Index

Note to the Reader: Throughout this index boldfaced page numbers indicate primary discussions of a topic. Italicized page numbers indicate illustrations.

A

AAA. See Authentication, Authorization, and Accounting (AAA)
aaa authentication login command, 385–386
aaa authentication login default local command, 700, 754
aaa authorization exec default local command, 754
aaa group server radius command, 385
aaa group server tacacs+ command, 386
aaa new-model command
    Ansible, 754
    NCM, 700
    RADIUS, 384
    TACACS+, 386
AAPs (Autonomous Access Points), 554, 597–598
ABRs (Area Border Routers), 166, 166
absorption in RF, 573–574, 574
abstraction, hardware, 667
access attacks, 365–366
access-class command, 302
access control, physical, 376–377, 376
access control lists (ACLs). See access lists
access layer in three-layer hierarchical model, 12–13
access links in VLANs, 225
access-list command, 295–296, 303
access-list deny command, 296–301, 304
access-list deny host command, 296
access-list deny tcp command, 304
access-list deny tcp any command, 304
access-list deny tcp any host command, 305–306
access-list permit command, 302
access-list permit any command, 299
access-list permit ip command, 307
access-list permit ip any command, 306
access-list remark command, 313
access lists, 290
    exam essentials, 316
    extended
        configuring, 519–521, 520
    examples, 307–310, 307, 309
overview, 303–307
    verifying, 521–522
introduction, 291–294
masquerade attacks, 371
monitoring, 313–315
named, 310–312
remarks, 312–313
review questions, 317–318
security issues mitigated by, 294–295
standard, 295–301, 299–301
summary, 316
Telnet, 302–303
wildcards with, 296–298
access points (APs)
    autonomous, 597–598
    endpoints, 497
wireless channels, 568–569, 568
WLCs
    configuring, 625–628, 626–628
    joining, 607–610, 608
    modes, 629–632, 630–633
    types, 610–611, 610
access ports in VLANs, 225–226, 225
Access switch in DTP, 540
accidental attacks, 369
ACI tool, 708
Acknowledgment number field in TCP segment, 44
ACLs. See access lists
Active Directory server role, 498
active gain in RF, 573
active mode in NBAR, 456
active routers in HSRP, 416–418, 417–418, 421
Active state in HSRP, 426
active timers in HSRP, 420
ActiveX controls, 374
AD (administrative distances)
    dynamic routing, 150–151
    static routing, 143
ad hoc networks, 556–557, 557
Address Resolution Protocol (ARP)
    IP routing process, 122–126, 130
    operation, 58–60, 59
addresses
  IP. See IP addresses
MAC. See MAC (Media Access Control)
adresses
addressing technique in QoS, 456
adjacencies in OSPF, 167
Adjacency Table in forwarding traffic flow, 705, 705
administrative distances (ADs)
dynamic routing, 150–151
static routing, 143
Advanced Research Projects Agency
  (ARPA), 31
advertising default routes, 157–158
AES-CCMP encryption, 583
agents in SNMP, 37, 349
Aggregation in collapsed core, 13
AHs (Authentication Headers) in IPsec,
  439–440, 439
alerts in network health, 692–693, 693
Allow AAA Override setting, 652
alternative ports in STP, 255
amplitude in RF, 571, 572
anonymous FTP, 35
anonymous user accounts, 387–388
Ansible, 750–751
  ad-hoc example, 756
  installation, 751–752, 752
  inventory, 753
  lab setup, 753–755, 754
  modules, 755–756
  playbook example, 756–763
  settings, 752
ansible-playbook cisco.yml command,
  761
Ansible Tower, 763
antennas
  free space path loss, 573
  RF, 569
  wireless, 556
anti-replay service in ESP, 440
any command, 299
anycasts in IPv6, 468–469, 472
APIC-EM, 708
APIPA (Automatic Private IP Addressing), 42
APIs (Application Programming Interfaces),
  679–683, 681–683
appliances in virtualization, 665
Application-layer attacks, 373
application signatures in QoS, 456
application-specific integrated circuits
  (ASICs), 5
APs. See access points (APs)
Area Border Routers (ABRs), 166, 166
areas in OSPF, 168, 172–175, 174
arp command, 108
ARPA (Advanced Research Projects
  Agency), 31
ARPA.net, 31
ASAv tool, 665
ASBRs (Autonomous System Boundary
  Routers), 166
ASICs (application-specific integrated
circuits), 5
ASs (autonomous systems) in IGRP, 150
assurance in DNA Center, 729–730, 730–731
asymmetric encryption in IPsec transforms,
  440–441
audit trails, 370
audits in security, 392–393
authentication
  ESP, 440
  external, 383–386, 383
  Kerberos, 399–400, 400
  local, 395
  methods, 381–382, 382
  multifactor, 397
PKI, 398–399, 398–399
  security server, 382–383
Windows, 382
  wireless networks, 581–582, 581–582
Authentication, Authorization, and
  Accounting (AAA)
  components, 380
  process, 383, 383
RADIUS, 639
  WLAN servers, 650–651, 650
Authentication Headers (AHs) in IPsec,
  439–440, 439
authentication server role in identity based
  networking, 380
authenticator role in identity based
  networking, 380
Authentico technology, 374
Auto switch in DTP, 540
autoconfiguration in IPv6
  stateful, 476–477, 476
  stateless, 474–476, 474
automatic account lockouts, 393–394
Automatic Private IP Addressing (APIPA), 42
Autonomous Access Points (AAPs), 554, 597–598
Autonomous System Boundary Routers (ASBRs), 166
autonomous systems (ASs) in IGRP, 150
auxiliary passwords, 405
AWX, 763

