard, 657–658

- overview of, 475
- Policy section, 654
- Provision section, 654
- SD-WAN architecture, 334

**DNS (Domain Name System), 577****Docker, 533****documents, XML (Extensible Markup Language), 318–319****Domain Name System (DNS), 577****domains, VTP (VLAN Trunking Protocol), 12****domain-specific language (DSL), 365–366****DoS (denial-of-service) attacks, 386, 620****Down states (OSPF), 86****Downlink MACsec, 282****downloadable access control lists (dACLs), 288****DRaaS (disaster recovery as a service), 442****Dropbox, 441****DRs (designated routers), 85–86****DSCPs (differentiated services code points), 220–221, 495, 497, 626****DSL (domain-specific language), 365–366****dst-ip method, 53****dst-mac method, 53****dst-port method, 54****DTLS (Datagram Transport Layer Security), 412, 414****DTP (Dynamic Trunking Protocol), 9–11****DUAL (diffusing update algorithm), 61****dump() method, 311****dumps() method, 311****dynamic assignment, 280****dynamic auto mode (DTP), 9****dynamic desirable mode (DTP), 9****Dynamic Multipoint VPN (DMVPN), 559–560****dynamic NAT (Network Address Translation), 134, 137–138****Dynamic Trunking Protocol (DTP), 9–11****E****EAP (Extensible Authentication Protocol), 254–257, 289****eBGP (external BGP), 104–105, 113–114****echo operation (ICMP), IP Service Level Agreement (SLA) for, 644–647****ECN (explicit congestion notification), 495****edge, network**

- definition of, 381–382

- edge nodes, 479–480

- edge ports, 27

- edge routers, 460–461

- security threats to, 267

**edit-config operation (NETCONF), 663****EEM (Embedded Event Manager), 351–362****applets**

- actions, 355–357, 359–360

- creating, 357–359

- architecture, 354–355

- benefits of, 351–362

- definition of, 352

- event detectors, 354–355

- further reading, 362

- policies, 355–360

- scripts, 353, 358–360

- server, 354

- Tel (Tool Command Language), 351, 352, 358–359

**EF (Expedited Forwarding), 497****EGP (exterior gateway protocol), 104–105****egress tunnel routers (ETRs), 575****EIDs (endpoint identifiers), 474, 478, 574, 575, 581–582****EID-to-RLOC mapping, 474**

**EIGRP (Enhanced Interior Gateway Routing Protocol), 68–78**

- authentication, 76
- configuration, 69–70
- FD (feasible distance), 69
- feasibility conditions, 69
- feasible successors, 69
- metrics, 73–75
- named mode, 76–78
- neighbor tables, 70–72
- RD (reported distance), 69
- route summarization, 78
- routing tables, 75–76
- successor routes, 68
- successors, 68
- topology tables, 72–75
- verifying, 70

**Elastic Beanstalk, 440****elasticity of cloud computing, 435****electromagnetic fields (EMF), 168–169****Elevation plane pattern, 180****elif statement, 309****else statement, 309, 311****Email Security Appliance (ESA), 272, 274****Embedded Event Manager. See EEM (Embedded Event Manager)****Embedded Event Manager (EEM), 154****Embedded Wireless Controller (EWC), 422–424****embedded wireless deployments, 411, 422–424****Embedded Wireless, SD-Access, 481****EMF (electromagnetic fields), 168–169****enable password command, 198–199****enable secret command, 199–200****Encapsulated Remote SPAN (ERSPAN), 635–637****Encapsulating Security Payload (ESP), 564****encapsulation, VXLAN (Virtual Extensible LAN), 480****encapsulation dot1q command, 16****encoding formats**

definition of. *See* data-encoding formats

**JSON (JavaScript Object Notation)**

data types, 320

file structure, 319–320

formatting, 320–321

further reading, 324

XML (Extensible Markup Language) compared to, 321

**XML (Extensible Markup Language)**

characteristics of, 317–318

documents, 318–319

further reading, 324

JSON (JavaScript Object Notation) compared to, 321

syntax for, 318

**encryption**

AES (Advanced Encryption Standard), 252, 420

AES-256, 420

CAPWAP (Control and Provisioning of Wireless Access Points), 414

GCM (Galois/Counter Mode), 252

TKIP (Temporal Key Integrity Protocol), 251–252

**ENCS (Enterprise Network Compute Systems), 420, 540****endpoint identifiers (EIDs), 474, 478, 574, 575, 581–582****endpoints, Cisco AMP for Endpoints, 271****Enforcement phase (TrustSec), 280****enhanced object tracking (EOT) event detector, 354****enterprise network architecture options, 383–390**

Layer 2 access design, 385–386

Layer 3 access design, 386–387

SD-Access. *See* SD-Access

simplified campus design, 388–389

three-tier design, 383–384

two-tier design, 384–385

**Enterprise Network Compute Systems (ENCS), 420, 540**

**enterprise network design. See network design**

**Enterprise NFV (Network Function Virtualization). See Cisco Enterprise Network Function Virtualization (NFV)**

**enterprise wireless. See WLANs (wireless LANs)**

**EOT (enhanced object tracking) event detector, 354**

**errdisable recovery cause bpduguard command, 33**

**errdisable recovery internal command, 33**

**error messages, traceroute, 596**

**ERSPAN (Encapsulated Remote SPAN), 635–637**

**erspan-id command, 636**

**ESA (Email Security Appliance), 272, 274**

**E-Series servers, 539–540**

**ESP (Encapsulating Security Payload), 564**

**Established state (BGP), 107**

**EtherChannels, 47–54**

LACP (Link Aggregation Control Protocol), 48–52

overview of, 47–48

PAgP (Port Aggregation Protocol), 52–54

**ETRs (egress tunnel routers), 575**

**eval() method, 321**

**event detectors, EEM (Embedded Event Manager), 354–355**

**events, Cisco DNA Center, 338**

**EWC (Embedded Wireless Controller), 422–424**

**EWC-AP (Cisco Embedded Wireless Controller on Catalyst Access Points), 422–424**

**exception handling, Python, 311**

**Exchange states (OSPF), 87**

**EXEC modes**

access control to, 197–203

enable password command, 198–199

enable secret command, 199–200

line passwords, 197–198

usernames, 200–203

EXEC session timeouts, 205–206

**exec-timeout command, 205**

**exec-timeout minutes seconds command, 205**

**exit() command, 303**

**Expedited Forwarding (EF), 497**

**explicit congestion notification (ECN), 495**

**exporters, flow**

configuration, 628

definition of, 627

flow, 627, 628

flow exporter mapping to flow monitor, 629–630

**Exstart states (OSPF), 87**

**extended ACLs (access control lists), 225–226**

**Extended commands field (ping command), 600**

**extended ping**

example of, 601–602

fields, 599–601

**extended traceroute command, 595–597**

**Extensible Authentication Protocol (EAP), 254–257, 289**

**Extensible Markup Language. See XML (Extensible Markup Language)**

**Extensive Active Directory, Cisco ISE (Identity Services Engine) support for, 289**

**exterior gateway protocol (EGP), 104–105**

**external BGP (eBGP), 104–105, 113–114**

**External type 1 LSAs (link-state advertisements), 94**



**External type 2 LSAs (link-state advertisements), 94**

## F

**Fabric in a Box, 482**

**fabric roles, SD-Access, 477–482**

- border nodes, 480
- control plane nodes, 478–479
- definition of, 477–478
- edge nodes, 479–480
- Embedded Wireless, 481
- Fabric in a Box, 482
- fabric WLCs (Wireless LAN Controllers), 481
- fabric-mode APs, 481
- intermediate nodes, 480
- shared services, 482

**fabric wired connectivity, 337**

**fabric WLCs (Wireless LAN Controllers), 481**

**fabric-mode APs, 481**

**facility element (syslog), 615**

**FAST (EAP-Flexible Authentication via Secure Tunneling), 289**

**fast switching, 512**

**Fast Transition (FT), 186–187**

**feasibility conditions, 69**

**feasible distance (FD), 69**

**feasible successors, 69**

**Feature Manager (FM), 517**

**FEC (forward error correction), 455**

**Federal Communications Commission (FCC), 170**

**Federal Information Processing Standard (FIPS) 140–2, 289**

**FHRPs (first-hop redundancy protocols), 460**

- definition of, 392
- GLBP (Gateway Load Balancing Protocol), 150–153, 397–398
- HSRP (Host Standby Router Protocol), 143–147

authentication in, 392–393

configuration, 143–147

GLBP (Gateway Load Balancing Protocol) compared to compared to, 397

overview of, 392–395

states, 144

versions of, 392–393

VRRP (Virtual Router Redundancy Protocol) compared to, 396

object tracking with, 154

VRRP (Virtual Router Redundancy Protocol), 147–150, 396–397

**FIB (forwarding information base), 62, 63–64, 513**

**field-programmable gate array (FPGA), 471**

**file data type, 307**

**File services, 337**

**filename extensions**

.pp, 366

.py, 304, 310

**filtering, URL, 456**

**finally block, 311**

**firewalls**

application-aware, 456

NGFWs (Next-Generation Firewalls), 276–277

**first-hop redundancy protocols.**

**See FHRPs (first-hop redundancy protocols)**

**Flex+Bridge mode (APs), 177**

**FlexConnect mode (APs), 177**

**FlexConnect wireless deployments, 410, 415–418**

**Flexible NetFlow, 625–631**

benefits of, 625–626

capabilities of, 626

components of, 626–627

flow exporter mapping to flow monitor, 629–630

flow exporters, 627, 628

flow monitor, 627, 628–629

flow monitor configuration on interface, 630–631

flow records, 627–628

flow samplers, 627

### **FlexVPN, 561–562**

### **floating static routes, 66**

### **flow exporters, 627, 628**

configuration, 628

definition of, 627

mapping to flow monitor, 629–630

### **flow monitor**

configuration, 628–629, 630–631

definition of, 627

flow exporter mapping to, 629–630

### **flow records**

configuration, 627–628

definition of, 627

### **flow samplers, 627**

### **FM (Feature Manager), 517**

### **format method, 307**

### **formatting JSON (JavaScript Object Notation), 320–321**

### **forward delay time, 25**

### **forward error correction (FEC), 455**

### **forwarding information base (FIB), 62–64, 513**

### **forwarding plane, SDN (software-defined networking) architecture, 240**

### **Forwarding state (Layer 2 ports), 24, 26**

### **forwarding traffic**

assured forwarding (AFxy), 497

CEF (Cisco Express Forwarding), 495, 512–515

benefits of, 512

components of, 513–514

modes of operation, 514–515

Expedited Forwarding (EF), 497

fast switching, 512

overview of, 506–509

PIM (Protocol Independent Multicast), 162

process switching, 511

### **FPGA (field-programmable gate array), 471**

### **free space path loss, 171**

### **frequency seconds command, 645, 647**

### **FT (Fast Transition), 186–187**

### **Full states (OSPF), 87**

### **fully meshed networks, 558**

### **fully specified static routes, 65–66**

### **functions and methods, 307**

cli.cli(), 305

cli.clip(), 305

cli.configure(), 306

cli.configurep(), 306

cli.execute(), 305

cli.executep(), 305

dst-ip, 53

dst-mac, 53

dst-port, 54

dump(), 311

dumps(), 311

eval(), 321

format, 307

load(), 311

loads(), 311

in Python, 306–307

replace, 307

src-dst-ip, 54

src-dst-mac, 54

src-dst-port, 54

src-ip, 54

src-mac, 54

src-port, 54

startswith, 307

### **further reading**

BGP (Border Gateway Protocol), 121

Cisco DNA Center, 660

Cisco EEM (Embedded Event Manager), 362

Cisco SD-WAN (Software-Defined Wide Area Network), 466

cloud computing, 450

- configuration management and orchestration tools, 378
- device access control, 218
- DNA Center and vManage APIs, 344
- infrastructure security, 237
- IP (Internet Protocol) services, 166
- IP Service Level Agreement (SLA), 660
- Layer 2 technologies, 58
- Layer 3 technologies, 101
- monitoring, 640
- NAC (network access control), 296
- network assurance and troubleshooting, 611
- network design, 408
- network security design, 285
- network virtualization, 543, 571, 586
- Python, 314
- QoS (quality of service), 503
- REST (representational state transfer) APIs, 245, 349
- RESTCONF (Representational State Transfer Configuration Protocol), 671
- SD-Access, 484
- switching, 523
- wireless security, 262
- WLANs (wireless LANs), 192, 431
- YANG (Yet Another Next Generation), 332

