

Index

Numerics

- 2.4-GHz band, [17](#), [20](#), [641](#)**
- 2.5GBASE-T, [404–405](#), [641](#)**
- 4G/5G, [428–429](#), [641](#)**
- 5GBASE-T, [404–405](#)**
- 5-GHz band, [17](#), [641](#)**
- 6-GHz band, [70](#), [641](#)**
- 10BASE-T, [404](#), [641](#)**
- 10GBASE-T, [404](#), [641](#)**
- 40GBASE-T, [404](#), [641](#)**
- 100BASE-T, [404](#), [641](#)**
- 802.1Q header, marking, [333–334](#)**
- 802.1x, [47–48](#)**
- 802.11, [7–8](#). *See also* [wireless networks](#)**
 - amendments, [18–19](#)
 - beacon, [8](#)
 - Wi-Fi generational names, [20](#)
- 1000BASE-SX, [641](#)**
- 1000BASE-T, [404](#), [641](#)**

A

AAA (authentication, authorization, and accounting), 198, 642, 644

accounting, 198

authentication, 198

authorization, 198

RADIUS, 199–200

TACACS+, 199–200

access control, physical, 200

access interface, 642

access layer, 494, 502, 642

access link, 417, 642

access switch, 399, 402

access-class command, 171–173

access-list command, 121–122, 126, 130–131. *See also* IP ACL (access control list)

implicit deny, 124

log keyword, 129

permit any, 124

reverse engineering from ACL to address range, 131–133

syntax, 125

accounting, 198, 642

ACE (access control entry), 511, 642

ACI (Application Centric Infrastructure), 446, 483–484, 643

APIC (Application Policy Infrastructure Controller), 487

EPG (endpoint group), 486

operating model with intent-based networking, 486–488

spine and leaf design, 484–485

ACK flag, 100

ACL (access control list), 329, 642. *See also* IP ACL (access control list)

- ARP, 253

- persistence, 642

- resequencing, 642

- sequence number, 642

active mode, FTP, 386–387

active/standby model, HSRP (Hot Standby Router Protocol), 356

ad hoc wireless network, 14, 642

administrative distance, 642

AES (Advanced Encryption Standard), 51

AF (Assured Forwarding), 336

agent

- based architecture, 643

- SNMP, 370

agentless architecture, 563, 643

AI (artificial intelligence), 517, 643

- for automation, 518

- ChatGPT, 518–523

- generative, 517–518

- ML (machine learning), 518

- narrow, 517–518

AI Ops, 523–524, 643

AireOS WLC, 61–63, 79

- configuring the WLAN, 81–83

- configuring WLAN security, 83–84

- create a new WLAN, 80–81

- creating a dynamic interface, 79–80

algorithm

- AES, 51

CBC-MAC (Cipher Block Chaining Message Authentication Code), [51](#)

changing the encoding type for enable secret password command, [209–210](#)

hash, [209](#)

RC4 cipher, [47](#)

scheduling, [338–339](#)

SHA-256, [209](#)

amendments, IEEE 802.11, [18–19](#)

amplification attack, [191](#), [643](#)

ANSI (American National Standards Institute), [404](#)

Ansible, [562–563](#), [643](#)

antenna, [42](#)

AP (access point), [642](#). *See also* **WLC (wireless LAN controller)**

association request/response, [9](#), [19](#)

authentication, [44](#)

autonomous, [24–25](#), [27](#), [58](#)

beacon frame, [8](#), [66](#)

BSA (basic service area), [8](#)

BSS (basic service set), [8](#)

Cisco

FlexConnect Mode, [32](#), [36–37](#)

modes, [35–36](#)

Cisco Meraki, [26](#)

fake, [44–46](#)

group key, [45](#)

IBSS (independent basic service set), [13–14](#)

infrastructure mode, [8](#)

lightweight, [28](#)

management platform, [26](#)

mesh, [17](#)

- multigig Ethernet, 406
- radios, 19
- repeater mode, 14
- roaming, 13
- SOHO (small office/home office), 408
- supporting multiple SSIDs on, 11–12

API (application programming interface), 478, 489–491, 643

- authentication, 537–539
- data serialization language, 541–542
- development environment tool, 536–541
- documentation, 536
- Java, 480
- need for data modeling language, 542–544
- RESTful, 480–481, 510, 528–529
 - cacheable*, 530
 - client/server architecture*, 529
 - stateless operation*, 530
 - URIs*, 534–536
- southbound, 664

APIC (Application Policy Infrastructure Controller), 487, 643

application/s

- batch, 326
- data, 325–326
- Postman, 537–541
- signatures, 332
- voice and video, 327–328
- well-known port numbers, 99
- WWW (World Wide Web), 98

architecture

- agentless, 563
- client/server, 529

software-defined, [481](#)

wireless

autonomous AP, [24–25](#)

cloud-based AP, [26–27](#)

control plane, [27](#)

data plane, [27](#)

split-MAC, [28–32](#), [36–37](#)

ARP, [250–251](#)

ACLs, [253](#)

gratuitous, [251–252](#)

message fields, [251](#)

reply, [643](#)

array, JSON (JavaScript Object Notation), [547–549](#)

ASIC (application-specific integrated circuit), [476](#), [643](#)

association request/response, [9](#), [19](#), [644](#)

attack/s, [191](#)

brute-force, [86](#), [196](#), [644](#)

buffer overflow, [194](#), [644](#)

DHCP, [241–242](#), [248](#)

dictionary, [196](#)

DoS (denial of service), [212](#)

pharming, [195](#)

phishing, [195](#)

reconnaissance, [193–194](#)

smishing, [195](#)

spear phishing, [195](#)

spoofing, [188–189](#)

amplification, [191](#)

denial-of-service, [189–190](#)

distributed denial-of-service, [190](#)

man-in-the-middle, [44](#), [191–193](#)

reflection, 191

vishing, 195

watering hole, 195

whaling, 195

authentication. *See also* password/s

AAA, 198

API, 537–539

multifactor, 199

wireless, 43

802.1x/EAP, 47–48

AP (access point), 44

client, 43–44

EAP-FAST (EAP Flexible Authentication by Secure Tunneling), 48–49

EAP-TLS (EAP Transport Layer Security), 50

LEAP (Lightweight EAP), 48–49

open, 46

PEAP (Protected EAP), 49

WEP (Wired Equivalent Privacy), 47

authorization, 198, 644

automation, 518, 523

configuration, 561–562

data center, 484

impact on network management, 489–491

autonomous AP, 24–25, 27, 58, 644

AVC (Application Visibility and Control), 217

AVF (active virtual forwarder), 364

AVG (active virtual gateway), 364

B

band, 20, 644. *See also* channel

2.4-GHz, 17

5-GHz, 17

6-GHz, 70

channels, 17

bandwidth, 324–325, 644

baseline, 524

batch traffic, 326

beacon, 802.11, 8

beacon frame, 66, 644

bidirectional communication, wireless network, 7

binary wildcard mask, 123–124

biometric credentials, 197

bridge

outdoor, 16

point-to-point bridged link, 16

workgroup, 15–16

brute-force attack, 86, 196, 644

BSA (basic service area), 8

BSS (basic service set), 8–9, 24, 644

DS (distribution system), 10–12

independent, 13–14

traffic flows, 9

BSSID (basic service set identifier), 8–9

buffer overflow attack, 194, 644

building, ACLs, 155

C

CA (certificate authority), 49

cable

CAT 5E, 405–406

CAT 6, 405

fiber-optic, 406, 429

UTP (unshielded twisted-pair), 403–405

cable Internet, 427–428

CAC (call admission control), 340–341

cacheable, 644

campus LAN, 398–399. *See also* SD-Access; two-tier campus LAN

access switches, 399

distribution switches, 399–400

Ethernet UTP links at the access layer, 403–405

fiber uplinks, 406–407

multigig Ethernet, 405–406

three-tier, 400–402

two-tier, 399–400

full mesh, 403

partial mesh, 403

uplinks, 403

CAPWAP (Control and Provisioning of Wireless Access Points), 29, 36, 644

CAT 5E cable, 405–406, 645

CAT 6 cable, 645

CBC-MAC (Cipher Block Chaining Message Authentication Code), 51

CBWFQ (Class-Based Weighted Fair Queuing), 339

CCMP (Counter/CBC-MAC Protocol), 51

CCNA exam 200–301

- adjustments for your second attempt, [595–596](#)
- advice on how to answer questions, [590–592](#)
- gap analysis, [589–590](#)
- other study tasks, [596](#)
- practice exam events, [586–587](#)
- practice exams in the CCNA premium edition, [592](#)
- practice questions, [585](#)
- preparation, [583–584](#)
 - 24 hours before your exam*, [582–583](#)
 - 30 minutes before your exam*, [583](#)
 - one week before exam*, [582](#)
- question types, [578–580](#)
- review, [584–585](#)
- scoring, [587](#)
- self-assessment suggestions, [587–589](#)
- time check method, [581–582](#)
- time management, [580–581](#)
- topic order, [607–617](#)
- updates, [572–576](#)