B
backups designated routers (BDRs) in OSPF, 167
backup ports in STP, 255
badge readers, 376–377
bandwidth
  multimedia applications, 223
  OSPF, 170
  RF, 571
  WANs, 17
baselines in SNMP, 37
basic service areas (BSAs), 557–558, 558
basic service set identifiers (BSSIDs), 559
basic service sets (BSSs), 557 558, 558
BDRs (backup designated routers) in OSPF, 167
Berkeley Software Distribution (BSD), 31
BGP (Border Gateway Protocol), 150
binary numbering system for IP addresses, 61
biometrics, 397 398
BIOS passwords, 391
BIP-GMAC-256 (Broadcast/Multicast Integrity Protocol Galois Message Authentication Code), 587
bit flipping in PSK, 584
bits in IP addresses, 60
blade servers, 497
block acknowledgments for wireless channels, 569
block sizes with wildcards, 297–298
blocked ports in STP, 255
bookshelves in Chef, 772
Bootstrap Protocol (BootP), 40–42, 41
Border Gateway Protocol (BGP), 150
BPDU (Bridge Protocol Data Unit) in STP, 254, 256
BPDU Guard, 276 277
bridge IDs in STP, 254, 267–273, 268
bridge mode for WLC access points, 632, 632
bridge port roles in STP, 254–255
Bridge Protocol Data Unit (BPDU) in STP, 254, 256
bridges
  STP, 253–254
  transparent, 6
  wireless networks, 562–564, 563–564
broadcast addresses
  description, 60, 67
  Layer 2, 68, 68
  Layer 3, 68–69, 69
broadcast domains
  description, 4–5
  flat networks, 221, 221
Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256), 587
broadcast SSIDs, 648
broadcast storms, loop avoidance for, 202, 203
broadcasts
  flat networks, 221
  IPv6, 468
  multimedia applications, 223
  OSPF networks, 168
  VLANs, 223
bronze queues, 651
brute-force attacks, 372
BSAs (basic service areas), 557–558, 558
BSD (Berkeley Software Distribution), 31
BSSIDs (basic service set identifiers), 559
BSSs (basic service sets), 557 558, 558
Buffer full/source quench message, 56
buffering
  congestion management, 458, 458
  IP routing process, 124
bytes in IP addresses, 60
cabling
Catalyst switches, 206
Ethernet, 19–24, 19–24
overview, 17–19
CAM (content addressable memory) table, 213
campus architecture in SDN, 711, 711
CAPWAP (Control And Provisioning of Wireless Access Point), 598–599
capwap ap controller ip address command, 607
CAs (certificate authorities), 396, 398
Catalyst switch configuration
overview, 204–206, 205
port security, 210–212
S1, 206–207
S2, 207–208
S3, 208–210
verifying, 212–214
CBAC (Context-Based Access Control), 369
CBWFQ (Class Based Weighted Fair Queuing), 459–460
CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), 583
CDP. See Cisco Discovery Protocol (CDP)
cdp enable command, 339
cdp holdtime command, 339
cdp run command, 339
cdp timer command, 339
CEF (Cisco Express Forwarding)
forwarding traffic flow, 705
router internal process, 127
central office (CO), 17
central syslog, 694–695, 694
certificate authorities (CAs), 396, 398
certificates, 396–397
Challenge Handshake Authentication Protocol (CHAP), 370
Chanalyzer tool, 631, 631
channel-group 1 mode command, 280–281
Channel Service Unit/Data Service Unit (CSU/DSU) devices, 16
channels in wireless networks, 565
2.4GHz band, 565–566, 566
2.4GHz/5GHz, 569
5GHz band, 566–567, 567
multiple APs, 568–569, 568
overlap techniques, 567
CHAP (Challenge Handshake Authentication Protocol), 370
character-mode access, 401
Chargen attacks, 369
Checksum field
TCP segment, 44
UDP segment, 46
chef generate cookbook command, 778
chef generate repo chef-repo command, 775
chef-server-ctl org-create command, 775
chef-server-ctl reconfigure command, 774
chef-server-ctl user-create command, 775
Chef tool, 772–774, 773
lab setup, 777–781, 777
server installation, 774–775
verifying results, 781, 781
workstation installation, 775–776
child bridges in wireless networks, 562
CIDR (Classless Inter-Domain Routing), 80 81
Cisco Discovery Protocol (CDP), 338
neighbor information, 340–343
timers and holdtime, 338–339, 339
topology documentation, 344–346, 344, 346
WLC, 634–636, 634–635
Cisco Dynamic Multipoint Virtual Private Network (DMVPN), 443
Cisco Express Forwarding (CEF)
forwarding traffic flow, 705
router internal process, 127
Cisco Firepower NGFW, 8–9, 8
Cisco HyperFlex, 666
Cisco Secure Services Client (CSSC), 599
Cisco Unified Wireless Networks (CUWN), 596–601, 597–598, 601
class A addresses, 64–65
Class B addresses
description, 65
subnetting, 93–101
Class Based Weighted Fair Queuing (CBWFQ), 459–460
Class C addresses
description, 65–66
subnetting, 82–93, 85–86, 88
Class D and E addresses, 63
Class of Service (CoS) in QoS, 455
class selectors in QoS, 456
classes
protocols, 152
Puppet, 771
QoS, 455–456
classful routing in RIP, 153–154
Classless Inter-Domain Routing (CIDR), 80–81
classless routing in RIP, 153
clear ip nat translation command, 329
clients
    identity based networking, 380
    redundancy, 412–414, 413–414
    WLANs, 653–655, 653–654
clock rate command, 138
clock synchronization in NTP, 347–348, 348
clones in virtualization, 667
CLOS architecture, 712, 712
cloud deployment model, 600–601, 601
Cloud Service Router 1000v (CSR1000v), 665
CO (central office), 17
Code bits field in TCP segment, 44
collapsed core topologies, 13, 13
collision domains
    flat networks, 221
    switches for, 3–5, 3
colons (:)
    JSON, 677
    Python, 673
Command Runner in DNA Center, 728–729, 729
commas (,)
    JSON, 677
    Python, 672–673
comments for access lists, 312–313
Common Spanning Tree (CST), 260–261, 260
compare configs feature, 700–701, 701
compatibility in VPNs, 436
complexity of passwords, 390
confidentiality in ESP, 440
config cdp enable command, 634
config interface address dynamic-interface command, 621
config interface address management command, 615
config interface address service-port command, 617
config interface address virtual command, 619
config interface create command, 620
config interface group create int-group command, 622
config interface group interface add wlan-int-group command, 623
config lag enable command, 625
config network secureweb command, 639
config network ssh command, 637
config network telnet command, 636
config network webmode command, 638
config radius acct add command, 643
config radius auth add command, 641
config route add command, 613
config serial baudrate command, 612
config tacacs auth add command, 643–645
config wlan broadcast-ssid command, 648
config wlan create command, 647
config wlan enable command, 648
config wlan interface command, 648
config wlan radius_server auth add command, 650–651
config wlan security command, 650
configuration
    Catalyst switches
        overview, 204–206, 205
        port security, 210–212
        S1, 206–207
        S2, 207–208
        S3, 208–210
        verifying, 212–214
    CDP, 634–636, 634–635
    extended access lists, 519–521, 520
    GRE tunnels, 443–445
    HSRP, 423–425, 423
    HTTP, 637–638, 638
    HTTPS, 638–639, 638
    IP routing, 132–133, 132
        Corp router, 133–135
        LA router, 139–141
        SF router, 135–138
    IPv6 protocol, 484, 484
        autoconfiguration, 474–477, 474, 476
        Corp, 485, 487–488
        DHCPv6 servers, 476–477
        ICMPv6 servers, 479–483, 479, 481–482
        LA, 486–488
        SF, 486
    NAT
        dynamic, 325–326
        overloading, 326–327
        static, 325
        verifying, 327
    OSPF, 175, 175
        areas, 172–175, 174
        Corp router, 175–176
        enabling, 171
        LA router, 177–179, 177
loopback interfaces, 180–182
SF router, 176–177
verifying, 182–188
port channels, 280–282
Python commands, 673–676
RADIUS, 384 385, 639 643, 640 642
RIP
Corp router, 153–154
LA router, 155–156
SF router, 154–155
SNMP, 351–352, 691–692
SSH, 637, 637
syslog, 354–356, 355
TACACS+, 385–386, 643–646,
643–646
telnet, 636, 636
tools. See Configuration Management
trunk ports, 236–240
VLANs
inter-VLAN routing, 240–246, 241–242,
244, 246
overview, 231–234
switch port assignments, 234–236
WLCs
access points, 625–628, 626–628
switches, 602–604, 602
Configuration Management, 744
Ansible. See Ansible
Chef, 772–781, 777, 781
DevOps, 748, 748
exam essentials, 782
IaC, 748–750
Puppet, 764–772, 766
review questions, 783 785
summary, 781
team silos, 744–747, 745–747
configured VLANs, 225
conflicts in DHCP, 42
congestion
avoidance tools, 460–461, 461
management tools, 457–460, 458–460
connectionless protocols, 45
connections
user account limits, 388
WLAN clients, 653–655, 653–654
connectivity for IP network. See IP network
connectivity
console passwords, 402–403
console ports
Catalyst switches, 205
WLCs, 611–612, 612
content addressable memory (CAM) table,
213
Context-Based Access Control (CBAC), 369
contract employees, 387
Control And Provisioning of Wireless Access
Point (CAPWAP), 598–599
control plane
description, 703
separating, 709–710, 709–710
core in fiber-optic cabling, 22–23, 22–23
core layer in three-layer hierarchical model,
11–12
Corp router configuration
DHCP, 140–141
IP routing, 133–135
IPv6, 485, 487 488
OSPF, 175–176
RIP, 153–154
routing tables, 129
static routing, 144–146
CoS (Class of Service) in QoS, 455
costs
OSPF, 170–171
STP, 254, 256–257
VPNs, 435
Counter Mode with Cipher Block Chaining
Message Authentication Code Protocol
(CCMP), 583
CPE (customer premises equipment), 16
CQ (Custom Queueing), 459
CRC (cyclic redundancy check)
IP header, 53
IP routing process, 123–126
ISLs, 228
crossover cable, 20–21, 20–21
CRUD verbs in REST API, 681
crypto key generate rsa command, 357
crypto key generate rsa general-keys
command, 724
crypto key generate rsa modulus command, 754
CSR1000v (Cloud Service Router 1000v), 665
CSSC (Cisco Secure Services Client), 599
CST (Common Spanning Tree), 260–261, 260
CSU/DSU (Channel Service Unit/Data Service Unit) devices, 16
curl command, 109
curly braces ({} in JSON, 677
Custom Queueing (CQ), 459
customer premises equipment (CPE), 16
CUWN (Cisco Unified Wireless Networks), 596–601, 597–598, 601
cyclic redundancy check (CRC)
  IP header, 53
  IP routing process, 123–126
  ISLs, 228

development
  diagnostics addresses, 158
  default-router command, 509
documentation
  administrative distances, 151
gateways, 124–125, 510–512
  RIP routes, 157–158
  routing, 147–148
  DELAY state in neighbor discovery, 528
  delays in QoS, 452
  DELETE verb in REST API, 681
demarcation points, 16
denial of service (DoS) attacks, 366, 368–370
deny tcp host command, 520
description command
  joining APs, 609–610
  WLC switches, 603–604
  Description field in syslog messages, 353
designated ports in STP, 254
designated routers (DRs) in OSPF, 167
desirable switch in DTP, 540
desktops
  access layer, 12
  endpoints, 496
  Destination Address field in IPv6 headers, 478
  destination addresses in IP routing process, 121–131
destination hosts, 124–125
  Destination IP address field in IP header, 53
  destination network parameter, 142
  Destination port field
    TCP segment, 44
    UDP segment, 46
  destination ports in TCP, 49–50
  Destination unreachable message in ICMP, 55
device provisioning protocol (DPP), 587
DevOps, 748, 748
DHCP. See Dynamic Host Configuration Protocol (DHCP)
DHCP Addr. Assignment setting in WLANs, 652
DHCP/HTTP Profiling setting in WLANs, 652
DHCPv6 server configuration, 476–477
diagnostic addresses, 107
differentiated services code point (DSCP), 455–456
diffraction in RF, 576–577, 577
digital certificates, 396–397
Digital Network Architecture (DNA) Center
  assurance, 729–730, 730–731
  Command Runner, 728–729, 729
  discovery, 719–721, 720
  EasyQoS, 732, 734, 733–734
  exam essentials, 737
  LAN Automation, 734–735, 735
  network hierarchy, 721–723, 721–722
  overview, 718–719, 719
  Path Trace, 731–732, 732
  REST API, 736, 736
  review questions, 738–741
  SDN, 708
  Software Defined Access, 735
  summary, 736–737

digital certificates
  in WLANs, 652
templates, 723–724, 724
topology, 724–725, 725
upgrades, 725–728, 726–727
Digital Signal 0 (DS0) connections, 17
Dijkstra algorithm, 164
directional antennas, 556, 573
Directory Access Protocol (DAP), 396
Disabled state in STP ports, 255
disabling
telnet, 636
user accounts, 387
discovery
CDP. See Cisco Discovery Protocol (CDP)
DNA Center, 719–721, 720
neighbors, 480–483, 481–482, 523–531, 524–525
distance-vector protocols, 152
distinguished names (DNs) in X.500 standard, 396
distributed vSwitches, 666
distribution layer in three-layer hierarchical model, 12
distribution systems (DSs)
access points, 554
infrastructure basic service sets, 559
WLC ports, 613–614, 613
DIX group, 17
DMVPNs (Dynamic Multipoint Virtual Private Networks), 443, 717
DNA Center. See Digital Network Architecture (DNA) Center
DNA scanners, 397
dnf install https command, 764
dnf localinstall command, 774
DNs (distinguished names) in X.500 standard, 396
DNS (Domain Name Service)
joining APs, 607–608, 608
overview, 39–40, 39
server role, 498
dns-server command, 609
documentation for topologies, 344–346, 344
DoD model, 31–33, 32–33
domain-name command, 609
Domain Name Service (DNS)
joining APs, 607–608, 608
overview, 39–40, 39
server role, 498
domains
broadcast, 4–5, 221, 221
collision, 3–5, 3, 221
QoS, 455
door locks, 377
DORA process in DHCP, 41
DoS (denial of service) attacks, 366, 368–370
dotted-decimal notation, 61
downfade in RF, 575
DPP (Device Provisioning Protocol), 5
Dragonblood exploit, 586
Dragonfly handshake, 586
dropped packets in QoS, 452
DRs (designated routers) in OSPF, 167
DSCP (Differentiated Services Code Point), 455–456
DSs (distribution systems)
access points, 554
infrastructure basic service sets, 559
WLC ports, 613–614, 613
DTP (Dynamic Trunk Protocol), 233, 238, 539–540
duplex settings, 513
duplicate address detection (DAD), 482, 482, 524
Dynamic ARP Inspection (DAI), 379
dynamic command, 237–238
Dynamic Host Configuration Protocol (DHCP)
access points
joining, 608 609
wireless, 554
Corp router configuration, 140–141
overview, 40–42, 41
server role, 498
snooping, 378–379, 379
virtual machine servers, 663
dynamic interface in WLCs, 614, 619–621, 620–621
dynamic IP routing, 150–152
Dynamic Multipoint Virtual Private Networks (DMVPNs), 443, 717
dynamic NAT, 322, 325–326
dynamic routing, 119
Dynamic Trunk Protocol (DTP), 233, 238, 539–540
E