## G

- Galois Message Authentication Code (GMAC), 282**
- Galois/Counter Mode Advanced Encryption Standard (AES-GCM), 282**
- Galois/Counter Mode (GCM), 252**
- Gateway Load Balancing Protocol (GLBP), 150–153, 397–398**
- gateways. See also BGP (Border Gateway Protocol)**
  - ABGs (active virtual gateways), 398
  - EGP (exterior gateway protocol), 104–105
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 68–78
    - authentication, 76
    - configuration, 69–70
    - FD (feasible distance), 69
    - feasibility conditions, 69
    - feasible successors, 69
    - metrics, 73–75
    - named mode, 76–78
    - neighbor tables, 70–72
    - RD (reported distance), 69
    - route summarization, 78
    - routing tables, 75–76
    - successor routes, 68
    - successors, 68
    - topology tables, 72–75
    - verifying, 70
  - GLBP (Gateway Load Balancing Protocol), 150–153, 397–398
  - SIG (Secure Internet Gateway), 456
- GCM (Galois/Counter Mode), 252**
- GCP (Google Cloud Platform), 421, 439**
- Generic Routing Encapsulation. See GRE (Generic Routing Encapsulation)**
- GET action (HTTP), 336, 346**
- get operation (NETCONF), 663**
- get-config operation (NETCONF), 663**
- gf3ed, 131**
- GitHub, Postman on, 340**
- GLBP (Gateway Load Balancing Protocol), 150–153, 397–398**
- glbp command, 150–153**
- globally scoped addresses[ref="157"], 157**
- GLOP addresses, 157**
- GMAC (Galois Message Authentication Code), 282**
- Google**
  - Google App Engine, 440
  - Google Cloud Platform (GCP), 421, 439

Google Workspace, 441

gRPC (RPC framework by Google),  
328–329

**GoToMeeting, 441**

**grain, SaltStack, 371**

**GRE (Generic Routing Encapsulation),  
547–548, 552–556**

benefits of, 552–553

characteristics of, 553

configuration, 554–556

definition of, 552

GRE Tunneling over IPsec, 567–568

packet format, 554

troubleshooting, 556

tunnel topology, 552

verifying, 556

**GRE Tunneling over IPsec, 567–568**

**groups, mobility, 187–188**

**gRPC (RPC framework by Google),  
328–329**

**guaranteed rate service, 494**

**guest access, 290**

**guest life cycle management, Cisco  
ISE (Identity Services Engine), 289**

**Guest Shell, 533**

configuration, 301–302

entering/exiting, 303–304

**guest tunneling, 188**

**guestshell run python command,  
302–303**

## H

---

**hard resets (BGP), 111**

**hardware redundancy. See also  
control plane; data plane**

NSF (Nonstop Forwarding), 405

overview of, 400

SSO (Stateful Switchover),  
400–405

**Hatch, Thomas S.369**

**headers, LISP (Cisco Locator/ID  
Separation Protocol), 577–578**

**Hello packets**

EIGRP (Enhanced Interior Gateway  
Routing Protocol), 71

HSRP (Host Standby Router  
Protocol), 393, 395

OSPF (open shortest path first), 87

**hello time, 24–25**

**hello timers (HSRP), 395**

**help() command, 304–305, 306**

**helper utilities, Python, 306**

**hertz (Hz), 169**

**hierarchical LAN design model**

access layer, 381–382

core layer, 382–383

distribution layer, 382

overview of, 380–381

**hold timers (HSRP), 395**

**host files, Ansible, 374**

**Host Standby Router Protocol. See  
HSRP (Host Standby Router Protocol)**

**host tracking database (HTDB), 478**

**hosted hypervisors, 528–529**

**hosted private cloud, 444**

**hosts, IGMP (Internet Group  
Management Protocol), 158**

**HSRP (Host Standby Router Protocol),  
143–147**

authentication in, 392–393

configuration, 143–147

GLBP (Gateway Load Balancing  
Protocol) compared to compared  
to, 397

overview of, 392–395

states, 144

versions of, 392–393

VRRP (Virtual Router Redundancy  
Protocol) compared to, 396

**HTDB (host tracking database), 478**

**HTTP (Hypertext Transfer Protocol)**

actions, 346

DELETE, 346

GET, 336, 346

POST, 346

PUT, 346  
HTTPS, 240–245  
  monitoring of HTTP destinations,  
  647–648  
  status codes, 347–348  
**HTTPS (HTTP Secure), 240–245**  
**hub-and-spokes networks, 558**  
**hybrid cloud, 444–445**  
**hypervisors, 527–530**

## I

---

**IaaS (Infrastructure as a Service), 421, 438–439, 452, 456**  
**IANA (Internet Assigned Numbers Authority), 157**  
**iBGP (internal BGP), 104–105**  
**ICMP echo operation, 644–648**  
**ICV (Integrity Check Value), 281**  
**idempotency, 363**  
**Identity Services Engine. See ISE (Identity Services Engine)**  
**Idle state (BGP), 106**  
**IDSs (intrusion detection systems), 456, 538**  
**IEEE (Institute of Electrical and Electronics Engineers), 48. See also 802.11 wireless standards; LACP (Link Aggregation Control Protocol); STP (Spanning Tree Protocol)**  
**IETF (Internet Engineering Task Force), 104. See also OSPF (open shortest path first)**  
  CAPWAP (Control and Provisioning of Wireless Access Points), 176, 412–415  
  NETMOD working group, 327  
**if statement, 309**  
**IGMP (Internet Group Management Protocol), 156, 157–161**  
  hosts, 158  
  join and leave operations, 159–160  
  queriers, 158  
  snooping, 159–161  
  versions of, 158  
**IKE (Internet Key Exchange), 563**  
**import cli command, 305**  
**import statement, 328**  
**incidence response, NAC (network access control), 290**  
**include statement, 328**  
**individual point-to-point networks, 558**  
**Infrastructure as a Service (IaaS), 421, 438–439, 452, 456**  
**infrastructure security, 219**  
  ACLs (access control lists), 219, 507, 538  
  definition of, 220  
  extended, 225–226  
  named, 226–228  
  port, 229  
  rules for implementation of, 221–222  
  standard, 224–225  
  VLAN, 230–231  
  wildcard masking, 222–224  
  CoPP (control plane policing), 233–235  
  further reading, 237  
**ingress tunnel routers (ITRs), 575**  
**Init state**  
  HSRP (Host Standby Router Protocol), 144, 393  
  OSPF (open shortest path first), 86  
**inside global addresses, 135**  
**inside local addresses, 135**  
**instance command, 40–41**  
**Institute of Electrical and Electronics Engineers. See IEEE (Institute of Electrical and Electronics Engineers)**  
**integrated services (IntServ), 487, 493**  
**Integrated Services Virtual Router (ISRV), 539**  
**Integration API, 338**  
**Integrity Check Value (ICV), 281**  
**intelligent queueing, 494**  
**Intent API, 335**

interarea prefix LSAs (link-state advertisements) for ABRs

**interarea prefix LSAs (link-state advertisements) for ABRs, 96**

**interarea router LSAs (link-state advertisements) for ASBRs, 97**

**interface vlan command, 16**

**intermediate nodes, SD-Access, 480**

**internal BGP (iBGP), 104–105**

**internal buffers, 614**

**internal private cloud, 444**

**internal spanning tree (IST), 41**

**Internet Assigned Numbers Authority (IANA), 157**

**Internet Engineering Task Force. See IETF (Internet Engineering Task Force)**

**Internet Group Management Protocol. See IGMP (Internet Group Management Protocol)**

**Internet Key Exchange (IKE), 563**

**Internet of Things (IoT), 452, 652**

**Internet Protocol routing. See IP (Internet Protocol) routing**

**Internet Protocol services. See IP (Internet Protocol) services**

**Internet Security Association and Key Management Protocol (ISAKMP), 563**

**inter-VLAN routing, 15**

**intra-area prefix LSAs (link-state advertisements), 97**

**intra-controller roaming, 186**

**intrusion detection systems (IDSs), 456, 538**

**intrusion prevention systems (IPSs), 456, 537, 538**

**inventory, Ansible, 373**

**iOS and Samsung Client Device Analytics, 657**

**IOS CLI sessions, access control to, 194–196**

**IOS EXEC modes, access control to, 197–203**

enable password command, 198–199

enable secret command, 199–200

line passwords, 197–198

usernames, 200–203

**IoT (Internet of Things), 452, 652**

**iox command, 302**

**IOx Guest Shell**

configuration, 301–302

entering/exiting, 303–304

**IP (Internet Protocol) routing**

addresses, 222–224, 463

IP flow, 621–622

IP Service Level Agreement (SLA), 641–651

benefits of, 643–644

capabilities of, 643

definition of, 643

event detector, 354

further reading, 660

ICMP echo operation, 644–647

measurement of IP SLA UDP

jitter operation, 647–648

monitoring of HTTP destinations, 647–648

requirements for, 643–644

IPAM (IP Address Management), 334, 482

IPv4, 104, 412

IPv6, 104, 289, 412

outer LISP IP headers, 578

overview of, 60–61

path selection, 62–64

AD (administrative distance), 62–64

FIB prefix length, 62, 63–64

metrics, 63, 64

routing algorithms, 61–62

routing tables, 105–106

static routing, 65–66

**IP (Internet Protocol) services, 123.**

**See also IPsec VPNs**

FHRPs (first-hop redundancy protocols), 460

GLBP (Gateway Load Balancing Protocol), 150–153

- HSRP (Host Standby Router Protocol), 143–147, 392–395, 396–397
  - object tracking with, 154
  - VRRP (Virtual Router Redundancy Protocol), 147–150
- further reading, 166
- IGMP (Internet Group Management Protocol), 156
- IP multicast, 156
  - benefits of, 156
  - IGMP (Internet Group Management Protocol), 157–161
  - multicast group addressing, 157
  - PIM (Protocol Independent Multicast), 156, 161–164
- NAT (Network Address Translation), 134–135, 461, 538
  - configuration topology, 135
  - dynamic NAT, 134, 137–138
  - overview of, 134–135
  - PAT (Port Address Translation), 134, 138–141
  - static NAT, 134, 136–137
- NTP (Network Time Protocol), 124–132, 615
  - access lists, 132
  - authentication, 131–132
  - need for, 124–125
  - peer and server associations, 125–126
  - peers, 130
  - router configuration, 125–130
- PAT (Port Address Translation), 138–141
- ip access-group access-list name command, 227**
- ip access-group access-list number command, 226**
- ip access-list extended name command, 227**
- ip access-list log-update command, 228**
- IP Address Management (IPAM), 334, 482**
- IP explicit congestion notification (ECN), 495**
- ip flow command, 623**
- ip flow-top-talker command, 624**
- ip flow-top-talkers command, 625**
- ip http authentication local command, 669**
- ip http secure-server command, 669**
- ip nat inside command, 136, 138**
- ip nat inside source list acl command, 138**
- ip nat inside source list acl pool nat-pool-name command, 138**
- ip nat inside source static inside-local-ip inside-global-ip command, 136**
- ip nat inside static command, 136**
- ip nat outside command, 136, 138**
- ip nat pool nat-pool-name starting-ip ending-ip prefix-length prefix-length command, 138, 140**
- ip nat translations command, 136, 139**
- ip ospf authentication key-chain command, 83**
- ip ospf authentication message-digest command, 82**
- ip ospf cost command, 81, 92**
- ip ospf dead-interval command, 92**
- ip ospf hello-interval command, 92**
- ip ospf message-digest-key *key-id* md5 *key* command, 82**
- ip ospf message-digest-key *key-id* md5 *key* command, 82**
- ip ospf priority command, 92**
- ip ospf *process-id* area *area-id* command, 87–88**
- IP precedence (IPP), 495**
- ip route command, 65–66**
- IP Security. See IPSec VPNs**
- IP Service Level Agreement (SLA), 641–651**
  - benefits of, 643–644
  - capabilities of, 643