CDP (Cisco Discovery Protocol), 283, 645

- configuration, [286](#)
- hold time, [287](#)
- send time, [287](#)
- show commands, [283](#)
- verification, [286–287](#)

cdp enable command, 286

cdp timer command, 287

CE (customer edge), 424

cell, 645

centralized architecture, 477

centralized configuration files, [555–557](#)

centralized control plane, [645](#)

centralized WLC deployment, [32](#)

certificate

digital, [197](#)

X.509, [30](#)

channel, [17](#), [18](#), [20](#), [645](#)

Chat Ops, [524](#), [645](#)

ChatGPT, [518–523](#)

CIDR (Classless Interdomain Routing), [300](#), [302](#), [645](#)

block, [301](#)

Cisco Catalyst Center, as network management platform, [514–515](#)

CIR (committed information rate), [343](#)

Cisco 8000V router, [461](#)

Cisco AnyConnect Secure Mobility Client, [645](#)

Cisco AP

connections, [58–59](#)

FlexConnect Mode, [36–37](#)

modes, [35–36](#)

OfficeExtend, [37](#)

Cisco ASA (Adaptive Security Appliance), [216](#)

Cisco Catalyst 8000V, [645](#)

Cisco Catalyst Center, [494](#), [496–497](#), [509–510](#), [645](#)

differences with traditional management, [516–517](#)

GUIs, [515](#)

as network management platform, [514–515](#)

RESTful API call to, [536–541](#)

scalable groups, [510–512](#)

similarities to traditional management, [515–516](#)

topology map, [515](#)

Cisco DNA (Digital Network Architecture), [494](#)

Cisco Meraki, [26](#)

Cisco Prime Infrastructure, [645](#)

Cisco SD-Access, [484](#), [494](#), [512–513](#), [645](#)

Cisco Catalyst Center, [496–497](#), [509–510](#)

differences with traditional management, [516–517](#)

GUIs, [515](#)

as network management platform, [514–515](#)

scalable groups, [510–512](#)

similarities to traditional management, [515–516](#)

topology map, [515](#)

fabric, [497–498](#)

edge node, [506](#)

routed access layer design, [502](#)

host mobility, [498](#)

ITR (ingress tunnel router), [506–508](#)

overlay, [497–498](#), [503](#)

LISP for discovery and location, [505–509](#)

VXLAN tunnels, [504–505](#)

SGT (scalable group tag), [513–514](#)

underlay, [497–499](#)

supported hardware, [500](#)

using existing gear, [499–500](#)

using new gear, [501–503](#)

Cisco Secure Client, [646](#)

Cisco server hardware, [440–441](#)

Cisco Talos Intelligence Group, [219](#)

classification, [329–330](#), [646](#)

NBAR2 (next-generation Network Based Application Recognition), [331–332](#)

on routers, [331–332](#)

VRF (virtual routing and forwarding), [454–456](#)

clear ip nat translation command, [305](#), [313–314](#)

client, NTP (Network Time Protocol), [281](#)

clock set command, [279](#)

clock summer-time command, [279](#)

cloud/cloud computing, [448–449](#)

attributes, [448–449](#)

-based AP architecture, [26–27](#), [646](#)

-based WLC deployment, [32](#), [646](#)

enterprise WAN connection to the, [456](#)

accessing public cloud services using the Internet, [456–457](#)

using Internet to connect to the public cloud, [457–458](#)

IaaS (Infrastructure as a Service), [451–452](#)

management, [460–464](#), [646](#)

PaaS (Platform as a Service), [453–454](#)

private, [449–450](#)

public, [450–451](#), [460](#)

connecting with private WAN, [458–459](#)

intercloud exchange, [459–460](#)

SaaS (Software as a Service), [452–453](#)

service catalog, [449–450](#), [646](#)

“as a service” model, [451](#)

code integrity, [646](#)

codec, voice, [327](#)

collapsed core, [400](#), [646](#)

command/s. See also configuration

access-class, [171–173](#)

access-list, [121–122](#), [126](#), [130–131](#). *See also* IP ACL (access control list)

- implicit deny*, [124](#)
 - log keyword*, [129](#)
 - permit any*, [124](#)
 - reverse engineering from ACL to address range*, [131–133](#)
 - syntax*, [125](#)
- cdp enable, [286](#)
- cdp timer, [287](#)
- CDP-related, [295–296](#)
- clear ip nat translation, [305](#), [313–314](#)
- clock set, [279](#)
- clock summer-time, [279](#)
- copy, [379](#), [383–384](#)
- copy running-config startup-config, [228](#)
- crypto key generate rsa, [221](#)
- DAI-related, [261–262](#)
- debug, [273](#), [276–277](#)
- debug ip nat, [314](#)
- DHCP-related, [261](#)
- dig, [194](#)
- dir, [380–381](#)
- enable, [198](#)
- enable password, [206](#), [221](#)
 - interactions with enable secret command*, [206–207](#)
- enable secret, [206](#), [221](#)
 - changing the encoding type*, [209–210](#)
 - deleting*, [208](#)
 - hash function*, [207–208](#)
 - interactions with enable password command*, [206–207](#)
- errdisable recovery cause psecure-violation, [237](#)
- errdisable recovery interval, [237](#)
- ip access-group, [176](#)
- ip access-list, [138–139](#)

- ip access-list resequence, [175](#)
- ip arp inspection validate, [258–259](#)
- ip arp inspection vlan, [255](#)
- ip dhcp snooping, [246–248](#)
- ip helper-address, [168](#)
- ip inside source static, [303](#)
- ip nat inside source, [312](#), [315](#)
- ip nat pool, [311](#)
- line console 0, [221](#)
- line vty, [221](#)
- lldp run, [290–291](#)
- LLDP-related, [295](#)
- logging buffered, [271](#)
- logging host, [271](#)
- logging-related, [294–295](#)
- login, [221](#)
- login local, [221](#)
- more, [377](#)
- NAT-related, [319–320](#)
- no cdp enable, [286](#)
- no enable secret, [208](#), [221](#)
- no shutdown, [237](#), [248](#)
- nslookup, [194](#)
- ntp master, [279](#), [281–282](#)
- ntp server, [278–279](#)
- NTP-related, [295–296](#)
- ping, [164](#)
- pwd, [380–381](#)
- service password-encryption, [205–206](#), [221](#)
- show access-lists, [126–127](#)
- show cdp, [283](#)
- show cdp neighbors, [284–285](#)

- show cdp neighbors detail, [285–286](#)
- show file systems, [377](#)
- show flash, [379–381](#)
- show ip access-list, [126–127](#), [132](#), [153](#)
- show ip arp inspection, [256](#)
- show ip arp inspection statistics, [257](#)
- show ip dhcp snooping, [247](#), [249](#), [256](#)
- show ip interface, [153](#)
- show ip nat statistics, [312–313](#)
- show ip nat translations, [309](#), [312](#), [314](#), [317](#)
- show lldp, [291](#)
- show lldp entry, [289–290](#)
- show lldp neighbors, [288](#)
- show logging, [271](#), [274–275](#)
- show ntp associations, [281–282](#)
- show ntp status, [280](#), [282](#)
- show port-security, [232](#)
- show port-security interface, [228–229](#), [232](#), [234–235](#)
- show running-config, [126](#), [139–140](#), [155](#), [164](#), [168](#), [205–206](#), [227](#), [234](#), [308–309](#), [311](#), [316](#), [377](#)
- shutdown, [231](#), [237](#), [248](#)
- switchport mode, [236](#)
- switchport mode access, [227](#)
- switchport port-security access, [227](#)
- switchport port-security mac-address, [236–237](#)
- switchport port-security maximum, [237](#)
- terminal monitor, [296](#)
- transport input, [221](#)
- transport input ssh, [205](#)
- username password, [210](#), [221](#)
- username secret, [210](#), [221](#)
- verify, [381–382](#)

- whois, [194](#)
- common ACL, [175–176](#), [646](#)**
- communities, SNMP, [375](#)**
- complex matching, [330–331](#)**
- “computationally difficult”, [207](#), [209](#)**
- configuration/s**
 - AireOS WLC, [79](#)
 - configuring the WLAN, [81–83](#)*
 - configuring WLAN security, [83–84](#)*
 - create a dynamic interface, [79–80](#)*
 - create a new WLAN, [80–81](#)*
 - automation, [561–562](#)
 - CDP (Cisco Discovery Protocol), [286](#)
 - DAI (Dynamic ARP Inspection), [259](#)
 - on a Layer 2 switch, [254–257](#)*
 - limiting message rates, [257–258](#)*
 - optional message checks, [258–260](#)*
 - DHCP snooping, [245–246](#), [249](#)
 - on a Layer 2 switch, [246–248](#)*
 - limiting DHCP message rates, [248–249](#)*
 - drift, [554–555](#), [646](#)
 - dynamic NAT (Network Address Translation), [310–312](#)
 - extended IP ACL, [150–151](#)
 - files, [555–557](#)
 - IOS-XE WLC, [67–69](#)
 - apply the policy tag to some APs, [78–79](#)*
 - mapping the WLAN and policy profiles to a policy tag, [77](#)*
 - policy profile, [74–77](#)*
 - profile, [69–74](#)*
 - LLDP (Link Layer Discovery Protocol), [290–291](#)