E1 connections, 17
EasyQoS in DNA Center, 732–734, 733–734
eavesdropping, 366–368
ECDH (Elliptic Curve Diffie-Hellman) exchange, 587
ECDSA (Elliptic Curve Digital Signature Algorithm), 587
ECMP (Equal Cost Load Balancing), 714
EIGRP (Enhanced IGRP), 151
EIGRPv6 protocol, 483
Elliptic Curve Diffie-Hellman (ECDH) exchange, 587
Elliptic Curve Digital Signature Algorithm (ECDSA), 587
email
  e-mail bombs, 369
  server role, 498
enable command, 401
enable mode in DNA Center templates, 723
enable password command, 401
enable sec ncmEnable command, 700
enable secret password command, 401
Enable Session Timeout setting, 652
enabling
  OSPF, 171
  passwords, 401–402
Encapsulating Security Payload (ESP), 440
capsulation command, 240
capsulation for VLANs, 240–242
encryption
  ESP, 440
  IPsec transforms, 440–441, 441
  passwords, 405–406
PKI, 399, 399
  wireless networks, 581–582, 581–582
WPA3-Enterprise, 587
endpoints, 496–497
Enhanced IGRP (EIGRP), 151
enterprise-managed VPNs, 436–438, 436
entrances, 377
Equal Cost Load Balancing (ECMP), 714
erase start command, 135
erase startup-config command, 133
errors in QoS, 452
ESP (Encapsulating Security Payload), 440
ESSs (extended service sets), 560–561, 561
ESXi, 669
EtherChannel, 278–279, 279, 283
Ethernet cabling, 19, 19
crossover cable, 20–21, 20–21
fiber-optic, 22–23, 22–23
Power over Ethernet, 23–24, 24
straight-through cable, 20, 20–21
UTP gigabit wiring, 21–22, 22
EUI-64 addresses, 474–476, 474, 476
exec-timeout command, 403
exit interface parameter, 143
expiration of passwords, 390, 394–395
extended access lists
  configuring, 519–521, 520
description, 292
examples, 307, 310, 307, 309
overview, 303–307
verifying, 521–522
extended service sets (ESSs), 560–561, 561
exterior gateway protocol (EGP), 150
external authentication, 383–386, 383
external EIGRP, 151
external threats, 365
extranet VPNs, 436

F
fabric in SDN, 718
Facility field in syslog messages, 353
facts
  Ansible, 763
  Puppet, 771
fast switching in router internal process, 127
FastEthernet interface, 230
FCS (Frame Check Sequence)
  IP routing process, 123–125
  PSK, 584
  UDP segment, 46
FHRP (First Hop Redundancy Protocol), 414
  416, 415
FIB (Forwarding Information Base) table, 705
fiber-optic cabling, 22–23, 22–23
FIFO (First In First Out) queues in congestion management, 459
File Transfer Protocol (FTP), 35–36, 35
files
   server role, 498
   transferring, 35–36, 35–36
filters
   frame, 197
   switches, 195–196, 196
Firepower Threat Defense (FTD) devices, 10, 294, 364
Firepower Threat Defense Virtual, 665
firewalls, 6–10, 7, 290–291, 291
First Hop Redundancy Protocol (FHRP), 414–416, 415
First In First Out (FIFO) queues in congestion management, 459
5GHz band, 566–567, 567
Flags field
   IP header, 53
   TCP segment, 44
flat networks, structure of, 221, 221
FlexBridge mode in WLC access points, 632, 633
FlexConnect mode in WLC access points, 629
flexibility in VLANs, 224
floating static routes, 144
Flow Label field in IPv6 headers, 478
for loops in Python, 673–674
40Mhz channels, 569
forward/filter decisions, 197–199
forward/filter tables, 195–197, 197
Forwarding Information Base (FIB) table, 705
forwarding ports in STP, 254–255
forwarding traffic flow, 704 706, 704–706
FQDNs (fully qualified domain names), 40
fragile attacks, 372
Fragment offset field in IP header, 53
Frame Check Sequence (FCS)
   IP routing process, 123–125
   PSK, 584
   UDP segment, 46
frame filtering, 197–199, 197–198
frame protection in WPA3-Enterprise, 587
frame tagging in VLANs, 227–228
free space path loss in RF, 572–573, 573
frequencies, RF. See radio frequency (RF)
Fresnel zones, 579
FTD (Firepower Threat Defense) devices, 10, 294, 364
FTP (File Transfer Protocol), 35–36, 35
fully qualified domain names (FQDNs), 40
G
   gain in RF, 571, 573
   Galois/Counter Mode Protocol (GCMP-256), 587
   Gateway Load Balancing Protocol (GLBP), 416
gateways
   IP network connectivity, 510–512
   IP routing, 124–125
   of last resort, 147
   GCMP-256 (Galois/Counter Mode Protocol), 587
   Generic Routing Encapsulation (GRE), 438
   GET messages in SNMP, 349–350
   Get-NetIPAddress cmdlet, 303
   GET verb in REST API, 681
   GETBULK feature in SNMP, 37
   getpass command in Python, 671–674
   GLBP (Gateway Load Balancing Protocol), 416
   global NAT names, 322–323, 323–324
   global unicast addresses, 471, 471, 473
gold queues, 651
   gratuitous ARP in DHCP, 42
   GRE (Generic Routing Encapsulation), 438
   GRE tunnels
      configuration, 443–445
      GRE over IPsec, 442–443
      overview, 441–442, 442
      verifying, 445–447
   group roles in HSRP, 421–422, 422
   guards, 377
guests in virtualization, 665
guestshell command, 769
H
   hand scanners, 397
   hardware abstraction, 667
   hardware addresses in IP routing process, 122–126
   hardware health, 697, 697
   Hardware Virtualized Machines (HVMs), 668
   Hashed Message Authentication Mode (HMAC), 587
   Header checksum field in IP header, 53
   Header length field
      IP header, 53
      TCP segment, 44
   FQDNs (fully qualified domain names), 40
headers in IPv6 protocol, 477–479, 477
health
  hardware, 697, 697
networks, 692–693, 693
Hello protocol in OSPF, 167–169, 169
hello timers in HSRP, 419
hexadecimal numbering system for IP addresses, 61
hierarchical addressing, 61–64
histories, password, 394–395
HMAC (Hashed Message Authentication Mode), 587
hold timers in HSRP, 419
holdtime in CDP, 338–339, 339
Hop Limit field in IPv6 headers, 478
hops in distance-vector protocols, 151
Hops/time exceeded message in ICMP, 56
IP address, 61
Host-to-Host layer, 42
description, 32
key concepts, 46–47, 47
port numbers, 48–51
TCP, 43–45, 43
UDP, 45–46, 46
hostname command, 357
hostnames
  resolving, 39, 39
WLCs, 605
Hot Standby Router Protocol (HSRP), 416–418
configuration, 423–425, 423
group roles, 421–422, 422
interface tracking, 422, 422
load balancing, 427, 428
preemption, 425
states, 426
timers, 419–421, 420
troubleshooting, 428–429
verifying, 425–427
virtual MAC addresses, 418 419
HTTP (Hypertext Transfer Protocol) attacks, 374
overview, 37–38, 38
WLCs, 637–638, 638
HTTPS (Hypertext Transfer Protocol Secure) overview, 38
WLCs, 638–639, 638
hubs, 2–3, 3
HVMs (Hardware Virtualized Machines), 668
Hyper-V, 669
Hypertext Markup Language (HTML)
  attacks, 374
Hypertext Transfer Protocol (HTTP)
  overview, 37–38, 38
WLCs, 637 638, 638
Hyper Text Transfer Protocol Secure (HTTPS)
  overview, 38
WLCs, 638–639, 638
hypervisors
  server role, 498
  virtualization, 665, 668–669

