



Index

Numbers

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

A

AAA (authentication, authorization,
 and accounting), 796, 803, 958
 configuring for network device access
 control, 805–809
 RADIUS, 804–805
 TACACS+, 803–804
 use cases, 803
 verification, 809
AAR (Application-Aware Routing),
 665–666
ABR (area border router), 205–206,
 957
absolute timeout command, 802–803
access layer, 625–627, 957
access ports, 11–12, 957
access-list command, 782–784
ACL (access control list), 295,
 781–782, 957
 AS_Path filtering, 309–311
 conditional debugging, 692–693
 configuring for CoPP, 817–818
 controlling access to vty line, 796–797
 downloadable, 788
 extended, 296
 named, 784–785
 numbered, 782–783
 numbered extended, 783–784
 port, 785–786
 standard, 295–296
 VLAN, 786–788
 wildcard mask, 782
Active state, BGP, 254
AD (administrative distance), 132,
 133–135, 957
address family, 248, 957
adjacency table, 29
advertisements
 BGP, 260–261
 OSPF, default route, 187–188
 VTP (VLAN Trunking Protocol), 97
AF (Assured Forwarding) PHB,
 388–390
agent-based automation tools. *See*
 automation tools

- agentless automation tools. *See* automation tools
- aggregate-address command, 267–274
 - as_set keyword, 276–277
 - summary-only keyword, 272
- AIGP (Accumulated Interior Gateway Protocol), 323–324
- algorithm
 - distance vector, 128–129
 - enhanced distance vector, 129–130
 - link-state, 130–131
 - path vector, 131–132
 - queuing, 406–408
 - transform sets, 478–480
- allowed VLAN, 14–15
- AMP (Advanced Malware Protection), 742–744, 957, 959
- amplitude, 520, 957
- anchor controller, 957
- Ansible, 912–913
 - CLI commands, 916
 - inventory file, 917
 - playbooks, 913–914, 917–930
 - workflow, 913
 - YAML files, 915–916
- antenna/s, 309–311
 - beamwidth, 563
 - directional, 567–570
 - EIRP (effective isotropic radiated power), 526, 538
 - free space path loss, 527–529
 - gain, 525–526, 562
 - isotropic, 526
 - link budget, 526–527
 - omnidirectional, 564–566
 - parabolic dish, 569–570
 - patch, 567–568
 - polarization, 563–564
 - radiation pattern, 560–562
 - RSSI (received signal strength indicator), 530–531
 - spatial multiplexing, 535–536
 - wave propagation, 513–514
 - Yagi, 565–569
- anycast gateway, 656
- API (application programming interface), 850–855, 857, 957. *See also* Postman
 - Cisco DNA Center
 - Network Device*, 864–867
 - Token*, 862–864
 - Cisco vManage, 867–868
 - Authentication*, 868
 - Fabric Device*, 869–870
 - HTTP status codes, 862
 - JSON (JavaScript Object Notation), 861–862
 - northbound, 855–856
 - REST (Representational State Transfer), 856
 - southbound, 856
 - XML (Extensible Markup Language), 860–861
- applets, EEM, 895
 - debugging, 896–898
 - manually executing, 899–901
 - syslog, 896
 - WR MEM, 898
- AP (access point). *See also* antenna/s; Cisco lightweight APs; roaming
 - autonomous, 545–546
 - Cisco lightweight, 547
 - customization*, 558–559
 - discovering a WLC*, 554–555
 - integrated antennas*, 565–566
 - maintaining WLC availability*, 556–557

- pairing with a WLC, 552*
- policy tag, 558*
- RF tag, 558*
- segmenting wireless configurations, 557–559*
- selecting a WLC, 555–556*
- site tag, 558*
- special-purpose modes, 547–548*
- split-MAC architecture, 547*
- state machine, 552–554*
- client density, 559–560
- Probe Requests, 587
- troubleshooting connectivity issues, 617–620
- architecture. *See also* hierarchical LAN design**
- AMP (Advanced Malware Protection), 743–744
- Chef, 905
- Cisco ENFV (Enterprise Network Functions Virtualization), 843
- Cisco SD-WAN, 661–662
- LISP (Cisco Locator/ID Separation Protocol), 497
 - control plane, 497–498*
 - data plane, 498–499*
- SD-Access, 646–647
 - network layer, 647–648*
 - physical layer, 647*
 - underlay network, 648–649*
- area range command, 223**
- area/s, 173–174, 204–207, 217**
 - filtering, 225–227
 - ID, 207
- ARP (Address Resolution Protocol), 19–20, 957**
- AS (autonomous systems), 127, 157, 958**
- ASICs (application-specific integrated circuits), 4, 30**
- ASNs (autonomous system numbers), 246**
- AS_Path, 957**
- as_set keyword. *See also* keywords**
- atomic aggregate attribute, 274–276, 958**
- authentication, 603**
 - Enhanced FlexAuth, 766
 - password, 790–793
 - WebAuth, 764
 - Central, 765*
 - Local, 764–765*
 - wireless, 593
 - EAP, 597–602*
 - Open Authentication, 593–594*
 - pre-shared key, 595–597*
 - WebAuth, 603–606*
- Authentication API, 868**
- auto-cost reference bandwidth command, 189**
- automation tools**
 - Ansible, 912–913
 - CLI commands, 916*
 - inventory file, 917*
 - playbooks, 913–914, 917–930*
 - workflow, 913*
 - YAML files, 915–916*
 - Chef, 904
 - architecture, 905*
 - comparison with Puppet, 906*
 - cookbooks, 906*
 - demo_install.rb, 906–908*
 - kitchen, 906*
 - recipe, 906*
 - server, 906*
 - server deployments, 906*

comparing, 924–925
 Puppet, 902

- agent/server communication*, 902
- components*, 902
- installation modes*, 903
- manifests*, 903–904
- modules*, 903

 Puppet Bolt, 922

- command line*, 922–923
- tasks*, 922, 923

 Salt SSH, 923–924
 autonomous APs, 545–546, 574–576, 958
 Auto-RP, 364
 auxiliary port, 802
 AVG (active virtual gateway), 441

B

backbone area, 958
 bare-metal server, 828
 Bc (committed burst size), 395
 BDR (backup designated router), 177–178, 958

- election, 190–192
- placement, 192–194

 beacon, 909
 beamwidth, 563, 958
 BGP (Border Gateway Protocol), 244, 290–291

- address family, 248
- Adj-RIB-In table, 262
- Adj-RIB-Out table, 262, 265
- ASNs (autonomous system numbers), 246
- best path selection, 318–319

Accumulated Interior Gateway Protocol metric, 323–324
eBGP over iBGP, 327
local preference attribute, 322–323
locally originated via network or aggregate advertisement, 323
lowest IGP metric, 327–328
lowest neighbor address, 329
minimum cluster list length, 329
multi-exit discriminator, 326–327
origin type, 325–326
overview, 320–321
prefer path from the oldest eBGP session, 328
router ID, 328–329
shortest AS path, 324–325
using longest match, 319–320
weight attribute, 321–322
 community, 313, 958

- conditionally matching*, 315–317
- enabling support*, 314–315
- extended*, 314
- private*, 314, 317–318
- well-known*, 314

 conditional matching, 295

- ACL*, 295–296
- IPv6 prefix list*, 299–300
- prefix list*, 299
- prefix matching*, 297–299
- regex*, 300–301

 configuration, 256–257

- network advertisement*, 261
- requirements*, 255

 deterministic routing, 293–294
 inter-router communication, 248–249
 IPv6

- configuring*, 277–282
- route summarization*, 282–285
- Loc-RIB table, 262, 263–264
- loop prevention, 247–248
- messages, 252
- multihoming, 291, 958
 - branch transit routing*, 293–295
 - Internet transit routing*, 292–293
 - resiliency in service providers*, 291–292
- multiprotocol, 277
- neighbor state, 253
 - Active*, 254
 - Connect*, 254
 - Established*, 255
 - Idle*, 254
 - OpenConfirm*, 255
 - OpenSent*, 254–255
- neighbors, 249
- network statements, 260–261
- NLRI (Network Layer Reachability Information), 248
- PA (path attribute), 247
- packets, 252
- peering, 279
- receiving and viewing routes, 262–265
- redistributing routes into an IGP, 267
- route advertisement/s, 260–261
 - from indirect sources*, 265–268
- route aggregation, 267–268
 - with AS_SET*, 276–277
 - aggregate-address command*, 267–274
 - atomic aggregate attribute*, 274–276
- route filtering, 306–307
 - AS_Path ACL filtering*, 309–311
 - distribute lists*, 307
 - prefix lists*, 308
 - route maps*, 311–313
- route maps, 301–302
 - command syntax*, 301
 - complex matching*, 304
 - components*, 301
 - conditional match options*, 302–303
 - continue keyword*, 305–306
 - multiple conditional match conditions*, 303–304
 - optional actions*, 304–305
- sessions, 249–250
 - clearing*, 313
 - eBGP*, 251
 - iBGP*, 250–251
- verification, 257–260
- bootstrap router, 366–367
- border nodes, SD-Access, 654
- BPDU (bridge protocol data unit), 40, 958
- BPDU filter, 72–73, 958
- BPDU guard, 70–72, 958
- broadcast domain, 6, 959
- broadcast networks, OSPF, 194–195
- broadcast traffic, 339
- BSS (basic service set), 592
- BSS (business support system), 836

C

- CAM (content addressable memory), 17, 960
- campus network
 - Layer 2 access layer, 634–636
 - Layer 3 access layer, 636–637
 - SD-Access design, 640
 - simplified campus design, 637–639

- three-tier design, 634
- two-tier design, 632
- candidate RP (rendezvous point), 364–365, 366–367
- capabilities, NETCONF, 874
- CAPWAP (Control and Provisioning of Wireless Access Points), 552, 959
- carrier signal, 531, 959
- CBWFQ (class-based weighted fair queuing), 407–408
 - commands, 410–411
 - configuring, 410–414
- CEF (Cisco Express Forwarding), 27, 959
 - hardware, 30
 - software, 29–30
- Central Web Authentication, 765
- centralized forwarding, 28
- centralized wireless deployment, 548–550
- channel, 517, 959
- Chef, 904
 - architecture, 905
 - comparison with Puppet, 906
 - cookbooks, 906
 - demo_install.rb, 906–908
 - kitchen, 906
 - recipe, 906
 - server, 906
 - server deployments, 906
- CIR (committed information rate), 395
- Cisco Advanced Malware Protection, 742–744
- Cisco DevNet. *See* DevNet
- Cisco DNA Center, 642
 - assurance, 728, 733–734
 - Assurance tab*, 729
 - main page*, 728–729
 - management*, 657
 - Network Time Travel*, 728–729
 - Path Trace*, 731
 - search capabilities*, 730–731
 - Token API*, 862–864
 - workflow*, 660
 - design workflow, 658
 - management layer, 657
 - policy workflow, 658–659
 - provision workflow, 659–660
- Cisco ENFV (Enterprise Network Functions Virtualization), 842–843
 - architecture, 843
 - management and orchestration, 843–844
 - NFVIS (network function virtualization infrastructure software), 846–847
 - virtual network functions and applications, 845
- Cisco FlexVPN, 486
- Cisco FMC (Firewall Management Center), 753
- Cisco IBNS (Identity-Based Networking Services) 2.0, 766
- Cisco ISE (Identity Services Engine), 657, 756–758, 959
- Cisco lightweight AP, 547, 966. *See also* antenna/s; roaming
 - customization, 558–559
 - discovering a WLC, 554–555
 - integrated antennas, 565–566
 - intercontroller roaming, 579
 - intracontroller roaming, 577–579
 - maintaining WLC availability, 556–557
 - Network Device API, 864–867
 - pairing with a WLC, 552
 - policy tag, 558
 - RF tag, 558

- segmenting wireless configurations, 557–559
- selecting a WLC, 555–556
- site tag, 558
- special-purpose modes, 547–548
- split-MAC architecture, 547
- state machine, 552–554
- Cisco NCP (Network Control Platform), 656**
- Cisco SAFE (Secure Architectural Framework), 959**
 - advanced threat defense protection, 740–741
 - AMP (Advanced Malware Protection), 742–744
 - Cisco FMC (Firewall Management Center), 753
 - Cisco ISE (Identity Services Engine), 756–758
 - Cisco Secure Client, 744
 - Cisco Secure Cloud Analytics, 755–756
 - Cisco Secure Email, 748–749
 - Cisco Secure Firewall, 751–752, 959
 - Cisco Secure IPS, 749–751
 - Cisco Secure Network Analytics, 753–755
 - Cisco Secure Web Appliance, 746–748
 - key, 740
 - Malware Analytics, 742
 - next-generation endpoint security, 737–741
 - PINs (places in the network), 738–739
 - security concepts, 739–740
 - Talos, 741–742
 - Umbrella, 744–745
- Cisco SD-WAN**
 - AAR (Application-Aware Routing), 665–666
 - architecture, 661–662
 - Cloud OnRamp, 664–665
 - for IaaS*, 668–669
 - for SaaS*, 666–668
 - edge devices, 663–664
 - SD-WAN policy, 665
 - vAnalytics, 664
 - vBond orchestrator, 662–663
 - vManage NMS, 663
 - vSmart controllers, 663
- Cisco Secure Client, 744**
- Cisco Secure Cloud Analytics, 755**
 - Network Analytics SaaS, 755–756
 - Public Cloud Monitoring, 755
- Cisco Secure Email, 748–749**
- Cisco Secure Firewall, 751–752, 959**
- Cisco Secure Malware Analytics, 742, 959**
- Cisco Secure Network Analytics, 753–755**
- Cisco Secure Web Appliance, 746–748**
- Cisco Talos, 741–742, 960**
- Cisco TrustSec, 766–767, 960**
 - egress enforcement, 770–771
 - ingress classification, 767–768
 - propagation, 768–770
- Cisco Umbrella, 744–745, 960**
- Cisco vManage APIs, 867–868**
 - Authentication, 868
 - Fabric Device, 869–870
- Cisco wireless deployments, 548**
 - centralized, 548–550
 - cloud-based, 550
 - controller-less, 551
 - distributed, 551
- class-based policing, 398**
- classification, 381–382**

- ingress, 767–768
- Layer 7, 382
- clear ip bgp command, 313**
- clear ip ospf process command, 193–194**
- clear mac address-table dynamic command, 17**
- clear ospf process command, 181**
- clearing BGP sessions, 313**
- CLI (command-line interface), 960. *See also* IOS XE**
 - pros and cons, 854–855
 - terminal lines, 788–789
- client density, 559–560**
- Cloud OnRamp, 664–665**
 - for IaaS, 668–669
 - for SaaS, 666–668
- cloud-based wireless deployment, 550**
- code. *See also* Python**
 - editing, 881–882
 - functions, 888
 - manifest, 903–904
 - recipe, 906
- collections, Postman, 858–859**
- collision domains, 5–6, 960**
- command/s. *See also* keywords**
 - absolute timeout, 802–803
 - access-list, 782–784
 - aggregate-address, 267–274
 - Ansible, 916
 - area range, 223
 - auto-cost reference bandwidth, 189
 - CBWFQ, 410–411
 - clear ip bgp, 313
 - clear ip ospf process, 193–194
 - clear mac address-table dynamic, 17
 - clear ospf process, 181
 - debug event manager action cli, 896–898
 - debug ip ospf adj, 687, 690–691
 - debug ip ospf hello, 687–689, 690–691
 - default-information originate, 187
 - device hardening, 822–823
 - do show ip ospf neighbor, 691–692
 - do show logging, 702–703
 - encapsulation dot1q, 22
 - errdisable recovery cause bpduguard, 71–72
 - event manager run, 899
 - fhrp version vrrp v3, 440–441
 - file prompt quiet, 899
 - interface vlan, 23
 - ip access-list, 784–785
 - ip address, 21
 - ip address secondary, 21
 - ip flow monitor, 715
 - ip ospf area, 180
 - ip ospf network broadcast, 689–690
 - ip route, 138
 - ip sla, 725–727
 - ipv6 address, 21
 - lacp max-bundle, 116–117
 - lacp rate fast, 115
 - logging buffered ?, 702
 - logout-warning, 802–803
 - mac address-table static vlan, 16
 - match, 382–384
 - monitor session destination interface, 718
 - name, 8
 - neighbor distribute-list, 307
 - network area, 178
 - no switchport, 23
 - passive-interface, 237–238