## IP Service Level Agreement (SLA)

- definition of, 643
- event detector, 354
- further reading, 660
- ICMP echo operation, 644
- measurement of IP SLA UDP jitter operation, 647–648
- monitoring of HTTP destinations, 647–648
- requirements for, 644

**ip sla operation-number command, 645, 647**

**ip sla responder command, 648–649**

**ip sla schedule operation-number command, 647**

**ip ssh timeout seconds authentication-retries number command, 204**

**ip ssh version 2 command, 204**

**ip summary-address eigrp command, 78**

**IP type of service (ToS) byte, 496**

**IPAM (IP Address Management), 334, 482**

**IPSec VPNs, 558–562**

- Cisco IOS FlexVPN, 561–562
- Cisco IOS VTIs (Virtual Tunnel Interfaces), 560–561
- DMVPN (Dynamic Multipoint VPN), 559–560
- GRE Tunneling over IPsec, 567–568
- IP Security (IPsec), 562–567
  - AH (Authentication Header), 564
  - configuration, 564–567
  - definition of, 562
  - ESP (Encapsulating Security Payload), 564
  - features of, 562–563
  - IKE (Internet Key Exchange), 563
  - modes of operation, 567
  - verifying, 565–567
- site-to-site VPNs, 558–559

**IPSS (intrusion prevention systems), 456, 537, 538**

**ipv6 unicast-routing command, 97, 98**

**ISAKMP (Internet Security Association and Key Management Protocol), 563**

**ISE (Identity Services Engine), 212, 272–273, 288–289, 468–469, 472. See also REST (representational state transfer) APIs; SD-Access**

**ISR 4000 routers, 539–540**

**ISRV (Integrated Services Virtual Router), 539**

**issues, returning information about, 336**

**IST (internal spanning tree), 41**

**ITRs (ingress tunnel routers), 575**

**ITSM (IT Service Management), 334**

## J

---

**JavaScript, 321**

**JavaScript Object Notation. See JSON (JavaScript Object Notation)**

**jitter, 491, 647–648**

**JSON (JavaScript Object Notation)**

- data types, 320
- file structure, 319–320
- formatting, 320–321
- parsing Python output to, 310–311
- XML (Extensible Markup Language) compared to, 321

## K

---

**keepalive messages (BGP), 106**

**key caching, 186**

**keychains, 82–83**

**keys, cryptographic, 186**

**Know Your Network request paths, 336**

**KVM, 289, 528**

## L

---

**L2TP (Layer 2 Tunneling Protocol), 560**

**L2VPNs (Layer 2 VPNs), 104**

**L3VPNs (Layer 3 VPNs), 104–105**



**LACP (Link Aggregation Control Protocol), 48–52****LANs (local area networks). See also network design; WLANs (wireless LANs)**

- hierarchical LAN design model

- access layer, 381–382

- core layer, 382–383

- distribution layer, 382

- overview of, 380–381

- LAN Automation, 471

**Layer 2 technologies, 1. See also switching**

- access design, 385–386

- EtherChannels, 47–54

- LACP (Link Aggregation Control Protocol), 48–52

- overview of, 47–48

- PAgP (Port Aggregation Protocol), 52–54

- further reading, 58

- L2TP (Layer 2 Tunneling Protocol), 560

- L2VPNs (Layer 2 VPNs), 104

- Layer 2 roaming, 187

- Layer 2 security

- EAP (Extensible Authentication Protocol) authentication, 254–257

- Open Authentication, 249–251

- PSK (pre-shared key) authentication, 251–253

- overlays, 471, 581

- parameters, 495

- STP (Spanning Tree Protocol), 19–45

- BPDU (bridge protocol data unit) messages, 19–20

- BPDU Filter, 35–36

- BPDU Guard, 33–34

- Bridge Assurance, 37–38

- designated port elections, 20–25

- Loop Guard, 36–37

- MST (Multiple Spanning Tree), 40–45

- overview of, 19–20

- port roles, 26–28

- port states, 26

- PortFast, 32–33

- root bridges, 20–25

- Root Guard, 31–32

- root ports, 20–25

- RSTP (Rapid Spanning Tree Protocol), 25–28

- switch priorities, 28–31

- timers, 24–25

- UDLD (Unidirectional Link Detection), 38–40

- VLANs (virtual LANs), 3–17

- 802.1Q trunking, 7–9

- assignment of, 4–6

- creating, 4–5

- DTP (Dynamic Trunking Protocol), 9–11

- inter-VLAN routing, 16–17

- overview of, 3

- VTP (VLAN Trunking Protocol), 11–15

**Layer 3 technologies, 59. See also BGP (Border Gateway Protocol); IP (Internet Protocol) routing; switching**

- access design, 386–387

- EIGRP (Enhanced Interior Gateway Routing Protocol), 68–78

- authentication, 76

- benefits of, 68

- configuration, 69–70

- FD (feasible distance), 69

- feasibility conditions, 69

- feasible successors, 69

- metrics, 73–75

- named mode, 76–78

- neighbor tables, 70–72

- RD (reported distance), 69

- route summarization, 78

- routing tables, 75–76

## Layer 3 technologies

- successor routes, 68
  - successors, 68
  - topology tables, 72–75
  - verifying, 70
- further reading, 101
- L2VPNs (Layer 2 VPNs), 104–105
- Layer 3 roaming, 187
- Layer 3 security, 257–260
- OSPF (open shortest path first), 80–98, 460
  - areas, 83–84
  - authentication, 82–83
  - basic configuration, 87–90
  - costs, 81
  - default route advertisements, 91
  - definition of, 80
  - Dijkstra shortest path first algorithm, 80–81
  - LSAs (link-state advertisements), 80–81, 92–93
  - LSDB (link-state database), 80–81
  - neighbors and adjacencies, 85–87
  - optimizations, 92
  - OSPFv2, 80
  - OSPFv3, 80, 95–98
  - packet types, 87
  - passive interfaces, 91
  - path selection, 93–94
  - RID (router ID), 91
  - route summarization, 95
  - states, 86
  - verifying, 87
  - versions of, 80
- overlays, 472, 582
- parameters, 495
- Layer 4 parameters, 495**
- Layer 7 parameters, 495**
- leaf nodes, YANG (Yet Another Next Generation), 329**
- leaf-list nodes, YANG (Yet Another Next Generation), 329**
- Learning state (Layer 2 ports), 24, 26, 144, 393**
- Lightweight Access Point Protocol (LWAPP), 176, 412**
- lightweight mode (APs), 176**
- lightweight wireless deployments, 412**
- limited-scope addresses, 157**
- line passwords, 197–198**
- Link Aggregation Control Protocol (LACP), 48–52**
- link-state advertisements (LSAs), 80–81, 92–93, 97**
- link-state algorithms, 61**
- link-state database (LSDB), 80–81**
- link-state request (LSR) packets, 87**
- link-state update (LSU) packets, 87**
- LISP (Locator/ID Separation Protocol), 474**
  - architecture, 577–578
  - benefits of, 574–575
  - components of, 574–576
  - definition of, 573
  - deployment environment, 576–577
  - limitations of, 573
- list data type, 307**
- list nodes, YANG (Yet Another Next Generation), 329**
- Listening state (Layer 2 ports), 24, 26, 144, 393**
- LLQ (low-latency queueing), 499**
- load, CPU, 490**
- load() method, 311**
- load sharing, HSRP (Host Standby Router Protocol), 394**
- Loading states (OSPF), 87**
- loads() method, 311**
- local CLI sessions, 195**
- local mode (APs), 177**
- Local preference attribute (BGP), 108**
- Local Web Authentication, 294**
- location services**
  - CMX (Cisco Mobile Experience), 427–428

- CMX Analytics, 428
- CMX Connect, 428
- wireless, 418–422
- Locator/ID Separation Protocol (LISP), 474**
- log keyword, 230**
- logging configuration, syslog, 617–618**
- logging rate-limit command, 617**
- login local command, 204**
- log-input keyword, 225**
- Loop Guard, 36–37**
- Loose field**
  - ping command, 600
  - traceroute command, 597
- low-latency queueing (LLQ), 499**
- LSACK (link-state ack), 87**
- LSAs (link-state advertisements), 80–81, 92–93**
- LSDB (link-state database), 80–81**
- LSR (link-state request) packets, 87**
- LSU (Link-state update) packets, 87**
- LWAPP (Lightweight Access Point Protocol), 176, 412**

## M

---

- MAC Authentication Bypass (MAB), 292–293, 472**
- MAC security key agreement (MKA), 282**
- machine learning algorithms, 657**
- MAC-in-UDP encapsulation, 582**
- MACsec, 281–282**
- malware, Cisco AMP (Advanced Malware Protection), 271–272**
- management information base (MIB), 604–605**
- management plane**
  - SD-Access, 472, 474
  - SD-WAN (Software-Defined Wide Area Network), 459
- managers, SNMP (Simple Network Management Protocol), 604**
- manifests, Puppet, 366**
- map resolvers (MRs), 479, 576**
- map server/map resolver (MS/MR), 576**
- map servers (MSs), 478, 576**
- mapping agents, RP, 163–164**
- mapping EID-to-RLOC, 474**
- masters**
  - Puppet, 366
  - SaltStack, 370
- match command, 230, 627**
- max age time, 25**
- Maximum Time to Live field (traceroute command), 597**
- maximum transmission unit (MTU), 554**
- maximum-paths command, 94, 109**
- maximum-ratio combining, 174**
- MD5 authentication, 76, 80, 82, 395**
- MED (multi-exit discriminator), 62**
- Meraki, 272, 418–422**
- message-of-the-day (MOTD) banner, 367, 374–375**
- messages**
  - BGP (Border Gateway Protocol), 106
  - BPDU (bridge protocol data unit), 19–20
  - syslog
    - severity levels, 616–617
    - table of, 615–616
  - traceroute, 596
- metadata, Chef, 368**
- methods. See functions and methods**
- metric rib-scale command, 74**
- metrics**
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 73–75
  - IP (Internet Protocol) routing, 64
  - OSPF (open shortest path first), 81
    - in path selection, 63
- metric-type option, 91**
- mGRE (Multipoint GRE), 547–548**

MHSRP, HSRP (Host Standby Router Protocol) configured with

**MHSRP, HSRP (Host Standby Router Protocol) configured with, 394**

**MIB (management information base), 604–605**

**Microsoft Active Directory, 289**

**Microsoft Azure, 439, 452**

**Microsoft Hyper-V, 289, 528**

**Microsoft Office 365, 452**

**MIMO (multi-input, multi-out), 173–174**

**Minimum Time to Live field (traceroute command), 597**

**minions, Salt, 370**

**MLs (multilayer switches), 509, 517–520**

**MNEMONIC element (syslog), 615**

**mobile experiences**

CMX (Cisco Mobile Experience), 427–428

CMX Analytics, 428

CMX Connect, 428

Mobility Express, 423–424

mobility groups, 187–188

**model-driven programmability stack.**

**See also data models**

components of, 316–317

JSON (JavaScript Object Notation)

data types, 320

file structure, 319–320

formatting, 320–321

further reading, 324

XML (Extensible Markup Language)

characteristics of, 317–318

documents, 318–319

further reading, 324

syntax for, 318

**models**

hierarchical LAN design

access layer, 381–382

core layer, 382–383

distribution layer, 382

overview of, 380–381

QoS (quality of service), 487, 493–494

WLAN (wireless LAN), 410–411

autonomous, 410, 411–412

centralized, 410, 412–415

Cisco FlexConnect, 410, 415–418

cloud-based, 411, 418–422

embedded, 411, 422–424

overview of, 409, 410–411

SD-Access. *See* SD-Access

**modes of operation**

APs (access points)

autonomous mode, 176

bridge mode, 177

Flex+Bridge mode, 177

FlexConnect mode, 177

lightweight mode, 176

local mode, 177

monitor mode, 177

rogue detector mode, 177

SE-Connect mode, 177

sniffer mode, 177

IP Security (IPsec), 567

**Modular QoS CLI (MQC), 500**

**modules**

Ansible, 374

Cisco Python module, 304–305

Puppet, 366–367

**monitor mode (APs), 177**

**monitoring, 613**

ERSPAN (Encapsulated Remote SPAN), 635–637

further reading, 640

HTTP destinations, 647–648

NetFlow, 620–631

benefits of, 620–621

capabilities of, 620

configuration, 623

data reporting, 622

Flexible NetFlow, 625–631

IP flow, 621–622

top talkers, 625

verifying, 623–624

RSPAN (Remote Switch Port Analyzer), 634–635

SPAN (Switch Port Analyzer), 632–633

syslog, 614–618
 

- configuration, 617–618
- definition of, 614
- message elements, 615–616
- severity levels, 616–617