IaC (Infrastructure as Code), 748–750
ICMP (Internet Control Message Protocol), 122–126, 129
  attacks, 369
  in IP routing process, 122–126, 129
  smurf attacks, 372
ICMPv6 protocol
  IP network connectivity, 523–531, 524–525
  server configuration, 479–483, 479, 481–482
Identification field in IP header, 53
identifying VLANs, 224–229, 225–226, 228
identity based networking, 379–380, 380
IDs for WLANs, 647
IEEE Ethernet standards, 17–19
  IEEE 802.1, 228–229, 228
  IEEE 802.1d, 259
  IEEE 802.1s, 260, 267
  IEEE 802.1w, 260
  IEEE 802.11i, 585
ifconfig command, 506, 506
IGP (interior gateway protocol), 150
implicit denies, 292, 306
import command in Python, 672
inbound access lists, 293
INICMP (incomplete) state in neighbor discovery, 528
independent basic service sets (IBSSs), 556–557, 557
Individualized Data Protection (IDP), 587
INFORM operation in SNMP, 350
Infrastructure as Code (IaC), 748–750
infrastructure basic service sets, 558–559
Initial state in HSRP, 426
Initialization vectors (IVs) in PSK, 584
input errors in IP network connectivity, 514
input queue drops, 513
inside global (IG) addresses in NAT, 330
inside NAT network names, 322–323, 323–324
Inter-Switch Link (ISL) routing, 228
inter-VLAN routing (IVR)
  configuring, 240–246, 241–242, 244, 246
description, 231, 231
exam essentials, 247
overview, 229–231, 230–231
review questions, 248–250
summary, 247
interactive commands for DNA Center templates, 723
interface configuration in SDN underlay, 714
Interface Groups
  WLANs, 648
  WLCs, 622–623, 622–623
interface information for networks,
695–697, 696
interface loopback command, 180, 715
interface port-channel command, 279, 281
interface range command, 234–236
interface tracking in HSRP, 422, 422
interface tunnel number command, 444
interface vlan command, 603
interior gateway protocol (IGP), 150
internal routers, 290–291, 291
internal threats, 365
Internet Control Message Protocol (ICMP),
122–126, 129
Internet layer, 51–52
  ARP, 58–60, 59
description, 32
  ICMP, 55 58, 56, 58
  IP, 52–55, 53–54
Internet of Things (IoT), 497
Internet Protocol (IP), 52–55, 53–54
Intrusion Prevention Systems (IPSs), 6–10, 8
inventory in Ansible, 763
IoT (Internet of Things), 497
IP (Internet Protocol), 52–55, 53–54
ip access-group out command, 299–300, 307, 312
ip access-list command, 311
ip access-list command, 311
ip access-list extended command, 315, 520–521
ip access-list standard command, 311
ip add command
  joining APs, 609
  SDN, 715
  WLC switches, 603
ip address command, 715
IP addresses, 60
  access lists. See access lists; extended access lists
  APIPA, 42
  DHCP, 40–42, 41
  FHRP, 415, 415
  hierarchical scheme, 61–64
    Class A, 64 65
    Class B, 65
    Class C, 65–66
  network addresses, 61–64, 62
  special purpose, 63–64
  IP routing process, 121–131
  IPv4, 67–70, 68–69
  IPv6. See IPv6 protocol
  Layer-3 EtherChannel, 283
  NAT. See Network Address Translation (NAT)
  private, 66–67
  spoofing, 371
  subnets. See subnets and subnetting switches, 206
terminology, 60
troubleshooting, 110–113
  exam essentials, 114
  Linux, 506–507, 506–507
  Mac OS, 504–506, 504–506
  OS parameters, 108–109
  overview, 106 108, 106
  problem determination, 109–113, 110–113
  review questions, 115–116
  summary, 114
  Windows 10, 498–504, 499–503
  WLCs, 605–606
  ip default-gateway command, 210
  ip dhcp excluded-address command, 609
  ip dhcp pool command, 609
ip domain-name command, 40, 357, 754
IP headers, 52–54, 53–54
ip nat inside source command, 325–326, 330–333
ip nat outside command, 326, 332
ip nat pool command, 325–326, 330–332
ip nat translation max-entries command, 329
ip nat translation timeout command, 330
IP network connectivity
  exam essentials, 545
  extended access lists, 519–522, 520
  IPv6 networks, 522–531, 523–525
  overview, 507–518, 508
  review questions, 546–548
  SPAN, 518–519, 518
  summary, 544–545
  VLANs, 531–544, 532
ip ospf cost command, 171
ip ospf mtu-ignore command, 714
ip ospf network point-to-point command, 715
IP phone endpoints, 497
ip route command, 142–143, 515
IP routing
  administrative distances, 150–151
  basics, 118–121, 120
  classes, 152
  configuration, 132–133, 132
    Corp router, 133–135
    LA router, 139–141
    RIP, 153–154
    SF router, 135–138
  default routing, 147–148
  DHCP, 140–141
  distance-vector, 152
  dynamic, 150–152
  exam essentials, 159–160
  examples, 127–132, 128, 130–131
  process, 121–127, 121, 123
  review questions, 161–162
  router internal process, 126–127
  SDN, 714
static, 142–143
  Corp router, 144–146, 144
  LA router, 146–147
  SF router, 145–146
  verifying, 148–150
  summary, 159
ip routing command, 714
IP services
  exam essentials, 358–359
  LLDP, 346–347
  NTP, 347, 348, 348
  review questions, 360–362
  SNMP, 348–352, 349–350
  SSH, 357–358
  summary, 358
  syslog, 352–356, 355
ip ssh version command, 357
ip subnet-zero command, 81–82
ipconfig command
  description, 109
  IP network connectivity, 509, 512
  neighbor discovery, 528
  Windows 10, 502–504, 502–503
IPsec
  GRE over IPsec, 442–443
  introduction, 438–439
  transforms, 439–441, 439, 441
IPSs (Intrusion Prevention Systems), 6–10, 8
IPv4 addresses, 67–68
  broadcasts, 68–69, 69
  multicast, 70, 70
  subnets. See subnets and subnetting
  unicast, 69, 69
ipv6 address command, 473–474
ipv6 enable command, 474
IPv6 protocol, 466
  addresses
    manual assignment, 472–473
    special, 472–473
    structure, 469, 469
    types, 470–472, 471
  benefits and uses, 467–469
  configuration, 484, 484
    autoconfiguration, 474–477, 474, 476
    Corp router, 485, 487–488
    DHCPv6 servers, 476–477
    ICMPv6 servers, 479–483, 479, 481–482
    LA router, 486, 486–488
  exam essentials, 490–491
  headers, 477–479, 477
  IP network connectivity, 522–531, 523–525
  need for, 467
  review questions, 492–493
  routing protocols, 483
ipv6 route command – Link Aggregation Group (LAG)

shortened expressions, 469–470
static routing, 483–484, 484
summary, 490
temporary addresses, 529
ipv6 route command, 487–488, 531
ipv6 route static command, 488
ipv6 unicast-routing command, 473, 485–486
IVR. See inter-VLAN routing (IVR)

J

Java blocking, 369
JavaScript Object Notation (JSON), 676–679
jitter in QoS, 452
joining access points, 607–610
JSON (JavaScript Object Notation), 676–679

K

Kerberos protocol, 399–400, 400
key command, 385–386
keys
  IPsec transforms, 441
  PSK, 584
knives in Chef, 772, 776
KVM hypervisor, 669

L

L2F (Layer 2 Forwarding), 438
L2TP (Layer 2 Tunneling Protocol), 438
LA router configuration
  IP routing, 139–141
  IPv6, 486–488
  OSPF, 177–179, 177
  RIP, 155–156
  static routing, 146–147
LACP (Link Aggregation Control Protocol), 279
LAG (Link Aggregation Group), 623–625, 624
LAN Automation, 734–735, 735
Land.c attacks, 369
LANs (local area networks)
  overview, 2, 3
  VLANs. See VLANs (virtual LANs)
vs. WANs, 15–16
wireless. See wireless networks
laptop endpoints, 496
last-resort parameter for passwords, 401
Layer 2 broadcasts, 67, 68
Layer 2 Forwarding (L2F), 438
Layer 2 MPLS VPNs, 437
Layer 2 security, 378–380, 378–380
Layer 2 switching
  address learning by, 195–197, 196
  Catalyst switches. See Catalyst switch configuration
  exam essentials, 215
  forward/filter decisions, 197–199, 197–198
  loop avoidance, 202–204, 203
  port security, 199–202, 199
  review questions, 216–218
  summary, 215
  switching services, 194–195
Layer 2 Tunneling Protocol (L2TP), 438
Layer 3 broadcasts, 68–69, 69
Layer 3 EtherChannel, 283
Layer 3 MPLS VPNs, 438
layered approaches in topologies, 13
LDAP (Lightweight Directory Access Protocol), 395–396
leaf-and-spine topology, 14–15, 14–15
leaf switches in SDN, 712
Learn state in HSRP, 426
Learning state in STP ports, 255
Length field in UDP segment, 46
length of passwords, 391–392
licensing in DNA Center, 720
Lightweight Access Point Protocol (LWAPP), 564
lightweight access points, 554
Lightweight Directory Access Protocol (LDAP), 395–396
lightweight WLAN deployment model, 598–599, 598
limits on connections, 388
line command, 401–402
line aux command, 405
line console command, 402–403
line of sight in RF, 578–579, 579
line vty command, 337, 404
Link Aggregation Control Protocol (LACP), 279
Link Aggregation Group (LAG), 623–625, 624
link costs in STP, 256–257
Link layer, 32
Link Layer Discovery Protocol (LLDP), 346–347
link-local addresses, 471, 471, 474
Link State Advertisements (LSAs)
  forwarding traffic flow, 704
  OSPF, 167–168
Link State Database (LSDB), 704, 704
link-state protocols, 152
Link State Updates (LSUs) in OSPF, 169–170
links in OSPF, 167
Linux, IP address troubleshooting in, 506–507, 506–507
Listen state in HSRP, 426
Listening state in STP ports, 255
LLDP (Link Layer Discovery Protocol), 346–347
LLDP-MED (Media Endpoint Discovery), 346
lldp receive command, 346–347
lldp run command, 346
lldp transmit command, 346–347
LLQ (Low Latency Queuing), 459, 460
load balancing in HSRP, 427, 428
local area networks (LANs)
  overview, 2, 3
  VLANs. See VLANs (virtual LANs)
  vs. WANs, 15–16
  wireless. See wireless networks
local authentication, 395
local loops, 17
local mode for WLC access points, 629
local NAT names, 322–323, 323–324
Lock and Key, 370
lockouts for user accounts, 393–394
locks, door, 377
log command, 306
logging command, 354–355
logging bufferd command, 354
logging console command, 354
logging host command, 356, 695
logging informational command, 355
logging trap command, 356
logging trap debugging command, 695
logging trap informational command, 356
logical addresses, 52
login command, 402
login local command, 357
logs for real-time alerts, 370
loopback addresses
  description, 67
  IP network connectivity, 510
  IP troubleshooting, 107
loopback interfaces in OSPF, 179–182, 179 loops
  avoiding, 195, 202–204, 203
  Python language, 673–674
Low Latency Queuing (LLQ), 459, 460
LSA flooding, 169–170
LSAs (Link State Advertisements)
  forwarding traffic flow, 704
  OSPF, 167–168
LSDB (Link State Database), 704, 704
LSUs (Link State Updates) in OSPF, 169–170
LWAPP (Lightweight Access Point Protocol), 564

M

mac address-table command, 214
MAC forward/filter tables, 195–199, 196
MAC (Media Access Control) addresses
  Catalyst switches, 213–214
  FHRP, 415
  HSRP, 418–419
  IP routing process, 130–131, 130
  IPv6 autoconfiguration, 474–475
  learning by layer 2 switching, 195–197, 196
  neighbor discovery, 480, 524
  port security, 210–211
  Proxy ARP, 412–413
  RSTP, 264, 266
  SPAN, 518
  STP, 257, 259
  STP failure consequences, 273–274
  wireless channels, 569
MAC OS, IP address troubleshooting in, 504–506, 504–506
maintenance accounts, renaming, 388–389
malware, 375
man-in-the-middle attacks, 373
Management Information Base (MIB) in SNMP, 350, 350
management interface in WLCs, 614–615, 616
management plane, 702–703, 703
manifests in Puppet, 769–771
mantraps, 376, 376
manual assignment of IPv6 addresses, 472–473
many-to-many NAT, 322
marking in QoS, 455  456
mask parameter for static routing, 142
masks
   access lists, 296–298
   OSPF, 172
   subnets, 78–79
masquerade attacks, 371
Maximum Transmission Units (MTUs)
   ICMPv6 servers, 479–480
   SDN underlay, 714
MBSSIDs (multiple basic service set
   identifiers), 559, 560
Media Access Control addresses. See MAC
   (Media Access Control) addresses
Media Endpoint Discovery, 346
Meraki networks, 600–601, 601
mesh networks, 564, 565
message integrity code (MIC)
   PSK, 584
   WPA2 Enterprise, 585
messages, syslog, 352–355, 355
MIB (Management Information Base)
   in SNMP, 350, 350
MIC (message integrity code)
   PSK, 584
   WPA2 Enterprise, 585
migrations in virtualization, 667–668
Mills, David, 38
MILNET, 31
MIMO (Multiple-Input Multiple-Output), 569
minimum length of passwords, 391–392
MNEMONIC field in syslog messages, 353
mobile phone endpoints, 497
Mobility Express controllers, 599
Mobility/RF Group Name feature in WLCs, 606
modules
   Ansible, 755–756, 763
   Puppet, 771
monitor mode for WLC access points, 629
monitor session dest interface command, 519
monitor session source interface command, 519
MSTP (Multiple Spanning Tree Protocol), 267
MTUs (Maximum Transmission Units)
   ICMPv6 servers, 479–480
   SDN underlay, 714
multi-access networks, 168
multicasts
   addresses, 70, 70
   IPv6, 468, 472
   multimedia applications, 223
   neighbor discovery, 482
multifactor authentication, 397
multimedia applications, 223
multimode fiber-optic cabling, 23, 23
multipath in RF, 575–576, 575
multiple APs in wireless channels, 568–569, 568
multiple basic service set identifiers
   (MBSSIDs), 559, 560
Multiple-Input Multiple-Output (MIMO), 569
Multiple Spanning Tree Protocol (MSTP), 267