- ping, 675–676
 - extended*, 677–680
 - repeat option*, 676–677
- port-channel min-links, 115
- privilege levels, 793–796
- Puppet Bolt, 922–923
- remote-span, 721
- route-map, 301
- router ospf, 178
- SaltStack, 910–911
- sdm prefer, 30
- service-policy, 380
- show bgp ipv4 unicast, 263–265, 267–268
- show bgp ipv4 unicast neighbors, 258–260
- show bgp ipv4 unicast summary, 257
- show bgp ipv6 unicast neighbors, 281
- show bgp ipv6 unicast summary, 281–282
- show bgp summary, 257
- show etherchannel load-balance, 120
- show etherchannel port, 110–112
- show etherchannel summary, 108–109
- show flow record, 710–711
- show glbp, 443–444
- show interface port-channel, 110
- show interfaces status, 18–19, 71
- show interfaces switchport, 17–18
- show interfaces trunk, 13–14, 103
- show ip arp, 20
- show ip flow export, 707–708
- show ip interface brief, 23–24
- show ip nat translations, 450–452
- show ip ospf database summary, 215
- show ip ospf interface, 184–185, 689
- show ip ospf neighbor, 186, 686
- show ip route, 137, 139, 266–267
- show ip route bgp, 265
- show ip route ospf, 187
- show ipv6 interface brief, 24–25
- show ipv6 route, 146
- show ipv6 route ospf, 237, 238, 239
- show lacp counters, 113–114
- show lacp neighbor, 112–113
- show lacp sys-id, 117–118
- show logging, 703–704
- show mac address-table dynamic, 15–16
- show monitor session erspan-source session, 723–724
- show ntp associations, 423–424
- show ntp status, 422–423
- show ospfv3 interface, 236, 240
- show ospfv3 ipv6 neighbor, 236
- show pagp counters, 114
- show pagp neighbor, 113
- show running-config, 270–271
- show sdm prefer, 31–32
- show spanning-tree, 85–86
- show spanning-tree inconsistentports, 74
- show spanning-tree interface, 48–49, 70–71, 73
- show spanning-tree mst, 86–87, 88
- show spanning-tree mst configuration, 84–85
- show spanning-tree mst interface, 87
- show spanning-tree root, 42–45
- show spanning-tree vlan, 45–47, 61–62, 64–66
- show spanning-tree vlan detail, 49–50
- show standby, 435–438
- show track, 431–432
- show udld neighbors, 75–76
- show vlan, 9–10

- show vrrp, 439
- show vrrp brief, 441
- show vtp status, 99–101
- spanning-tree bpdudfilter enable, 72
- spanning-tree guard root, 68
- spanning-tree mode mst, 84
- spanning-tree pathcost method long, 41
- spanning-tree portfast, 68–70
- spanning-tree portfast bpduguard default, 70
- spanning-tree vlan forward-time, 40
- spanning-tree vlan hello-time, 40
- spanning-tree vlan max-age, 40
- spanning-tree vlan priority, 60
- spanning-tree vlan root, 60
- switchport access vlan, 12
- switchport mode access, 12
- switchport mode trunk, 12
- switchport trunk allowed vlan, 14–15
- switchport trunk native vlan, 14
- traceroute, 448, 680–683
 - extended*, 684–685
 - options*, 683
- transport input, 797–800
- tunnel mode ipsec, 493
- udld enable, 75
- undebg interface loopback0, 695
- vlan, 8
- vtp domain, 98–99
- vtp mode, 98–99
- vtp password, 98–99
- vtp version, 98–99
- communication, OSPFv3, 232–233**
- community, BGP, 313**
 - conditionally matching, 315–317
 - enabling support, 314–315
 - extended, 314
 - private, 314, 317–318
 - well-known, 314
- Community page, DevNet, 879**
- conditional debugging**
 - on a specific interface, 693–695
 - using ACLs, 692–693
- conditional matching, 295. *See also* route maps**
- ACL, 295
 - extended*, 296
 - standard*, 295–296
- BGP communities, 315–317
- prefix matching, 297–299
 - IPv6 prefix lists*, 299–300
 - prefix lists*, 299
- regex, 300–301
- configuration**
 - BGP (Border Gateway Protocol), 255–257, 261
 - DTP (Dynamic Trunking Protocol), 102
 - EtherChannel, 107–108
 - HSRP (Hot Standby Router Protocol), 434–435
 - MQC classification, 382–385
 - MST (Multiple Spanning Tree Protocol), 84
 - NTP (Network Time Protocol), 421–422
 - OSPF (Open Shortest Path First), 181–183
 - for all interfaces*, 178–180
 - with explicit IP addresses*, 179
 - with explicit subnet*, 179
 - interface-specific*, 180–181
 - network statement*, 178
 - OSPFv3, 233–235

- PTP (Precision Time Protocol), 427–429
- QoS (quality of service)
 - CBWFQ*, 410–414
 - class-based policing*, 398
- SNMP (Simple Network Management Protocol), 699–700
- trunk port, 13
- VRRP (Virtual Router Redundancy Protocol), 438–441
- VTP (VLAN Trunking Protocol), 98–99
- ZBFW (Zone-Based Firewall), 811–815
- configuration BPDUs**, 40
- congestion avoidance**, 408–410
- congestion management**, 406–408
- Connect state**, BGP, 254
- containers**, 830–831, 960
- control plane**
 - LISP (Cisco Locator/ID Separation Protocol), 497–498
 - nodes, SD-Access, 653–654
 - SD-Access, 649–650
 - VXLAN (Virtual eXtensible Local Area Network), 506
- controller layer**, SD-Access, 656–657
- controller-less wireless deployment**, 551
- convergence**
 - EIGRP (Enhanced Interior Gateway Routing Protocol), 164–166
 - RSTP (Rapid Spanning Tree Protocol), 55
 - STP (Spanning Tree Protocol)
 - with direct link failures*, 50–52
 - with indirect failures*, 52–53
- cookbook**, 906

- CoPP (Control Plane Policing)**, 817, 960
 - ACL configuration, 817–818
 - applying the policy map, 819–820
 - class map configuration, 818
 - policy map configuration, 819
 - verification, 820–822
- core layer**, 628–629, 960
- CQ (custom queuing)**, 407
- creating**
 - username, 790
 - VLANs, 8
 - VRF instance, 150
- CRUD functions**, 856
- CS (Class Selector) PHB**, 388
- CSMA/CD (Carrier Sense Multiple Access/Collision Detect)**, 5
- CST (Common Spanning Tree)**, 81–82, 960

D

- dACL (downloadable ACL)**, 788
- data link layer**, 4
- data model**, YANG, 870–872
- data plane**
 - LISP (Cisco Locator/ID Separation Protocol), 498–499
 - SD-Access, 650–651
- datastore**, NETCONF, 875
- dB (decibel)**, 522, 523–524, 961
 - Law of 3s, 522–523
 - Law of 10s, 523
 - Law of Zero, 522
- dBm (dB-milliwatt)**, 525, 961
- dead interval timer**, 961
 - OSPF, 190
 - OSPF (Open Shortest Path First), 689

- debug event manager action cli command, 898
- debug ip ospf adj command, 687, 690–691
- debug ip ospf hello command, 687–689, 690–691
- debugging, 685–686. *See also* diagnostic tools; troubleshooting
 - conditional
 - on a specific interface*, 693–695
 - using ACLs*, 692–693
- EEM actions, 896–898
- OSPF (Open Shortest Path First)
 - debug ip ospf adj command*, 687, 690–691
 - debug ip ospf hello command*, 687–689, 690–691
 - ip ospf network broadcast command*, 689–690
 - show ip ospf interface command*, 689
 - show ip ospf neighbor command*, 686
- default-information originate command, 187
- delay variation, 376
- demodulation, 961
- deterministic routing, 293–294
- device driver, 837
- device hardening, 822–823
- DevNet, 877–878, 961
 - Community page, 879
 - Documentation page, 878
 - Events page, 879
 - Learn page, 878
 - Technologies page, 878
- DF (Default Forwarding) PHB, 388
- diagnostic tools. *See also* Cisco DNA Center Assurance
 - IP SLA, 724
 - HTTP GET operation*, 726–728
 - ICMP echo operation*, 724–726
 - ping command, 675–676
 - extended*, 677–680
 - repeat option*, 676–677
 - traceroute command, 680–683
 - extended*, 684–685
 - options*, 683
- dictionary
 - Python, 885
 - YAML, 915–916
- DiffServ, 379, 961
- dipole antenna, 564–565, 961
- directional antenna, 567–570, 961
- directly attached static routes, 138–139, 961
- discontiguous networks, OSPF, 217–218
- displaying, trunk port information, 13
- distance vector algorithms, 128–129, 962
- distribute lists, 307, 962
- distributed forwarding, 28
- distributed wireless deployment, 551
- distribution layer, 627–628, 962
- distribution tree, 349
 - shared tree, 350–352
 - source tree, 349–350
- DMA (direct memory access), 837
- DMVPN (Cisco Dynamic Multipoint VPN), 486
- do show ip ospf neighbor command, 691–692
- do show logging command, 702–703
- Docker, 831, 832–833
- Documentation page, DevNet, 878
- downlink MACsec, 774

downstream interface, 962
 DP (designated port), 961
 DR (designated router), 176–178, 961
 election, 190–192
 placement, 192–194
 drop precedence, 390
 DRS (dynamic rate shifting), 538–540, 962
 DSCP per-hop behaviors. *See* PHB (per-hop behavior), 387
 DSSS (direct sequence spread spectrum), 533, 961
 DTLS (Datagram Transport Layer Security), 961
 DTP (Dynamic Trunking Protocol), 101, 962
 configuring, 102
 disabling trunk port negotiation, 103
 matrix for establishing a dynamic trunk link, 102
 modes, 102
 DUAL (diffusing update algorithm), 129
 dynamic routing protocol, 126–128

E

E plane, 962
 EAP (Extensible Authentication Protocol), 597–599, 760–762, 963
 configuring with external RADIUS servers, 600–602
 verification, 602
 eBGP, 962
 eBGP (external BGP) sessions, 251
 edge node, SD-Access, 652–653
 editing, code in GitHub, 881–882
 EEM (Embedded Event Manager), 901, 962
 applets, 895
 debugging, 896–898
 syslog, 896
 WR MEM, 898
 email variables, 899
 event detectors, 894–895
 Tcl scripts, 899–901
 EF (Expedited Forwarding) PHB, 390
 EGP (Exterior Gateway Protocol), 127–128. *See also* BGP (Border Gateway Protocol)
 EIGRP (Enhanced Interior Gateway Routing Protocol), 129–130
 AS (autonomous system), 157
 convergence, 164–166
 failure detection and timers, 164
 FD (feasible distance), 158
 feasibility condition, 158
 feasible successor, 158
 k value, 160–161
 load balancing, 163
 metric backward compatibility, 163
 neighbors, 160
 packets, 160
 path metric calculation, 160–162
 RD (reported distance), 158
 route summarization, 166–167
 successor/successor route, 158
 topology table, 159–160
 variance value, 163
 wide metric, 162
 EIRP (effective isotropic radiated power), 526, 538, 962
 email variables, EEM (Embedded Event Manager), 899
 EMs (element managers), 835
 encapsulation dot1q command, 22
 ENCOR 350–401 exam

- getting ready, 926–927
 - suggested plan for final review/study, 930
 - tools for final preparation, 927–930
 - updates, 932–934
 - encryption**
 - MACsec, 772–773
 - downlink*, 774
 - frame format*, 773–774
 - uplink*, 774
 - password, 789–790
 - endpoint**, 962
 - enhanced distance vector algorithms**, 129–130, 962. *See also* EIGRP (Enhanced Interior Gateway Routing Protocol)
 - Enhanced FlexAuth**, 766
 - enterprise network architecture**, 632
 - Layer 2 access layer, 634–636
 - Layer 3 access layer, 636–637
 - SD-Access design, 640
 - simplified campus design, 637–639
 - three-tier design, 634
 - two-tier design, 632
 - Env_Lab.py script**, 882–885
 - equal-cost multipathing**, 135–136, 163, 220, 962
 - errdisable recovery cause bpduguard command**, 71–72
 - ERSPAN (Encapsulated Remote SPAN)**, 722, 963
 - specifying the destination port, 723–724
 - specifying the source port, 722–723
 - ESP (Encapsulating Security Payload)**, 477–478
 - Established state**, BGP, 255
 - EtherChannel bundle**, 104, 105, 963
 - components, 104–105
 - configuring, 107–108
 - link-state propagation and detection, 105–106
 - load balancing traffic, 119–120
 - logical interface status fields, 109
 - member interface status fields, 109
 - multiple links with STP, 104
 - troubleshooting, 118–119
 - verifying the status, 108–110
 - viewing show etherchannel port command output, 110–112
 - Ethernet, collision domains**, 5–6
 - ETR (egress tunnel router)**, 962
 - event manager run command**, 899
 - Events page**, DevNet, 879
 - EXEC timeout**, 802
 - extended ACLs**, 296
 - extended communities**, BGP, 314
 - extended ping command**, 677–680
 - extended traceroute command**, 684–685
- ## F
-
- fabric**
 - SD-Access, 649
 - border nodes*, 654
 - control plane*, 649–650
 - control plane nodes*, 653–654
 - data plane*, 650–651
 - device roles*, 652
 - edge nodes*, 652–653
 - policy plane*, 651–652
 - WLC (wireless LAN controller), 654
 - Fabric Device API**, 869–870
 - fabric network**, 642. *See also* SD-Access
 - failure detection**, EIGRP, 164

FD (feasible distance), 158

feasibility condition, 158

feasible successor, 158

FHRP (first-hop redundancy protocol), 429–430, 963

- configuration, 442–443
- GLBP (Gateway Load Balancing Protocol), 441
 - AVF (active virtual forwarder)*, 442
 - AVG (active virtual gateway)*, 441
 - changing the load-balancing method*, 444–446
 - viewing the status*, 443–444
- HSRP (Hot Standby Router Protocol), 432–433
 - configuration*, 434–435
 - object tracking*, 436–438
 - versions*, 433
 - viewing the status*, 435–436
 - VIP (virtual IP) instance*, 433–434
- object tracking, 430
- VRRP (Virtual Router Redundancy Protocol), 438
 - legacy configuration*, 439
 - version 2 configuration*, 438
 - version 3 configuration*, 440–441
 - viewing the status*, 439

fhrp version vrrp v3 command, 440–441

FIB (Forwarding Information Base), 29, 132, 963

FIFO (first-in, first-out), 406

file prompt quiet command, 899

firewall

- next-generation, 751

- zone-based. *See* ZBFW (Zone-Based Firewall)

Flexible NetFlow, 709

- applying the flow monitor to the interfaces, 715–716
- creating a custom flow record, 709–711
- creating a flow exporter, 711–712
- creating a flow monitor, 713–714
- mapping the flow exporter to the flow monitor, 714

floating static route, 141–143, 963

flows, 706

forward delay, 40, 963

forwarding architecture, 25–26

- CEF (Cisco Express Forwarding), 27
 - hardware*, 30
 - software*, 29–30
- centralized forwarding, 28
- distributed forwarding, 28
- process switching, 26–27
- SDM (Switching Database Manager)
 - templates, 30–32
- TCAM (ternary content addressable memory), 27–28

free space path loss, 527–529

frequency, 514–515, 963

- 2.4 GHz band, 516
- 5 GHz band, 516
- 6 GHz band, 516
- channels, 517
- non-overlapping channel spacing, 518–519
- radio, 516
- signal bandwidth, 517–518

FTD (Firepower Threat Defense)

- software image, 963

fully specified static route, 141

functions. *See also* VNF (virtual network function)