- management, 488–489, 646
- management tools, 565–566, 646
 - Ansible*, 562–563
 - Terraform*, 563–565
- monitoring, 646
- monitoring and enforcement, 557–558
- named IP ACL, 139
- NAT (Network Address Translation), static, 308–309
- NTP (Network Time Protocol), 279–281
- PAT (Port Address Translation), 314–317
- port security, 225–228
- profile, 67
- provisioning, 558–559, 563, 647
- syslog, 273–274
- template, 559–561, 647
- variables, 560–561
- WLAN, 65–67
 - advanced settings*, 85–86
 - finalizing*, 86–87
 - QoS*, 85
- WLC (wireless LAN controller), 61–63

congestion avoidance, 346–347

connected mode, 647

connectionless protocol, 100–101

connection/s

- autonomous AP, 58
- Cisco AP, 58–59
- establishment, 647
- oriented protocol, 100–101
- TCP (Transmission Control Protocol), 100–101

container, 444, 647

Docker, [445–446](#)

engine, [445](#)

image, [445](#)

vendors, [445](#)

control plane, [27](#), [474–475](#), [647](#)

centralized, [477](#)

distributed architecture, [477](#)

LISP (Locator/ID Separation Protocol), [505–509](#)

controller, [477](#)

-based networks, [488–489](#), [491–492](#), [647](#)

Cisco Catalyst Center. *See* [Cisco Catalyst Center](#)

NBI (northbound interface), [479–481](#)

Open SDN, [483](#)

OpenDaylight, [482–483](#)

SBI (southbound interface), [478–479](#)

copy command, [379](#), [383–384](#)

copy running-config startup-config command, [228](#)

core design, [401](#), [647](#)

core layer, [647](#)

core switch, [402](#)

CoS (Class of Service), [646](#)

CPU

multithreading, [442](#)

virtual, [442](#)

CRUD (create, read, update, and delete) actions, [533–534](#), [647](#)

crypto key generate rsa command, [221](#)

CS (Class Selector), [336–337](#)

D

DAI (Dynamic ARP Inspection), 250, 649

configuration, 254–257, 259

limiting message rates, 257–258

logic, 253–254

optional message checks, 258–260

data center, 440, 442

automation and control, 484

network, 446

virtualization, 442–443

virtualized, 446–448

data modeling language, 542

data plane, 27, 473, 476, 648

data serialization language, 541–542, 546, 648

JSON (JavaScript Object Notation), 544

need for, 543–544

XML (eXtensible Markup Language), 544–545

YAML, 545–546

data structure

dictionary, 532

list, 532

variable, 477

debug command, 273, 276–277

debug ip nat command, 314

Declarative Model, 648

declarative policy model, 648

default router, 352, 355

delay, 325, 648

deleting, enable secret command, 208

denial-of-service attack, 189–190

deny any logic, 121, 648

deployment, WLC (wireless LAN controller), 35

centralized, 32

cloud-based, 32

distributed, 33–34

embedded, 34

destination port number, 96

device/s. *See also* IOS

discovery. *See* CDP (Cisco Discovery Protocol)

log messages, 270–271

debug command, 276–277

format, 272

severity levels, 272–273

storing for later review, 271

passwords, securing, 204–205

PoE (Power over Ethernet), 408–409

power classification, 410

power detection, 409–410

standards, 411

DevNet, 648

DevOps, 492

DHCP (Dynamic Host Configuration Protocol)

attack, 241–242, 248, 648

messages, filtering, 167–169

snooping, 240–241, 648

binding table, 244

configuration, 245–246, 249. See also configuration, DHCP snooping

filtering DISCOVER messages based on MAC address, 243–244

filtering messages that release IP addresses, 244–245

limiting DHCP message rates, 248–249

logic, 242–243

rules, 241, 243

dictionary attack, 196, 648

dictionary data structure, 532

DiffServ (Differentiated Services), 333, 335, 648

AF (Assured Forwarding), 336

CS (Class Selector), 336–337

EF (Expedited Forwarding), 336

guidelines for DSCP marking values, 337

dig command, 194

digital certificate, 197

dir command, 380–381

direction, ACL (access control list), 116–117

DISCOVER messages, filtering, 243–244

distributed architecture, 477

distributed control plane, 649

distributed denial-of-service attack, 190, 649

distributed WLC deployment, 33–34, 649

distribution layer, 649

distribution link, 649

distribution switch, 399–400, 402

full mesh, 400

partial mesh, 400

distribution system ports, 64

DMZ (demilitarized zone), 214

DNS (Domain Name System), 98–99, 105–106, 649
 messages, filtering, 163–164
 recursive lookup, 107–108
 resolution and requesting a web page, 106–107

Docker, 445–446

documentation, API, 536

domain-specific language, 649

DoS (denial of service) attack, 212, 648

DS (distribution system), 10–12, 649

DSCP (Differentiated Services Code Point), 330–331, 333, 649. *See also DiffServ (Differentiated Services)*

DSL (digital subscriber line), 426–427

DSLAM (digital access multiplexer), 427

dynamic NAT (Network Address Translation), 304–306
 configuration, 310–312
 troubleshooting, 317
 verification, 312–314

dynamic window, 102

E

EAP (Extensible Authentication Protocol), 47–48

EAP-FAST (EAP Flexible Authentication by Secure Tunneling), 48–49

EAP-TLS (EAP Transport Layer Security), 50

eavesdropping, 44–45

editing
 named IP ACL, 140–142
 numbered IP ACL, 143–144

EF (Expedited Forwarding), 336

E-LAN, 419–422, 649

elasticity, 448

E-Line, 418–421, 650

embedded wireless controller (EWC) deployment, 34

enable command, 198

enable password command, 206–207, 221

enable secret command, 206, 221, 650

 changing the encryption algorithm, 209–210

 deleting, 208

 hash function, 207–208

 interactions with enable password command, 206–207

encoding types

 enable secret command, 209

 username secret command, 211

encryption

 IPsec, 431–432

 key, 432

 MIC (message integrity check), 45–46

 password, 205–206

 TKIP (Temporal Key Integrity Protocol), 50–51

 wireless, 45

 CCMP (*Counter/CBC-MAC Protocol*), 51

 GCMP (*Galois/Counter Mode Protocol*), 51

End-to-End QoS Network Design, 328

enterprise network, 186–187

Enterprise QoS Solution Reference Network Design Guide, 328

EPG (endpoint group), 486

ephemeral ports, 97

errdisable recovery cause psecure-violation command, 237

errdisable recovery interval command, 237

error/s

detection, 94, 650

recovery, 94, 101–102, 650

ESS (extended service set), 650

ESSID (Extended Service Set Identifier), 12

Ethernet, 6. *See also* MetroE (Metro Ethernet)

10GBASE-T, 405

802.1Q header, marking, 333–334

access link, 650

fiber, 406–407

full-duplex mode, 8

half-duplex mode, 7–8

multigig, 405–406

Power over. *See* PoE (Power over Ethernet)

UTP standards, 404–405

WAN, 650

ETR (egress tunnel router), 649

EVC (Ethernet Virtual Connection), 419

EWC (embedded wireless controller), 650

exam. *See* CCNA exam 200–301

exploit, 188, 215, 650

extended IP ACL, 144–145, 650

configuration, 150–151

matching packets from web servers, 153–154

matching packets to web servers, 151–153

matching TCP and UDP port numbers, 147–150

matching the protocol, source IP, and destination IP, 145–146

syntax, 145–146

F

fabric, 497–498, 650

border node, 500

control-plane node, 500

edge node, 500, 506

routed access layer design, 502

fake AP, 44–46

FHRP (First Hop Redundancy Protocol), 350, 352

GLBP (Gateway Load Balancing Protocol), 362–363

active/active load balancing, 364–365

AVF (active virtual forwarder), 364

AVG (active virtual gateway), 364

similarities with HSRP and VRRP, 363–364

VIP (virtual IP address), 363

HSRP (Hot Standby Router Protocol)

active/standby model, 356, 359

failover, 357–358

Hello message, 358

Hold timer, 358

interface tracking, 359–360

load balancing, 359

preemption, 360–361

priority, 357

similarities with VRRP, 362

standby state, 357

versions, 361–362

VIP (virtual IP address), 357

virtual MAC address, 357

need for, 354–356

VRRP (Virtual Router Redundancy Protocol), 362–363

similarities with HSRP, 362

VIP (virtual IP address), 363

fiber Internet, 429, 650

fiber uplinks, 406–407

file system, IOS, 376–377, 379–381

filtering

DHCP messages, 167–169, 243–244

DNS messages, 163–164

ICMP messages, 164–165

OSPF messages, 165–167

packets

based on destination port, 148

based on source port, 148

SSH (Secure Shell), 169–171

Telnet, 169–171

URI (Uniform Resource Identifier), 217

finalizing WLAN configuration, 86–87

firewall, 211–212, 650

advanced features, 212

DMZ (demilitarized zone), 214

next-generation, 216–218

stateful, 212–213

zones, 213–214

first-match logic, IP ACL, 119

flash memory, 376, 651

FlexConnect Mode, 36–37, 651

flow, 327

flow control, 651

form factor, server, 441

format, log message, 272

forward acknowledgement, 101
forward secrecy, 53
fps (frames per second), 475–476
frame, 329
FTP (File Transfer Protocol), 99, 384–386, 651