N
NA (neighbor advertisement), 481, 482, 524–525, 525
name command, 602–603
named access lists, 292, 310–312
names
   maintenance accounts, 388–389
   NAT, 322–323
NAT. See Network Address Translation
   (NAT)
native VLANs
   frame tagging, 227–229
   modifying, 239–240
NBI (Northbound Interface), 707
NBMA (non-broadcast multi-access)
   network, 168
neighbor advertisement (NA), 481, 482, 524–525, 525
Neighbor Discovery Protocol (NDP), 480–483, 481–482, 523–531, 524–525
neighbor solicitation (NS), 481, 482, 524–525, 525
neighbors
   CDP, 340–343
   forwarding traffic flow, 704, 704
   IPv6 protocol, 480–483, 481–482, 523–531, 524–525
   OSPF, 167
Network Control Protocol (NCP), 30–31
network fundamentals
components, 2–6, 3–4, 6
Ethernet cabling, 19–24, 19–24
exam essentials, 24–25
firewalls and IPS, 6–10, 7–9
physical interfaces and cables, 17–19
review questions, 26–27
summary, 24
topologies, 10
collapsed core, 13, 13
spine-leaf, 14–15, 14–15
three-layer hierarchical model,
10–13, 11
WANs, 15–17
network interface cards (NICs), 555, 555

network management stations (NMSs) in
SNMP, 349
Network Monitoring Systems (NMSs),
690–691
central syslog, 694, 695, 694
hardware health, 697, 697
interface information, 695–697, 696
network health, 692–693, 692–693
network information, 697–699, 698–699
SNMP
configuration, 691–692
traps, 695, 695
Network Time Protocol (NTP), 38, 39,
347–348, 348
networks
attacks
Application-layer, 373
DoS, 368–370
eavesdropping, 366–368
HTML, 374
man-in-the-middle, 373
masquerade, 371
passwords, 372–373
primary, 365–366
repudiation, 371–372
rerouting, 371
session hijacking, 371
smurfing, 372
Trojan horse, 373–374
unauthorized access, 370
viruses, 373–374
WareZ, 370
worms, 373–374
DNA Center hierarchy, 721–723,
721–722
fundamentals. See network fundamentals
health, 692–693
information, 697–699, 698–699
security threats, 365
virtual. See VLANs (virtual LANs)
wireless. See wireless networks
WLCs. See wireless LAN controllers
(WLCs)
Next Generations Firewalls (NGFWs),
6–10, 7
Next Header field in IPv6 headers, 478
next hop address parameter, 142
no cdp enable command, 339
no cdp run command, 339
no ip route command, 515
no lldp run command, 346
no logging buffered command, 355
no logging console command, 355
no login command, 404
no service password-encryption command, 406
no service timestamps command, 356
no shutdown command, 212, 245
no switchport command, 715
node addresses in IP addresses, 61
nodes in Chef, 772
non-broadcast multi-access (NBMA) networks, 168
non-designated ports in STP, 254
non-repudiation, 372
non-root bridges in STP, 254
nonegotiate command, 238
Nonegotiate switch in DTP, 540
nonroot bridges, 562–564, 564
Northbound Interface (NBI), 707
NS (neighbor solicitation), 481, 482, 524–525, 525
tmp master command, 348
tmp server command, 347
nulling signals in RF, 576

OpenDaylight protocol, 708, 709
OpenFlow protocol, 708
operating systems (OSs), IP parameters for, 108–109
OpFlex protocol, 708
Opportunistic Wireless Encryption (OWE), 587
optical fiber converters, 17
Options field
IP header, 53
TCP segment, 44
Organizational IDs (OIDs) in SNMP, 350, 350
OSPF (Open Shortest Path First) protocol basics, 164–165
configuration, 175, 175
areas, 172–175, 174
Corp router, 175–176
LA router, 177–179, 177
SDN, 715
SF router, 176–177
verifying, 182–188
default ADs, 151
enabling, 171
cncsentials, 188
features, 164
loopback interfaces, 179–182, 179
LSA flooding, 169–170
overview, 166
review questions, 189–191
vs. RIP, 165
SPF tree calculation, 170–171
summary, 188
terminology, 166–169
wildcards, 173–175
OSs (operating systems), IP parameters for, 108–109
OTPs (one-time passwords), 381
out-of-order delivery in QoS, 453
outbound access lists, 293
output errors in IP network connectivity, 514
output queue drops, 513
outside NAT names, 322–323, 325
overlap channel techniques, 567
overlay in SDN, 716–717, 717
overload command, 326
overloading NAT, 322, 324, 324, 326–327
OWE (Opportunistic Wireless Encryption), 587

OC-3 connections, 17
OC-12 connections, 17
OC-48 connections, 17
octets in IP addresses, 60
OIDs (Organizational IDs) in SNMP, 350, 350
omni-directional antennas
description, 556
free space path loss, 573
one-time passwords (OTPs), 381
one-to-many NAT, 322
one-to-one NAT, 322
onePK protocol, 708
100Base-FX Ethernet, 18
100Base-TX Ethernet, 18
1000Base-CX Ethernet, 18
1000Base-LX Ethernet, 19
1000Base-SX Ethernet, 19
1000Base-T Ethernet, 18, 21–22, 22
1000Base-ZX Ethernet, 19
Open Shortest Path First protocol. See OSPF (Open Shortest Path First) protocol
Packet description Language Models (PDLMs), 456
packet fragmentation and reassembly, 369
packet sniffers, 366–367
PAgP (Port Aggregation Protocol), 279
Pairwise Master Key (PMK), 585
Pairwise Transient Keys (PTKs)
  PSK, 584
  WPA2 Enterprise, 585
parameters for operating systems, 108–109
paravirtualization, 668
parent bridges, 562
passive gain in RF, 573
passive-interface command, 157
passive mode in NBAR, 456
password aux command, 405
password console command, 402
password telnet command, 404
passwords
  attacks, 372–373
  authentication, 381
  auxiliary, 405
  BIOS and UEFI, 391
  complexity, 390
  console, 402–403
  enabling, 401–402
  encrypting, 405–406
  expiration, 390, 394–395
  histories, 394–395
  length, 391–392
  management features, 393–395
  requiring, 391
  screensavers, 390
  setting, 400–401
  single sign-on, 395
  special characters, 393
  strong, 389–390
  Telnet, 403–404
  WLCs, 605
PAT (Port Address Translation)
  configuration, 326–327
  description, 322
  overloading, 324–325, 324–325
  PATCH verb in REST API, 681
path costs in STP, 254
Path Trace in DNA Center, 731–732, 732
Payload Length field in IPv6 headers, 478
PCP (Priority Code Point), 455
PDLMs (Packet description Language Models), 456
Per-VLAN Spanning Tree+, 260–261, 261–262
perimeters, 290–291, 291, 377
permanent parameter, 143
PEs (Provider Edge routers), 437
pharming, 375
phishing, 375
physical access control, 376–377, 376
physical interfaces, 17–19
ping command
  ICMP, 56–57
  IP addresses, 107–108
  IP network connectivity, 510–516
  neighbor discovery, 525–526, 531
  static routing, 148–150
  VLANs, 536, 544
Ping of Death attacks, 369
pip command, 671
PKI (Public Key Infrastructure), 398–399, 398–399
platinum queues, 651
playbooks in Ansible, 763
plays in Ansible, 763
Plug and Play (PNP) in LAN Automation, 734–735
PMFs (Protected Management Frames), 586
PMK (Pairwise Master Key), 585
PNP (Plug and Play) in LAN Automation, 734–735
PoE (Power over Ethernet) light, 205
  overview, 23–24, 24
point-to-multipoint connections in OSPF, 168–169
point-to-point connections in OSPF, 168
Point-to-Point Tunneling Protocol (PPTP), 438
points of presence (POPs), 17
policers in QoS, 457, 457
policing in QoS, 456–457, 457
policy mapping settings, 651
POPs (points of presence), 17
Port Address Translation (PAT)
  configuration, 326–327
  description, 322
  overloading, 324–325, 324–325
Port Aggregation Protocol (PAgP), 279
port channels
   EtherChannel, 279
      verifying, 280–282, 280
Port Number field in RADIUS, 640
port-security command, 200–201
port VLAN IDs (PVIDs), 227
PortFast standard, 275–276, 275
ports and port numbers
   Catalyst switches, 205–206, 210–212
   EtherChannel, 278–279, 279
   Host-to-Host layer, 48–51
   Layer 2 security, 378
   root bridges, 253–255
   security for, 199–202, 199, 201, 210–212
   STP
      bridges, 254–255
      costs, 254
      states, 255–256
   VLANs, 225 226, 225, 234–236
   WLCs, 605, 611–614, 612–613
POST verb in REST API, 681
Postman program, 682
Power over Ethernet (PoE)
   light, 205
   overview, 23–24, 24
   powers of two, 79
PPTP (Point-to-Point Tunneling Protocol), 438
PQ (Priority Queuing), 459
pre-shared key (PSK)
   WLANs, 649, 649
   WPA and WPA2, 583–584
   WPA3, 586
preemption in HSRP, 425
prefix-length command, 331
prefix routing, 153
Priority Code Point (PCP), 455
Priority Queuing (PQ), 459
private IP addresses, 66–67
private keys in IPsec transforms, 441
PROBE state in IPsec transforms, 528
Process/Application layer, 33
   APIPA, 42
   BOOTP, 40–42, 41
   description, 32
   DHCP, 40–42, 41
   DNS, 39 40, 39
   FTP, 35–36, 35
   HTTP, 37–38, 38
   HTTPS, 38
   NTP, 38, 39
   SNMP, 37, 37
   SSH, 34–35, 35
   Telnet, 34, 34
   TFTP, 36, 36
process switching in router internal
   process, 127
profile names in WLANs, 647
propagations in RIP, 156–157
protect violation mode for port security, 200
Protected Management Frames (PMFs), 586
Protocol field in IP header, 53–55, 54
Provider Edge routers (PEs), 437
provider-managed VPNs, 436–438
Proxy Address Resolution Protocol (Proxy
   ARP), 412–414, 413–414
PSK (pre-shared key)
   WLANs, 649, 649
   WPA and WPA2, 583–584
   WPA3, 586
PTKs (Pairwise Transient Keys)
   PSK, 584
   WPA2 Enterprise, 585
Public Key Infrastructure (PKI), 398–399,
   398–399
public keys in IPsec transforms, 441
Puppet, 764
   agent installation, 769–770
   DC manifest file, 768–769
   installation, 764–765
   lab setup, 765–766, 766
   Puppet Enterprise, 771–772
   site manifest file, 766 767
   verifying results, 770–771
PUT verb in REST API, 681
PVIDs (port VLAN IDs), 227
PVST+ standard, 260
Quality of Service (QoS)
   classification and marking, 455–456
   congestion avoidance tools, 460–461, 461
   congestion management tools, 457–460,
      458–460
DNA Center, 732–734, 733–734
exam essentials, 461
   overview, 452–453
policing, shaping, and re-marking, 456–457, 457
review questions, 462–463
summary, 461
traffic characteristics, 453, 454, 453
trust boundaries, 454–455, 454
WLANs, 651, 651
queues
congestion management, 458–460, 458–459
IP network connectivity, 513
WLANs, 651