CRUD, 856

HTTP, 856

Python, 888

G

gain, 525–526, 562, 964

general-purpose CPU, 27

GET (Cisco Group Encrypted Transport) VPN, 486

get_dnac_devices.py script, 885–889

GitHub, 880, 964

code editing, 881–882

projects, 880–881

GLBP (Gateway Load Balancing Protocol), 441

AVF (active virtual forwarder), 442

AVG (active virtual gateway), 441

changing the load-balancing method, 444–446

configuration, 442–443

viewing the status, 443–444

grain, 909–910, 964

GRE (Generic Routing Encapsulation), 469

encapsulation, 469

encrypting traffic using IPsec profiles, 487–493

tunnel configuration, 470–474

verification, 474

H

H plane, 964

hard reset, BGP, 313

hardware, CEF (Cisco Express Forwarding), 30

header, VLAN, 8

hello packet, OSPF, 175

hello time, 40, 190, 689, 964

hierarchical LAN design, 624–625

access layer, 625–627

core layer, 628–629

distribution layer, 627–628

high availability

network design, 629

technologies, 630

SSO and NSF, 623–630

SSO/NSF with GR, 631

SSO/NSF with NSR, 631

SSO/NSF with NSR and GR, 631

host pool, 655, 964

HSRP (Hot Standby Router Protocol), 432–433

configuration, 434–435

object tracking, 436–438

versions, 433

viewing the status, 435–436

VIP (virtual IP) instance, 433–434

HTTP

functions, 856

status codes, 862

hubs, collision domain, 5–6

hypervisor, 828–829, 964

I

IaaS (infrastructure as a service), Cloud OnRamp, 668–669

IANA (Internet Assigned Numbers Authority), 247

iBGP (internal BGP) sessions, 250–251, 964

Idle state, BGP, 254

- IDS (intrusion detection system), 749
- IEEE (Institute of Electrical and Electronic Engineers) standards, 5
- 802.1D STP. *See* STP (Spanning Tree Protocol)
- 802.1p, 386
- 802.1Q, 7, 385
- 802.11, 533–535. *See also* wireless networks and theory
- IGMP (Internet Group Management Protocol), 337, 343–344, 965
 - message format, 344–345
 - snooping, 346–348, 964
 - version 2, 344
 - version 3, 346
- IGP (Interior Gateway Protocol), 127, 249
- IKE (Internet Key Exchange), 480, 965
 - version 1, 480–482
 - version 2, 482–484
- ingress classification, 767–768
- inside static NAT, 449–452
- installation modes, Puppet, 903
- integrated antennas, 565–566, 964
- inter-area routes, 207, 219, 222, 223–224, 965
- intercontroller roaming, 579, 965
- interface cost, OSPF, 189
- interface priority, LACP (Link Aggregation Control Protocol), 118
- interface vlan command, 23
- Internet, transit routing, 292–293
- intra-area routes, 207, 218–219, 965
- intracontroller roaming, 577–579, 965
- IntServ, 377–378
- inventory file, Ansible, 917
- I/O (input/output), 836
- IOS XE, 796–797
 - creating a username, 790
 - EXEC timeout, 802
 - hash options, 119–120
 - ip_input* process, 26
 - passwords
 - encryption*, 789–790
 - types of*, 789
 - privilege levels, 793–796
- ip access-list command, 784–785
- ip address command, 21
- ip address secondary command, 21
- IP addressing, 21–22. *See also* MAC (Media Access Control) address; NAT (Network Address Translation); PAT (Port Address Translation)
- ESP (Encapsulating Security Payload), 477–478
- multicast, 340
 - GLOP block*, 342
 - IANA-assigned addresses*, 340–341
 - internetwork control block*, 341
 - local network control block*, 341
 - organization-local scope addresses*, 342
 - Source Specific Multicast block*, 342
 - well-known reserved address*, 341
- routed subinterface, 22
- routed switch port, 23
- SVI (switched virtual interface), 23
- verification, 23–25
- ip flow monitor command, 715
- ip flow-top-talkers command, 708–709
- ip ospf area command, 180
- ip ospf network broadcast command, 689–690

ip route command, 138
IP SLA, 724, 965

- HTTP GET operation, 726–728
- ICMP echo operation, 724–726

ip sla command, 725–727
ip_input process, 26
IPS (intrusion prevention system), 749
IPsec, 475–476, 965

- authentication header, 476
- DMVPN (Cisco Dynamic Multipoint VPN), 486
- encryption, hashing, and keying methods, 478
- IKE (Internet Key Exchange), 480
 - version 1*, 480–482
 - version 2*, 482–484
- site-to-site configuration, 486–487
- site-to-site GRE over, 487–493
- site-to-site VTI over, 493–495
- transform set, 478–480
- VPN, 484–486
 - Cisco Dynamic Multipoint*, 486
 - Cisco FlexVPN*, 486
 - GET*, 486
 - remote access*, 486
 - site-to-site*, 486

IPv6, 21

- BGP configuration, 277–285
- OSPFv3 configuration, 234–235
- static routes, 145–146

ipv6 address command, 21
IRQ (interrupt request), 836
ISAKMP (Internet Security Association and Key Management Protocol), 480, 965
isotropic antenna, 526, 560–561, 965
IST (internal spanning tree), 83, 965

J

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

K

k value, 160–161, 965
kernel, 837
keyword/s

- access-list command, 782, 783
- aggregate-address command, 272, 276–277
- continue, 305–306
- show mac address-table dynamic command, 15
- show vlan command, 10–11
- switchport trunk allowed vlan command, 15

kitchen, 906
knife, 906

L

LACP (Link Aggregation Control Protocol), 106–107

- fast, 115
- interface priority, 118
- maximum number of EtherChannel member interfaces, 116–117
- minimum number of EtherChannel member interfaces, 115
- system priority, 117–118, 966
- viewing neighbor information, 112–113
- viewing packet counters, 113–114

lacp max-bundle command, 116–117

- lacp rate fast command, 115**
- latency, 162, 374**
 - jitter, 376
 - processing delay, 376
 - propagation delay, 375
 - satellite communication, 375
 - serialization delay, 375
- Law of 3s, 522–523**
- Law of 10s, 523**
- Law of Zero, 522**
- Layer 2 forwarding, 4–5, 966. *See also* switches**
 - MAC address table, 15–17
 - troubleshooting, 16
- Layer 2 roaming, 579–580**
- Layer 3 forwarding, 19, 966**
 - ARP (Address Resolution Protocol), 19–20
 - IP address assignment, 21–22
 - routed subinterfaces, 22*
 - routed switch ports, 23*
 - SVI (switched virtual interface), 23*
 - verification, 23–25*
 - packet routing, 20–21
 - on the same subnet, 19–20
- Layer 3 roaming, 581–583, 966**
- Layer 7 classification, 382**
- Learn page, DevNet, 878**
- LHR (last-hop router), 966**
- link aggregation protocols, 106. *See also* EtherChannel bundle**
 - EtherChannel configuration, 107–108
 - LACP (Link Aggregation Control Protocol), 106–107
 - fast, 115*
 - interface priority, 118*
 - maximum number of EtherChannel member interfaces, 116–117*
 - minimum number of EtherChannel member interfaces, 115*
 - system priority, 117–118*
 - viewing neighbor information, 112–113*
 - viewing packet counters, 113–114*
 - PAgP (Port Aggregation Protocol), 106, 113
- link budget, 526–527**
- link-state algorithm, 130–131, 966. *See also* OSPF (Open Shortest Path First)**
- LISP (Cisco Locator/ID Separation Protocol), 495–496, 649, 966**
 - architecture
 - control plane, 497–498*
 - data plane, 498–499*
 - components, 496–497
 - data path, 501–502
 - map registration and notification, 499–500
 - map request and reply, 500–501
 - proxy ETR, 502–503
 - proxy ITR, 503–504
 - routing architecture, 497
- LLQ (low-latency queuing), 407–408**
- load balancing, 966**
 - EIGRP, 163
 - EtherChannel, 119–120
 - unequal-cost, 136–137
- local bridge identifier, 40, 966**
- Local SPAN (Switched Port Analyzer), 717**
 - configuration examples, 719–720

- specifying the destination port, 718–719
- specifying the source port, 717–718
- Local Web Authentication, 764–765**
- locating devices in a wireless network, 584–587
- logarithm, 521–522
- logging buffered ? command, 702
- logout-warning command, 802–803
- looking glasses, 301
- loop guard, 74
- loop prevention, BGP, 247–248
- loopback networks, OSPF, 196–198
- LSA/s (link-state advertisement/s), 172, 209–210**
 - age and flooding, 210
 - OSPFv3, 232
 - sequence, 210
 - type 1, 210–212
 - type 2, 213–214
 - type 3, 213–217
- LSDB (link-state database), 172**

M

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

MIMO (multiple-input, multiple-output) system, 535
minions, 909
misconfiguration, MST (Multiple Spanning Tree Protocol)
 trunk link pruning, 90–91
 VLAN assignment to the IST, 89–90
MLS (multilayer switch), 4
mobility domain, 967
mobility group, 583–584, 967
modulation, 532–533, 967
 DRS (dynamic rate shifting), 538–540
 spread spectrum, 532–533
module, 967
 Puppet, 903
 Python, 886–887
monitor session destination interface command, 718
MP-BGP (multiprotocol BGP), 277
MQC (Modular QoS CLI), 379–381
 class-based marking, 392–393
 classification configuration, 382–385
MR (map resolver), 967
MRC (maximal-ratio combining), 538, 967
MRIB (Multicast Routing Information Base), 968
MS (map server), 967
MST (Multiple Spanning Tree Protocol), 80, 967
 configuring, 84
 instance, 82
 IST (internal spanning tree), 83
 misconfigurations
 trunk link pruning, 90–91
 VLAN assignment to the IST, 89–90
 region boundary, 90–91

MST region as the root bridge, 91
 MST region not a root bridge for any VLAN, 91
 topologies, 82–83
 tuning, 87
 changing the interface cost, 88
 changing the interface priority, 88–89
 verification, 84–87
multi-area topology, OSPF, 206–207
multicast, 337, 342–343
 addressing, 340
 GLOP block, 342
 IANA-assigned addresses, 340–341
 internetwork control block, 341
 local network control block, 341
 organization-local scope addresses, 342
 Source Specific Multicast block, 342
 well-known reserved addresses, 341
 architecture, 338
 group address, 339
 IGMP, 343–344
 message format, 344–345
 snooping, 346–348
 version 2, 344
 version 3, 346
 Layer 2 addresses, 342–343
 PIM, 349
 bootstrap router, 366–367
 dense mode, 354–356
 designated routers, 359–360
 distribution trees, 349
 forwarder, 361–363

- messages*, 354
- RP*, 350–351, 363–365
- RPF*, 360–361
- shared and source path trees*, 357–358
- shared tree join*, 358
- shared trees*, 350–352
- source registration*, 358
- source trees*, 349–350
- sparse mode*, 357
- SPT switchover*, 358–359
- terminology*, 352–354
- state, 968
- stream, 339

N

NAC (network access control), 758

- 802.1x, 758
 - authentication process flow*, 759–760
 - components*, 758
 - EAP methods*, 760–762
 - roles*, 758–760
- Cisco IBNS 2.0, 766
- Cisco TrustSec, 766–767
 - egress enforcement*, 770–771
 - ingress classification*, 767–768
 - propagation*, 768–770
- Enhanced FlexAuth, 766
- MAB (MAC Authentication Bypass), 762–764
- Web Authentication, 764
 - Central*, 765
 - Local*, 764–765

name command, 8

named ACL, 784–785

narrowband transmission, 532, 968

NAT (Network Address Translation), 446–447, 968

- pooled, 447–455
- static
 - inside*, 449–452
 - outside*, 452–455
- topology, 447–449
- types of, 447

native VLANs, 14, 968

NBAR2 (Next-Generation Network-Based Application Recognition), 382

NDP (Cisco Network Data Platform), 657

neighbor distribute-list command, 307

neighbor state, BGP, 253

- Active, 254
- Connect, 254
- Established, 255
- Idle, 254
- OpenConfirm, 255
- OpenSent, 254–255

neighbors

- BGP, 249
- EIGRP, 160
- OSPF, 175–185
 - adjacency requirements*, 181
 - state fields*, 186
 - verifying*, 185–186

NETCONF, 872, 968

- capabilities, 874
- comparison with SNMP, 873
- datastores, 875
- element, 873
- operations, 874
- RPC message, 875–876
- save configuration, 876
- shopping list analogy, 873–874
- transactions, 873

NetFlow, 706, 968

- collected traffic types, 706
- configuring and verifying talkers, 708–709
- enabling on a device, 706–707
- Flexible, 709
 - applying the flow monitor to the interfaces, 715–716*
 - creating a custom flow record, 709–711*
 - creating a flow exporter, 711–712*
 - creating a flow monitor, 713–714*
 - mapping the flow exporter to the flow monitor, 714*
- flows, 706
- verification, 707–708

network area command, 178**Network Device API, 864–867****network/s. *See also* enterprise network architecture; QoS (quality of service); routing and routing protocols; VLANs (virtual LANs)****campus**

- Layer 2 access layer, 634–636*
- Layer 3 access layer, 636–637*
- SD-Access design, 640*
- simplified campus design, 637–639*
- three-tier design, 634*
- two-tier design, 632*

fabric, 642. *See also* SD-Access**hierarchical LAN design, 624–625**

- access layer, 625–627*
- core layer, 628–629*
- distribution layer, 627–628*

high availability, 629**latency, 374**

- jitter, 376*

*processing delay, 376**propagation delay, 375**serialization delay, 375***layer, SD-Access, 647–648****OSPF, 194***broadcast, 194–195**discontiguous, 217–218**loopback, 196–198**point-to-point, 195–196***OSPFv3, 239–240****outages, 854****overlay, 466. *See also* overlay tunnels****virtual private. *See* VPN (virtual private network)****next-generation firewall, 751****NFV (network functions virtualization), 833–834, 968. *See also* Cisco ENFV (Enterprise Network Functions Virtualization)****NFVIS (network function virtualization infrastructure software), 846–847****NLRI (Network Layer Reachability Information), 248****no switchport command, 23****noise/noise floor, 530, 968****nonce, 968****non-overlapping channel spacing, 518–519****northbound API, 855–856****NSSA (Not-So-Stubby Area), 217****NTP (Network Time Protocol), 420–421, 968–969****configuration, 421–422****peers, 424–425****stratum preference, 424****verification, 422–423****viewing associations, 423–424****numbered ACL, 782–783****numbered extended ACL, 783–784**



- ul style="list-style-type: none;">
- object tracking, 430, 436–438
- OFDM (orthogonal frequency division multiplexing), 533, 969
- OHAI, 906
- OIF (outgoing interface), 969
- omnidirectional antennas, 564–566, 969
- Open Authentication, 593–594, 969
- OpenConfirm state, BGP, 255
- OpenSent state, BGP, 254–255
- optimization, OSPF, link-cost, 189
- orchestrator, NFV, 836
- OSI (Open Systems Interconnection) model, 3–4
- OSPF (Open Shortest Path First)
 - ABR (area border router), 205–206
 - area, 173–174, 204–207
 - area ID, 207
 - BDR (backup designated router), 177–178
 - election*, 190–192
 - placement*, 192–194
 - configuration
 - for all interfaces*, 178–180
 - with explicit IP addresses*, 179
 - with explicit subnet*, 179
 - interface-specific*, 180–181
 - OSPF network statement*, 178
 - dead interval timer, 190, 689
 - debugging
 - debug ip ospf adj command*, 687, 690–691
 - debug ip ospf hello command*, 687–689, 690–691
 - ip ospf network broadcast command*, 689–690
 - show ip ospf interface command*, 689
 - show ip ospf neighbor command*, 686
 - default route advertisement, 187–188
 - DR (designated router), 176–178
 - election*, 190–192
 - placement*, 192–194
 - equal-cost multipathing, 220
 - hello packets, 175
 - hello time, 190, 689
 - inter-area routes, 207, 219
 - inter-router communication, 174
 - intra-area routes, 207, 218–219
 - LSA/s (link-state advertisement/s), 172, 209–210
 - age and flooding*, 210
 - sequences*, 210
 - type 1*, 210–212
 - type 2*, 213–214
 - type 3*, 213–217
 - LSDB (link-state database), 172, 204–205
 - multi-area topology, 206–207
 - neighbors, 175–185
 - adjacency requirements*, 181
 - state fields*, 186
 - network, 194
 - broadcast*, 194–195
 - discontiguous*, 217–218
 - loopback*, 196–198
 - point-to-point*, 195–196
 - optimization, link-cost, 189
 - packet types, 174
 - passive interfaces, 181
 - RID (router ID), 175, 180–181
 - route filtering, 224–225
 - area*, 225–227