- active mode, 386–387
- client, 385
- control connection, 384, 386
- copying images, 382–384
- passive mode, 387
- server, 385

full drop, 347
full mesh, 400, 403, 651
full-duplex mode, 8

G

GCMP (Galois/Counter Mode Protocol), 51
generative AI, 517–518, 651
Get message, 371
GET response, 108
GetBulk message, 371
GetNext message, 371
GitHub, 557, 651
GLBP (Gateway Load Balancing Protocol), 356, 362–363, 651

- active/active load balancing, 364–365
- AVF (active virtual forwarder), 364
- AVG (active virtual gateway), 364
- similarities with HSRP and VRRP, 363–364

VIP (virtual IP address), [363](#)
gratuitous ARP, [251–252](#), [651](#)
GRE (Generic Routing Encapsulation), [432](#)
group key, [45](#)
GTC (Generic Token Card), [49](#)
GUI, Cisco Catalyst Center, [515](#)

H

half-duplex mode, [7–8](#)
hash function

- algorithm, [209](#)
- enable secret command, [207–208](#)
- MD5 (Message Digest 5), [207](#), [209](#)

HCL (HashiCorp Configuration Language), [564](#)
header fields

- IPv4, [109](#)
- TCP (Transmission Control Protocol), [95](#)
- UDP (User Datagram Protocol), [104](#)

hold timer

- CDP (Cisco Discovery Protocol), [287](#)
- HSRP (Hot Standby Router Protocol), [358](#)

host mobility, [498](#)
HSRP (Hot Standby Router Protocol), [356](#)

- active/standby model, [356](#), [359](#)
- failover, [357–358](#)
- Hello message, [358](#)
- Hold timer, [358](#)
- interface tracking, [359–360](#)
- load balancing, [359](#)

- preemption, [360–361](#), [652](#)
- priority, [357](#), [652](#)
- similarities with VRRP, [362](#)
- standby state, [357](#)
- versions, [361–362](#)
- VIP (virtual IP address), [357](#)

HTTP (Hypertext Transfer Protocol), [104](#), [652](#)

- GET response, [108](#)
- how an app is chosen to receive data, [109](#)
- request and response, [534](#)
- and REST APIs, [533](#)
- transferring files, [108–109](#)
- verbs, [534](#)
- versions
 - HTTP 1.0 and 1.1*, [110](#)
 - HTTP 3.0*, [111–112](#)
 - HTTP/2 and TLS*, [110–111](#)

HTTP/3, adjusting ACLs for, [154–155](#)

hub and spoke topology, [652](#)

human vulnerabilities, [195–196](#)

- pharming, [195](#)
- phishing, [195](#)
- social engineering, [195](#)
- spear phishing, [195](#)
- watering hole attack, [195](#)
- whaling, [195](#)

hybrid topology, [403](#)

hypervisor, [442](#), [444](#), [461](#), [652](#)

I

- IaaS (Infrastructure as a Service), 451–452, 653**
- IAC (infrastructure as code), 653**
- IANA (Internet Assigned Numbers Authority), 97**
- IBN (intent-based networking), 483, 486–488, 653**
- IBSS (independent basic service set), 13–14, 653**
- ICMP (Internet Control Message Protocol), message filtering, 164–165**
- IEEE 802.11, 7–8, 18–19**
- IEEE 802.3, 6**
- IFS (IOS File System), 653**
- Imperative Model, 652**
- Inform message, 372**
- inside global address, 303–304, 653**
- inside local address, 303–304, 653**
- inside source NAT, 302–303**
- integrity, message, 45–46**
- intercloud exchange, 459–460**
- interface**
 - access, 642
 - application programming, 478
 - southbound, 478–479
 - tracking, 359–360
 - user network, 417
- interference, wireless network, 7**
- Internet**
 - access, 426
 - 4G/5G, 428–429

cable, [427–428](#)

DSL (digital subscriber line), [426–427](#)

fiber, [429](#)

VPN, [425–426](#), [430–431](#). *See also* [VPN](#)

IOS. *See also* [command/s](#)

ACLs, [173–174](#)

configuring well-known port numbers, [149](#)

file system, [376–377](#)

filenames, [379](#)

image upgrade, [378](#)

using FTFP, [378–379](#)

verifying code integrity, [381–382](#)

listing files in the file system, [379–381](#)

log messages, [270–271](#)

configuration, [273–274](#)

debug command, [276–277](#)

format, [272](#)

severity levels, [272–273](#)

storing for later review, [271](#)

verification, [274–276](#)

passwords

encrypting, [205–206](#)

securing, [204–205](#)

IOS XE. *See also* [command/s](#); [device/s](#)

ACLs, [173–174](#)

common ACL, [175–176](#)

configuration menus, [61–63](#)

WLAN configuration, [67–69](#)

apply the policy tag to some APs, [78–79](#)

map the WLAN and policy profiles to a policy tag, [77](#)

policy profile, [74–77](#)

profile, 69–74

ip access-group command, 176

ip access-list command, 138–139

ip access-list resequence command, 175

IP ACL (access control list), 116, 118, 331, 511

adjusting for HTTP/3, 154–155

building, 155

common ACL, 175–176

comparing in IOS and IOS XE, 173–174

deny any logic, 121

DHCP messages, filtering, 167–169

DNS messages, filtering, 163–164

extended, 144–145

configuration, 150–151

matching packets from web servers, 153–154

matching packets to web servers, 151–153

matching TCP and UDP port numbers, 147–150

*matching the protocol, source IP, and destination IP,
145–146*

syntax, 145–146

ICMP messages, filtering, 164–165

implementing, 125, 156

list logic, 119–121

location and direction, 116–117

matching logic, 121–122

matching multiple nonconsecutive ports with eq parameter, 177

matching packets, 117–118

named, 138

configuration, 139

editing, 140–142

versus numbered, 138–139

verification, 139–140

numbered

editing, 143–144

versus named, 138–139

OSPF messages, filtering, 165–167

resequencing sequence numbers, 174–175

SSH, filtering, 169–171

standard numbered, 119, 125–129

taking action when a match occurs, 118

Telnet, filtering, 169–171

troubleshooting, 129–130

types of, 118–119

wildcard mask, 122–123

binary, 123–124

finding the right one to match a subnet, 124

ip arp inspection validate command, 258–259

ip arp inspection vlan command, 255

ip dhcp snooping command, 246–248

ip helper-address command, 168

ip inside source static command, 303

ip nat inside source command, 312, 315

ip nat pool command, 311

IPP (IP Precedence), 333, 653

IPS (intrusion prevention system), 215–216, 653

next-generation, 218–219

signature database, 215–216

IPsec, 431, 433–434, 653

remote access VPN, 433–434

transport mode, 434

tunnel mode, 434

IPv4

- header

 - fields*, [109](#)

 - marking*, [333](#)

- private addresses, [300–301](#)

ISDN (Integrated Services Digital Network), [426](#)

ITR (ingress tunnel router), [506–508](#)

J

Jinja2, [654](#)

jitter, [325](#), [654](#)

JSON (JavaScript Object Notation), [541–542](#), [544](#), [654](#)

- arrays, [547–549](#)

- beautified, [550](#)

- data serialization, [541–542](#)

- key:value pairs, [547](#)

- minified, [550](#)

- objects, [547–549](#)

K

key/s

- :value pair, [547](#), [654](#)

- encryption, [432](#)

- WEP (Wired Equivalent Privacy), [47](#)

L

label switching, [423](#)

LAN

campus, [398–399](#), [403](#). *See also* [campus LAN](#)
 access switches, [399](#)
 distribution switches, [399–400](#)
 fiber uplinks, [406–407](#)
 full mesh, [403](#)
 hybrid topology, [403](#)
 partial mesh, [403](#)
 star topology, [402](#)
 three-tier, [400–402](#)
 two-tier, [399–400](#)
collapsed core, [400](#)
core design, [401](#)
SOHO (small office/home office), [407–408](#)

leaf, [654](#)

LEAP (Lightweight EAP), [48–49](#)

lightweight AP (access point), [28](#)

line console 0 command, [221](#)

line vty command, [221](#)

LISP (Locator/ID Separation Protocol), [503](#), [505–509](#), [654](#)

list data structure, [532](#), [654](#)

list logic, IP ACL, [119–121](#)