R
R1 router configuration, 514–515
R2 router configuration, 515–516
RA (router advertisement) requests
DHCPv6 servers, 477
ICMPv6 servers, 480–481, 481
IPv6 autoconfiguration, 475
neighbor discovery, 524–525, 524
rack-mounted servers, 497
Radio Frequency Identification (RFID), 376–377
radio frequency (RF)
absorption, 574
diffraction, 576–577, 577
free space path loss, 572–573, 573
multipath, 575–576, 575
operational requirements, 578
Fresnel zones, 579
line of sight, 578, 579, 579
RSSI and SNR, 580, 580
reflection, 574–575, 574
refraction, 576, 576
scattering, 577–578, 577
wireless networks, 569–572, 570–572
RADIUS. See Remote Authentication Dial-In User Service (RADIUS)
radius server command, 385
range command, 234–236
RAP (Root Access Point) in WLC access points, 632
Rapid PVST+ standard, 260
Rapid Spanning Tree Protocol (RSTP), 262–267, 264–267
RDNs (relative distinguished names) in X.500 standard, 396
re-marking in QoS, 456–457, 457
REACH (reachable) state in neighbor discovery, 528
read operations in SNMP, 352
real-time alerts logs, 370
received signal strength indicator (RSSI), 580, 580
receiver sensitivity, 573
recipes in Chef, 772
reconnaissance attacks, 365
Redhat Linux, IP address troubleshooting in, 506–507, 506–507
redistribution, 157
redundancy
clients, 412–414, 413–414
exam essentials, 429
FHRP, 414–416, 415
HSRP. See Hot Standby Router Protocol
(review questions, 430–431
summary, 429
WLCs, 613–614, 617–618, 618
reflection in RF, 574–575, 574
refraction in RF, 576, 576
registered jack (RJ) connectors, 18
relative distinguished names (RDNs) in X.500 standard, 396
remark command, 313
remarks in access lists, 312–313
remote access VPNs, 436
Remote Authentication Dial-In User Service
(RADIUS)
configuration, 384–385
process, 384
server role, 498
WLANs, 650–651, 650
WLCs, 639–643, 640–642
renaming maintenance accounts, 388–389
repeaters, 561, 562
replay attacks, 371
Representational State Transfer (REST) API
DNA Center, 736, 736
overview, 679–683, 681–683
repudiation attacks, 371–372
request timed out message, 125
rerouting attacks, 371
reserved IP addresses, 63–64, 472–473
resolving hostnames, 39, 39
resources in Puppet, 771
REST (Representational State Transfer) API
DNA Center, 736, 736
overview, 679–683, 681–683
restrict violation mode for port security, 200
retinal scanners, 397
RF. See radio frequency (RF)
RFID (Radio Frequency Identification), 376–377
RIDs (router IDs) in OSPF, 167, 179–182, 179
RIP (Routing Information Protocol), 152–153
configuration
Corp router, 153–154
LA router, 155–156
SF router, 154–155
default ADs, 151
default routes, 157–158
vs. OSPF, 165
propagations, 156–157
RIPng protocol, 483
RJ (registered jack) connectors, 18
ROAS (router on a stick)
HSRP, 427
VLANs, 230, 230
rogue detector mode for WLC access points, 630
roles in Ansible, 763
Root Access Point (RAP) in WLC access points, 632
root bridges
STP, 253, 257–262, 258–262
wireless networks, 562–564, 564
root ports in STP, 254
round-robin scheduling, 458
route print command, 509
route tables, 509
router advertisement (RA) requests
DHCPv6 servers, 477
ICMPv6 servers, 480–481, 481
IPv6 autoconfiguration, 475
neighbor discovery, 524–525, 524
router IDs (RIDs) in OSPF, 167, 179–182, 179
router on a stick (ROAS)
HSRP, 427
VLANs, 230, 230
router ospf command, 171–173, 715
router rip command, 153–154
router solicitation (RS) requests
DHCPv6 servers, 477
ICMPv6 servers, 480–481, 481
IPv6 autoconfiguration, 475
neighbor discovery, 524–525, 524
roUTERS
internal, 290–291, 291
internal process, 126–127
overview, 3–6, 4
routing. See inter-VLAN routing (IVR); IP routing
Routing Information Protocol. See RIP
(Routing Information Protocol)
RS (router solicitation) requests
DHCPv6 servers, 477
ICMPv6 servers, 480–481, 481
IPv6 autoconfiguration, 475
neighbor discovery, 524–525, 524
RSA token cards, 382, 382
RSSI (received signal strength indicator), 580, 580
RSTP (Rapid Spanning Tree Protocol), 262–267, 264–267
running-config file, 314

S
S1 Catalyst switch configuration, 206–207
S2 Catalyst switch configuration, 207–208
S3 Catalyst switch configuration, 208–210
SAE (Simultaneous Authentication of Equals), 586
SBI (Southbound Interface), 708
scalability
VLANs, 224
VPNs, 436
scattering in RF, 577–578, 577
SCCM (System Center Configuration Manager), 663
schedules for congestion management, 458
screensaver passwords, 390
scripts in Python, 670–676
SD-Access, 735
SD-WAN, 708
SDN controllers. See Software Defined Networking (SDN) controllers
SE-Connect mode for WLC access points, 630, 631
secret parameter for passwords, 401
Secure Hypertext Transfer Protocol (SHTPP), 38
Secure Shell (SSH) protocol