- with summarization*, 225
- routing table, 208–209
- sample topology and configuration, 181–183
- SPT (shortest path tree), 172–173
- summarization, 220–222
 - inter-area*, 222, 223–224
 - metrics*, 222–223
- timers, 190
- verification
 - interface*, 184–185
 - neighbor adjacency*, 185–186
 - routes installed on the RIB*, 186–187
- versions, 170
- OSPFv3**, 230
 - communication, 232–233
 - configuration, 233–235
 - differences with OSPFv2, 231–232
 - IPv4 support, 240–242
 - IPv6 summarization, 238–239
 - LSAs (link-state advertisements), 232
 - network types, 239–240
 - passive interface, 237–238
 - verification, 235–237
- OSS (operations support system)**, 836
- OUI (organizationally unique identifier)**, 5
- outside static NAT**, 452–455
- overlay network/tunnels**, 466, 969
 - GRE (Generic Routing Encapsulation), 469
 - encapsulation*, 469
 - tunnel configuration*, 470–474
 - verification*, 474
 - IPsec, 475–476
 - authentication header*, 476
 - Cisco FlexVPN*, 486
 - DMVPN*, 486
 - encryption, hashing, and keying methods*, 478
 - ESP (Encapsulating Security Payload)*, 477–478
 - GET VPN*, 486
 - IKE (Internet Key Exchange)*, 480
 - IKEv1*, 480–482
 - IKEv2*, 482–484
 - remote access VPN*, 486
 - site-to-site GRE over*, 487–493
 - site-to-site VPN*, 486
 - site-to-site VTI over*, 493–495
 - transform set*, 478–480
 - VPN solutions*, 484–486
- LISP (Cisco Locator/ID Separation Protocol)**, 495–496
 - components*, 496–497
 - control plane*, 497–498
 - data path*, 501–502
 - data plane*, 498–499
 - map registration and notification*, 499–500
 - map request and reply*, 500–501
 - proxy ETR*, 502–503
 - proxy ITR*, 503–504
 - routing architecture*, 497
- recursive routing, 474–475
- VXLAN (Virtual eXtensible Local Area Network)**, 504–505, 507
 - control plane*, 506
 - VTEP*, 505–506
- OVS (Open vSwitch)**, 837
- OVS-DPDK**, 839–840

P

PA (path attribute), 247

packet/s

BGP, 252

EIGRP, 160

flow for virtualized systems, 837–839

loss, 376–377

OSPF, 174

OSPFv3, 232–233

routing, 20–21

VXLAN-GPO, 651

PACL (port ACL), 785–786

PAgP (Port Aggregation Protocol), 106

viewing neighbor information, 113

viewing packet counters, 114

parabolic dish antenna, 569–570, 969

passive interface, 969

OSPF, 181

OSPFv3, 237–238

passive-interface command, 237–238

password/s

encryption, 789–790

terminal line, 788–789, 790–793

types of, 789

PAT (Port Address Translation),
458–461, 970

patch antennas, 567–568, 970

path, 127

metrics

*EIGRP (Enhanced Interior
Gateway Routing Protocol),
160–163*

equal-cost multipathing, 135–136

*unequal-cost load balancing,
136–137*

selection, 132

Path Trace, 970

path vector algorithm, 131–132, 970

PBR (policy-based routing), 146–149

PCI passthrough, 840–841

Pearson Test Prep practice test, 927

accessing, 927–928

customizing your exams, 928–929

updating your exams, 929

peers, NTP (Network Time Protocol),
424–425

performance, VNF (virtual network
function), 836

PFS (Perfect Forward Secrecy), 482

phase, 519, 970

PHB (per-hop behavior), 387, 390–391,
970

Assured Forwarding, 388–390

Class Selector, 388

Default Forwarding, 388

Expedited Forwarding, 390

physical layer, SD-Access, 647

pillar, SaltStack, 909–910, 970

PIM (Protocol Independent Multicast),
337, 349

bootstrap router, 366–367

dense mode, 354–356

designated routers, 359–360

distribution tree, 349

shared tree, 350–352

source tree, 349–350

forwarder, 361–363

messages, 354

RP (rendezvous point), 350–351,
363–364

Auto-, 364

*candidate, 364–365,
366–367*

mapping agent, 365

static, 364

- RPF (Reverse Path Forwarding), 360–361
- shared and source path trees, 357–358
- shared tree join, 358
- source registration, 358
- sparse mode, 357
- SPT switchover, 358–359
- terminology, 352–354
- ping command, 675–676**
 - extended, 677–680
 - repeat option, 676–677
- playbooks, 913–914, 917–930, 970**
- point-to-point networks, OSPF, 195–196**
- polar plot, 970**
- polarization, 563–564, 970**
- policer**
 - class-based, 398
 - markdown, 395
 - placing in the network, 395
 - single-rate three-color, 399–400
 - single-rate two-color, 399–400
 - token bucket algorithm, 395–397
 - two-rate three-color, 403–405
- policy/ies**
 - based routing, 147, 970
 - CoPP. *See* CoPP (Control Plane Policing)
 - maps, 379–381
 - MQC (Modular QoS CLI), 379–381
 - plane, SD-Access, 651–652
 - SD-WAN, 665
 - service, 379
 - tag, 558
 - workflow, Cisco DNA, 658–659
- pooled NAT, 447–455, 970**
- port-channel min-links command, 115**
- portfast, 68–70**
- port/s**
 - access, 11–12
 - auxiliary, 802
 - switch, viewing the status, 17–19
 - trunk, 12
 - displaying information about, 13*
 - verifying status, 13–14*
- Postman, 857, 858**
 - collections, 858–859
 - dashboard, 857
 - History tab, 858
 - URL bar, 859–860
- power**
 - comparing against a reference, 524–525
 - dB (decibel), 522, 523–524
 - Law of 3s, 522–523*
 - Law of 10s, 523*
 - Law of Zero, 522*
 - dBm (dB-milliwatt), 525
 - effective isotropic radiated, 526
 - measuring changes along a signal path, 525–527
 - RF signal, 521
 - RSSI (received signal strength indicator), 530–531
- PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) lifecycle, 913**
- PQ (priority queuing), 407**
- prefix length, 132, 133, 970**
- prefix list, 299, 308, 970**
- prefix matching, 297–299**
 - IPv6 prefix list, 299–300
 - prefix list, 299
- pre-shared key authentication, 595–597**
- private community, BGP, 314, 317–318**

privilege level, IOS XE, 793–796, 971
 Probe Request, 587
 process switching, 26–27
 processing delay, 376
 propagation delay, 375
 protocol, network, 3
 proxy ETR, 971
 proxy ITR, 971
 PTK (Pairwise Transient Key), 598
 PTP (Precision Time Protocol), 425–426, 970
 configuration, 427–429
 Event message types, 426
 General message types, 426
Puppet, 902
 agent/server communication, 902
 comparison with Chef, 906
 components, 902
 Forge, 904
 installation modes, 903
 manifest, 903–904
 module, 903
Puppet Bolt, 922
 command line, 922–923
 tasks, 922, 923
push model, 904
 PVST (Per-VLAN Spanning Tree), 81–82, 971
Python, 911, 971
 functions, 888
 module, 886–887
 scripts
 conditions, 885
 dictionary, 885
 Env_Lab.py script, 882–885
 get_dnac_devices.py, 885–889
 quotation marks, 884
 strings, 884

Q

QAM (quadrature amplitude modulation), 533, 971
QoS (quality of service)
 CBWFQ (class-based weighted fair queuing), configuring, 410–414
 classification, 381–382
 configuring, 382–385
 Layer 7, 382
 congestion avoidance, 408–410
 congestion management, 406–408
 CoPP (Control Plane Policing), 817–818
 DiffServ, 379
 IntServ, 377–378
 marking, 385
 class-based, 392–393
 Layer 2, 385–386
 Layer 3, 386–387
 PCP (Priority Code Point), 386
 MQC framework, 379–381
 need for, 374
 jitter, 376
 lack of bandwidth, 374
 latency, 374–375
 packet loss, 376–377
 processing delay, 376
 propagation delay, 375
 serialization delay, 375
 PHB (per-hop behavior), 387
 Assured Forwarding, 388–390
 Class Selector, 388
 Default Forwarding, 388
 Expedited Forwarding, 390
 policers and shapers
 class-based, 398

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

scavenger class, 391
 trust boundary, 391–392
 wireless, 393–394

queuing algorithm, 406–408

R

radiation pattern, 560–562, 971

radio chain, 535

Radioactive Trace, 615–616

RADIUS, 971

RD (reported distance), 158

reactor, 909

receiver. *See also* antenna/s

power level, 530–531
 sensitivity level, 530

recipe, 906, 971

recursive static route, 139–140,
 474–475, 971

regex (regular expressions), 300–301,
 972

Remote SPAN (Switched Port
 Analyzer), 720–722

remote VPN access, 486

remote-span command, 721

reported distance, 972

REST (Representational State Transfer)
 API, 856

RESTCONF, 876–877, 972

RF (radio frequency), 516, 971. *See
 also* antenna/s
 2.4 GHz band, 516

5 GHz band, 516

6 GHz band, 516

amplitude, 520

carrier signal, 531

channels, 517

fingerprinting, 586, 972

modulation, 532–533

DRS (dynamic rate shifting),
 538–540

spread spectrum, 532–533

MRC (maximal-ratio combining), 538

narrowband transmissions, 532

noise/noise floor, 530

non-overlapping channel spacing,
 518–519

phase, 519

power, 521

signal bandwidth, 517–518

SNR (signal-to-noise ratio), 530–531

spatial multiplexing, 535–536

tag, 558

TBF (transmit beamforming), 536–538

W (watts), 521

wavelength, 519–520

RFID tag, 587

RIB (Routing Information Base), 132,
 134–135, 972

BGP, 262

verifying installed routes, 186–187

RID (router ID), 175, 180–181, 972

roaming

between autonomous APs, 574–576

intercontroller, 579

intracontroller, 577–579

Layer 2, 579–580

Layer 3, 581–583

rogue device, locating, 587

root bridge, 39, 60–63, 972

- root bridge identifier, 40, 972
- root guard, 68, 972
- root path cost, 40, 972
- root port, 972
- round robin, 406
- route aggregation, BGP
 - with AS_SET, 276–277
 - aggregate-address command, 267–274
- route filtering, 306–307
 - AS_Path ACL filtering, 309–311
 - distribute lists, 307
 - OSPF, 224–225
 - area*, 225–227
 - with summarization*, 225
 - prefix lists, 308
 - route maps, 311–313
- route map, 301–302, 972
 - command syntax, 301
 - complex matching, 304
 - components, 301
 - conditional match options, 302–303
 - continue keyword, 305–306
 - multiple conditional match conditions, 303–304
 - optional actions, 304–305
 - route filtering, 311–313
- route summarization
 - BGP, 274–276, 282–285
 - EIGRP, 166–167
 - OSPF, 220–222
 - inter-area*, 222, 223–224
 - metrics*, 222–223
- router ospf command, 178
- routing and routing protocols. *See also*
 - distance vector algorithm; enhanced distance vector algorithm; link-state algorithm; VRF (virtual routing and forwarding)
 - AD (administrative distance), 132, 133–135
 - deterministic, 293–294
 - distance vector algorithm, 128–129
 - dynamic, 126–128
 - enhanced distance vector algorithm, 129–130
 - FIB (Forwarding Information Base), 132
 - hybrid, 129
 - link-state algorithm, 130–131
 - metric, 132
 - path selection, 132
 - path vector algorithm, 131–132
 - policy-based, 146–149
 - prefix length, 132, 133
 - recursive, 474–475
 - RIB (Routing Information Base), 132, 134–135
 - static, 137
 - directly attached*, 138–139
 - floating*, 141–143
 - fully specified*, 141
 - IPv6*, 145–146
 - to null interfaces*, 143–145
 - recursive*, 139–140
 - table, 133, 208–209
- RP (rendezvous point), 350–351, 363–364, 972
 - Auto-, 364
 - candidate, 364–365, 366–367
 - mapping agents, 365
 - static, 364
- RP (route processor) engine, 28
- RPF (Reverse Path Forwarding), 360–361
- RSSI (received signal strength indicator), 530–531, 585, 971

RSTP (Rapid Spanning Tree Protocol),
36, 53–54

building the topology, 55

convergence, 55

port roles, 54

port states, 54

port types, 54–55

RSVP (Resource Reservation Protocol),
377–378

RTLS (real-time location services),
585–587

Ruby, 906. *See also* Chef

S

SaaS (software as a service), Cloud
OnRamp, 666–668

SAE (Simultaneous Authentication of
Equals), 595

Salt SSH, 923–924

SaltStack, 909

0MQ, 909

beacon, 909

commands, 910–911

grain, 909–910

jobs, 909

minion, 909

pillar, 909–910

reactor, 909

remote execution system, 909

scaling, 910

satellite communication, latency, 375

save configuration, NETCONF, 876

scalable group, 655–656

scaling, SaltStack, 910

scavenger class, 391

script

Python

conditions, 885

dictionary, 885

Env_Lab.py, 882–885

get_dnac_devices.py, 885–889

quotation marks, 884

strings, 884

Tcl, 899–901

SD-Access, 506–507, 643–646

anycast gateway, 656

architecture, 646–647

network layer, 647–648

physical layer, 647

underlay network, 648–649

campus fabric, 646

components, 646

controller layer, 656–657

fabric, 649

control plane, 649–650

control plane nodes, 653–654

data plane, 650–651

device roles, 652

edge nodes, 652–653

policy plane, 651–652

WLC (wireless LAN controller),
654

host pool, 655

scalable group, 655–656

VN (virtual network), 655

SDM (Switching Database Manager)
templates, 30–32

sdm prefer command, 30

SD-WAN, 661. *See also* Cisco SD-WAN

segmentation, 973

sensitivity level, 530, 973

serialization delay, 375

server/s

bare-metal, 828

- Chef, 906
- looking glass, 301
- virtualization, 826, 828
- VTP, 97
- service chaining, 973
- service policy, 379
- service-policy command, 380
- session, BGP, 249–250
 - eBGP*, 251
 - iBGP*, 250–251
- SGTs (Scalable Group Tags), 650, 973
- shapers. *See* policers; QoS (quality of service), policers and shapers
- shared trees, 350–352
- show bgp ipv4 unicast command, 263–265, 267–268
- show bgp ipv4 unicast neighbors command, 258–260
- show bgp ipv4 unicast summary command, 257
- show bgp ipv6 unicast neighbors command, 281
- show bgp ipv6 unicast summary command, 281–282
- show bgp summary command, 257
- show etherchannel load-balance command, 120
- show etherchannel port command, 110–112
- show etherchannel summary command, 108–109
- show flow monitor command, 714
- show flow record command, 710–711
- show glbp command, 443–444
- show interface port-channel command, 110
- show interfaces status command, 18–19, 71
- show interfaces switchport command, 17–18
- show interfaces trunk command, 13–14, 103
- show ip arp command, 20
- show ip flow export command, 707–708
- show ip interface brief command, 23–24
- show ip nat translations command, 450–452
- show ip ospf database summary command, 215
- show ip ospf interface command, 184–185, 689
- show ip ospf neighbor command, 186, 686
- show ip route bgp command, 265
- show ip route command, 137, 139, 266–267, 448
- show ip route ospf command, 187
- show ipv6 interface brief command, 24–25
- show ipv6 route command, 146
- show ipv6 route ospf command, 237, 238, 239
- show lacp counters command, 113–114
- show lacp neighbor command, 112–113
- show lacp sys-id command, 117–118
- show logging command, 703–704
- show mac address-table dynamic command, 15–16
- show monitor session erspan-source session command, 723–724
- show ntp associations command, 423–424
- show ntp status command, 422–423