LLDP (Link Layer Discovery Protocol), [283](#), [654](#)

 configuration, [290–291](#)
 examining information learned by, [287–290](#)
 MED (Media Endpoint Discovery), [292–293](#)
 timer, [287](#)
 TLV (type-length-value), [292](#)
 verification, [291–292](#)

lldp run command, [290–291](#)

LLM (Large Language Model), [521](#), [654](#)

LLQ (low-latency queuing), [339–341](#)

load balancing

active/active, [364–365](#)

HSRP (Hot Standby Router Protocol), [359](#)

local username, [654](#)

log message, [270–271](#), [274–276](#), [655](#). *See also* [syslog](#)

debug command, [276–277](#)

format, [272](#)

severity levels, [272–273](#)

storing for later review, [271](#)

logging buffered command, [271](#)

logging host command, [271](#)

logic

DAI (Dynamic ARP Inspection), [253–254](#)

DHCP snooping, [242–243](#)

login command, [221](#)

login local command, [221](#)

loss, [325](#), [655](#)

LWAPP (Lightweight Access Point Protocol), [29](#)

M

MAC (Media Access Control) layer, [28](#), [655](#). *See also* [split-MAC architecture](#)

MAC address/es, [8](#)

port security, [229–230](#)

virtual, [357](#)

malware, [194–195](#)

Trojan horse, [194](#)

virus, [194](#)

- worm, [194–195](#)
- management IP address, [25](#)**
- management plane, [475](#), [655](#)**
- manager, SNMP, [370](#)**
- man-in-the-middle attack, [44](#), [191–193](#), [655](#)**
- marking, [330](#), [332](#), [655](#)**
 - 802.1Q header, [333–334](#)
 - DSCP (Differentiated Services Code Point)
 - AF (Assured Forwarding), [336](#)*
 - CS (Class Selector), [336–337](#)*
 - EF (Expedited Forwarding), [336](#)*
 - guidelines, [337](#)*
 - fields, [334](#)
 - IP header, [333](#)
 - trust boundary, [334–335](#)
- matching, [117–118](#), [330–331](#). *See also* **ACL (access control list); QoS****
- IP ACL, [331](#)
 - logic, [121–122](#)*
 - matching TCP and UDP port numbers, [147–150](#)*
 - taking action when a match occurs, [118](#)
 - to web servers, [151–153](#)
 - from web servers, [153–154](#)
- MD5 (Message Digest 5), [207](#), [209](#), [381–382](#), [655](#)**
- MED (Media Endpoint Discovery), LLDP (Link Layer Discovery Protocol), [292–293](#)**
- memory**
 - flash, [376](#)
 - ternary content-addressable, [476](#)
- Meraki, [462](#)**

dashboard, [655](#)

default view, [462–463](#)

Topology and Path Visualization, [463–464](#)

mesh, [403](#), [655](#)

mesh AP, [17](#)

message/s

ARP, [251](#)

classification, [329–330](#). *See also* [classification](#)

DHCP, filtering, [167–169](#)

DNS, filtering, [163–164](#)

HSRP (Hot Standby Router Protocol), [357–358](#)

HTTP, [534](#)

ICMP, filtering, [164–165](#)

integrity check, [45–46](#)

LLDP (Link Layer Discovery Protocol), TLV (type-length-value), [292](#)

log, [270–271](#)

debug command, [276–277](#)

format, [272](#)

severity levels, [272–273](#)

storing for later review, [271](#)

OSPF, filtering, [165–167](#)

privacy, [44–45](#)

SNMP

Get, [371](#)

GetBulk, [371](#)

GetNext, [371](#)

Inform, [372](#)

Trap, [372](#)

MetroE (Metro Ethernet), [416](#), [655](#)

E-LAN, [419–420](#)

- E-Line, [418–419](#)
- EVC (Ethernet Virtual Connection), [419](#)
- IEEE Ethernet standards, [417–418](#)
- Layer 3 design, [420](#)
 - using E-LAN*, [421–422](#)
 - using E-Line*, [420–421](#)
- physical design and topology, [416–418](#)
- topology, [418](#)
- MIB (Management Information Base), [370](#), [372–374](#), [655](#)**
- mitigation technique, [655](#)**
- ML (machine learning), [517–518](#)**
- mobile phone, 4G/5G, [428–429](#)**
- monitoring, configuration, [557–558](#)**
- more command, [377](#)**
- MP-BGP (Multiprotocol BGP), [425](#)**
- MPGBP (Multiprotocol BGP), [656](#)**
- MPLS (Multiprotocol Label Switching), [422](#), [656](#)**
 - access link technologies, [424](#)
 - CE (customer edge), [424](#)
 - PE (provider edge), [424](#)
 - QoS (Quality of Service), [423](#)
 - VPN, [422–423](#)
 - Layer 3*, [424–425](#)
 - physical design and topology*, [423–424](#)
- MTU (maximum transmission unit), [326](#), [655](#)**
- multifactor authentication, [199](#), [656](#)**
- multifactor credentials, [197](#)**
- multigig Ethernet, [405–406](#), [656](#)**
- multimode fiber cable, [406](#)**

multiplexing, 95–97

multithreading, 442

N

named IP ACL, 138, 656

configuration, 139

editing, 140–142

versus numbered, 138–139

verification, 139–140

narrow AI, 517–518, 656

NAT (Network Address Translation), 300, 302, 656

dynamic, 304–306

configuration, 310–312

verification, 312–314

inside global address, 303–304

inside local address, 303–304

inside source, 302–303

Overload, 306–307

configuration, 314–317

verification, 317

static, 303

configuration, 308–309

verification, 309–310

troubleshooting, 317–318

NBAR2 (next-generation Network Based Application Recognition), 331–332

NBI (northbound interface), 479–481, 490, 494, 657

network/s. *See also* LAN; WAN; wireless network/s

baseline, 524

data center, 446

- fabric, [497–498](#)
- management, [488–491](#)
- outage, [353–354](#)
- overlay, [497](#), [498](#)
- private, [300–302](#)
- programmability, [472](#)
- redundancy, need for, [353–354](#)
- single point of failure, [353–354](#)
- tail drop, [347](#)
- traditional versus controller-based, [488–489](#), [491–492](#)
- traffic
 - bandwidth*, [324–325](#)
 - delay*, [325](#)
 - jitter*, [325](#)
 - types of*, [325](#)
- trust boundary, [334–335](#)
- underlay, [497–498](#)
- wireless, comparing with wired, [6–7](#)

next-generation firewall, [216–218](#)

NGFW (next-generation firewall), [216–218](#), [656](#)

NGIPS (next-generation IPS), [218–219](#), [657](#)

NIC (network interface card), [443](#)

NIST (National Institute of Standards and Technology), [51](#), [448–449](#)

NMS (Network Management System), [370](#), [374](#), [514–517](#), [656](#)

no cdp enable command, [286](#)

no enable secret command, [208](#), [221](#)

no shutdown command, [237](#), [248](#)

nonoverlapping channels, [18](#), [20](#), [657](#)

nslookup command, [194](#)

NTP (Network Time Protocol), [277–278](#), [656–657](#)

client/server mode, [281](#)

configuration, [279–281](#)

reference clock, [281](#)

setting the time and time zone, [278–279](#)

stratum, [281–282](#)

synchronization, [280](#)

ntp master command, [279](#), [281–282](#)

ntp server command, [278–279](#)

numbered IP ACL

editing, [143–144](#)

versus named, [138–139](#)

O

objects, JSON, [547–549](#)

OfficeExtend, [37](#)

OID (object ID), [372](#)

OM (Optical Multimode), [406–407](#), [657](#)

on-demand self-service, [657](#)

open authentication, [46](#)

Open SDN, [481–482](#)

OpenDaylight controller, [482–483](#)

OpenFlow, [482](#), [657](#)

operational network management, [489](#)

ordered data transfer, [657](#)

OSC (Open SDN Controller), [483](#)

OSI model, transport layer, [94](#)

OSPF (Open Shortest Path First), [165–167](#), [474–475](#)

outdoor bridge, [16](#)
output queuing, [338](#)
outside global, [658](#)
overlay, [497–498](#), [658](#). *See also* [Cisco SD-Access](#)

P

PaaS (Platform as a Service), [453–454](#), [658](#)
packet/s, [329](#). *See also* [IP ACL \(access control list\)](#); [traffic](#)
 complex matching, [330–331](#)
 filtering
 based on destination port, [148](#)
 based on source port, [148](#)
 matching, [117–118](#)
 MTU (maximum transmission unit), [326](#)
 VoIP (voice over IP), [327–328](#)
partial mesh, [400](#), [403](#), [658](#)
passive mode, FTP, [387](#)
passive scanning, [9](#), [658](#)
password/s. *See also* [enable password command](#); [enable secret command](#)
 alternatives, [196](#)
 biometric credentials, [197](#)
 digital certificate, [197](#)
 multifactor credentials, [197](#)
 brute-force attack, [196](#)
 clear-text, [207](#)
 dictionary attack, [196](#)
 enable, encoding with hashes, [206](#)
 encrypting, [205–206](#)
 guessing, [658](#)