**monitoring ports (SPAN), 632**

**monitors, flow**

- configuration, 628–631
- definition of, 627
- flow exporter mapping to flow monitor, 629–630

**MOTD (message-of-the-day) banner, 367, 374–375**

**MPLS (Multiprotocol Label Switching), 104–105**

**MQC (Modular QoS CLI), 500**

**MRs (map resolvers), 479, 576**

**MS/MR (map server/map resolver), 576**

**MSs (map servers), 479, 576**

**MST (Multiple Spanning Tree), 14, 40–45**

**MTU (maximum transmission unit), 554**

**multicast**

- benefits of, 156
- HSRP (Host Standby Router Protocol) messages, 393
- IGMP (Internet Group Management Protocol), 157–161
  - hosts, 158
  - join and leave operations, 159–160
  - queriers, 158
  - snooping, 160–161
  - versions of, 158
- multicast group addressing, 157
- OSPF (open shortest path first)
  - multicast addresses, 86
- PIM (Protocol Independent Multicast), 156, 161–164

NAT (Network Address Translation)

- forwarding modes, 162
- multicast distribution trees, 161
- RP (rendezvous points), 161, 163–164

**Multicloud, 456–457**

**multi-exit discriminator (MED), 62**

**multi-input, multi-out (MIMO), 173–174**

**multilayer switches (MLSs), 505, 509**

**Multiple Spanning Tree (MST), 14, 40–45**

**multiplexing, spatial, 173**

**Multipoint GRE (mGRE), 547–548**

**Multiprotocol Label Switching experimental values (MPLS EXP), 495**

**Multiprotocol Label Switching (MPLS), 104–105**

**multivendor support, Cisco DNA Center, 335, 338**

## N

**NAC (network access control). See also Cisco ISE (Identity Services Engine)**

- 802.1X, 290–292

- authentication initiation and message exchange, 292

- configuration, 291–292

- device roles, 291

- capabilities of, 290

- further reading, 296

- MAB (MAC Authentication Bypass), 292–293

- WebAuth, 293–295

**name command, 40–41**

**named ACLs (access control lists), 226–228**

**named mode (EIGRP), 76–78**

**namespaces, LISP deployment environment, 576–577**

**NAT (Network Address Translation), 134–135, 461, 538**

- configuration topology, 135

- dynamic NAT, 134, 137–138

## NAT (Network Address Translation)

- NAT-T (NAT traversal), 463, 563
- NVI (NAT virtual interface), 141
- overview of, 134–135
- PAT (Port Address Translation), 134, 138–141
- static NAT, 134, 136–137

**National Institute of Standards and Technology (NIST), 434****native (type 1) hypervisors, 528, 533****NAT-T (NAT traversal), 463, 563****NBAR (Network Based Application Recognition), 495****NCP (Network Control Platform), 472****ncsshd, 664–665****ndbmand, 664–665****NDP (Network Data Platform), 472****neighbor *ip-address* remote-as command, 112, 114****neighbors**

- BGP (Border Gateway Protocol)
  - definition of, 112
  - verifying, 116–117
- EIGRP (Enhanced Interior Gateway Routing Protocol) neighbor tables, 70–72
- NTP (Network Time Protocol), 125–130
- OSPF (open shortest path first), 85–87

**NETCONF (Network Configuration Protocol), 241, 326**

- benefits of, 663
- configuration, 664–666
- configuration datastores, 663–664
- definition of, 328–329, 662
- further reading, 671
- operations, 662–663

**netconf ssh command, 664–665****netconf-yang command, 664–665****netconf-yang feature candidate-datastore command, 664****NetFlow, 620–631**

- benefits of, 620–621

- capabilities of, 620
- configuration, 623
- data reporting, 622
- Flexible NetFlow, 625–631
  - benefits of, 625–626
  - capabilities of, 626
  - components of, 626–627
  - flow exporter mapping to flow monitor, 629–630
  - flow exporters, 627, 628
  - flow monitor, 627, 628–629
  - flow monitor configuration on interface, 630–631
  - flow records, 627–628
  - flow samplers, 627
- IP flow, 621–622
- top talkers, 625
- verifying, 623–624

**NETMOD working group, 327****NetOps, 652****network access control. See NAC (network access control)****Network Address Translation. See NAT (Network Address Translation)****network assurance, 587**

- further reading, 611
- SNMP (Simple Network Management Protocol), 604–608
  - components of, 604–605
  - configuration and verification, 607–608
  - operations, 605
  - security models and levels, 606–607
  - shortcomings of, 326
  - versions of, 606
- YANG (Yet Another Next Generation) as alternative to, 325
- troubleshooting
  - with debug, 589–593
- GRE (Generic Routing Encapsulation), 556
- overview of, 588

- with ping, 597–602
- with traceroute, 593–597
- traffic analysis, 589–593
- WLAN (wireless LAN)
  - configuration, 188–189
- Network Based Application Recognition (NBAR), 495**
- network command, 69, 87–88, 109, 112, 114, 117**
- Network Configuration Protocol. See NETCONF (Network Configuration Protocol)**
- Network Control Platform (NCP), 472**
- Network Data Platform (NDP), 472**
- network design, 379. See also wireless networking**
  - enterprise network architecture options, 383–390
    - Layer 2 access design, 385–386
    - Layer 3 access design, 386–387
    - SD-Access. *See* SD-Access
    - simplified campus design, 388–389
    - three-tier design, 383–384
    - two-tier design, 384–385
  - FHRPs (first-hop redundancy protocols)
    - definition of, 392
    - GLBP (Gateway Load Balancing Protocol), 397–398
    - HSRP (Host Standby Router Protocol), 392–395, 396, 397
    - VRRP (Virtual Router Redundancy Protocol), 396–397
  - further reading, 408
  - hardware redundancy
    - NSF (Nonstop Forwarding), 405
    - overview of, 400
    - SSO (Stateful Switchover), 400–405
  - hierarchical LAN design model
    - access layer, 381–382
    - core layer, 382–383
    - distribution layer, 382
    - overview of, 380–381
  - security design, 265
    - Cisco AMP (Advanced Malware Protection), 271–272
    - Cisco AnyConnect Secure Mobility Client, 272
    - Cisco Email Security, 274
    - Cisco Secure Network Analytics, 273
    - Cisco Secure Web Appliance, 273–274
    - Cisco Umbrella, 272–273
    - content security, 273–274
    - further reading, 285
    - MACsec, 281–282
    - NGFWs (Next-Generation Firewalls), 276–277
    - NGIPSs (Next-Generation IPSs), 275–276
    - SAFE security framework, 266–270
    - threat defense, 266–270
    - TrustSec, 279–280
- Network Discovery, 337**
- network edge. See edge, network**
- Network Function Virtualization. See NFV (Network Function Virtualization)**
- Network Health dashboard, 656**
- network layer reachability information (NLRI), 104–105**
- network layer, SD-Access, 471**
- network LSAs (link-state advertisements), 93, 96**
- network management system (NMS), 462**
- network processing units (NPU)s, 512**
- network security design, 265**
  - Cisco AMP (Advanced Malware Protection), 271–272
  - Cisco AnyConnect Secure Mobility Client, 272
  - Cisco Email Security, 274
  - Cisco Secure Network Analytics, 273

Cisco Secure Web Appliance,  
273–274

Cisco Umbrella, 272–273

content security, 273–274

further reading, 285

MACsec, 281–282

NGFWs (Next-Generation  
Firewalls), 276–277

NGIPSs (Next-Generation IPSs),  
275–276

SAFE security framework, 266–270

threat defense, 266–270

TrustSec, 279–280, 288–289,  
468–469, 475

### **Network Settings API, 336**

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

### **Network Time Travel, 656**

### **network virtualization, 545, 573**

definition of, 537

Enterprise NFV (Network Function  
Virtualization)

architecture, 538–539

benefits of, 537–538

hardware options, 539–540

further reading, 543, 571, 586

GRE (Generic Routing  
Encapsulation), 552–556

benefits of, 552–553

characteristics of, 553

configuration, 554–556

definition of, 552

GRE Tunneling over IPsec,  
567–568

packet format, 554

troubleshooting, 556

tunnel topology, 552

verifying, 556

hypervisors, 527–530

IPsec VPNs, 558–562

Cisco IOS FlexVPN, 561–562

Cisco IOS VTIs (Virtual Tunnel  
Interfaces), 560–561

DMVPN (Dynamic Multipoint  
VPN), 559–560

GRE Tunneling over IPsec,  
567–568

IP Security (IPsec), 562–567

site-to-site VPNs, 558–559

LISP (Cisco Locator/ID Separation  
Protocol)

architecture, 577–578

benefits of, 574–575

components of, 574–576

definition of, 573

deployment environment,  
576–577

limitations of, 573

overview of, 525–527

virtual switching, 535–536

VLAN ACLs (VACLs), 230–231

VLANs (virtual LANs), 526

VMs (virtual machines), 527–528,  
532–533

VRF (virtual routing and  
forwarding), 546–547

VRF-Lite, 547–550

benefits of, 548

configuration, 549–550

definition of, 547–548

VXLAN (Virtual Extensible LAN),  
580–584

benefits of, 580, 581

definition of, 581–582

overlays, 581–582

packet format, 580–581

VTEPs (VXLAN tunnel  
endpoints), 582–584

### **Next Hop Resolution Protocol (NHRP), 559**

### **Next\_Hop attribute (BGP), 108**

### **Next-Generation Firewall Virtual (NGFWv), 539**

### **Next-Generation Firewalls (NGFWs), 276–277**

### **Next-Generation IPSs (NGIPSs), 275–276**



**NFV (Network Function Virtualization), 336**

- architecture, 538–539
- benefits of, 537–538
- hardware options, 539–540
- NFVIS (NFV Infrastructure Software), 538

**NGFWs (Next-Generation Firewalls), 276–277****NGFWv (Next-Generation Firewall Virtual), 539****NGIPs (Next-Generation IPSs), 275–276****NHRP (Next Hop Resolution Protocol), 559****NIST (National Institute of Standards and Technology), 434****NLRI (network layer reachability information), 104–105****NMS (network management system), 462**

**no auto-summary command, 78**

**no exec-timeout command, 205**

**no switchport command, 51**

**noAuthNoPriv, 606–608**

**nodes**

- Chef, 368
- SD-Access
  - border nodes, 480
  - control plane, 478–479
  - edge nodes, 479–480
  - intermediate nodes, 480
- YANG (Yet Another Next Generation), 329

**none event detector (EEM), 355**

**non-fabric wireless connectivity, 337**

**Nonstop Forwarding (NSF), 405**

**normal mode (UDLD), 38–39**

**northbound APIs (application programming interfaces), 241**

**NOT operator, 308**

**notifications**

- BGP (Border Gateway Protocol), 106
- Cisco DNA Center, 338

**not-so-stubby areas (NSSAs), 93**

**NPUs (network processing units), 512**

**NSF (Nonstop Forwarding), 405**

**NSSA external LSA (link-state advertisement), 93**

**NSSAs (not-so-stubby areas), 93**

**NTP (Network Time Protocol), 124–132, 615**

- access lists, 132
- authentication, 131–132
- need for, 124–125
- peer and server associations, 125–126
- peers, 130
- router configuration, 125–130