- show ospfv3 interface command, 236, 240
- show ospfv3 ipv6 neighbor command, 236
- show pagp counters command, 114
- show pagp neighbor command, 113
- show running-config command, 270–271
- show sdm prefer command, 31–32
- show spanning-tree command, 85–86
- show spanning-tree inconsistentports command, 74
- show spanning-tree interface command, 48–49, 70–71, 73
- show spanning-tree mst command, 86–87, 88
- show spanning-tree mst configuration command, 84–85
- show spanning-tree mst interface command, 87
- show spanning-tree root command, 42–45
- show spanning-tree vlan command, 45–47, 61–62, 64–66
- show spanning-tree vlan detail command, 49–50
- show standby command, 435–438
- show track command, 431–432
- show uddl neighbors command, 75–76
- show vlan command, 9–11
- show vrrp brief command, 441
- show vrrp command, 439
- show vtp status command, 99–101
- signal bandwidth, 517–518
- single-rate three-color policer, 399–400
- single-rate two-color policer, 399–400
- SISO (single-in, single-out) system, 535
- site tag, 558
- site-to-site VPN, 486
 - GRE over IPsec, 487–493
 - VTI over IPsec, 493–495
- SLA (service-level agreement), 375. *See also* IP SLA
- SNMP (Simple Network Management Protocol), 695, 973
 - comparison with NETCONF, 873
 - configuration, 699–700
 - MIB (Management Information Base), 695, 697–699
 - operations, 696
 - trap, 695
 - version comparison, 695–696
- snmp-server enable traps command, 700
- SNR (signal-to-noise ratio), 530–531, 973
- soft reset, BGP, 313
- software, CEF (Cisco Express Forwarding), 29–30
- source tree, 349–350
- southbound API, 856
- SP (service provider), BGP multihoming, 291–292
- SPAN (Switched Port Analyzer), 716–717, 973
 - Encapsulated Remote, 722
 - specifying the destination ports,* 723–724
 - specifying the source ports,* 722–723
 - Local, 717
 - configuration examples,* 719–720
 - specifying the destination ports,* 718–719
 - specifying the source ports,* 717–718
 - Remote, 720–722, 973

- spanning-tree bpdupfilter enable command, 72
- spanning-tree guard root command, 68
- spanning-tree mode mst command, 84
- spanning-tree pathcost method long command, 41
- spanning-tree portfast bpduguard default command, 70
- spanning-tree portfast command, 68–70
- spanning-tree vlan forward-time command, 40
- spanning-tree vlan hello-time command, 40
- spanning-tree vlan max-age command, 40
- spanning-tree vlan priority command, 60
- spanning-tree vlan root command, 60
- spatial multiplexing, 535–536, 973
- split-MAC architecture, 547, 974
- spread spectrum, 532–533, 974
- SPT (shortest path tree), 973
- SR-IOV, 841–842
- SSH (Secure Shell), 800–802, 973
- standard ACL, 295–296
- state machine, Cisco lightweight AP, 552–554
- static NAT, 974
 - inside, 449–452
 - outside, 452–455
- static null route, 974
- static route, 137
 - directly attached, 138–139
 - floating, 141–143
 - fully specified, 141
 - IPv6, 145–146
 - to null interfaces, 143–145
 - recursive, 139–140
- static RP (rendezvous point), 364
- STP (Spanning Tree Protocol), 36, 67–68. *See also* MST (Multiple Spanning Tree Protocol); RSTP (Rapid Spanning Tree Protocol)
 - 802.1D, 38
 - BPDUs (bridge protocol data unit)*, 40
 - configuration BPDUs*, 40
 - forward delay*, 40
 - hello time*, 40
 - local bridge identifier*, 40
 - max age*, 40
 - path cost*, 41
 - port states*, 39
 - port types*, 39
 - root bridge*, 39
 - root bridge identifier*, 40
 - root path cost*, 40
 - system ID extension*, 40
 - system priority*, 40
 - TCN (topology change notification) BPDUs*, 40
- BPDUs filter, 72–73
- BPDUs guard, 70–72
- building the topology, 41
 - locating blocked designated switch ports*, 45–47
 - locating root ports*, 44–45
 - root bridge election*, 41–44
 - verification of VLANs on trunk links*, 48–49
- Error Recovery Service, 71–72
- loop guard, 74
- modifying port priority, 66–67
- modifying root port and blocked switch port locations, 63–66
- placing the root bridge, 60–63
- portfast, 68–70

- problems with unidirectional links, 73
- root guard, 68
- topology changes, 49–50
 - converging with direct link failures*, 50–52
 - indirect failures*, 52–53
- UDLD (Unidirectional Link Detection), 75–76
- stratum, 421, 974
- streaming, 339
- string, 884
- Stubby area, OSPF, 217
- subnet, 127
- successor/successor route, 158
- summarization, 974. *See also* route summarization
 - IPv6, 238–239
 - OSPF, 220–222
 - inter-area*, 222, 223–224
 - metrics*, 222–223
- supplicant, 974
- SVI (switched virtual interface), IP addressing, 23
- switch, 5. *See also* VLANs (virtual LANs)
 - collision domain, 5–6
 - multilayer, 4
 - port, viewing the status, 17–19
 - TCAM (ternary content addressable memory), 27–28
 - virtual, 831–833
- switchport access vlan command, 12
- switchport mode access command, 12
- switchport mode trunk command, 12
- switchport trunk allowed vlan command, 14–15
- switchport trunk native vlan command, 14
- syslog, 701, 974

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

T

- TACACS+, 803–804, 805, 974
- Talos, 741–742
- tasks, Puppet Bolt, 922, 923
- TBF (transmit beamforming), 536–538, 975
- Tc (committed time interval), 395
- TCAM (ternary content addressable memory), 27–28, 975
- Tcl, 899–901, 974
- TCN (topology change notification) BPDU, 40, 975
- TCP (Transmission Control Protocol), 249
- TCP/IP (Transmission Control Protocol/Internet Protocol), 3
- Technologies page, DevNet, 878
- Telnet, 974
- template, SDM (Switching Database Manager), 30–32
- terminal line
 - controlling access
 - using ACLs*, 796–797
 - using transport input command*, 797–800
 - line local username and password authentication, 790–793
 - password protection, 788–789

time synchronization, 420

NTP (Network Time Protocol),
420–421
 configuration, 421–422
 peers, 424–425
 stratum preference, 424
 verification, 422–423
 viewing associations, 423–424

PTP (Precision Time Protocol),
425–426
 configuration, 427–429
 Event message types, 426
 General message types, 426

timer

EIGRP, 164
OSPF, 190

Token API, 862–864**token bucket algorithm, 395–397****tools. *See also* automation tools;
commands****diagnostic**

IP SLA, 724–726
ping command, 675–680
traceroute command, 680–685

EEM (Embedded Event Manager), 901

applets, 895
debugging, 896–898
email variables, 899
event detector, 894–895
syslog applet, 896
WR MEM applet, 898

Postman, 857, 858

collections, 858–859
dashboard, 857
History tab, 850–858
URL bar, 859–860

Puppet, 902

agent/server communication,
902

components, 902

installation modes, 903

manifest, 903–904

module, 903

SaltStack, 909

0MQ, 909

beacon, 909

commands, 910–911

grain, 909–910

jobs, 909

minion, 909

pillar, 909–910

reactor, 909

remote execution system, 909

scaling, 910

topology/ies. *See also* convergence

MST (Multiple Spanning Tree Protocol), 82–83

NAT (Network Address Translation),
447–449

OSPF (Open Shortest Path First),
181–183

area, 204–207

multi-area, 206–207

OSPFv3, 233

table, 159–160, 975

ToS (Type of Service), 975**Totally Stubby area, 217****traceroute command, 448, 680–683**

extended, 684–685

options, 683

transform sets, IPsec, 478–480**transit routing, 975**

branch, 293–295

Internet, 292–293

transport input command, 797–800

troubleshooting. *See also* Cisco DNA Center Assurance; diagnostic tools
 EtherChannel bundle, 118–119
 Layer 2 forwarding, 16
 tools. *See* diagnostic tools
 wireless, 610–611
 wireless connectivity, 610–611
 at the AP, 617–620
 from the WLC, 611–616

trunk port, 12, 975
 configuring, 13
 displaying information about, 13
 verifying status, 13–14

trust boundary, 391–392

tuning, MST (Multiple Spanning Tree Protocol), 87
 changing the interface cost, 88
 changing the interface priority, 88–89

tunnel mode ipsec command, 493

tunnels. *See* overlay tunnels

two-rate three-color policers, 403–405

type 1 LSA, 210–212

type 2 LSA, 213–214

type 3 LSA, 213–217

U

UDLD (Unidirectional Link Detection), 75–76, 975

udld enable command, 75

Umbrella, 744–745

undebg interface loopback0 command, 695

underlay network, 648–649, 975

unequal-cost load balancing, 136–137, 975

unicast, 338

unknown unicast flooding, 6

uplink MACsec, 774

upstream, 975

user space, 837

username, creating, 790

V

VACL (VLAN ACL), 786–788

vAnalytics, 664

variables, EEM email, 899

variance value, 163, 976

vBond orchestrator, 662–663

verifying
 AAA (authentication, authorization, and accounting), 809
 BGP session, 257–260
 CoPP (Control Plane Policing), 820–822
 EAP-based authentication, 602
 EtherChannel status, 108–110
 GLBP (Gateway Load Balancing Protocol), 443–444
 GRE tunnels, 474
 IP address, 23–25
 line local username and password authentication, 792–793
 MST (Multiple Spanning Tree Protocol), 84–87
 NetFlow, 707–708
 NTP (Network Time Protocol), 422–423
 OSPF (Open Shortest Path First)
 interfaces, 184–185
 neighbor adjacencies, 185–186
 routes installed on the RIB, 186–187
 OSPFv3, 235–237
 trunk port status, 13–14
 VLAN on trunk links, 48–49

- VRRP (Virtual Router Redundancy Protocol), 439
- VTP (VLAN Trunking Protocol), 99–100
 - creating VLANs on the VTP domain server, 100*
 - with a transparent switch, 101*
- ZBFW (Zone-Based Firewall), 816–817
- viewing
 - NTP associations, 423–424
 - VLAN port assignments, 9–10
- VIM (Virtualized Infrastructure Manager), 834–835
- virtualization, 826, 828. *See also* NFV (network functions virtualization)
- vlan command, 8
- VLAN (virtual LAN), 7, 976
 - access port, 11–12
 - allowed, 14–15
 - creating, 8
 - loop prevention, 634–636
 - native, 14
 - packet structure, 8
 - viewing port assignments, 9–10
- vManage NMS, 663
- VM (virtual machine), 828, 976
 - comparison with containers, 830–831
 - guest OS, 830
 - hypervisor, 828–829
 - migration, 829–830
 - packet flow, 837–839
- VN (virtual network), 655, 976
- VNFs (virtual network functions), 834–836, 840–847
 - EM (element manager), 835
 - performance, 836
 - VIM (Virtualized Infrastructure Manager), 834–835
- VPN (virtual private network), 466, 976. *See also* overlay tunnels
 - Cisco Dynamic Multipoint, 486
 - Cisco Group Encrypted Transport, 486
 - IPsec, 484
 - remote access, 486
 - site-to-site, 486
- VRF (virtual routing and forwarding), 149–151
- VRRP (Virtual Router Redundancy Protocol), 438
 - configuration
 - legacy, 439*
 - version 2, 438*
 - version 3, 440–441*
 - viewing the status, 439
- vSmart controllers, 663
- vSwitch, 831–833, 976
- VTEP (virtual tunnel endpoint), 505–506, 976
- VTP (VLAN Trunking Protocol), 96–97, 976
 - communication, 97
 - configuring, 98–99
 - servers, 97
 - verification, 99–100
 - creating VLANs on the VTP domain server, 100*
 - with a transparent switch, 101*
 - versions, 97
- vtp domain command, 98–99
- vtp mode command, 98–99
- vtp password command, 98–99
- vtp version command, 98–99
- vty line. *See also* terminal line
 - controlling access
 - using ACLs, 796–797*

using transport input command,
797–800

SSH (Secure Shell), 800–802

VXLAN (Virtual eXtensible Local Area Network), 504–505, 507, 650, 976

control plane, 506

VTEP, 505–506

W

W (watt), 521

WAN, 642

wave propagation, 513–514

wavelength, 519–520, 977

Web Authentication, 603, 764, 976

Central, 765

Local, 764–765

wireless authentication, 603–606

well-known communities, BGP, 314

WFQ (weighted fair queuing), 407

wide metric, 162, 977

Wi-Fi, 533, 534

wildcard mask, 782

wireless networks and theory. *See*
also Cisco lightweight APs; Cisco
wireless deployments; power

antenna/s, 309–311

beamwidth, 563

directional, 567–570

EIRP (effective isotropic radiated power), 526

free space path loss, 527–529

gain, 525–526, 562

isotropic, 526

link budget, 526–527

omnidirectional, 564–566

parabolic dish, 569–570

patch, 567–568

polarization, 563–564

RSSI (received signal strength indicator), 530–531

wave propagation, 513–514

Yagi, 565–569

AP

autonomous, 545–546

Cisco, 547–548

client density, 559–560

authentication, 593

EAP, 597–602

Open Authentication, 593–594

pre-shared key, 595–597

WebAuth, 603–606

BSS (basic service set), 592

device location, 584–587

frequency, 514–515

power

comparing against a reference,
524–525

dB (decibel), 522–524

dBm (dB-milliwatt), 525

*measuring changes along a sig-
nal path*, 525–527

RF signal, 521

QoS (quality of service), 393–394

radio chain, 535

RF (radio frequency), 516

2.4 GHz band, 516

5 GHz band, 516

6 GHz band, 516

amplitude, 520

carrier signal, 531–532

channels, 517

modulation, 532–533

MRC (maximal-ratio combining),
538

narrowband transmissions, 532
noise/noise floor, 530
non-overlapping channel spacing, 518–519
phase, 519
power, 521
signal bandwidth, 517–518
SNR (signal-to-noise ratio), 530–531
spread spectrum, 532–533
TBF (transmit beamforming), 536–538
W (watts), 521
 roaming
 between autonomous APs, 574–576
 intercontroller, 579
 intracontroller, 577–579
 Layer 2, 579–580
 Layer 3, 581–583
 rope analogy, 512–513
 spatial multiplexing, 535–536
 troubleshooting connectivity issues, 610–611
 at the AP, 617–620
 from the WLC, 611–616
 wavelength, 519–520
WLC (wireless LAN controller), 276–277, 545, 977. *See also* Cisco lightweight APs
 fabric, 654
 mobility groups, 583–584
 pairing with a lightweight AP, 552
 split-MAC architecture, 547
 troubleshooting client connectivity issues, 611–613

checking the AP properties, 614–615
 checking the client's association and signal status, 613
 checking the client's properties, 614
 Radioactive Trace, 615–616
WPA (Wi-Fi Protected Access), 595–597, 977
WR MEM applet, 898
WRED (weighed random early detection), 390
WRR (weighted round robin), 406

X-Y

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

Z

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

This page intentionally left blank



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

APPENDIX B

Memory Tables

Chapter 7

Table 7-2 EIGRP Terminology

Term	Definition
	The route with the lowest path metric to reach a destination. The successor route for R1 to reach 10.4.4.0/24 on R4 is R1→R3→R4.
Successor	
	The metric value for the lowest-metric path to reach a destination. The feasible distance is calculated locally using the formula shown in the “Path Metric Calculation” section, later in this chapter. The FD calculated by R1 for the 10.4.4.0/24 network is 3328 (that is, 256+256+2816).
	The distance reported by a router to reach a prefix. The reported distance value is the feasible distance for the advertising router. R3 advertises the 10.4.4.0/24 prefix with an RD of 3072. R4 advertises the 10.4.4.0/24 to R1 and R2 with an RD of 2816.
Feasibility condition	
Feasible successor	A route that satisfies the feasibility condition and is maintained as a backup route. The feasibility condition ensures that the backup route is loop free. The route R1→R4 is the feasible successor because the RD 2816 is lower than the FD 3328 for the R1→R3→R4 path.