- IOS, securing, [204–205](#)
- policy, [196](#)
- SNMP, [374–375](#)
- vulnerabilities, [196](#)
- PAT (Port Address Translation), [306–307](#)**
 - configuration, [314–317](#)
 - troubleshooting, [318](#)
 - verification, [317](#)
- PD (powered device), [409, 659](#)**
- PE (provider edge), [424, 660](#)**
- PEAP (Protected EAP), [49](#)**
- personal mode, WPA (Wi-Fi Protected Access), [52–53](#)**
- pharming, [195, 658](#)**
- PHB (per-hop behavior), [322, 658](#)**
- phishing, [195, 658](#)**
- physical access control, [200](#)**
- physical ports, WLC (wireless LAN controller), [63–65](#)**
- ping command, [164](#)**
- PKI (Public Key Infrastructure), [50](#)**
- playbook, Ansible, [563](#)**
- PoE (Power over Ethernet), [408–409, 658–659](#)**
 - and LAN design, [411](#)
 - power classification, [410](#)
 - power detection, [409–410](#)
 - standards, [411](#)
- point-to-point bridged link, [16, 658](#)**
- policing, [340, 342–344, 658](#)**
- policy**
 - Cisco SD-Access, [513](#)

password, 196

profile, 74–77

tag, 68

PoP (point of presence), 417, 658

port security, 224–225, 659

configuration, 225–228

MAC addresses, 229–230

protect mode, 233–234

restrict mode, 234–235

shutdown mode, 231–233

sticky secure MAC addresses, 225

verification, 228–229

violation modes, 230–231

port/s, 659

distribution system, 64

ephemeral, 97

number, 96–98

untrusted, 665

user, 97

well-known, 97, 99, 149

Postman, 537–541

practicing CLI skills, 593–595

predictive analytics, 524

preemption, HSRP (Hot Standby Router Protocol), 360–361

on-premise cloud. *See* private cloud

prioritization, 338

priority queue, 340, 659

privacy, message, 44–45

private cloud, 449–450, 659

private networks, 300–302

private WAN, connecting to the cloud with, [458–459](#)

probe request, [659](#)

profile

configuration, [67](#)

policy, [74–77](#)

WLAN configuration, [69–74](#)

programming, variables, [530–531](#)

data structure, [477](#)

simple, [531](#)

protect mode, port security, [233–234](#)

protocol, connectionless/connection-oriented, [100–101](#)

provider, [660](#)

PSE (power sourcing equipment), [409](#), [659](#)

public cloud, [450–451](#), [460](#), [660](#)

intercloud exchange, [459–460](#)

private WAN and Internet VPN access to the, [458–459](#)

using Internet to connect to the, [457–458](#)

public IPv4 addresses, [300](#)

pull model, [660](#)

push model, [563](#), [660](#)

pwd command, [380–381](#)

Python

dictionary data structure, [532](#)

list data structure, [532](#)

Q

QFP (Quantum Flow Processor), [476](#)

QoE (quality of experience), [326](#)

QoS (Quality of Service), 322, 324, 660. *See also* traffic

CAC (call admission control), 340–341

classification, 329–330

NBAR2 (next-generation Network Based Application Recognition), 331–332

on routers, 331–332

congestion avoidance, 346–347

DiffServ, 333, 335

AF (Assured Forwarding), 336

CS (Class Selector), 336–337

EF (Expedited Forwarding), 336

guidelines for DSCP marking values, 337

marking, 330, 332

802.1Q header, 333–334

fields, 334

IP header, 333

MPLS (Multiprotocol Label Switching), 423

policing, 342–344

queuing, 337–338

class-based weighted fair, 339

classifier function, 338

low-latency, 339–341

output, 338

prioritization, 338–339

round-robin scheduling, 338–339

on routers and switches, 329

shaping, 341–342, 344–346

trust boundary, 334–335

WLAN, configuring, 85

queuing, 329–330, 337–338, 660

class-based weighted fair, 339

classifier function, 338

- low-latency, [339–341](#)
- output, [338](#)
- prioritization, [338](#)

QUIC, [660](#)

R

radio, AP, [19](#)

RADIUS, [199–200](#), [660](#)

rapid elasticity, [660](#)

rate limit, DAI (Dynamic ARP Inspection), [257–258](#)

RC4 cipher algorithm, [47](#)

RCA (Root Cause Analysis), [524](#)

read-only community, [660](#)

read-write community, [660](#)

reassociation frame, [13](#), [661](#)

reconnaissance attack, [661](#)

recursive DNS lookup, [107–108](#), [661](#)

redundancy

- need for, [353–354](#)
- single point of failure, [353–354](#)

reference clock, NTP (Network Time Protocol), [281](#)

reflection attack, [191](#), [661](#)

reliability, TCP (Transmission Control Protocol), [101–102](#)

remote access VPN

- with IPsec, [433–434](#)
- with TLS, [434–435](#)

repeater, [14](#)

resequencing ACL sequence numbers, [174–175](#)

resource pooling, 448, 661

RESTful API/s, 480–481, 510, 528–529

cacheable, 530

client/server architecture, 529

CRUD actions, 533–534

and HTTP, 533

stateless operation, 530

URIs, 534–536

restrict mode, port security, 234–235

RF signals, 7

RF tag, 78–79

RFC (Request for Comments)

791, 333

793, 95

1065, “Structure and Identification of Management Information for TCP/IP-based Internets”, 370

1918, 301

2475, 335

3986, 535–536

7348, 498

roaming, 13, 661

round-robin scheduling, 338–339, 661

round-trip delay, 325

routed access layer, 502

router/s, 505. *See also* device/s; IOS; IOS XE

classification, 331–332

data plane processing, 473

default, 352, 355

filtering for vty access, 171–173

flash memory, 376

- FTP password and username configuration, [383–384](#)
- ingress tunnel, [506–508](#)
- login security, [204](#)
- QoS, [329](#)
- VRF (virtual routing and forwarding), [455–456](#)
- wireless, [407](#)
- rules, DHCP snooping, [241, 243](#)**

S

- SaaS (Software as a Service), [452–453, 663](#)**
- SAE (Simultaneous Authentication of Equals), [53](#)**
- SBI (southbound interface), [478–479, 494](#)**
- scheduling, round-robin, [338–339](#)**
- scoring, exam, [587](#)**
- SD-Access, [663](#)**
- SDN (Software-Defined Networking), [472, 663](#). *See also controller***
 - ACI (Application Centric Infrastructure), [484](#)
 - APIC (Application Policy Infrastructure Controller), [487](#)*
 - EPG (endpoint group), [486](#)*
 - operating model with intent-based networking, [486–488](#)*
 - spine and leaf design, [484–485](#)*
 - automation, [489–491](#)
 - controller, [477](#)
 - NBI (northbound interface), [479–481](#)
 - ONF (Open Networking Foundation) model, [481–482](#)
 - OpenDaylight controller, [482–483](#)
 - SBI (southbound interface), [478–479](#)
- security. *See also* [attack/s](#); [authentication](#); [port security](#)**
 - exploit, [188](#)

- firewall, [211–212](#)
 - advanced features*, [212](#)
 - next-generation*, [216–218](#)
 - stateful*, [212–213](#)
 - zones*, [213–214](#)
- group-based, [513–514](#)
- IPS (intrusion prevention system), [215–216](#)
 - next-generation*, [218–219](#)
 - signature database*, [215–216](#)
- mitigation techniques, [188](#)
- password, IOS, [204–205](#)
- program, [200](#)
- shared-key, [47](#)
- threat/s, [188](#)
- vulnerability, [187–188](#)
- wireless
 - TKIP (Temporal Key Integrity Protocol)*, [50–51](#)
 - WPA (Wi-Fi Protected Access)*, [51–52](#)
 - WPA2*, [52](#)
 - WPA3*, [52](#)
 - WPA-Personal mode*, [52–53](#)
- WLAN, configuration, [83–84](#)
- zones, [213–214](#)

segment, [662](#)

self-healing wireless coverage, [32](#)

self-service, [448](#)

send time, CDP (Cisco Discovery Protocol), [287](#)

sender hardware address, [662](#)

serial console, [461](#)

server. *See also* VM (virtual machine)

- blade, [441](#)

- Cisco hardware, [440–441](#)
- form factor, [441](#)
- FTP (File Transfer Protocol), [385](#)
- NIC, [443](#)
- NTP (Network Time Protocol), [281](#)
- rack, [440](#)
- UCS (Unified Computing system), [485](#)
- virtualization, [441–443](#)
- web, [667](#)

service password-encryption command, [205](#), [206](#), [221](#)

severity level, log message, [272–273](#)

SGT (scalable group tag), [513–514](#), [661](#)

SHA-256, [209](#)