**ntp access-group command, 132**

**ntp associations command, 126**

**ntp authenticate command, 131**

**ntp authentication-key key-id md5 key-string command, 131**

**ntp master stratum-number command, 126–127**

**ntp peer ip-address command, 126**

**ntp server ip-address command, 126–127**

**ntp server server-ip-address key key-id command, 131**

**ntp status command, 126**

**ntp trusted-key key-id command, 131**

**number data type, 306**

**Numeric display field (traceroute command), 597**

**NVI (NAT virtual interface), 141**

**O**

**Oakley, 563**

**object tracking**

- with FHRPs (first-hop redundancy protocols), 154
- HSRP (Host Standby Router Protocol), 394

off mode (VTP)

**off mode (VTP), 13**

**Office 365, 452**

**omnidirectional antennas, 181–182**

**OMP (Overlay Management Protocol), 459, 463**

**onboarding devices, 289**

**ONF (Open Networking Foundation), 241**

**on-premises infrastructure, 447**

**Open Authentication, 249–251**

**open messages (BGP), 106**

**Open Networking Foundation (ONF), 241**

**open shortest path first. See OSPF (open shortest path first)**

**open shortest path first (OSPF), 460**

**Open vSwitch, 536**

**OpenConfirm state (BGP), 107**

**OpenDNS, 272–273**

**OpenFlow, 241**

**OpenSent state (BGP), 107**

**OpenShift, 440**

**open-source tools**

Ansible, 372–375

Chef, 367–369

Puppet, 365–367

SaltStack, 369–371

**operational planes. See planes of operation**

**operational tools, Cisco DNA Center, 337**

**operators, 308**

**OpFlex, 241**

**optimization**

application, 455

OSPF (open shortest path first), 92

TCP (Transmission Control Protocol), 455

**optional nontransitive attributes (BGP), 108**

**OR operator, 308**

**Oracle VirtualBox, 529**

**orchestration plane, SD-WAN (Software-Defined Wide Area Network), 459**

**orchestration tools, 363–364**

agent-based

Chef, 367–369

definition of, 365

Puppet, 365–367

SaltStack, 369–371

agentless

Ansible, 372–375

Bolt, 375–376

comparison of, 376

further reading, 378

**orchestrators, vBond, 461**

**origin attribute (BGP), 108**

**OSPF (open shortest path first), 80–98, 460**

areas, 83–84

authentication, 82–83

basic configuration, 87–90

costs, 81

default route advertisements, 91

definition of, 80

Dijkstra shortest path first algorithm, 80–81

LSAs (link-state advertisements), 80–81, 92–93

LSDB (link-state database), 80–81

neighbors and adjacencies, 85–87

optimizations, 92

OSPFv2, 80

OSPFv3, 80, 95–98

packet types, 87

passive interfaces, 91

path selection, 93–94

RID (router ID), 91

route summarization, 95

states, 86

verifying, 87

versions of, 80

**ospfv3 process-id ipv6 area area-id command, 98**

**outbound vty access list, 224**

**outer LISP IP headers, 578**

**outer LISP UDP headers, 578**

**output**

ping command, 598

traceroute command, 594

**outside global addresses, 135**

**outside local addresses, 135**

**Overall Health dashboard, 657–658**

**Overlay Management Protocol (OMP), 459, 463**

**overlays**

SD-Access, 471–472

VXLAN (Virtual Extensible LAN), 581–582

## P

**PaaS (Platform as a Service), 440**

**Packet Description Language Module (PDLM), 495**

**packet switching mode, 490**

**packets**

ACK, 258–259

EIGRP (Enhanced Interior Gateway Routing Protocol), 71

GRE (Generic Routing Encapsulation), 554

LISP (Cisco Locator/ID Separation Protocol), 577–578

OSPF (open shortest path first), 87

packet loss, 489–490

SYN, 258

SYN-ACK, 258

VXLAN (Virtual Extensible LAN), 580–581

**PACLs (port ACLs), 229**

**PAGP (Port Aggregation Protocol), 52–54**

**Pairwise Transient Key (PTK), 186–187**

**PAP, Cisco ISE (Identity Services Engine) support for, 289**

**Parallels, 529**

**paranoid updates, 80–81**

**parsing Python output to JSON, 310–311**

**passive interface default command, 91**

**passive *interface-id* command, 91**

**passive interfaces, OSPF (open shortest path first), 91**

**passive mode (LACP), 48**

**passwords**

configuration, 197–198

in OSPF (open shortest path first), 82

types of, 196

**PAT (Port Address Translation), 134, 138–141**

**patch antennas, 183**

**path selection**

IP (Internet Protocol), 62–64

AD (administrative distance), 62–64

FIB prefix length, 62, 63–64  
metrics, 63, 64

OSPF (open shortest path first), 93–94

**Path Trace, 337, 656**

**path vector algorithm, 62, 107–111**

**path virtualization. See virtualization, network**

**PDLM (Packet Description Language Module), 495**

**PEAP, Cisco ISE (Identity Services Engine) support for, 289**

**peers. See neighbors**

**percent sign (%), 615**

**performance optimization. See optimization**

**PETRs (proxy ETRs), 576**

**PHBs (per-hop behaviors), 497**

**physical layer, SD-Access, 471**

**PIM (Protocol Independent Multicast), 156, 161–164**

BSR (Bootstrap Router), 164

## PIM (Protocol Independent Multicast)

- forwarding modes, 162
- multicast distribution trees, 161
- PIM Sparse-Dense Mode, 162
- PIM-DM (PIM Dense Mode), 162
- PIM-SM (PIM Sparse Mode), 162
- RP (rendezvous points), 161, 163–164

**ping command, 375–376, 597–602**

- extended ping, 599–602
- output characters, 598
- repeat count with, 599
- simple example, 598–599
- with size specified, 599

**PINs (places in the network), 266–268****PITRs (proxy ITRs), 576****places in the network (PINs), 266–268****plaintext authentication, 80, 394–395****plane patterns, 180–181****planes of operation**

- control plane, 400
- data plane, 400
- LISP (Cisco Locator/ID Separation Protocol), 577
- SD-Access, 458–459, 474–475
- SDN (software-defined networking) architecture, 240
- SD-WAN (Software-Defined Wide Area Network), 459
- VRF-Lite, 548

**Platform as a Service (PaaS), 440****playbooks, Ansible, 373****plays, Ansible, 373****point-to-point links, 27****policies**

- Cisco EEM (Embedded Event Manager), 355–360
- Cisco ISE (Identity Services Engine), 288
- life cycle management, 290
- SLA (service level agreement), 455

**policing, 497–498****policy mapping, 480****policy plane, SD-Access, 474****Policy section, DNA Center, 654****policy-map command, 234–235****port ACLs (PACLs), 229****Port Address Translation (PAT), 134, 138–141****Port Aggregation Protocol (PAgP), 52–54****Port Number field (traceroute command), 597****port-channel load-balance command, 54****PortFast, 32–33, 386****ports**

- assigning to VLANs, 4–6
- SPAN destination ports, 632
- STP (Spanning Tree Protocol)
  - default port cost values, 22–23
  - designated port elections, 20–25
  - port cost values, 22
  - roles, 26–27
  - root ports, 20–25
  - states, 24, 26

**POST action (HTTP), 346****Postman, 243, 340****.pp file extension, 366****prefix length (FIB), 62, 63–64****prefix statement, 328****pre-shared key (PSK) authentication, 251–253****print statement, 307****priority**

- HSRP (Host Standby Router Protocol), 394
- switches, 28–31

**private cloud, 420–421, 444****private IP (Internet Protocol) addresses, 463****privilege levels, 206–208****privilege mode level level command, 206–207**

**Probe count field (traceroute command), 597**

**process switching, 511**

**processing delay, 490**

**profiles**

device, 289

NAC (network access control), 290

QoS (quality of service), 501

**propagation delay, 490**

**Propagation phase (TrustSec), 280**

**Protocol [ip] field**

ping command, 600

traceroute command, 596

**Protocol Buffers, 329**

**Protocol Independent Multicast (PIM), 156, 161–164**

forwarding modes, 162

multicast distribution trees, 161

RPs (rendezvous points), 161, 163–164

**Provision section, DNA Center, 654**

**proxy ETRs (PETRs), 576**

**proxy ITRs (PITRs), 576**

**proxy xTRs (PxTRs), 480, 576**

**PSK (pre-shared key) authentication, 251–253**

**PTK (Pairwise Transient Key), 186–187**

**public cloud, 421–422, 444**

**public IP (Internet Protocol) addresses, 463**

**Puppet, 365–367. See also Bolt**

**PUT action (HTTP), 346**

**PxTRs (proxy xTRs), 480, 576**

**.py extension, 304, 310**

**Python, 299–314, 533**

Boolean operators, 308

capabilities of, 303

Cisco Python module, 304–305

CLI commands, 305–306

colon (:) in, 308–309

conditional statements, 308–309

data types, 306–307

exception handling, 311

further reading, 314

Guest Shell environment

configuration, 301–302

entering/exiting, 303–304

helper utilities and functions, 306

methods, 307

output, parsing to JSON, 310–311

overview of, 300

releases

comparison of, 301

verifying, 302–303

scripts

requirements for, 309–310

running, 304

## Q

**QoS (quality of service), 487, 538**

ACLs (access control lists), 507, 508

classification, 495–497

congestion avoidance, 500

congestion management, 499

DSCPs (differentiated services code points), 497

further reading, 503

marking, 495–497

models and components, 487, 493–494

need for, 488–489

delay, 490

jitter, 491

lack of bandwidth, 491

packet loss, 489–490

objective of, 488

PHBs (per-hop behaviors), 497

policing, 497–498

SD-WAN (Software-Defined Wide Area Network), 455

shaping, 497–498

wireless, 500–501

queriers, 158

Query packets (EIGRP), 71

queueing (congestion management), 494, 499

## R

radio frequency (RF), 168–170

RADIUS protocol, 211–212

  Cisco ISE (Identity Services Engine) support for, 289

  configuration, 215–216

  EAP (Extensible Authentication Protocol) authentication, 254–257

raise keyword, 311

ransomware, 273

Rapid Spanning Tree Protocol (RSTP), 25–28

RBAC (role-based access control), 206–208

RD (reported distance), 69

reactors, SaltStack, 370–371

received signal strength indicator (RSSI), 171

recipes, Chef, 368–369

Record field

  ping command, 600

  traceroute command, 597

records, flow, 627–628

recursive static routes, 65

redundancy, hardware. *See also* control plane; data plane

  NSF (Nonstop Forwarding), 405

  overview of, 400

  SSO (Stateful Switchover), 400–405

    benefits of, 401

    configuration on Cisco Catalyst 4500X, 401

    show redundancy clients command, 403–405

    verifying, 401–402

Reliable Transport Protocol (RTP), 70

remote CLI sessions, 195

Remote Procedure Call (RPC), 662

Remote Switch Port Analyzer (RSPAN), 634–635

remote-span command, 634

rendezvous points (RPs), 161, 163–164

Repeat count field (ping command), 600

repeat count, ping command for, 599

replace method, 307

Reply packets (EIGRP), 71

reported distance (RD), 69

representational state transfer APIs. *See* REST (representational state transfer) APIs

Representational State Transfer Configuration Protocol. *See* RESTCONF (Representational State Transfer Configuration Protocol)