Table 7-3 EIGRP Packet Types

Opcode Value	Packet Type	Function
1		Used to transmit routing and reachability information with other EIGRP neighbors
2	Request	
3	Query	
4	Reply	
5		Used for discovery of EIGRP neighbors and for detecting when a neighbor is no longer available

Chapter 8

Table 8-2 OSPF Packet Types

Type	Packet Name	Functional Overview
1		These packets are for discovering and maintaining neighbors. Packets are sent out periodically on all OSPF interfaces to discover new neighbors while ensuring that other adjacent neighbors are still online.
2		These packets are for summarizing database contents. Packets are exchanged when an OSPF adjacency is first being formed. These packets are used to describe the contents of the LSDB.
3		These packets are for database downloads. When a router thinks that part of its LSDB is stale, it may request a portion of a neighbor's database by using this packet type.
4		These packets are for database updates. This is an explicit LSA for a specific network link and normally is sent in direct response to an LSR.
5		These packets are for flooding acknowledgment. These packets are sent in response to the flooding of LSAs, thus making flooding a reliable transport feature.

Table 8-9 OSPF Network Types

Type	Description	DR/BDR Field in OSPF Hellos	Timers
	Default setting on OSPF-enabled Ethernet links.	Yes	
	Default setting on OSPF-enabled Frame Relay main interface or Frame Relay multipoint subinterfaces.		Hello: 30 Wait: 120 Dead: 120
Point-to-point	Default setting on OSPF-enabled Frame Relay point-to-point subinterfaces.		
	Not enabled by default on any interface type. Interface is advertised as a host route (/32) and sets the next-hop address to the outbound interface. Primarily used for hub-and-spoke topologies.	No	Hello: 30 Wait: 120 Dead: 120
Loopback		N/A	N/A

Chapter 13

Table 13-2 IP Multicast Addresses Assigned by IANA

Designation	Multicast Address Range
Local network control block	
Internetwork control block	
Ad hoc block I	224.0.2.0 to 224.0.255.255
Reserved	224.1.0.0 to 224.1.255.255
SDP/SAP block	224.2.0.0 to 224.2.255.255
Ad hoc block II	224.3.0.0 to 224.4.255.255
Reserved	224.5.0.0 to 224.255.255.255
Reserved	225.0.0.0 to 231.255.255.255
	232.0.0.0 to 232.255.255.255
GLOP block	233.0.0.0 to 233.251.255.255
Ad hoc block III	233.252.0.0 to 233.255.255.255
Reserved	234.0.0.0 to 238.255.255.255
Administratively scoped block	

Table 13-3 Well-Known Reserved Multicast Addresses

IP Multicast Address	Description
224.0.0.0	Base address (reserved)
224.0.0.1	All hosts in this subnet (all-hosts group)
224.0.0.2	All routers in this subnet
224.0.0.5	All OSPF routers (AllSPFRouters)
224.0.0.6	All OSPF DRs (AllDRouters)
224.0.0.9	All RIPv2 routers
224.0.0.10	All EIGRP routers
	All PIM routers
224.0.0.18	VRRP
	IGMPv3
224.0.0.102	HSRPv2 and GLBP
224.0.1.1	NTP
	Cisco-RP-Announce (Auto-RP)
	Cisco-RP-Discovery (Auto-RP)

The IGMP message format fields are defined as follows:

- **Type:** This field describes five different types of IGMP messages used by routers and receivers:
 - _____ (type value 0x16) is a message type also commonly referred to as an IGMP join; it is used by receivers to join a multicast group or to respond to a local router's membership query message.

- **Version 1 membership report** (type value 0x12) is used by receivers for backward compatibility with IGMPv1.
- **Version 2 leave group** (type value 0x17) is used by receivers to indicate they want to stop receiving multicast traffic for a group they joined.
- _____ (type value 0x11) is sent periodically to the all-hosts group address 224.0.0.1 to see whether there are any receivers in the attached subnet. It sets the group address field to 0.0.0.0.
- **Group specific query** (type value 0x11) is sent in response to a leave group message to the group address the receiver requested to leave. The group address is the destination IP address of the IP packet and the group address field.
- _____: This field is set only in general and group-specific membership query messages (type value 0x11); it specifies the maximum allowed time before sending a responding report in units of one-tenth of a second. In all other messages, it is set to 0x00 by the sender and ignored by receivers.
- _____: This field is the 16-bit 1s complement of the 1s complement sum of the IGMP message. This is the standard checksum algorithm used by TCP/IP.
- _____: This field is set to 0.0.0.0 in general query messages and is set to the group address in group-specific messages. Membership report messages carry the address of the group being reported in this field; group leave messages carry the address of the group being left in this field.

The following list defines the common PIM terminology illustrated in Figure 13-14:

- **Reverse Path Forwarding (RPF) interface:** _____

- **RPF neighbor:** _____

- _____: Toward the source of the tree, which could be the actual source in source-based trees or the RP in shared trees. A PIM join travels upstream toward the source.
- _____: The interface toward the source of the tree. It is also known as the RPF interface or the incoming interface (IIF). An example of an upstream interface is R5's Te0/1/2 interface, which can send PIM joins upstream to its RPF neighbor.

- _____ : Away from the source of the tree and toward the receivers.
- _____ : Any interface that is used to forward multicast traffic down the tree, also known as an outgoing interface (OIF). An example of a downstream interface is R1's Te0/0/0 interface, which forwards multicast traffic to R3's Te0/0/1 interface.
- _____ : The only type of interface that can accept multicast traffic coming from the source, which is the same as the RPF interface. An example of this type of interface is Te0/0/1 on R3 because the shortest path to the source is known through this interface.
- _____ : Any interface that is used to forward multicast traffic down the tree, also known as the downstream interface.
- _____ : A group of OIFs that are forwarding multicast traffic to the same group. An example of this is R1's Te0/0/0 and Te0/0/1 interfaces sending multicast traffic downstream to R3 and R4 for the same multicast group.
- **Last-hop router (LHR):** _____
- _____
- **First-hop router (FHR):** _____
- _____
- _____ : A topology table that is also known as the multicast route table (mroute), which derives from the unicast routing table and PIM. MRIB contains the source S, group G, incoming interfaces (IIF), outgoing interfaces (OIFs), and RPF neighbor information for each multicast route as well as other multicast-related information.
- _____ : A forwarding table that uses the MRIB to program multicast forwarding information in hardware for faster forwarding.
- _____ : The multicast traffic forwarding state that is used by a router to forward multicast traffic. The multicast state is composed of the entries found in the mroute table (S, G, IIF, OIF, and so on).

There are currently five PIM operating modes:

- _____
- _____
- _____
- _____
- _____

Table 13-4 PIM Control Message Types

Type	Message Type	Destination	PIM Protocol
0		224.0.0.13 (all PIM routers)	PIM-SM, PIM-DM, Bidir-PIM, and SSM
1	Register	RP address (unicast)	PIM-SM
2	Register stop	First-hop router (unicast)	PIM SM
3		224.0.0.13 (all PIM routers)	PIM-SM, Bidir-PIM, and SSM
4	Bootstrap	224.0.0.13 (all PIM routers)	PIM-SM and Bidir-PIM
5	Assert	224.0.0.13 (all PIM routers)	PIM-SM, PIM-DM, and Bidir-PIM
8		Bootstrap router (BSR) address (unicast to BSR)	PIM-SM and Bidir-PIM
9	State refresh	224.0.0.13 (all PIM routers)	PIM-DM
10	DF election	224.0.0.13 (all PIM routers)	Bidir-PIM

B

Chapter 14

There are three different QoS implementation models:

- _____: QoS is not enabled for this model. It is used for traffic that does not require any special treatment.
- _____: Applications signal the network to make a bandwidth reservation and to indicate that they require special QoS treatment.
- _____: The network identifies classes that require special QoS treatment.

The following traffic descriptors are typically used for classification:

- **Internal:** QoS groups (locally significant to a router)
- **Layer 1:** Physical interface, subinterface, or port
- **Layer 2:** _____
- **Layer 2.5:** MPLS experimental (EXP) bits
- **Layer 3:** _____
- **Layer 4:** _____
- **Layer 7:** _____

The following traffic descriptors are used for marking traffic:

- **Internal:** QoS groups
- _____: 802.1Q/p Class of Service (CoS) bits

- **Layer 2.5: MPLS Experimental (EXP) bits**
- _____: Differentiated Services Code Points (DSCP) and IP Precedence (IPP)

The TCI field is a 16-bit field composed of the following three fields:

- _____ (PCP) field (3 bits)
- _____ (DEI) field (1 bit)
- _____ (VLAN ID) field (12 bits)

Four PHBs have been defined and characterized for general use:

- _____: The first 3 bits of the DSCP field are used as CS bits. The CS bits make DSCP backward compatible with IP Precedence because IP Precedence uses the same 3 bits to determine class.
- _____: Used for best-effort service.
- _____: Used for guaranteed bandwidth service.
- **Expedited Forwarding (EF) PHB:** _____

Cisco IOS policers and shapers are based on token bucket algorithms. The following list includes definitions that are used to explain how token bucket algorithms operate:

- **Committed Information Rate (CIR):** _____
- _____
- _____: The time interval, in milliseconds (ms), over which the committed burst (Bc) is sent. Tc can be calculated with the formula $Tc = (Bc [bits] / CIR [bps]) \times 1000$.
- _____: The maximum size of the CIR token bucket, measured in bytes, and the maximum amount of traffic that can be sent within a Tc. Bc can be calculated with the formula $Bc = CIR \times (Tc / 1000)$.
- **Token:** _____
- **Token bucket:** A bucket that accumulates tokens until a maximum predefined number of tokens is reached (such as the Bc when using a single token bucket); these tokens are added into the bucket at a fixed rate (the CIR). Each packet is checked for conformance to the defined rate and takes tokens from the bucket equal to its packet size; for example, if the packet size is 1500 bytes, it takes 12,000 bits (1500×8) from the bucket. If there are not enough tokens in the token bucket to send the packet, the traffic conditioning mechanism can take one of the following actions:
 - _____
 - _____
 - _____

There are different policing algorithms, including the following:

- _____
- _____
- _____

Many queuing algorithms are available, but most of them are not adequate for modern rich-media networks carrying voice and high-definition video traffic because they were designed before these traffic types came to be. The legacy queuing algorithms that predate the MQC architecture include the following:

- _____ : _____ involves a single queue where the first packet to be placed on the output interface queue is the first packet to leave the interface (first come, first served). In FIFO queuing, all traffic belongs to the same class.
- _____ : With _____, queues are serviced in sequence one after the other, and each queue processes one packet only. No queues starve with round robin because every queue gets an opportunity to send one packet every round. No queue has priority over others, and if the packet sizes from all queues are about the same, the interface bandwidth is shared equally across the round robin queues. A limitation of round robin is it does not include a mechanism to prioritize traffic.
- _____ : _____ was developed to provide prioritization capabilities for round robin. It allows a weight to be assigned to each queue, and based on that weight, each queue effectively receives a portion of the interface bandwidth that is not necessarily equal to the other queues' portions.
- _____ : _____ is a Cisco implementation of WRR that involves a set of 16 queues with a round-robin scheduler and FIFO queuing within each queue. Each queue can be customized with a portion of the link bandwidth for each selected traffic type. If a particular type of traffic is not using the bandwidth reserved for it, other traffic types may use the unused bandwidth. CQ causes long delays and also suffers from all the same problems as FIFO within each of the 16 queues that it uses for traffic classification.
- _____ : _____, four queues in a set (high, medium, normal, and low) are served in strict-priority order, with FIFO queuing within each queue. The high-priority queue is always serviced first, and lower-priority queues are serviced only when all higher-priority queues are empty. For example, the medium queue is serviced only when the high-priority queue is empty. The normal queue is serviced only when the high and medium queues are empty; finally, the low queue is serviced only when all the other queues are empty. At any point in time, if a packet arrives for a higher queue, the packet from the higher queue is processed before any packets in lower-level queues. For this reason, if the higher-priority queues are continuously being serviced, the lower-priority queues are starved.

- Weighted Fair Queuing (WFQ): The Weighted Fair Queuing (WFQ) algorithm automatically divides the interface bandwidth by the number of flows (weighted by IP Precedence) to allocate bandwidth fairly among all flows. This method provides better service for high-priority real-time flows but can't provide a fixed-bandwidth guarantee for any particular flow.

The current queuing algorithms recommended for rich-media networks (and supported by MQC) combine the best features of the legacy algorithms. These algorithms provide real-time, delay-sensitive traffic bandwidth and delay guarantees while not starving other types of traffic. The recommended queuing algorithms include the following:

- Class-Based Weighted Fair Queuing (CBWFQ): Class-Based Weighted Fair Queuing (CBWFQ) enables the creation of up to 256 queues, serving up to 256 traffic classes. Each queue is serviced based on the bandwidth assigned to that class. It extends WFQ functionality to provide support for user-defined traffic classes. With Class-Based Weighted Fair Queuing (CBWFQ), packet classification is done based on traffic descriptors such as QoS markings, protocols, ACLs, and input interfaces. After a packet is classified as belonging to a specific class, it is possible to assign bandwidth, weight, queue limit, and maximum packet limit to it. The bandwidth assigned to a class is the minimum bandwidth delivered to the class during congestion. The queue limit for that class is the maximum number of packets allowed to be buffered in the class queue. After a queue has reached the configured queue limit, excess packets are dropped. Class-Based Weighted Fair Queuing (CBWFQ) by itself does not provide a latency guarantee and is only suitable for non-real-time data traffic.
- Low Latency Queueing (LLQ): Low Latency Queueing (LLQ) is CBWFQ combined with priority queuing (PQ) and it was developed to meet the requirements of real-time traffic, such as voice. Traffic assigned to the strict-priority queue is serviced up to its assigned bandwidth before other CBWFQ queues are serviced. All real-time traffic should be configured to be serviced by the priority queue. Multiple classes of real-time traffic can be defined, and separate bandwidth guarantees can be given to each, but a single priority queue schedules all the combined traffic. If a traffic class is not using the bandwidth assigned to it, it is shared among the other classes. This algorithm is suitable for combinations of real-time and non-real-time traffic. It provides both latency and bandwidth guarantees to high-priority real-time traffic. In the event of congestion, real-time traffic that goes beyond the assigned bandwidth guarantee is policed by a congestion-aware policer to ensure that the non-priority traffic is not starved.

Chapter 16

Table 16-3 IPsec Security Services

Security Service	Description	Methods Used
	Verifies the identity of the VPN peer through authentication.	<ul style="list-style-type: none"> ■ Pre-Shared Key (PSK) ■ Digital certificates
	Protects data from eavesdropping attacks through encryption algorithms. Changes plaintext into encrypted ciphertext.	<ul style="list-style-type: none"> ■ Data Encryption Standard (DES) ■ Triple DES (3DES) ■ Advanced Encryption Standard (AES) <p>The use of DES and 3DES is not recommended.</p>

Security Service	Description	Methods Used
	Prevents <i>man-in-the-middle</i> (MitM) attacks by ensuring that data has not been tampered with during its transit across an unsecure network.	Hash Message Authentication Code (HMAC) functions: <ul style="list-style-type: none"> ■ Message Digest 5 (MD5) algorithm ■ Secure Hash Algorithm (SHA-1) The use of MD5 is not recommended.
	Prevents MitM attacks where an attacker captures VPN traffic and replays it back to a VPN peer with the intention of building an illegitimate VPN tunnel.	Every packet is marked with a unique sequence number. A VPN device keeps track of the sequence number and does not accept a packet with a sequence number it has already processed.

IPsec supports the following encryption, hashing, and keying methods to provide security services:

- DES: A 56-bit symmetric data encryption algorithm that can encrypt the data sent over a VPN. This algorithm is very weak and should be avoided.
- 3DES: A data encryption algorithm that runs the DES algorithm three times with three different 56-bit keys. Using this algorithm is no longer recommended. The more advanced and more efficient AES should be used instead.
- AES: A symmetric encryption algorithm used for data encryption that was developed to replace DES and 3DES. AES supports key lengths of 128 bits, 192 bits, or 256 bits and is based on the Rijndael algorithm.
- MD5: A one-way, 128-bit hash algorithm used for data authentication. Cisco devices use MD5 HMAC, which provides an additional level of protection against MitM attacks. Using this algorithm is no longer recommended, and SHA should be used instead.
- SHA-1: A one-way, 160-bit hash algorithm used for data authentication. Cisco devices use the SHA-1 HMAC, which provides additional protection against MitM attacks.
- DH: An asymmetric key exchange protocol that enables two peers to establish a shared secret key used by encryption algorithms such as AES over an unsecure communications channel. A DH group refers to the length of the key (modulus size) to use for a DH key exchange. For example, group 1 uses 768 bits, group 2 uses 1024, and group 5 uses 1536, where the larger the modulus, the more secure it is. The purpose of DH is to generate shared secret symmetric keys that are used by the two VPN peers for symmetrical algorithms, such as AES. The DH exchange itself is asymmetrical and CPU intensive, and the resulting shared secret keys that are generated are symmetrical. Cisco recommends avoiding DH groups 1, 2, and 5 and instead using DH groups 14 and higher.