SHA512, verifying IOS code integrity, [381–382](#)

shaping, [341–342](#), [344–346](#), [662](#)

shared key, [47](#), [662](#)

show access-lists command, [126–127](#)

show cdp commands, [283](#)

show cdp neighbors command, [284–285](#)

show cdp neighbors detail command, [285–286](#)

show flash command, [379–381](#)

show ip access-list command, [126–127](#), [132](#), [153](#)

show ip arp inspection command, [256](#)

show ip arp inspection statistics command, [257](#)

show ip dhcp snooping command, [247](#), [249](#), [256](#)

show ip interface command, [153](#)

show ip nat statistics command, [312–313](#)

show ip nat translations command, [309](#), [312](#), [314](#), [317](#)

show lldp command, [291](#)

- show lldp entry command, 289–290**
- show lldp neighbors command, 288**
- show logging command, 271, 274–275**
- show ntp associations command, 281–282**
- show ntp status command, 280, 282**
- show port-security command, 232**
- show port-security interface command, 228–229, 232, 234–235**
- show running-config command, 126, 139–140, 155, 164, 168, 205–206, 208, 227, 234, 308–309, 311, 316, 377**
- shutdown command, 231, 237, 248**
- shutdown mode, port security, 231–233**
- signature database, IPS (intrusion prevention system), 215–216**
- signatures, application, 332**
- simple variable, 531**
- single point of failure, 353–354. *See also* FHRP (First Hop Redundancy Protocol)**
- site tag, 78–79**
- site-to-site VPN, 430–433, 662**
- sliding window, 102, 662**
- smishing, 195**
- SNMP (Simple Network Management Protocol), 99, 662–663**
 - ACLs, 374**
 - agent, 370**
 - clear-text password, 374–375**
 - communities, 375**
 - Get message, 371**
 - GetBulk message, 371**
 - GetNext message, 371**
 - Inform message, 372**

manager, [370](#)

MIB (Management Information Base), [370](#), [372–374](#), [655](#)

NMS (Network Management System), [370](#), [374](#)

securing, [374–375](#)

Trap notification, [372](#)

versions, [375](#)

snooping, DHCP, [240–241](#)

binding table, [244](#)

configuration, [245–246](#), [249](#). *See also* [configuration, DHCP snooping](#)

filtering DISCOVER messages based on MAC address, [243–244](#)

filtering messages that release IP addresses, [244–245](#)

limiting DHCP message rates, [248–249](#)

logic, [242–243](#)

rules, [241](#)

social engineering, [195](#), [663](#)

socket, [97](#). *See also* [port/s](#)

software container. *See* [container](#)

SOHO (small office/home office), [407–408](#), [663](#)

source NAT, [663](#)

SP (service provider), [662](#)

access link, [417](#)

intercloud exchange, [459–460](#)

spear phishing, [195](#), [664](#)

spine and leaf design, [484–485](#), [664](#)

split-MAC architecture, [28–32](#), [36–37](#), [664](#)

CAPWAP (Control and Provisioning of Wireless Access Points), [29–31](#)

WLC functions, [32](#)

spoofing attack, 188–189, 664

 amplification attack, 191

 denial-of-service, 189–190

 man-in-the-middle, 44, 191–193

 reflection, 191

SSH (Secure Shell), 169–171, 204

SSID (Service Set Identifier), 8–9, 44, 662

 autonomous AP, 25

 supporting multiple on one AP, 11–12

STA (station), 664

standalone mode, 664

standard numbered IP ACL, 119, 125–129

standards

 IEEE 802.11, amendments, 18–19

 PoE (Power over Ethernet), 411

star topology, 402, 664

stateful firewall, 212–213

stateless operation, 664

static NAT (Network Address Translation), 303

 configuration, 308–309

 troubleshooting, 317

 verification, 309–310

sticky secure MAC addresses, 225

storage, variable, 542–543

STP (Spanning Tree Protocol), 474

stratum, 281–282

subnet, matching with an ACL, 124

switch/es. *See also* device/s; IOS; IOS XE

 access, 399, 402

ASIC (application-specific integrated circuit), 476

core, 402

data plane, 475–476

distribution, 399–400, 402

fps (frames per second), 475–476

LAN, 222

Layer 2, 505

login security, 204

port security, 224–225

configuration, 225–228

MAC addresses, 229–230

protect mode, 233–234

restrict mode, 234–235

shutdown mode, 231–233

sticky secure MAC addresses, 225

verification, 228–229

violation modes, 230–231

QoS, 329

TOR (Top of Rack), 446

virtual, 443–444

switchport mode access command, 227

switchport mode command, 236

switchport port-security access command, 227

switchport port-security mac-address command, 236–237

switchport port-security maximum command, 237

SYN flag, 100

synchronization, NTP (Network Time Protocol), 280

syntax

access-list command, 125

extended IP ACL, 145–146

syslog, [270](#), [664](#)

configuration, [273–274](#)

debug command, [276–277](#)

verification, [274–276](#)

T

TACACS+, [199–200](#)

tag

policy, [68](#)

RF, [78–79](#)

site, [78–79](#)

tail drop, [347](#)

TCAM (ternary content-addressable memory), [476](#), [664](#)

TCP (Transmission Control Protocol), [94](#), [95](#)

congestion avoidance, [346–347](#)

connection establishment, [100](#)

connection termination, [100–101](#)

error recovery and reliability, [101–102](#)

forward acknowledgement, [101](#)

header fields, [95](#)

multiplexing, [95–96](#)

popular applications and their well-known port numbers, [99](#)

port numbers, [96–98](#), [147–150](#)

socket, [97](#)

windowing, [102–103](#), [346–347](#)

TCP/IP. *See also* TCP (Transmission Control Protocol); UDP (User Datagram Protocol); web browser

DNS (Domain Name System), [98–99](#), [105–106](#)

recursive lookup, [107–108](#)

resolution and requesting a web page, [106–107](#)

HTTP (Hypertext Transfer Protocol), [104](#)
 how an app is chosen to receive data, [109](#)
 transferring files, [108–109](#)
model, transport layer, [94](#)
SNMP (Simple Network Management Protocol), [99](#)
TFTP (Trivial File Transfer Protocol), [99](#)
URI (Uniform Resource Identifier), [104–105](#)
WWW (World Wide Web), [98](#)

Telnet, [169–171, 204](#)

template, configuration, [559–561](#)

terminal monitor command, [296](#)

Terraform, [563–565, 664](#)

TFTP (Trivial File Transfer Protocol), [99, 387–388, 665](#). *See also* [FTP \(File Transfer Protocol\)](#)

threats, [188, 194–195, 665](#). *See also* [attack/s](#)

three-tier campus LAN, [400–402](#)

TIA (Telecommunications Industry Association), [404](#)

time

 interval, shaper, [345–346](#)

 NTP, setting, [278–279](#)

TKIP (Temporal Key Integrity Protocol), [50–51](#)

TLS (Transport Layer Security), [434–435, 665](#)

TLV (type-length-value), LLDP (Link Layer Discovery Protocol), [292](#)

tools. *See also* [QoS \(Quality of Service\)](#)

 API development environment, [536–541](#)

 ChatGPT, [518–523](#)

 configuration management

Ansible, [562–563](#)

Terraform, [563–565](#)

- congestion avoidance, [347](#)
- development, [453](#)

topology

- hybrid, [403](#)
- MetroE (Metro Ethernet), [418](#)
- MPLS VPN, [423–424](#)
- star, [402](#)

TOR (Top of Rack) switch, [446](#)

ToS (type of service) byte, [333](#)

traffic

- bandwidth, [324–325](#)
- batch, [326](#)
- data application, [325–326](#)
- delay, [325](#)
- flow, [327](#)
- jitter, [325](#)
- prioritization, [341](#)
- types of, [325](#)
- voice and video application, [327–328](#)

transport input command, [221](#)

transport input ssh command, [205](#)

transport layer, [94](#)

Trap notification, [372](#)

Trojan horse, [194](#), [665](#)

troubleshooting

- IP ACL (access control list), [129–130](#)
- NAT (Network Address Translation), [317–318](#)

trust boundary, [334–335](#)

trusted port, [665](#)

tunnel

CAPWAP (Control and Provisioning of Wireless Access Points), [29–31](#)

VPN, [430](#)

tunneling, VXLAN, [504](#)

two-tier campus LAN, [399–400](#)

full mesh, [403](#)

hybrid topology, [403](#)

star topology, [402](#)

uplinks, [403](#)

U

UCS (Unified Computing system), [441](#), [485](#), [665](#)

UDP (User Datagram Protocol), [94](#), [103](#)

data transfer, [103–104](#)

header, [104](#)

multiplexing, [95–96](#)

port numbers, matching, [147–150](#)

underlay, [497–498](#), [665](#). *See also* [Cisco SD-Access](#)

UNI (user network interface), [417](#)

unidirectional communication, wireless network, [7](#)

untrusted port, [665](#)

updates, exam, [572–576](#)

upgrade, IOS image, [378–379](#)

uplink, fiber, [406–407](#)

UPoE (Universal Power over Ethernet), [665](#)

URI (Uniform Resource Identifier), [104–105](#), [665–666](#)

format, [535–536](#)

using with REST to specify the resource, [534–536](#)

URL (Universal Resource Locator), [105](#), [217](#)