Request packets (EIGRP), 71

requests, REST (representational state transfer) APIs, 243

requests for comments. *See* RFCs (requests for comments)

reserved link-local addresses, 157

Resign messages (HSRP), 393

resource providers, Chef, 368

Resource Reservation Protocol (RSVP), 494

resources

  Chef, 368

  Puppet, 367

REST (representational state transfer) APIs

  definition of, 242

  response codes, 345–349

    further reading, 349

    HTTP status codes, 347–348

    interpretation of, 346

  security, 240–245

RESTCONF (Representational State Transfer Configuration Protocol), 242, 326

  configuration, 669–670

- CRUD (create, read, update, and delete) mapping with, 668–669
- definition of, 328–329, 668
- further reading, 671
- restconf command, 669**
- RESTful DNA Center API, 335–336**
- return on investment (ROI), 527**
- reverse-path forwarding (RPF), 161–162**
- revision command, 40–41**
- RF (radio frequency), 168–170**
- RFCs (requests for comments)**
  - RFC 1112, 158
  - RFC 1918, 135
  - RFC 2236, 158
  - RFC 2474, 497
  - RFC 2597, 497
  - RFC 2858, 104
  - RFC 3268, 497
  - RFC 3376, 158
  - RFC 4271, 103
  - RFC 4541, 160–161
  - RFC 5059, 164
  - RFC 6020, 327
- RIB (routing information base), 62, 405**
- RID (router ID), 91**
- RLOCs (routing locators), 474, 574, 576, 581–582**
- roaming, wireless, 185–188**
- rogue detector mode (APs), 177**
- Rogue Management, 657**
- ROI (return on investment), 527**
- role-based access control (RBAC), 206–208**
- roles, Ansible, 373**
- ROMMON mode, 195**
- root bridges (STP), 20–25**
- Root Guard, 31–32**
- root ports, 20–27**
- root primary command, 29–31**
- route summarization**
  - EIGRP (Enhanced Interior Gateway Routing Protocol), 78
  - OSPF (open shortest path first), 95
- route verification, BGP (Border Gateway Protocol), 118**
- routed access design, 386–387**
- router bgp command, 112, 114**
- router eigrp command, 69, 76–78**
- router ID (RID), 91**
- router LSAs (link-state advertisements), 93, 96**
- router ospfv3 command, 97, 98**
- router-id command, 91, 98**
- routing, IP. See IP (Internet Protocol) routing**
- routing event detector, 355**
- routing information base (RIB), 62, 405**
- routing locators (RLOCs), 474, 574, 576, 581–582**
- routing tables (EIGRP), 75–76**
- RP mapping agents, 163**
- RPC (Remote Procedure Call), 662**
- RPC framework by Google (gRPC), 328–329**
- RPF (reverse-path forwarding), 161–162**
- RPCs (rendezvous points), 161, 163–164**
- RSPAN (Remote Switch Port Analyzer), 634–635**
- RSSI (received signal strength indicator), 171**
- RSTP (Rapid Spanning Tree Protocol), 25–28**
- RSVP (Resource Reservation Protocol), 494**
- RTP (Reliable Transport Protocol), 70**
- running configuration datastore (NETCONF), 664**
- running scripts**
  - EEM (Embedded Event Manager), 358–360
  - Python, 304

## S

**SaaS (Software as a Service), 441, 452, 457**

**SAFE security framework, 266–270**

**SaltStack, 369–371**

**samplers, flow, 627**

**SAP (Security Association Protocol), 282**

### scripts

EEM (Embedded Event Manager)

purpose of, 353

running, 358–360

Python. *See* Python

**SD-Access, 451**

architecture, 471–472

definition of, 411

fabric roles and components, 477–482

border nodes, 480

control plane nodes, 478–479

definition of, 477–478

edge nodes, 479–480

Embedded Wireless, 481

Fabric in a Box, 482

fabric WLCs (Wireless LAN Controllers), 481

fabric-mode APs, 481

intermediate nodes, 480

shared services, 482

further reading, 484

operational planes, 474–475

overview of, 390, 467–469

**SDM (Switching Database Manager)**

changing, 518–519

features of, 517–518

templates, 517–520

verifying, 519–520

**sdm prefer command, 518–520**

**SDN (software-defined networking) architecture, 240. *See also* SD-Access; SD-WAN (Software-Defined Wide Area Network)**

**SD-WAN (Software-Defined Wide Area Network). *See also* Cisco DNA Center**

architecture, 334–335

common use cases, 454–457

application performance optimization, 455

Cisco Multicloud, 456–457

secure automated WAN, 454–455

secure DIA (Direct Internet Access), 456

components of, 459–464

planes of operation, 459

vBond orchestrators, 461

vManage, 461–462

vSmart controllers, 459–460

WAN edge routers, 460–461

definition of, 451

delivery, 452

deployment considerations, 463–464

further reading, 466

need for, 453–454

overview of, 452–453

**SE-Connect mode (APs), 177**

**SecOps, 652**

**SecTAG, 281**

**Secure Cloud Analytics, 273**

**Secure Internet Gateway (SIG), 456**

**Secure Network Analytics, 273**

**Secure Shell. *See* SSH (Secure Shell)**

**Secure Sockets Layer. *See* SSL (Secure Sockets Layer)**

**Secure Web Appliance, 273–274**

**Security Association Protocol (SAP), 282**

**security group ACLs (SGACLs), 288–289**

**security group tags (SGTs), 279, 288–289, 468–469**

**segmentation, VPN, 269, 463**

**seq no element (syslog), 615**

**serialization delay, 490**

**server mode (VTP), 13**



**servers**

- Chef, 368
- Cisco E-Series, 539–540
- Cisco Secure Access Control Server, 212
- Cisco UCS C-Series, 539
- EAP (Extensible Authentication Protocol) authentication, 254
- EEM (Embedded Event Manager), 354
- MSs (map servers), 478, 576
- NMS (network management system), 462
- syslog, 614–618
  - configuration, 617–618
  - definition of, 614
  - message elements, 615–616
  - severity levels, 616–617

**service level agreements. See SLA (service level agreement)****service models, cloud computing**

- BaaS (backup as a service), 442
- DRaaS (disaster recovery as a service), 442
- IaaS (Infrastructure as a Service), 438–439
- PaaS (Platform as a Service), 440
- SaaS (Software as a Service), 441
- XaaS (Anything as a Service), 442

**service set identifiers (SSIDs), 248–249, 411****service-policy command, 234–235****Session Traversal Utilities for NAT (STUN) servers, 463****Set DF bit in IP header field (ping command), 600****severity levels, syslog, 615, 616–617****SGACLs (security group ACLs), 288–289****SGT Exchange Protocol (SXP), 280****SGTs (security group tags), 279, 288–289, 468–469****shaping, 497–498****shared services, SD-Access, 482****shared trees, 161****shebang (#!), 310****shells**

- Python Guest Shell
  - configuration, 301–302
  - entering/exiting, 303–304
- SSH (Secure Shell), 662
  - access control with, 195, 203–206
  - configuration, 204–206
  - versions of, 203

**shortest path first (SPF) algorithm, 61, 80–81****shortest path tree (SPT), 161****show adjacency command, 513–514****show command, 622****show crypto isakmp sa command, 565–567****show etherchannel load-balance command, 54****show etherchannel summary command, 50–52****show flow record CUSTOM command, 627****show glbp command, 151****show interface *interface* switchport command, 6, 11****show interface port-channel 1 command, 50–51****show interface trunk command, 11****show iox-service command, 302****show ip bgp command, 109–110, 113, 115–116, 117–118****show ip bgp neighbors command, 113, 116–117****show ip bgp summary command, 113****show ip cache flow command, 623****show ip cef command, 513–514****show ip eigrp interfaces command, 70****show ip eigrp neighbors command, 71****show ip flow export command, 623****show ip flow interface command, 623****show ip flow top-talkers command, 625**

show ip interface brief command

show ip interface brief command, 16

show ip nat translations command, 138

show ip ospf interface brief command, 88–89

show ip ospf interface command, 87–89, 92

show ip ospf neighbor [detail] command, 87–88

show ip ospf neighbor command, 89

show ip protocol command, 74–75, 90

show ip route bgp command, 118

show ip route eigrp command, 75–76

show ip route ospf command, 87–90

show ip sla configuration command, 647

show ip ssh command, 204

show ip statistics command, 649

show ip summary command, 649

show ipv6 route ospf command, 98

show logging command, 590–591

show mac address-table command, 516–517

show monitor session 1 command, 633

show monitor session 2 command, 634

show monitor session erspan-source session command, 636

show netconf-yang datastores command, 664–665, 666

show netconf-yang sessions command, 664, 666, 669

show netconf-yang statistics command, 664–665, 666

show ospfv3 interface command, 98

show ospfv3 ipv6 neighbor command, 98

show platform software yang-management process command, 664–665, 666, 669

show redundancy clients command, 403–405

show snmp host command, 607

show spanning-tree command, 21, 25

show spanning-tree mst command, 43–45

show spanning-tree mst configuration command, 41–43

show spanning-tree summary command, 22–23

show spanning-tree vlan 1 command, 22–23, 29–30

show standby command, 144

show vlan brief command, 4, 5–6

show vrrp command, 148

show vtp status command, 15

SIG (Secure Internet Gateway), 456

signal-to-noise ratio (SNR), 171–172

Simple Network Management Protocol. *See* SNMP (Simple Network Management Protocol)

simple password authentication, 82

simplified campus design, 388–389

Site Design API, 336

site management APIs, 336–337

sites, definition of, 336

site-to-site VPNs, 558–559

SKEME, 563

SLA (service level agreement), 154, 268, 455

definition of, 642

IP SLA, 641–651

benefits of, 643–644

capabilities of, 643

definition of, 643

further reading, 660

ICMP echo operation, 644–647

measurement of IP SLA UDP jitter operation, 647–648

monitoring of HTTP destinations, 647–648

requirements for, 644

sniffer mode (APs), 177

SNMP (Simple Network Management Protocol), 604–608

components of, 604–605

- configuration and verification, 607–608
- event detectors, 354
- operations, 605
- security models and levels, 606–607
- shortcomings of, 326
- versions of, 606
- YANG (Yet Another Next Generation) as alternative to, 325
- snooping, IGMP (Internet Group Management Protocol), 160–161**
- SNR (signal-to-noise ratio), 171–172**
- Software as a Service (SaaS), 441, 452, 457**
- Software Image Management (SWIM), 336**
- Software-Defined Access. See SD-Access**
- software-defined networking (SDN) architecture, 240**
- Software-Defined Wide Area Network. See SD-WAN (Software-Defined Wide Area Network)**
- sort-by bytes command, 625**
- Source address field (traceroute command), 597**
- Source address or interface field (ping command), 600**
- source trees, 161**
- source-specific multicast (SSM), 157, 162**
- southbound APIs (application programming interfaces), 241–242**
- SPAN (Switch Port Analyzer), 632–633**
- Spanning Tree Protocol. See STP (Spanning Tree Protocol)**
- spanning-tree bpdudfilter enable command, 35**
- spanning-tree bpduguard {enable | disable} command, 33–34**
- spanning-tree guard loop command, 36**
- spanning-tree guard root command, 32**
- spanning-tree loopguard default command, 36**
- spanning-tree mode mst command, 41–43**
- spanning-tree mode rapid-pvst command, 25**
- spanning-tree mst configuration command, 40–41**
- spanning-tree mst forward-time command, 45**
- spanning-tree mst hello-time command, 45**
- spanning-tree mst *instance-id* cost cost command, 43**
- spanning-tree mst *instance-id* port-priority *priority* command, 43**
- spanning-tree mst max-age command, 45**
- spanning-tree pathcost method command, 22**
- spanning-tree pathcost method long command, 22–23**
- spanning-tree portfast bpdudfilter default command, 35**
- spanning-tree portfast bpduguard default command, 33–34**
- spanning-tree portfast command, 33**
- spanning-tree portfast default command, 33**
- spanning-tree portfast disable command, 33**
- spanning-tree portfast trunk command, 33**
- spanning-tree vlan command, 29**
- spatial multiplexing, 173**
- Speak state (HSRP), 144, 393**
- speed, CPU, 490**
- SPF (shortest path first) algorithm, 61, 80–81**
- split method, 307**
- src-dst-ip method, 54**
- src-dst-mac method, 54**
- src-dst-port method, 54**
- src-ip method, 54**