- _____: A public-key (digital certificates) cryptographic system used to mutually authenticate the peers.
- _____: A security mechanism in which a locally configured key is used as a credential to mutually authenticate the peers.

Table 16-4 Allowed Transform Set Combinations

Transform Type	Transform	Description
Authentication header	ah-md5-hmac	Authentication header with the MD5 authentication algorithm (not recommended)
	ah-sha-hmac	Authentication header with the SHA authentication algorithm
	ah-sha256-hmac	Authentication header with the 256-bit SHA authentication algorithm
	ah-sha384-hmac	Authentication header with the 384-bit SHA authentication algorithm
	ah-sha512-hmac	Authentication header with the 512-bit SHA authentication algorithm
	esp-aes	ESP with the 128-bit AES encryption algorithm
	esp-gcm esp-gmac	ESP-GCM—ESP with either a 128-bit (default) or a 256-bit authenticated encryption algorithm ESP-GMAC—ESP with either 128-bit (default) or a 256-bit authentication algorithm without encryption
	esp-aes 192	ESP with the 192-bit AES encryption algorithm
	esp-aes 256	ESP with the 256-bit AES encryption algorithm
	esp-des esp-3des	ESPs with 56-bit and 168-bit DES encryption (no longer recommended)
	esp-null	Null encryption algorithm
	esp-seal	ESP with the 160-bit SEAL encryption algorithm
	esp-md5-hmac	ESP with the MD5 (HMAC variant) authentication algorithm (no longer recommended)
	esp-sha-hmac	ESP with the SHA (HMAC variant) authentication algorithm
	comp-lzs	IP compression with the Lempel-Ziv-Stac (LZS) algorithm

Table 16-5 Major Differences Between IKEv1 and IKEv2

IKEv1	IKEv2
Exchange Modes	
Minimum Number of Messages Needed to Establish IPsec SAs	
	Four
Supported Authentication Methods	
Pre-Shared Key (PSK) Digital RSA Certificate (RSA-SIG) Public key Both peers must use the same authentication method.	Pre-Shared Key Digital RSA Certificate (RSA-SIG) Asymmetric authentication is supported. Authentication method can be specified during the IKE_AUTH exchange.
Next Generation Encryption (NGE)	
	AES-GCM (Galois/Counter Mode) mode SHA-256 SHA-384 SHA-512 HMAC-SHA-256 Elliptic Curve Diffie-Hellman (ECDH) ECDH-384 ECDSA-384
Attack Protection	
MitM protection Eavesdropping protection	

Table 16-6 Cisco IPsec VPN Solutions

Features and Benefits	Site-to-Site IPsec VPN	Cisco DMVPN	Cisco GET-VPN	FlexVPN	Remote Access VPN
Product interoperability	Multivendor	Cisco only	Cisco only	Cisco only	Cisco only

Features and Benefits	Site-to-Site IPsec VPN	Cisco DMVPN	Cisco GET-VPN	FlexVPN	Remote Access VPN
Key exchange	IKEv1 and IKEv2	IKEv1 and IKEv2 (both optional)	IKEv1 and IKEv2	IKEv2 only	TLS/DTLS and IKEv2
Scale	Low	Thousands for hub-and-spoke; hundreds for partially meshed spoke-to-spoke connections	Thousands	Thousands	Thousands
Topology	Hub-and-spoke; small-scale meshing as manageability allows	Hub-and-spoke; on-demand spoke-to-spoke partial mesh; spoke-to-spoke connections automatically terminated when no traffic present	Hub-and-spoke; any-to-any	Hub-and-spoke; any-to-any and remote access	Remote access
Routing	Not supported	Supported	Supported	Supported	Not supported
QoS	Supported	Supported	Supported	Native support	Supported
Multicast	Not supported	Tunneled	Natively supported across MPLS and private IP networks	Tunneled	Not supported
Non-IP protocols	Not supported	Not supported	Not supported	Not supported	Not supported

Features and Benefits	Site-to-Site IPsec VPN	Cisco DMVPN	Cisco GET-VPN	FlexVPN	Remote Access VPN
Private IP addressing	Supported	Supported	Requires use of GRE or DMVPN with Cisco GET-VPN to support private addresses across the Internet	Supported	Supported
High availability	Stateless failover	Routing	Routing	Routing IKEv2-based dynamic route distribution and server clustering	Not supported
Encapsulation	Tunneled IPsec	Tunneled IPsec	Tunnel-less IPsec	Tunneled IPsec	Tunneled IPsec/TLS
Transport network	Any	Any	Private WAN/ MPLS	Any	Any

There are two different ways to encrypt traffic over a GRE tunnel:

- _____
- _____

Following are the definitions for the LISP architecture components illustrated in Figure 16-5.

- _____: An _____ is the IP address of an endpoint within a LISP site. EIDs are the same IP addresses in use today on endpoints (IPv4 or IPv6), and they operate in the same way.
- _____: This is the name of a site where LISP routers and EIDs reside.
- _____: _____ are LISP routers that LISP-encapsulate IP packets coming from EIDs that are destined outside the LISP site.
- _____: _____ are LISP routers that de-encapsulate LISP-encapsulated IP packets coming from sites outside the LISP site and destined to EIDs within the LISP site.
- _____: _____ refers to routers that perform ITR and ETR functions (which are most routers).

- _____: _____ are just like ITRs but for non-LISP sites that send traffic to EID destinations.
- _____: _____ act just like ETRs but for EIDs that send traffic to destinations at non-LISP sites.
- _____: _____ refers to a router that performs PITR and PETR functions.
- _____: A _____ is a router that performs the functions of any or all of the following: ITR, ETR, PITR, and/or PETR.
- _____: An _____ is an IPv4 or IPv6 address of an ETR that is Internet facing or network core facing.
- _____: This network device (typically a router) learns EID-to-prefix mapping entries from an ETR and stores them in a local EID-to-RLOC mapping database.
- _____: This network device (typically a router) receives LISP-encapsulated map requests from an ITR and finds the appropriate ETR to answer those requests by consulting the map server.
- _____: When MS and the MR functions are implemented on the same device, the device is referred to as an _____.

To facilitate the discovery of VNIs over the underlay Layer 3 network, *virtual tunnel endpoints (VTEPs)* are used. VTEPs are entities that originate or terminate VXLAN tunnels. They map Layer 2 and Layer 3 packets to the VNI to be used in the overlay network. Each VTEP has two interfaces:

- _____: These interfaces on the local LAN segment provide bridging between local hosts.
- _____: This is a core-facing network interface for VXLAN. The IP interface's IP address helps identify the VTEP in the network. It is also used for VXLAN traffic encapsulation and de-encapsulation.

The VXLAN standard defines VXLAN as a data plane protocol, but it does not define a VXLAN control plane; it was left open to be used with any control plane. Currently four different VXLAN control and data planes are supported by Cisco devices:

- _____
- _____
- _____
- _____

Chapter 17

Table 17-4 A Summary of Common 802.11 Standard Amendments

Standard	2.4 GHz?	5 GHz?	Data Rates Supported	Channel Widths Supported
			1, 2, 5.5, and 11 Mbps	22 MHz
			6, 9, 12, 18, 24, 36, 48, and 54 Mbps	22 MHz
			6, 9, 12, 18, 24, 36, 48, and 54 Mbps	20 MHz
			Up to 150 Mbps* per spatial stream, up to 4 spatial streams	20 or 40 MHz
			Up to 866 Mbps per spatial stream, up to 4 spatial streams	20, 40, 80, or 160 MHz
			Up to 1.2 Gbps per spatial stream, up to 8 spatial streams	20, 40, 80, or 160 MHz

* 802.11ax is designed to work on any band from 1 to 7 GHz, provided that the band is approved for use.

Chapter 22

The hierarchical LAN design divides networks or their modular blocks into the following three layers:

- Access layer: _____
- Distribution layer: _____
- Core layer (also referred to as _____): _____

Chapter 23

With SD-Access, an evolved campus network can be built that addresses the needs of existing campus networks by leveraging the following capabilities, features, and functionalities:

- _____: SD-Access replaces manual network device configurations with network device management through a single point of automation, orchestration, and management of network functions through the use of Cisco DNA Center. This simplifies network design and provisioning and allows for very fast, lower-risk deployment of network devices and services using best-practice configurations.
- _____: SD-Access enables proactive prediction of network-related and security-related risks by using telemetry to improve the performance of the network, endpoints, and applications, including encrypted traffic.

- _____: SD-Access provides host mobility for both wired and wireless clients.
- _____: *Cisco Identity Services Engine (ISE)* identifies users and devices connecting to the network and provides the contextual information required for users and devices to implement security policies for network access control and network segmentation.
- _____: Traditional access control lists (ACLs) can be difficult to deploy, maintain, and scale because they rely on IP addresses and subnets. Creating access and application policies based on group-based policies using Security Group Access Control Lists (SGACLs) provides a much simpler and more scalable form of policy enforcement based on identity instead of an IP address.
- _____: With SD-Access it is easier to segment the network to support guest, corporate, facilities, and IoT-enabled infrastructure.
- _____: SD-Access makes it possible to leverage a single physical infrastructure to support multiple virtual routing and forwarding (VRF) instances, referred to as *virtual networks (VNs)*, each with a distinct set of access policies.

There are three basic planes of operation in the SD-Access fabric:

- _____
- _____
- _____

There are five basic device roles in the fabric overlay:

- _____: This node contains the settings, protocols, and mapping tables to provide the endpoint-to-location (EID-to-RLOC) mapping system for the fabric overlay.
- _____: This fabric device (for example, core layer device) connects external Layer 3 networks to the SDA fabric.
- _____: This fabric device (for example, access or distribution layer device) connects wired endpoints to the SDA fabric.
- _____: This fabric device connects APs and wireless endpoints to the SDA fabric.
- _____: These are intermediate routers or extended switches that do not provide any sort of SD-Access fabric role other than underlay services.

There are three types of border nodes:

- _____: Connects only to the known areas of the organization (for example, WLC, firewall, data center).
- _____: Connects only to unknown areas outside the organization. This border node is configured with a default route to reach external unknown

networks such as the Internet or the public cloud that are not known to the control plane nodes.

- _____: Connects transit areas as well as known areas of the company. This is basically a border that combines internal and default border functionality into a single node.

The Cisco SD-WAN solution has four main components and an optional analytics service:

- _____: These physical or virtual devices forward traffic across transports (i.e., WAN circuits/media) between locations.
- _____: This SD-WAN controller persona provides a single pane of glass (GUI) for managing and monitoring the SD-WAN solution.
- _____: This SD-WAN controller persona is responsible for advertising routes and data policies to edge devices.
- _____: This SD-WAN controller persona authenticates and orchestrates connectivity between edge devices, vManage, and vSmart controllers.
- _____: This is an optional analytics and assurance service.

Chapter 25

In addition to providing standard firewall functionality, a *next-generation firewall* (NGFW) can block threats such as advanced malware and application-layer attacks. According to Gartner, Inc.'s definition, a NGFW firewall must include:

- _____
- _____
- _____
- _____

At the core of Cisco Secure Network Analytics are the following components:

- _____: The _____ is the control center for Cisco Secure Network Analytics. It aggregates, organizes, and presents analysis from up to 25 Flow Collectors, Cisco ISE, and other sources. It offers a powerful yet simple-to-use web console that provides graphical representations of network traffic, identity information, customized summary reports, and integrated security and network intelligence for comprehensive analysis. The Network Analytics Manager is available as a hardware appliance or a virtual machine.
- _____: The _____ collect and analyze enterprise telemetry data such as NetFlow, IP Flow Information Export (IPFIX), and other types of flow data from routers, switches, firewalls, endpoints, and other network devices. The Flow Collectors can also collect telemetry from proxy data sources, which can

be analyzed by Global Threat Analytics, formerly Cognitive Threat Analytics. It can also pinpoint malicious patterns in encrypted traffic using Encrypted Traffic Analytics (ETA), without having to decrypt it, to identify threats and accelerate response. Flow Collectors are available as hardware appliances and as virtual machines.

- _____: The _____ is required for the collection, management, and analysis of flow telemetry data and aggregates flows at the Network Analytics Manager as well as to define the volume of flows that can be collected.

Cisco Secure Cloud Analytics supports two deployment models:

- _____
- _____

802.1x comprises the following components:

- _____: This message format and framework defined by RFC 4187 provides an encapsulated transport for authentication parameters.
- _____: Different authentication methods can be used with EAP.
- _____: This Layer 2 encapsulation protocol is defined by 802.1x for the transport of EAP messages over IEEE 802 wired and wireless networks.
- _____: This is the AAA protocol used by EAP.

802.1x network devices have the following roles:

- _____: Software on the endpoint communicates and provides identity credentials through EAPoL with the authenticator. Common 802.1x supplicants include Windows and macOS native supplicants as well as Cisco AnyConnect. All these supplicants support 802.1x machine and user authentication.
- _____: A network access device (NAD) such as a switch or wireless LAN controller (WLC) controls access to the network based on the authentication status of the user or endpoint. The authenticator acts as the liaison, taking Layer 2 EAP-encapsulated packets from the supplicant and encapsulating them into RADIUS packets for delivery to the authentication server.
- _____: A RADIUS server performs authentication of the client. The authentication server validates the identity of the endpoint and provides the authenticator with an authorization result, such as accept or deny.

There are two methods available for propagating an SGT tag: inline tagging (also referred to as *native tagging*) and the Cisco-created protocol SGT Exchange Protocol (SXP):

- _____: With _____, a switch inserts the SGT tag inside a frame to allow upstream devices to read and apply policy. _____ is completely independent of any Layer 3 protocol (IPv4 or IPv6), so the frame or packet can preserve the SGT tag throughout the network infrastructure (routers, switches, firewalls, and so on) until it reaches the egress point. The

downside to _____ is that it is supported only by Cisco network devices with ASIC support for TrustSec. If a tagged frame is received by a device that does not support _____ in hardware, the frame is dropped. Figure 25-9 illustrates a Layer 2 frame with a 16-bit SGT value.

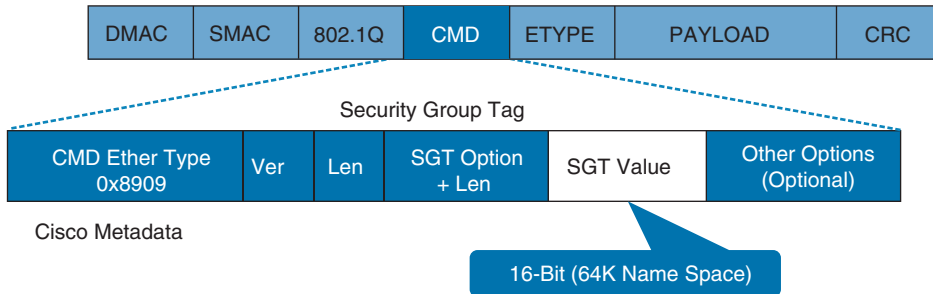


Figure 25-9 Layer 2 Ethernet Frame with an SGT Tag

- _____: _____ is a _____ used for network devices that do not support _____ in hardware. Using _____, IP-to-SGT mappings can be communicated between _____ switches and other network devices. _____ switches also have an SGT mapping database to check packets against and enforce policy. The _____ peer that sends IP-to-SGT bindings is called a *speaker*. The IP-to-SGT binding receiver is called a *listener*. _____ can be single-hop or multi-hop, as shown in Figure 25-10.