- user ports, 97**
- username password command, 210, 221**
- username secret command, 210, 221**
- UTP (unshielded twisted-pair), 404–405, 666**
- UTP (unshielded twisted-pair) cabling, 403–404**
- uWGB (universal workgroup bridge), 16**

V

- variable, 530–531**
 - configuration, 560–561
 - data structure, 477. *See also* data structure
 - simple, 531
 - storing, 542–543
- vCPU (virtual CPU), 442, 666**
- vendors**
 - container, 445
 - virtualized data center, 443
- verbs, HTTP, 534**
- verification**
 - CDP (Cisco Discovery Protocol), 286–287
 - dynamic NAT (Network Address Translation), 312–314
 - LLDP (Link Layer Discovery Protocol), 291–292
 - named IP ACL, 139–140
 - NAT (Network Address Translation), 309–310
 - PAT (Port Address Translation), 317
 - port security, 228–229
 - syslog, 274–276
- verify command, 381–382**
- version/s**

control, [555–557](#)

HSRP (Hot Standby Router Protocol), [361–362](#)

SNMP, [375](#)

video

prioritization, [341](#)

QoS requirements, [328](#)

violation mode, [230–231](#), [666](#)

VIP (virtual IP address), [357](#), [363](#), [666](#)

virtual console, [461](#)

virtual MAC address, [357](#)

virtualization

data center, [446–448](#)

hypervisor, [442](#), [444](#), [461](#)

server, [441–443](#)

vendors, [443](#)

virus, [194](#), [215–217](#), [666](#)

vishing, [195](#)

VLAN (virtual local-area network), [10–11](#), [25](#)

VM (virtual machine), [442](#), [447](#), [666](#)

versus container, [444](#)

PaaS (Platform as a Service), [453](#)

vNIC (virtual NIC), [443](#), [666](#)

VoIP (voice over IP)

prioritization, [341](#)

QoS requirements, [327–328](#)

VPN, [430–431](#), [458](#), [666](#)

Internet, [425–426](#)

IPsec, [431](#)

MPLS (Multiprotocol Label Switching), [422–423](#)

Layer 3, [424–425](#)

- physical design and topology, 423–424*
- remote access
 - with IPsec, 433–434*
 - with TLS, 434–435*
- site-to-site, 430–433
- tunnel, 430
- VRF (virtual routing and forwarding), 425, 454–456, 666**
- VRRP (Virtual Router Redundancy Protocol), 356, 362–363**
- vSwitch (virtual switch), 443–444, 666**
- vty, access control, 171–173**
- vulnerability/ies, 187–188, 667**
 - human, 195–196
 - pharming, 195*
 - phishing, 195*
 - social engineering, 195*
 - spear phishing, 195*
 - watering hole attack, 195*
 - whaling, 195*
 - password, 196
- VXLAN, 498, 503–505, 667**

W

WAN. *See also* MetroE (Metro Ethernet)

- connection to the cloud, 456
 - accessing public cloud services using the Internet, 456–457*
 - using Internet to connect to the public cloud, 457–458*
- link, 37
- MPLS (Multiprotocol Label Switching), 422
 - access link technologies, 424*

- CE (customer edge)*, [424](#)
 - PE (provider edge)*, [424](#)
 - QoS*, [423](#)
 - VPN*, [422–423](#)
 - private, [430](#), [458–459](#)
 - Software-Defined, [484](#)
- watering hole attack**, [195](#), [667](#)
- web browser**, [104](#)
 - DNS recursive lookup, [107–108](#)
 - DNS resolution and requesting a web page, [106–107](#)
 - how an app is chosen to receive data, [109](#)
 - transferring files with HTTP, [108–109](#)
- web server**, [104–105](#), [667](#)
- web-based GUI, WLC (wireless LAN controller)**, [59–61](#)
- well-known ports**, [97](#), [99](#), [149](#)
- WEP (Wired Equivalent Privacy)**, [47](#), [50](#)
- WGB (workgroup bridge)**, [15–16](#), [667](#)
- whaling**, [195](#), [667](#)
- whitespace**, [550](#)
- whois command**, [194](#)
- Wi-Fi, generational names**, [20](#)
- Wi-Fi Alliance**, [51–53](#), [407](#)
- wildcard mask**, [122–123](#), [667](#)
 - binary, [123–124](#)
 - finding the right one to match a subnet, [124](#)
- windowing**, [102–103](#), [346–347](#)
- wireless network/s. *See also* WLC (wireless LAN controller)**
 - 2.4-GHz band, [17](#)
 - 4G/5G, [428–429](#)

5-GHz band, [17](#)

ad hoc, [14](#)

AP (access point). *See also* [AP \(access point\)](#); [autonomous AP](#); [Cisco AP/s](#)

association request/response, [9](#), [19](#)

autonomous, [24–25](#)

beacon frame, [8](#)

BSA (basic service area), [8](#)

BSS (basic service set), [8](#)

cloud-based architecture, [26–27](#)

IBSS (independent basic service set), [13–14](#)

infrastructure mode, [8](#)

management platform, [26](#)

mesh, [17](#)

outdoor bridge, [16](#)

radios, [19](#)

repeater mode, [14](#)

roaming, [13](#)

supporting multiple SSIDs on, [11–12](#)

architecture

autonomous AP, [24–25](#)

cloud-based AP, [26–27](#)

split-MAC, [28–32](#), [36–37](#)

authentication, [43](#)

802.1x/EAP, [47–48](#)

AP (access point), [44](#)

client, [43–44](#)

EAP-FAST (EAP Flexible Authentication by Secure Tunneling), [48–49](#)

EAP-TLS (EAP Transport Layer Security), [50](#)

LEAP (Lightweight EAP), [48–49](#)

open, [46](#)

- PEAP (Protected EAP)*, [49](#)
- WEP (Wired Equivalent Privacy)*, [47](#)
- bands, [17](#)
- bidirectional communication, [7](#)
- BSS (basic service set), [8–9](#)
 - distribution system (DS)*, [10–12](#)
 - traffic flows*, [9](#)
- channel, [17–18](#)
- comparing with wired networks, [6–7](#)
- encryption, [45](#)
 - CCMP (Counter/CBC-MAC Protocol)*, [51](#)
 - GCMP (Galois/Counter Mode Protocol)*, [51](#)
- ESS (extended service set), [12–13](#)
- interference, [7](#)
- MIC (message integrity check), [45–46](#)
- RF signals, [7](#)
- secure connection, [42](#)
- security, WPA (Wi-Fi Protected Access), [51–53](#)
- self-healing, [32](#)
- SOHO (small office/home office), [407–408](#)
- WGB (workgroup bridge), [15–16](#)

WLAN

- configuration, [65–67](#)
 - advanced settings*, [85–86](#)
 - on AireOS WLC*, [79–83](#)
 - finalizing*, [86–87](#)
 - on IOS-XE WLC*, [67–79](#)
 - QoS*, [85](#)
- open authentication, [46](#)

WLC (wireless LAN controller), [29](#), [32](#), [667](#). *See also* **IOS-XE WLC**

- AireOS, [79](#)

- configuring the WLAN, 81–83*
- configuring WLAN security, 83–84*
- create a new WLAN, 80–81*
- creating a dynamic interface, 79–80*

CAPWAP (Control and Provisioning of Wireless Access Points), 29–31

centralized deployment, 32

cloud-based deployment, 32

configuration, 61–63

deployment models, 35

distributed deployment, 33–34

embedded wireless controller (EWC) deployment, 34

IOS-XE

- apply the policy tag to some APs, 78–79*

- configuring a policy profile, 74–77*

- mapping the WLAN and policy profiles to a policy tag, 77*

- WLAN configuration, 67–79*

physical ports, 63–65

virtual interface, 65

web-based GUI, 59–61

WLAN configuration, 65–67

- apply the policy tag to some APs, 78–79*

- map the WLAN and policy profiles to a policy tag, 77*

- policy profile, 74–77*

- profile, 69–74*

WMI (wireless management interface), 65

WMI (wireless management interface), 65

worm, 194–195, 667

WPA (Wi-Fi Protected Access), 51–52

- client authentication modes, 52

- personal mode, 52–53

versions, [52](#)

write community, [667](#)

WWW (World Wide Web), [98](#), [104](#)

X-Y-Z

X.509 certificate, [30](#)

XML (eXtensible Markup Language), [544–545](#), [667](#)

YAML, [545–546](#), [667](#)

zone

demilitarized, [214](#)

firewall, [213–214](#)

ZTP (zero touch provisioning), [462](#), [667](#)



Register your product at **ciscopress.com/register** to unlock additional benefits:

- Save 35%* on your next purchase with an exclusive discount code
- Find companion files, errata, and product updates if available
- Sign up to receive special offers on new editions and related titles

Get more when you shop at **ciscopress.com**:

- Everyday discounts on books, eBooks, video courses, and more
- Free U.S. shipping on all orders
- Multi-format eBooks to read on your preferred device
- Print and eBook Best Value Packs

*Discount code valid for 30 days; may not be combined with any other offer and is not redeemable for cash. Offer subject to change.

Cisco Press