src-mac method

**src-mac method, 54**

**src-port method, 54**

**SSH (Secure Shell), 662**

access control with, 195, 203–206

configuration, 204–206

versions of, 203

**SSIDs (service set identifiers), 248–249, 411**

**SSL (Secure Sockets Layer), 272**

Cisco DNA Center communication, 242

Cisco ISE communication, 242  
proxies, 456

**SSM (source-specific multicast) addresses, 157, 162**

**SSO (Stateful Switchover), 400–405**

benefits of, 401

configuration on Cisco Catalyst 4500X, 401

show redundancy clients command, 403–405

verifying, 401–402

**stacking, simplified campus design with, 388–389**

**StackWise, 388–389, 482**

**standalone mode, Cisco FlexConnect, 416–418**

**standalone wireless deployments. See autonomous wireless deployments**

**standard ACLs (access control lists), 224–225**

**standby command, 143–144**

**Standby state (HSRP), 144, 393**

**startswith method, 307**

**startup configuration datastore (NETCONF), 663**

**Stateful Switchover. See SSO (Stateful Switchover)**

**statements, 308–309. See also commands; functions and methods**

action, 230

augment, 328

elif, 309

else, 309, 311

if, 309

import, 328

include, 328

network, 112, 114, 117

prefix, 328

print, 307

raise, 311

try/except blocks, 311

when, 328

**states**

BGP (Border Gateway Protocol), 106–107, 115–116

HSRP (Host Standby Router Protocol), 144, 393

Layer 2 ports, 24

OSPF (open shortest path first), 86

STP (Spanning Tree Protocol), 24, 26

**static assignment, 280**

**static NAT (Network Address Translation), 134, 136–137**

**static routing, 65–66**

**static RPs (rendezvous points), 161**

**status codes, HTTP (Hypertext Transfer Protocol), 347–348**

**Stealthwatch Cloud, 273**

**STP (Spanning Tree Protocol), 19–45, 386**

BPDU (bridge protocol data unit) messages, 19–20

BPDU Filter, 35–36

BPDU Guard, 33–34

Bridge Assurance, 37–38

designated port elections, 20–25

Loop Guard, 36–37

MST (Multiple Spanning Tree), 40–45

overview of, 19–20

port roles, 26–28

port states, 26

PortFast, 32–33

root bridges, 20–25

- Root Guard, 31–32
- root ports, 20–25
- RSTP (Rapid Spanning Tree Protocol), 25–28
- switch priorities, 28–31
- timers, 24–25
- UDLD (Unidirectional Link Detection), 38–40
- Strict field**
  - ping command, 600
  - traceroute command, 597
- string data type, 306–307**
- STUN (Session Traversal Utilities for NAT) servers, 463**
- successor routes, 68**
- successors, 68**
- summary LSA (link-state advertisement), 93**
- summary-address command, 78, 95**
- SWIM (Software Image Management), 336**
- Switch Port Analyzer (SPAN), 632–633**
- switching, 505**
  - definition of, 471
  - further reading, 523
  - MLSs (multilayer switches), 509, 517–520
  - STP (Spanning Tree Protocol), 19–45, 386
    - BPDU (bridge protocol data unit) messages, 19–20
    - BPDU Filter, 35–36
    - BPDU Guard, 33–34
    - Bridge Assurance, 37–38
    - designated port elections, 20–25
    - Loop Guard, 36–37
    - MST (Multiple Spanning Tree), 40–45
    - overview of, 19–20
    - port roles, 26–28
    - port states, 26
    - PortFast, 32–33
    - root bridges, 20–25
    - Root Guard, 31–32
    - root ports, 20–25
    - RSTP (Rapid Spanning Tree Protocol), 25–28
    - switch priorities, 28–31
    - UDLD (Unidirectional Link Detection), 38–40
  - tables, 515–520
    - CAM (Content-Addressable Memory), 507–508, 515–517
    - TCAM (Ternary Content-Addressable Memory), 507, 517–520
  - traffic forwarding
    - CEF (Cisco Express Forwarding), 495, 512–515
    - fast switching, 512
    - overview of, 506–509
    - process switching, 511
    - virtual, 535–536
- Switching Database Manager. See SDM (Switching Database Manager)**
- switchport access vlan command, 5**
- switchport command, 6**
- switchport mode access command, 5**
- switchport mode dynamic auto command, 9**
- switchport mode dynamic desirable command, 9**
- switchport mode trunk command, 10**
- switchport nonegotiate command, 10**
- SXP (SGT Exchange Protocol), 280**
- SYN packets, 258**
- SYN-ACK packets, 258**
- syslog, 614–618**
  - configuration, 617–618
  - definition of, 614
  - event detectors, 355
  - message elements, 615–616
  - severity levels, 616–617

## T

---

### tables

- BGP (Border Gateway Protocol), 105–106
- CAM (Content-Addressable Memory), 507–508, 515–517
- EIGRP (Enhanced Interior Gateway Routing Protocol)
  - authentication, 76
  - named mode, 76–78
  - neighbor tables, 70–72
  - route summarization, 78
  - routing tables, 75–76
  - topology tables, 72–75
- RIB (routing information base), 405
  - for switching, 515–520
- TCAM (Ternary Content-Addressable Memory), 507, 508, 517–520
  - FM (Feature Manager), 517
  - SDM (Switching Database Manager) templates, 517–520

**TAC (Technical Assistance Center), 655–656**

### TACACS+

- configuration, 211
- overview of, 211

### tags

- definition of, 337
- SGTs (security group tags), 279, 288–289, 468–469

**Talos Security Intelligence and Research Group, 271**

### Target IP address field

- ping command, 600
- traceroute command, 596

**targets, SaltStack, 371**

### tasks

- Ansible, 373
- definition of, 337

**TCA (Topology Change Acknowledgement) BPDUs, 20**

**TCAM (Ternary Content-Addressable Memory), 507, 508, 517–520**

- FM (Feature Manager), 517
- SDM (Switching Database Manager)
  - changing, 518–519
  - features of, 517–518
  - templates, 517–520
  - verifying, 519–520

**Tcl (Tool Command Language), 351, 352, 358–359**

**TCN (Topology Change Notification) BPDUs, 19**

**TCO (total cost of ownership), 335, 526–527**

### TCP (Transmission Control Protocol)

- ACK packets, 258–259
- optimization, 455
- SYN packets, 258
- SYN-ACK packets, 258

**TE (traffic engineering), 574**

**Technical Assistance Center (TAC), 655–656**

**Telnet, 195**

### templates

- Ansible, 373
- configuration, 337
- SDM (Switching Database Manager), 517–520
  - changing, 518–519
  - features of, 517–518
  - verifying, 519–520

**Temporal Key Integrity Protocol (TKIP), 251–252**

**terminal lines, 195**

**Ternary Content-Addressable Memory. See TCAM (Ternary Content-Addressable Memory)**

**Threat Grid, 271, 272**

**three-tier network design, 383–384**

**time exceeded error message, 596**

### Timeout in seconds field

- ping command, 600
- traceroute command, 597

**timeouts, configuration, 205–206**

**timers, STP (Spanning Tree Protocol), 24–25**

**timestamp element (syslog), 615**

**Timestamp field**

ping command, 600

traceroute command, 597

**Time-to-Live (TTL), 509, 593–594**

**TKIP (Temporal Key Integrity Protocol), 251–252**

**TLOCs (transport locators), 463**

**TLS (Transport Layer Security)**

Cisco DNA Center communication, 242

Cisco ISE communication, 242

EAP-Transport Layer Security (TLS), 289

**Token API, 243**

**Tool Command Language (Tcl), 351, 352, 358–359**

**top talkers, configuration, 625**

**topology**

BGP (Border Gateway Protocol), 113  
definition of, 336

EIGRP (Enhanced Interior Gateway Routing Protocol), 72–75

GRE (Generic Routing Encapsulation) tunnels, 552

HSRP (Host Standby Router Protocol), 145

NAT (Network Address Translation), 135, 136

site-to-site VPNs, 558–559

VRRP (Virtual Router Redundancy Protocol), 148

**Topology Change Acknowledgement (TCA) BPDUs, 20**

**Topology Change Notification (TCN) BPDUs, 19**

**ToS (type of service) byte, 496**

**total cost of ownership (TCO), 335, 526–527**

**traceroute command, 593–597**

extended traceroute, 595–597

messages, 596

output characters, 594

simple example, 594–595

**traffic analysis, with debug, 589–593**

ACLs (access control lists) with, 589–590

conditional debugging, 592–593

debug message buffering, 590–591

output format, 589

**traffic engineering (TE), 574**

**traffic forwarding**

CEF (Cisco Express Forwarding), 495, 512–515

benefits of, 512

components of, 513–514

modes of operation, 514–515

fast switching, 512

overview of, 506–509

process switching, 511

**transmission quality. See QoS (quality of service)**

**transmit beamforming, 173–174**

**transparent mode (VTP), 13**

**transport input ssh command, 204**

**Transport Layer Security. See TLS (Transport Layer Security)**

**transport locators (TLOCs), 463**

**transport mode (IPsec), 567**

**transversal, NAT, 463**

**tree structure, YANG (Yet Another Next Generation), 329–330**

**troubleshooting, 587**

Cisco vManage troubleshooting and utility APIs, 339

with debug, 589–593

ACLs (access control lists) with, 589–590

conditional debugging, 592–593

debug message buffering, 590–591

output format, 589

further reading, 611

GRE (Generic Routing Encapsulation), 556

## troubleshooting

- overview of, 588
- with ping, 597–602
  - extended ping command, 601–602
  - extended ping fields, 599–601
  - output characters, 598
  - ping command to repeat count, 599
  - ping command with size specified, 599
  - simple example, 598–599
- with traceroute, 593–597
  - extended traceroute, 595–597
  - messages, 596
  - output characters, 594
  - simple example, 594–595
- traffic analysis, 589–593
  - ACLs (access control lists) with, 589–590
  - conditional debugging, 592–593
  - debug message buffering, 590–591
  - output format, 589
- WLAN (wireless LAN)
  - configuration, 188–189

**trunking**

- 802.1Q, 7–9
- DTP (Dynamic Trunking Protocol), 9–11
- VTP (VLAN Trunking Protocol), 11–15
  - advertisements, 13–14
  - configuration, 14–15
  - definition of, 11–12
  - domains, 12
  - verifying, 15
  - versions of, 14
  - VTP modes, 13

**TrustSec, 279–280, 288–289, 468–469, 475**

**try/except blocks, 311**

**TTL (Time-to-Live), 509, 593–594**

**TTLS (Tunneled Transport Layer Security), 289**

**tunnel mode (IPsec), 567**

**tunnel routers (xTRs), 576**

**tunneling. See CAPWAP (Control and Provisioning of Wireless Access Points); GRE (Generic Routing Encapsulation)**

**two-tier network design, 384–385**

**Two-way states (OSPF), 86**

**type 0 passwords, 196**

**type 1 hypervisors, 528, 533**

**type 2 hypervisors, 528–529**

**type 4 passwords, 196**

**type 5 passwords, 196**

**type 7 passwords, 196**

**type 8 passwords, 196**

**type 9 passwords, 196**

**type() command, 306**

**Type of service field (ping command), 600**

**type of service (ToS) byte, 496**

**U**

**UCS (Unified Computing System), Puppet support on, 365**

**UCS C-Series servers, 539**

**UDLD (Unidirectional Link Detection), 38–40**

**udld {aggressive | enable | message time *interval*} command, 39**

**udld {enable | aggressive | disable} command, 39**

**UDP (User Datagram Protocol), 412, 593–594, 622**

- jitter, measurement of, 647–648
- outer LISP UDP headers, 578

**Umbrella, 272–273**

**underlays, SD-Access, 471**

**unicast, 156**

**Unidirectional Link Detection (UDLD), 38–40**

**Unified Computing System (UCS), Puppet support on, 365**

**Unified Wireless Network, 412**



**UP (user priority), 500**  
**update messages (BGP), 106**  
**Update packets (EIGRP), 71**  
**Uplink MACsec, 282**  
**URL filtering, 456**  
**use cases**  
 IP Service Level Agreement (SLA)  
 ICMP echo operation, 644–647  
 measurement of IP SLA UDP  
 jitter operation, 647–648  
 monitoring of HTTP  
 destinations, 647–648  
 SD-WAN (Software-Defined Wide  
 Area Network), 454–457  
 application performance  
 optimization, 455  
 Cisco Multicloud, 456–457  
 secure automated WAN, 454–455  
 secure DIA (Direct Internet  
 Access), 456  
**User Datagram Protocol. See UDP  
 (User Datagram Protocol)**  
**user priority (UP), 500**  
**User-Defined Networking, 657**  
**usernames, 200–203**  
**users, returning information about,  
 336**