overview, 34–35, 35, 357–358
WLCs, 637, 637
Secure-shutdown command, 211–212
Secure Sockets Layer (SSL), 435
security, 364
access lists. See access lists
audits, 392–393
authentication, 381–386, 382–383,
398–400, 398–400
biometrics, 397–398
Catalyst switch configuration, 210–212
certificates, 396–397
eam essentials, 407
Layer 2, 378–380, 378–380
LDAP, 395–396
malware, 375
multifactor authentication, 397
network attacks. See networks
passwords. See passwords
physical access control, 376–377, 376
port, 199–202, 199, 201
REST API, 683
review questions, 408–410
summary, 407
training, 375
user accounts, 386–389
user awareness, 374–375
VLANs, 223–224
VPNs. See virtual private networks
(VPNs)
wireless networks
authentication and encryption, 581 582,
581–582
comparisons, 588
settings, 648–651, 649–650
WEP, 582–583
WPA and WPA2, 583–585
Security Accounts Manager (SAM), 395
security protocols in IPsec transforms,
439–440, 439
security server authentication, 382–383
segment format
TCP, 43–45, 43
UDP, 46, 46
sensitivity of receivers, 573
sensor mode for WLC access points, 632
seq no field in syslog messages, 353
Sequence Number field
ESP, 440
TCP segment, 44
Server Address field in RADIUS, 639
Server Index field in RADIUS, 639
server name command, 385
servers
Chef, 772, 774–775
forms, 497
roles, 498
virtual machines, 663–664, 663–664
service password-encryption command, 406
service ports in WLCs, 605, 612–617, 612,
617
service sequence-numbers command, 356
service set identifiers (SSIDs)
overview, 559–560, 560
WLANs, 647–648
WLCs, 606, 611
service timestamps log datetime msec
command, 347
services in Puppet, 771
session hijacking, 371
SET messages in SNMP, 349–350
Severity field in syslog messages, 353
severity levels in syslog, 353
SF router configuration
IP routing, 135–138
IPv6, 486
OSPF, 176–177
RIP, 154–155
static routing, 145–146
shapers in QoS, 457, 457
shaping in QoS, 456–457, 457
Shared Secret field in RADIUS, 639
Shared Secret Format field in RADIUS, 639
shortened expressions in IPv6, 469–470
Shortest Path First (SPF) algorithm, 152,
170–171
show access-list command, 314–315,
520–522
show access-lists command, 516
show cdp command, 339
show cdp neighbors command, 269,
340–341, 345, 635
show cdp neighbors detail command, 341,
346, 635
show client detail command, 654–655
show controllers command, 138
show dtp interface command, 537, 539–541
show etherchannel port-channel command, 281
show etherchannel summary command, 282
show interface command, 212
show interface summary command, 615
show interface trunk command, 237–238
show interface tunnel command, 446
show interfaces command
  GRE tunnels, 446
  IP network connectivity, 512
show interfaces switchport command, 234, 532, 534, 537, 539–540, 543
show interfaces trunk command, 537, 539, 541, 543
show ip access-list command, 314
show ip arp command, 108, 124
show ip dhcp binding command, 149
show ip dhcp pool command, 149
show ip interface command, 314–315, 522
show ip interface brief command
  Catalyst switches, 212
  GRE tunnels, 445–446
  IP network connectivity, 514
  Puppet results, 770
show ip nat statistics command, 329
show ip nat translations command, 327–328
show ip ospf command, 180–181, 183–184
show ip ospf database command, 184–185
show ip ospf interface command, 185–186
show ip ospf neighbor command, 186–187, 716
show ip protocols command, 187–188
show ip route command
  Corp router, 129
  IP network connectivity, 514–515
  IP routing, 120–121
  OSPF, 182–183
  routing tables, 134–135, 137–138
  static routes, 145–147
show ip route ospf command, 716
show ipv6 interface brief command, 488–489, 527
show ipv6 neighbors command, 528
show ipv6 route command, 485–487, 530
show logging command, 355
show mac address-table command, 198, 213–214, 532–535
show monitor command, 519
show ntp command, 348
show ntp associations command, 348
show ntp status command, 348
show port-security command, 211
show port summary command, 211
show running-config command
  Catalyst switches, 212
  CDP, 344–345, 346
  IP access lists, 314
  passwords, 405
  VLANs, 239
show spanning-tree command, 268–271
show spanning-tree summary command, 271–272
show spanning-tree vlan command, 268, 270–271
show standby command, 425
show standby brief command, 425–426
show vlan command, 233, 235, 532–534, 537
show vlan brief command, 532, 535, 538
SHTPP (Secure Hypertext Transfer Protocol), 38
shutdown command, 212
shutdown mode in port security, 200
signal-to-noise ratio (SNR) in RF, 580, 580
signatures in QoS, 456
silos, 744–747, 745–747
silver queues, 651
Simple Network Management Protocol (SNMP), 348–349, 349
  configuration, 351–352, 691–692
  MIB, 350, 350
  overview, 37, 37
  traps, 695, 695
Simultaneous Authentication of Equals (SAE), 586
single-mode fiber-optic cabling, 23, 23
single sign-on (SSO), 395
site manifest file in Puppet, 766–767
site-to-site VPNs, 436
slash notation (/) for subnets, 80–81
Small Office Home Office Network (SOHO), 2–3, 3
smart cards, 377
smurf attacks, 372
snapshots in virtualization, 667
sniffer mode for WLC access points, 629, 630
SNMP. See Simple Network Management Protocol (SNMP)
snmp-server community command, 351, 691
snmp-server contact command, 351
snmp-server enable traps command, 691–692
snmp-server host command, 691
snmp-server location command, 351
snmp-server source-interface traps command, 691
snooping in DHCP, 378–379, 379
SNR (signal-to-noise ratio) in RF, 580, 580
soft tokens in authentication, 381
software addresses, 52
Software Defined Access, 735
Software Defined Networking (SDN) controllers, 690
components, 712–713
fabric, 718
overlay, 716–717, 717
underlay, 713–716, 713
control plane, 709, 710, 709–710
controller-based architectures, 710–712, 711–712
DNA Center. See Digital Network Architecture (DNA) Center
exam essentials, 737
introduction, 706–707, 707
NBI, 707
NCMs, 699–702, 700–701
NMS monitoring, 690–699, 692–699
review questions, 738–741
SBI, 708
solutions, 708, 709
summary, 736–737
traditional networking, 702–706, 703–706
SOHO (Small Office Home Office Network), 2–3, 3
solicited-node address in neighbor discovery, 481–482
Source Address field in IPv6 headers, 478
Source IP address field in IP header, 53
Source port field
TCP segment, 44
UDP segment, 46
Southbound Interface (SBI), 708
SPAN feature, 518–519, 518
spanning portfast trunk command
joining APs, 610
WLCs, 625
spanning-tree mode rapid-pvst command, 272
spanning-tree portfast command, 276, 609
spanning-tree portfast bpduguard default command, 277
spanning-tree portfast trunk command, 604
Spanning Tree Protocol (STP), 252–253, 253
BPDU Guard, 276–277
bridge IDs, 267–273, 268
bridge port roles, 254–255
convergence, 256
exam essentials, 284
failure consequences, 273–275, 273–274
link costs, 256–257
operations, 257–259, 257–259
port states, 255–256
PortFast, 275–276, 275
review questions, 285–287
root bridges, 257, 259, 258–259
summary, 284
terms, 253–254
types, 259–260
CST, 260–261, 260
MSTP, 267
PVST+, 260–261, 261–262
RSTP, 262, 267, 264–267
spanning-tree vlan command, 270–271
spatial multiplexing, 569
Speak state in HSRP, 426
spear phishing, 375
special characters in passwords, 393
special purpose IP addresses, 63–64, 472, 473
Spectrum Expert tool, 630, 631
speed settings in IP network connectivity, 513
SPF (Shortest Path First) algorithm, 152, 170–171
spine/leaf architecture
overview, 14, 15, 14, 15
SDN, 712, 712
split MAC WLAN deployment model, 599–600
spoofing IP addresses, 371
Sputnik launch, 31
spyware, 375
square brackets ([]) in JSON, 677
SSH (Secure Shell) protocol
overview, 34–35, 35, 357–358
WLCs, 637, 637
SSIDs (service set identifiers)
overview, 559–560, 560
WLANs, 647–648
WLCs, 606, 611
SSL (Secure Sockets Layer), 435
SSO (single sign-on), 395
STALE state in neighbor discovery, 528
stand-alone WLAN deployment model, 597–598, 597
standard access lists, 292, 295–301, 299–301
standard vSwitches, 665
standby group ip virtual_ip command, 423
standby ip command, 425
standby name command, 424–425
standby preemption command, 425
standby priority command, 424–425
standby routers in HSRP, 416–418, 417–418, 421
Standby state in HSRP, 426
standby timers in HSRP, 420
standby timers msec command, 421
stateful autoconfiguration in IPv6, 476–477
stateless autoconfiguration in IPv6, 474–476, 474, 476
states
HSRP, 426
STP ports, 255–256
static IP addressing, 42
static MAC address, 214
static NAT, 322, 325
static routing, 119
Corp router, 144–146, 144
default ADs, 151
IP routing, 148–150
IPv6 protocol, 483–484, 484
LA router, 146–147
overview, 142–143
SF router, 145–146
stations in SNMP, 349
status messages in REST API, 681–682
Status option in WLANs, 648
sticky command, 201, 214
storage and Storage Spaces in virtualization, 666
STP. See Spanning Tree Protocol (STP)
straight-through cable, 20, 20–21
strict priority scheduling, 458
strong passwords, 389–390
structured threats, 365
stub routers, 147
subinterfaces in VLANs, 240
subnets and subnetting, 76
basics, 76–77, 77
CIDR, 80–81
Class B addresses, 93–101
Class C addresses, 82–93, 85 86, 88
creating, 77–78
test essentials, 102
ip subnet-zero, 81–82
masks, 78–79
powers of two, 79
review questions, 103–104
summary, 102
VLANs, 241
Support for CoA field in RADIUS, 640
SVI (switched virtual interface), 231
sweet feature alerts, 587
switch ports
LED, 206
VLANs, 234–236
switched virtual interface (SVI), 231
switches
IP addresses, 206
overview, 3–6, 3, 6
virtualization, 665–666
WLCs, 602–604, 602
switchport command, 234–236
switchport access command, 237–238
switchport access vlan command, 532, 536
joining APs, 609
WLC switches, 604
switchport mode command, 237–238, 537, 540
switchport mode access command
joining APs, 609
port security, 200
WLC switches, 604
switchport mode dynamic command, 537, 540–542
switchport mode trunk command
joining APs, 610
port channels, 280–281
WLC switches, 604
WLCs, 625
switchport nonegotiate command, 238
switchport port-security command, 200–201, 211
switchport port-security mac-address command, 210
switchport trunk allowed command, 238–239
switchport trunk allowed vlan command, 281
switchport trunk encapsulation command, 239
switchport trunk encapsulation dot1q command
joining APs, 610
port channels, 280–281
VLANs, 542
WLC switches, 604
WLCs, 625
switchport trunk native command, 239
switchport trunk native vlan command
joining APs, 610
VLANs, 537, 542, 544
switchports in joining APs, 609–610
symmetric encryption in IPsec transforms, 440
SYN floods, 369
syn packet acknowledgments, 50
synchronization with NTP, 347–348, 348
dslog, 352–354
  central, 694–695, 694
  configuration and verification, 354–356, 355
System Center Configuration Manager (SCCM), 663
system LED, 205, 205
system mtu command, 714

T

T1 connections, 17
T3 connections, 17
tablet endpoints, 497
tacacs-server command, 386
tasks in Ansible, 763
TCP. See Transmission Control Protocol (TCP)
TCP/IP. See Transmission Control Protocol/
  Internet Protocol (TCP/IP)
team silos, 744–747, 745–747
telnet command
  extended access lists, 520–521
  IP network connectivity, 516–518
Telnet protocol
  IP access lists, 302–303
  overview, 34, 34
  passwords, 403–404
  WLCs, 636, 636
templates
  Ansible, 763
  DNA Center, 723–724, 724
temporary employees, 387
temporary IPv6 addresses, 529
10Base-T Ethernet, 18
10GBase-T Ethernet, 19
Terminal Access Controller Access Control
  System (TACACS+), 370
  configuration, 385–386
  process, 385
  server role, 498
  WLCs, 643–646, 643–646
terminal monitor command, 352
testing NAT, 328–333, 330–332
TFTP (Trivial File Transfer Protocol), 36, 36
thin protocols, 45
thrashing of MAC tables, 203
three-layer hierarchical model, 10, 11
  access layer, 12–13
  core layer, 11–12
  distribution layer, 12
tickets in Kerberos, 400
TIDs (traffic identifiers) in QoS, 456
time to live (TTL) in IP header, 53
timers
  CDP, 338–339, 339
  HSRP, 419–421, 420
Timestamp field in syslog messages, 353
token cards in authentication, 381–382, 382
toll networks, 17
top-of-rack (ToR) design, 14–15, 14
topologies, 10
collapsed core, 13, 13
database, 168
DNA Center, 724–725, 725
documentation, 344–346, 344, 346
spine-leaf, 14–15, 14–15
three-layer hierarchical model, 10–13, 11
WANs, 15–17
ToR (top-of-rack) design, 14–15, 14
Total length field in IP header, 53
tower end servers, 497
traceroute command
  ICMP, 56, 108
  IP network connectivity, 511
  neighbor discovery, 527
traffic characteristics in QoS, 453–454, 453
Traffic Class field in IPv6 headers, 478
traffic flow in ESP, 440
traffic identifiers (TIDs) in QoS, 456
training for security, 375
transferring files, 35–36, 35–36
transforms in IPsec, 439–441, 439, 441
translation timeout in NAT, 330
Transmission Control Protocol (TCP), 43
attacks, 369
IP, 52–55, 53–54
key concepts, 46–47, 47
port numbers, 48–51
segment format, 43–45, 43
Transmission Control Protocol/Internet Protocol (TCP/IP)
ARP, 58–60, 59
destination ports, 49–50
and DoD model, 31–33, 32–33
exam essentials, 71–72
history, 30–31
Host-to-Host layer. See Host-to-Host layer
ICMP, 55–58, 56
IP addresses. See IP addresses
Process/Application layer. See Process/Application layer
review questions, 73–74
summary, 71
syn packet acknowledgments, 50
UDP, 45–46
transparent bridging, 6
transport input command, 357–358
transport input ssh command, 404
Transport layer, 32
TRAP operation in SNMP, 350
traps
SNMP, 37, 349, 695, 695
syslog, 355–356
Trivial File Transfer Protocol (TFTP), 36, 36
Trojan horse attacks, 373–375
troubleshooting
HSRP, 428–429
IP addresses, 110–113
exam essentials, 114
Linux, 506–507, 506–507
Mac OS, 504–506, 504–506
OS parameters, 108–109
overview, 106–108, 106
problem determination, 109, 113, 110–113
review questions, 115–116
summary, 114
Windows 10, 498–504, 499–503
IP network connectivity
test essentiels, 435
extended access lists, 519–522, 520
IPv6 networks, 522–531, 523–525
overview, 507–518, 508
review questions, 546–548
SPAN, 518–519, 518
summary, 544–545
VLANs, 531–544, 532
NAT, 328–333, 330–332
trunks, 537–544
trunck command, 237–238
trunk links, 226–227, 226
trunk ports, 236–240
trunk switches, 540
trunks, troubleshooting, 537–544
trust boundaries in QoS, 454–455, 454
trusted domains in QoS, 455
trusted networks, 291, 291
TTL (time to live) in IP header, 53
tunnel destination, 445
tunnel mode command, 444
tunnel source command, 445
tunnels, GRE, 441–447, 442
2-tier topologies, 13, 13
2.4GHz band, 565–566, 566
2.4GHz/5GHz, 569
Type I hypervisors, 668–669
type II hypervisors, 668–669
type of Service field
IP header, 53
QoS, 455
U
Ubuntu Linux, IP address troubleshooting
in, 506–507, 506–507
UDP. See User Datagram Protocol (UDP)
UEFI passwords, 391
unauthorized access, 370
underlay in SDN, 713, 713
interface configuration, 714–715
MTU, 714
OSPF configuration, 715
verifying, 716
unicasts
addresses, 69, 69
IPv6, 468, 470–471, 471
UNII (Unlicensed National Information Infrastructure) bands, 566–567, 567
unique local addresses, 471
UNIX Berkeley Software Distribution, 31
unshielded twisted-pair (UTP) cabling, 18
unstructured threats, 365
untrusted domains in QoS, 455
untrusted networks, 291, 291
upfade in RF, 576
upgrades in DNA Center, 726–727
upstream routing, 240
Urgent field in TCP segment, 44
use-tacacs parameter for passwords, 401
user accounts, 386–387
anonymous, 387–388
connection limits, 388
disabling, 387
lockouts, 393–394
maintenance, 388 389
user awareness for security, 374–375
User Datagram Protocol (UDP), 45
DHCP, 41
key concepts, 46–47, 47
port numbers, 48–51
segment format, 46, 46
username command, 357
username ansible priv command, 754
username ncm secret ncmPass command, 700
usernames
authentication, 381
WLCs, 605
UTP gigabit wiring, 21–22, 22
UTP (unshielded twisted-pair) cabling, 18

V
variables
Ansible, 753, 763
DNA Center templates, 723
verifying
bridge IDs, 267–273, 268
Catalyst switches, 212–214
Chef results, 781, 781
extended access lists, 521–522
GRE tunnels, 445–447
HSRP, 425–427
IP routing, 148–150
NAT, 327
OSPF, 182–188
port channels, 280–282, 280
Puppet results, 770 771
SDN, 716
syslog, 354–356, 355
Version field
IP header, 53
IPv6 headers, 478
video traffic in QoS, 453–454, 453
violation command, 211
virtual circuits
port numbers, 50
TCP, 43
Virtual Extensible LANs (VXLANs), 716
virtual interface in WLCs, 614, 618–619, 619
virtual LANs. See VLANs (virtual LANs)
virtual MAC addresses in HSRP, 418–419
virtual machines
fundamentals, 662–664, 663–664
migrations, 667
virtual private dial-up networks (VPDNs), 438
virtual private LAN switching service (VPLS), 437
virtual private networks (VPNs)
benefits, 435–436
enterprise-managed and provider-managed, 436 438, 436 437
exam essentials, 447
GRE tunnels, 441–447, 442
IPsec transforms, 439–441, 439, 441
overview, 434–435, 435
review questions, 448–450
summary, 447
virtual private wire service (VPWS), 437
Virtual Router Redundancy Protocol (VRRP), 416
virtual routers in HSRP, 416–417, 421
Virtual Tunnel Interface (VTI) mode, 443
VirtualBox, 670
virtualization
components, 665–666
text, 666–667
features, 666–667
review questions, 685–687
solutions, 669 670
summary, 684
types, 668
virtual machines
fundamentals, 662–664, 663–664
migrations, 667
viruses, 373–375
vlan command, 232–233, 602–603, 609
VLAN Trunk Protocol (VTP), 232
VLANs (virtual LANs), 220
broadcast control, 223
configuration, 231–234
inter-VLAN routing, 240–246, 241–242, 244, 246
switch port assignments, 234–236
trunk ports, 236–240
exam essentials, 247
flexibility and scalability, 224
frame tagging, 227–228
identifying, 224–229, 225–226, 228
ISL for, 228
joining APs, 609
operation, 220–223, 221–222
review questions, 248–250
routing between, 229–231, 230–231
security, 223–224
summary, 247
troubleshooting, 531–532, 532
scenario, 532–537
trunks, 537–544
trunk links, 226–227, 226
VMware ESXi, 669
VMware virtual SANs, 666
VMware Workstation/Fusion, 669
voice access ports, 226
voice traffic in QoS, 453–454, 453
VPDNs (virtual private dial-up networks), 438
VPLS (virtual private LAN switching
service), 437
VPNs. See virtual private networks (VPNs)
vSwitches, 665–666
VTP (VLAN Trunk Protocol), 232
VTY, access lists for, 302–303
VXLANs (Virtual Extensible LANs), 716

W

WALK operation in SNMP, 350
WANs (wide area networks), 4, 15–16
bandwidth, 17
terms, 16–17, 16
WAPs. See access points (APs)
WareZ attacks, 370
WCS (Wireless Control System), 599
WDS (Wireless Domain Services), 598
web server role, 498
Weighted Fair Queueing (WFQ), 459
weighted fair scheduling, 458
weighted random early detection (WRED), 461
WEP (Wired Equivalent Privacy), 582–583
WFQ (Weighted Fair Queueing), 459
Wi-Fi Protected Access (WPA), 583–585
wide area networks (WANs), 4, 15–16
bandwidth, 17
terms, 16–17, 16
wildcards
access lists, 296–298
OSPF, 173–175, 174
Windows field in TCP segment, 44
Windows 10, IP address troubleshooting in,
498–504
Windows authentication, 382
Wired Equivalent Privacy (WEP), 582–583
wireless access points (WAPs). See access
tools (APs)
wireless antennas, 556
Wireless Control System (WCS), 599
Wireless Domain Services (WDS), 598
wireless LAN controllers (WLCs), 554–555
access points, 610–611, 610
configuring, 625–628, 626–628
modes, 629–632, 630–633
exam essentials, 655–656
initial setup, 604–606
interface types, 614–615, 614
dynamic, 619–621, 620–621
Interface Groups, 622 623,
622–623
LAG, 623–625, 624
management, 615, 616
redundancy-management, 617–618,
618
service port, 616–617, 617
virtual, 618 619, 619
joining APs, 607–610, 608
management access connections, 633
CDP, 634–636, 634–635
HTTP, 637–638, 638
HTTPS, 638–639, 638
RADIUS, 639–643, 640–642
SSH, 637, 637
TACACS+, 643–646, 643–646
telnet, 636, 636
port types, 611–614, 612–613
wireless metro area networks (WMANs) – yum localinstall command 839

review questions, 657–660
summary, 655
switch configuration, 602–604, 602
WLANs
  advanced settings, 652, 652
  client connections, 653 655, 653 654
  creation, 646–648, 647–648
  policy mapping settings, 651
  QoS profiles, 651, 651
  security, 648–651, 649–650
wireless metro area networks (WMANs), 552
wireless network interface cards, 555, 555
wireless networks, 550
  channels, 565
  2.4GHz band, 565–566, 566
  2.4GHz/5GHz, 569
  5GHz band, 566–567, 567
  multiple APs, 568–569, 568
  overlap techniques, 567
deployment models, 596–597
  cloud, 600–601, 601
  lightweight, 598–599, 598
  split MAC, 599–600
  stand-alone, 597–598, 597
devices, 553–556, 554–555
exam essentials, 588 589
forms, 551–553, 551
principles, 556
  basic service sets, 557–558, 558
  bridges, 562–564, 563–564
  extended service sets, 560–561, 561
  independent basic service sets, 556 557
  infrastructure basic service sets, 558–559
  mesh networks, 564, 565
  repeaters, 561, 562
  service set identifiers, 559–560, 560
radio frequency. See radio frequency (RF)
review questions, 590 593
security
  802.11i standard, 585
  authentication and encryption, 581–582, 581–582
comparisons, 588
WEP, 582–583
WPA and WPA2, 583–585
WPA2 Enterprise, 585
WPA3, 586, 586
summary, 588
wireless personal area networks (WPANs), 551
Wireless Solution Engine (WLSE), 598
wireless wide area networks (WWANs), 553
WLCs. See wireless LAN controllers (WLCs)
WLSE (Wireless Solution Engine), 598
WMANs (wireless metro area networks), 552
Workstation nodes in Chef, 772
workstations in Chef, 772, 775 776
worms, 373–375
WPA (Wi-Fi Protected Access), 583–585
WPA2
  wireless networks, 583–585
  WPA2 Enterprise, 585
WPA3, 586
  WPA3-Enterprise, 587
  WPA3-Personal, 586–587
WPANs (wireless personal area networks), 551
WRED (weighted random early detection), 461
write operations in SNMP, 352
WWANs (wireless wide area networks), 553

X
X.500 standard, 396
X.509 certificates, 396 397
Xen hypervisor, 669

Y
yagi antennas, 556
YAML Ain’t Markup Language (YAML), 679
yum localinstall command, 775