## V

**VACLs (VLAN ACLs), 230–231**  
**Validate reply data? field (ping  
 command), 600**  
**vAnalytics, 462**  
**variable-length subnet masking  
 (VLSM), 80**  
**vDSs (vSphere Distributed Switches),  
 461, 533, 536**  
**vEdge, 460**  
**VEEAM Cloud Connect, 442**  
**Verbose field**  
 ping command, 600  
 traceroute command, 597  
**virtual CPU (vCPU), 532**  
**Virtual Extensible LAN. See VXLAN  
 (Virtual Extensible LAN)**  
**virtual LANs. See VLANs (virtual LANs)**  
**virtual machine manager (VMM), 528**  
**virtual machines (VMs), 527–528,  
 532–533**  
**virtual network identifiers (VNIs), 582**  
**virtual NIC (vNIC), 532–533**  
**virtual pathing. See virtualization,  
 network**  
**virtual private network (VPN)  
 segmentation, 454, 463**  
**Virtual Private Networks Version 4  
 (VPNv4), 104**  
**Virtual Router Redundancy Protocol  
 (VRRP), 147–150, 396–397, 460**  
**virtual routing and forwarding (VRF),  
 463, 546–547, 582**  
**Virtual Switching System (VSS),  
 388–389, 535–536**  
**Virtual Tunnel Interfaces (VTIs),  
 560–561**  
**virtual Wide Area Application Services  
 (vWAAS), 539**  
**virtual Wireless LAN Controllers  
 (vWLCs) | Wireless LAN Controllers  
 (vWLCs), 539**  
**virtualization, network, 545, 573. See  
 also cloud computing; VLANs (virtual  
 LANs); VPN (virtual private network)**  
 definition of, 537  
 Enterprise NFV (Network Function  
 Virtualization)  
 architecture, 538–539  
 benefits of, 537–538  
 hardware options, 539–540  
 further reading, 543, 571, 586  
 GRE (Generic Routing  
 Encapsulation), 552–556  
 benefits of, 552–553  
 characteristics of, 553  
 configuration, 554–556  
 definition of, 552  
 GRE Tunneling over IPsec,  
 567–568

- packet format, 554
- troubleshooting, 556
- tunnel topology, 552
- verifying, 556
- hypervisors, 527–530
- IPsec VPNs, 558–562
  - Cisco IOS FlexVPN, 561–562
  - Cisco IOS VTIs (Virtual Tunnel Interfaces), 560–561
  - DMVPN (Dynamic Multipoint VPN), 559–560
  - GRE Tunneling over IPsec, 567–568
  - IP Security (IPsec), 562–567
  - site-to-site VPNs, 558–559
- LISP (Cisco Locator/ID Separation Protocol)
  - architecture, 577–578
  - benefits of, 574–575
  - components of, 574–576
  - definition of, 573
  - deployment environment, 576–577
  - limitations of, 573
- overview of, 525–527
- virtual switching, 535–536
- VLAN ACLs (VACLs), 230–231
- VMM (virtual machine manager), 528
- VMs (virtual machines), 527–528, 532–533
- VNFs (virtualized network functions), 538
- vNIC (virtual NIC), 532–533
- VRF (virtual routing and forwarding), 463, 546–547, 582
- VRF-Lite, 547–550
  - benefits of, 548
  - configuration, 549–550
  - definition of, 547–548
- VRRP (Virtual Router Redundancy Protocol), 147–150, 396–397, 460
- VSS (Virtual Switching System), 388–389, 535–536
- VTIs (Virtual Tunnel Interfaces), 560–561
- vWAAS (virtual Wide Area Application Services), 539
- vWLCs (virtual Wireless LAN Controllers), 539
- VXLAN (Virtual Extensible LAN), 580–584
  - benefits of, 580, 581
  - definition of, 581–582
  - overlays, 581–582
  - packet format, 580–581
  - VNIs (VXLAN network identifiers), 582
  - VTEPs (VXLAN tunnel endpoints), 582–584
- virtualized network functions (VNFs), 538**
- vlan access-map name sequence command, 230**
- VLAN ACLs (VACLs), 230–231**
- vlan command, 4**
- vlan filter vlan-access-map-name vlan-list command, 230**
- VLANs (virtual LANs), 3–17, 526**
  - 802.1Q trunking, 7–9
  - assignment of, 4–6
  - creating, 4–5
  - DTP (Dynamic Trunking Protocol), 9–11
  - inter-VLAN routing, 16–17
  - overview of, 3
  - VTP (VLAN Trunking Protocol), 11–15
    - advertisements, 13–14
    - configuration, 14–15
    - definition of, 11–12
    - domains, 12
    - verifying, 15
    - versions of, 14
    - VTP modes, 13
- VLSM (variable-length subnet masking), 80**
- vManage, 461–462**

- API integrations, 338–342
  - administrative and management APIs, 339
  - configuration APIs, 339
  - connecting to, 339–340
  - device real-time monitoring APIs, 339
  - device state statistics bulk API, 339
  - further reading, 344
  - Postman development tool, 340
  - REST operations on vManage web server, 341–342
  - troubleshooting and utility APIs, 339
  - use cases, 339
- HTTP status codes, 347–348
- VMM (virtual machine manager), 528**
- vMotion, 533**
- VMs (virtual machines), 527–528, 532–533**
- VMware ESXi, 289, 528, 533, 535**
- VMware Fusion, 529**
- VMware Host Client, 533**
- VMware vSphere Standard Switch (vSS), 535–536**
- VMware Workstation, 529**
- VNFs (virtualized network functions), 538**
- VNIs (VXLAN network identifiers), 474–475, 582**
- VoIP (voice over IP), 620**
- VPN (virtual private network)**
  - IPsec VPNs, 558–562
    - Cisco IOS FlexVPN, 561–562
    - Cisco IOS VTIs (Virtual Tunnel Interfaces), 560–561
    - DMVPN (Dynamic Multipoint VPN), 559–560
    - GRE Tunneling over IPsec, 567–568
    - IP Security (IPsec), 562–567
      - site-to-site VPNs, 558–559
    - segmentation, 269, 454, 463
- VRF (virtual routing and forwarding), 463, 546–547, 582**
- VRF-Lite, 547–550**
  - benefits of, 548
  - configuration, 549–550
  - definition of, 547–548
- VRRP (Virtual Router Redundancy Protocol), 147–150, 396–397, 460**
- vrrp command, 147–148**
- vSmart controllers, 459–460**
- vSphere Distributed Switches (vDSs), 533, 536**
- vSphere Standard Switch (vSS), 535–536**
- VSS (Virtual Switching System), 388–389, 535–536**
- vSS (vSphere Standard Switch), 536**
- vSwitch, 535–536**
- VTEPs (VXLAN tunnel endpoints), 582–584**
- VTIs (Virtual Tunnel Interfaces), 560–561**
- VTP (VLAN Trunking Protocol), 11–15**
  - advertisements, 13–14
  - configuration, 14–15
  - definition of, 11–12
  - domains, 12
  - verifying, 15
  - versions of, 14
  - VTP modes, 13
- vtp domain command, 14**
- vtp mode command, 14**
- vtp password command, 14**
- vtp primary command, 14**
- vty lines, 195–196**
- vWaaS (virtual Wide Area Application Services), 539**
- vWLCs (virtual Wireless LAN Controllers), 539**
- VXLAN (Virtual Extensible LAN), 474–475, 580–584**
  - benefits of, 580, 581
  - definition of, 581–582

## VXLAN (Virtual Extensible LAN)

- encapsulation/decapsulation, 480
- overlays, 581–582
- packet format, 580–581
- VNIs (VXLAN network identifiers), 582
- VTEPs (VXLAN tunnel endpoints), 582–584

**VXLAN network identifiers (VNIs), 474–475, 582**

## W

**WAN edge routers, 460–461**
**WANs (wide area networks). See SD-WAN (Software-Defined Wide Area Network)**
**watts (W), 169–170**
**Web Authentication (WebAuth), 472**
**Web passthrough, 257**
**Web Security Appliance (WSA), 272**
**WebAuth, 257–260, 293–295, 472**

- configuration, 259–260
- how it works, 257–259

**WebEx, 441**
**weighted fair queueing (WFQ), 494**
**weighted random early detection (WRED), 221, 494, 500**
**well-known discretionary attributes (BGP), 108**
**well-known mandatory attributes (BGP), 107–108**
**WEP (Wired Equivalent Privacy), 251**
**WFQ (weighted fair queueing), 494**
**when statement, 328**
**Wi-Fi 4 standard, 172–173**
**Wi-Fi 5 standard, 173**
**Wi-Fi 6 Readiness dashboard, 656–657**
**Wi-Fi 6 standard, 173**
**Wi-Fi Multimedia (WMM), 500**
**Wi-Fi Protected Access. See WPA (Wi-Fi Protected Access)**
**wildcard masking, 222–224**
**Wired Equivalent Privacy (WEP), 251**
**Wireless Active Sensor, 656**
**wireless LAN controllers (WLCs), 481, 538**
**wireless LANs. See WLANs (wireless LANs)**
**wireless location services, 418–422**
**wireless networking. See WLANs (wireless LANs)**
**wireless security**

- AES (Advanced Encryption Standard), 252
- APs (access points), 262
- EAP (Extensible Authentication Protocol) authentication, 254–257
- further reading, 262
- GCM (Galois/Counter Mode), 252
- Open Authentication, 249–251
- overview of, 247–249
- PSK (pre-shared key) authentication, 251–253
- SSIDs (service set identifiers), 248–249
- TKIP (Temporal Key Integrity Protocol), 251–252
- WebAuth, 257–260
  - configuration, 259–260
  - how it works, 257–259
- WEP (Wired Equivalent Privacy), 251
- WPA (Wi-Fi Protected Access), 251–253
  - definition of, 251–252
  - WPA2 Enterprise, 252
  - WPA2 Personal, 252
  - WPA3 Enterprise, 252
  - WPA3 Personal, 252–253

**WLANs (wireless LANs), 167, 248. See also wireless security**

- APs (access points). *See* APs (access points)
- deployment models, 410–411
  - autonomous, 410, 411–412
  - centralized, 410, 412–415

- Cisco FlexConnect, 410, 415–418
- cloud-based, 411, 418–422
- embedded, 411, 422–424
- overview of, 409, 410–411
- SD-Access. *See* SD-Access
- free space path loss, 171
- further reading, 192, 431
- IEEE (Institute of Electrical and Electronics Engineers) wireless standards, 172–173
- MIMO (multi-input, multi-out), 173–174
- multiple radios for, 173–174
- QoS (quality of service), 500–501
- RF (radio frequency), 168–170
- RSSI (received signal strength indicator), 171
- SD-Access architecture, 471
- SNR (signal-to-noise ratio), 171–172
- troubleshooting, 188–189
- wireless location services, 427–428
- wireless roaming, 185–188
- WLCs (Wireless LAN Controllers), 538**
  - AP (access point) interaction, 178–183
    - antenna types, 181–183
    - discovery, 178–180
    - plane patterns, 180–181
  - fabric, 481
- WMM (Wi-Fi Multimedia), 500**
- World Wide Web Consortium (W3C), 317**
- WPA (Wi-Fi Protected Access), 251**
  - definition of, 251–252
  - WPA2 Enterprise, 252
  - WPA2 Personal, 252
  - WPA3 Enterprise, 252
  - WPA3 Personal, 252–253

- WRED (weighted random early detection), 221, 494, 500**
- WSA (Web Security Appliance), 272**

## X

---

- x86 compute resources, 538**
- XaaS (Anything as a Service), 442**
- XML (Extensible Markup Language)**
  - characteristics of, 317–318
  - documents, 318–319
  - further reading, 324
  - JSON (JavaScript Object Notation) compared to, 321
  - syntax for, 318
- xTRs (tunnel routers), 576**

## Y

---

- Yagi antennas, 183**
- YAML (Yet Another Markup Language), 373**
- YANG (Yet Another Next Generation) data models, 325–332**
  - characteristics of, 326–327
  - further reading, 332
  - nodes in, 329
  - tree structure of, 329–330
  - types of, 327–329

## Z

---

- zero-touch provisioning, 419, 454**
- Zerto, 442**