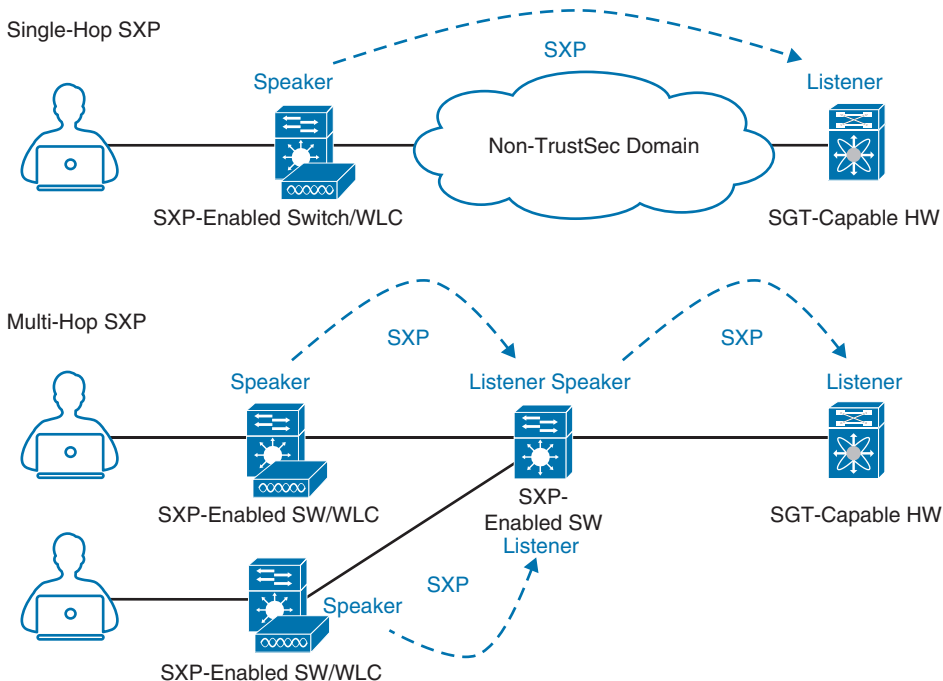


Figure 25-10 Single-Hop and Multi-Hop SXP Connections

Chapter 26

While many different kinds of ACLs can be used for packet filtering, only the following types are covered in this chapter:

- **Numbered standard ACLs:** These ACLs define packets based solely on the source network, and they use the numbered entries _____ and _____.
- **Numbered extended ACLs:** These ACLs define packets based on source, destination, protocol, port, or a combination of other packet attributes, and they use the numbered entries _____ and _____.
- _____: These ACLs allow standard and extended ACLs to be given names instead of numbers and are generally preferred because they can provide more relevance to the functionality of the ACL.
- _____: These ACLs can use standard, extended, named, and named extended MAC ACLs to filter traffic on Layer 2 switch ports.
- _____: These ACLs can use standard, extended, named, and named extended MAC ACLs to filter traffic on VLANs.

The Cisco IOS CLI by default includes three privilege levels, each of which defines what commands are available to a user:

- _____: Includes the **disable**, **enable**, **exit**, **help**, and **logout** commands.
- _____: Also known as _____ mode. The command prompt in this mode includes a greater-than sign (R1>). From this mode it is not possible to make configuration changes; in other words, the command **configure terminal** is not available.
- _____: Also known as _____ mode. This is the highest privilege level, where all CLI commands are available. The command prompt in this mode includes a hash sign (R1#).

AAA is an architectural framework for enabling a set of three independent security functions:

- _____: Enables a user to be identified and verified prior to being granted access to a network device and/or network services.
- _____: Defines the access privileges and restrictions to be enforced for an authenticated user.
- _____: Provides the ability to track and log user access, including user identities, start and stop times, executed commands (that is, CLI commands), and so on. In other words, it maintains a security log of events.

Chapter 27

There are two types of hypervisors, as illustrated in Figure 27-2:

- Type 1: _____
- Type 2: _____

Cisco ENFV delivers a virtualized solution for network and application services for branch offices. It consists of four main components that are based on the ETSI NFV architectural framework:

- _____: Cisco DNA Center provides the VNF management and NFV orchestration capabilities. It allows for easy automation of the deployment of virtualized network services, consisting of multiple VNFs.
- _____: VNFs provide the desired virtual networking functions.
- _____: An operating system that provides virtualization capabilities and facilitates the deployment and operation of VNFs and hardware components.
- _____: x86-based compute resources that provide the CPU, memory, and storage required to deploy and operate VNFs and run applications.

Chapter 28

Table 28-3 HTTP Functions and Use Cases

HTTP Function	Action	Use Case
	Requests data from a destination	Viewing a website
	Submits data to a specific destination	Submitting login credentials
	Replaces data in a specific destination	Updating an NTP server
	Appends data to a specific destination	Adding an NTP server
	Removes data from a specific destination	Removing an NTP server

Table 28-4 CRUD Functions and Use Cases

CRUD Function	Action	Use Case
	Inserts data in a database or application	Updating a customer's home address in a database
	Retrieves data from a database or application	Pulling up a customer's home address from a database
	Modifies or replaces data in a database or application	Changing a street address stored in a database
	Removes data from a database or application	Removing a customer from a database

Table 28-5 HTTP Status Codes

HTTP Status Code	Result	Common Reason for Response Code
	OK	Using GET or POST to exchange data with an API
	Created	Creating resources by using a REST API call
	Bad Request	Request failed due to client-side issue
	Unauthorized	Client not authenticated to access site or API call
	Forbidden	Access not granted based on supplied credentials
	Not Found	Page at HTTP URL location does not exist or is hidden

This page intentionally left blank

Memory Tables Answer Key

Chapter 7

Table 7-2 EIGRP Terminology

Term	Definition
Successor route	The route with the lowest path metric to reach a destination. The successor route for R1 to reach 10.4.4.0/24 on R4 is R1→R3→R4.
Successor	The first next-hop router for the successor route. The successor for 10.4.4.0/24 is R3.
Feasible distance (FD)	The metric value for the lowest-metric path to reach a destination. The feasible distance is calculated locally using the formula shown in the “Path Metric Calculation” section, later in this chapter. The FD calculated by R1 for the 10.4.4.0/24 network is 3328 (that is, 256+256+2816).
Reported distance (RD)	The distance reported by a router to reach a prefix. The reported distance value is the feasible distance for the advertising router. R3 advertises the 10.4.4.0/24 prefix with an RD of 3072. R4 advertises the 10.4.4.0/24 to R1 and R2 with an RD of 2816.
Feasibility condition	A condition under which, for a route to be considered a backup route, the reported distance received for that route must be less than the feasible distance calculated locally. This logic guarantees a loop-free path.
Feasible successor	A route that satisfies the feasibility condition and is maintained as a backup route. The feasibility condition ensures that the backup route is loop free. The route R1→R4 is the feasible successor because the RD 2816 is lower than the FD 3328 for the R1→R3→R4 path.

Table 7-3 EIGRP Packet Types

Opcode Value	Packet Type	Function
1	Update	Used to transmit routing and reachability information with other EIGRP neighbors
2	Request	Used to get specific information from one or more neighbors
3	Query	Sent out to search for another path during convergence
4	Reply	Sent in response to a query packet
5	Hello	Used for discovery of EIGRP neighbors and for detecting when a neighbor is no longer available

Chapter 8

Table 8-2 OSPF Packet Types

Type	Packet Name	Functional Overview
1	Hello	These packets are for discovering and maintaining neighbors. Packets are sent out periodically on all OSPF interfaces to discover new neighbors while ensuring that other adjacent neighbors are still online.
2	Database description (DBD) or (DDP)	These packets are for summarizing database contents. Packets are exchanged when an OSPF adjacency is first being formed. These packets are used to describe the contents of the LSDB.
3	Link-state request (LSR)	These packets are for database downloads. When a router thinks that part of its LSDB is stale, it may request a portion of a neighbor's database by using this packet type.
4	Link-state update (LSU)	These packets are for database updates. This is an explicit LSA for a specific network link and normally is sent in direct response to an LSR.
5	Link-state ack	These packets are for flooding acknowledgment. These packets are sent in response to the flooding of LSAs, thus making flooding a reliable transport feature.

Table 8-9 OSPF Network Types

Type	Description	DR/BDR Field in OSPF Hellos	Timers
Broadcast	Default setting on OSPF-enabled Ethernet links.	Yes	Hello: 10 Wait: 40 Dead: 40
Non-broadcast	Default setting on OSPF-enabled Frame Relay main interface or Frame Relay multipoint subinterfaces.	Yes	Hello: 30 Wait: 120 Dead: 120
Point-to-point	Default setting on OSPF-enabled Frame Relay point-to-point subinterfaces.	Yes	Hello: 10 Wait: 40 Dead: 40
Point-to-multipoint	Not enabled by default on any interface type. Interface is advertised as a host route (/32) and sets the next-hop address to the outbound interface. Primarily used for hub-and-spoke topologies.	No	Hello: 30 Wait: 120 Dead: 120
Loopback	Default setting on OSPF-enabled loopback interfaces. Interface is advertised as a host route (/32).	N/A	N/A

Chapter 13

Table 13-2 IP Multicast Addresses Assigned by IANA

Designation	Multicast Address Range
Local network control block	224.0.0.0 to 224.0.0.255
Internetwork control block	224.0.1.0 to 224.0.1.255
Ad hoc block I	224.0.2.0 to 224.0.255.255
Reserved	224.1.0.0 to 224.1.255.255
SDP/SAP block	224.2.0.0 to 224.2.255.255
Ad hoc block II	224.3.0.0 to 224.4.255.255
Reserved	224.5.0.0 to 224.255.255.255
Reserved	225.0.0.0 to 231.255.255.255
Source Specific Multicast (SSM) block	232.0.0.0 to 232.255.255.255
GLOP block	233.0.0.0 to 233.251.255.255
Ad hoc block III	233.252.0.0 to 233.255.255.255
Reserved	234.0.0.0 to 238.255.255.255
Administratively scoped block	239.0.0.0 to 239.255.255.255

Table 13-3 Well-Known Reserved Multicast Addresses

IP Multicast Address	Description
224.0.0.0	Base address (reserved)
224.0.0.1	All hosts in this subnet (all-hosts group)
224.0.0.2	All routers in this subnet
224.0.0.5	All OSPF routers (AllSPFRouters)
224.0.0.6	All OSPF DRs (AllDRouters)
224.0.0.9	All RIPv2 routers
224.0.0.10	All EIGRP routers
224.0.0.13	All PIM routers
224.0.0.18	VRRP
224.0.0.22	IGMPv3
224.0.0.102	HSRPv2 and GLBP
224.0.1.1	NTP
224.0.1.39	Cisco-RP-Announce (Auto-RP)
224.0.1.40	Cisco-RP-Discovery (Auto-RP)

The IGMP message format fields are defined as follows:

- **Type:** This field describes five different types of IGMP messages used by routers and receivers:
- **Version 2 membership report** (type value 0x16) is a message type also commonly referred to as an IGMP join; it is used by receivers to join a multicast group or to respond to a local router's membership query message.

- **Version 1 membership report** (type value 0x12) is used by receivers for backward compatibility with IGMPv1.
- **Version 2 leave group** (type value 0x17) is used by receivers to indicate they want to stop receiving multicast traffic for a group they joined.
- **General membership query** (type value 0x11) is sent periodically to the all-hosts group address 224.0.0.1 to see whether there are any receivers in the attached subnet. It sets the group address field to 0.0.0.0.
- **Group specific query** (type value 0x11) is sent in response to a leave group message to the group address the receiver requested to leave. The group address is the destination IP address of the IP packet and the group address field.
- **Max response time:** This field is set only in general and group-specific membership query messages (type value 0x11); it specifies the maximum allowed time before sending a responding report in units of one-tenth of a second. In all other messages, it is set to 0x00 by the sender and ignored by receivers.
- **Checksum:** This field is the 16-bit 1s complement of the 1s complement sum of the IGMP message. This is the standard checksum algorithm used by TCP/IP.
- **Group address:** This field is set to 0.0.0.0 in general query messages and is set to the group address in group-specific messages. Membership report messages carry the address of the group being reported in this field; group leave messages carry the address of the group being left in this field.

The following list defines the common PIM terminology illustrated in Figure 13-14:

- **Reverse Path Forwarding (RPF) interface:** The interface with the lowest-cost path (based on administrative distance [AD] and metric) to the IP address of the source (SPT) or the RP, in the case of shared trees. If multiple interfaces have the same cost, the interface with the highest IP address is chosen as the tiebreaker. An example of this type of interface is Te0/1/2 on R5 because it is the shortest path to the source. Another example is Te1/1/1 on R7 because the shortest path to the source was determined to be through R4.
- **RPF neighbor:** The PIM neighbor on the RPF interface. For example, if R7 is using the RPT shared tree, the RPF neighbor would be R3, which is the lowest-cost path to the RP. If it is using the SPT, R4 would be its RPF neighbor because it offers the lowest cost to the source.
- **Upstream:** Toward the source of the tree, which could be the actual source in source-based trees or the RP in shared trees. A PIM join travels upstream toward the source.
- **Upstream interface:** The interface toward the source of the tree. It is also known as the RPF interface or the incoming interface (IIF). An example of an upstream interface is R5's Te0/1/2 interface, which can send PIM joins upstream to its RPF neighbor.

- **Downstream:** Away from the source of the tree and toward the receivers.
- **Downstream interface:** Any interface that is used to forward multicast traffic down the tree, also known as an outgoing interface (OIF). An example of a downstream interface is R1's Te0/0/0 interface, which forwards multicast traffic to R3's Te0/0/1 interface.
- **Incoming interface (IIF):** The only type of interface that can accept multicast traffic coming from the source, which is the same as the RPF interface. An example of this type of interface is Te0/0/1 on R3 because the shortest path to the source is known through this interface.
- **Outgoing interface (OIF):** Any interface that is used to forward multicast traffic down the tree, also known as the downstream interface.
- **Outgoing interface list (OIL):** A group of OIFs that are forwarding multicast traffic to the same group. An example of this is R1's Te0/0/0 and Te0/0/1 interfaces sending multicast traffic downstream to R3 and R4 for the same multicast group.
- **Last-hop router (LHR):** A router that is directly attached to the receivers, also known as a leaf router. It is responsible for sending PIM joins upstream toward the RP or to the source.
- **First-hop router (FHR):** A router that is directly attached to the source, also known as a root router. It is responsible for sending register messages to the RP.
- **Multicast Routing Information Base (MRIB):** A topology table that is also known as the multicast route table (mroute), which derives from the unicast routing table and PIM. MRIB contains the source S, group G, incoming interfaces (IIF), outgoing interfaces (OIFs), and RPF neighbor information for each multicast route as well as other multicast-related information.
- **Multicast Forwarding Information Base (MFIB):** A forwarding table that uses the MRIB to program multicast forwarding information in hardware for faster forwarding.
- **Multicast state:** The multicast traffic forwarding state that is used by a router to forward multicast traffic. The multicast state is composed of the entries found in the mroute table (S, G, IIF, OIF, and so on).

There are currently five PIM operating modes:

- PIM Dense Mode (PIM-DM)
- PIM Sparse Mode (PIM-SM)
- PIM Sparse Dense Mode
- PIM Source Specific Multicast (PIM-SSM)
- PIM Bidirectional Mode (Bidir-PIM)

Table 13-4 PIM Control Message Types

Type	Message Type	Destination	PIM Protocol
0	Hello	224.0.0.13 (all PIM routers)	PIM-SM, PIM-DM, Bidir-PIM, and SSM
1	Register	RP address (unicast)	PIM-SM
2	Register stop	First-hop router (unicast)	PIM SM
3	Join/prune	224.0.0.13 (all PIM routers)	PIM-SM, Bidir-PIM, and SSM
4	Bootstrap	224.0.0.13 (all PIM routers)	PIM-SM and Bidir-PIM
5	Assert	224.0.0.13 (all PIM routers)	PIM-SM, PIM-DM, and Bidir-PIM
8	Candidate RP advertisement	Bootstrap router (BSR) address (unicast to BSR)	PIM-SM and Bidir-PIM
9	State refresh	224.0.0.13 (all PIM routers)	PIM-DM
10	DF election	224.0.0.13 (all PIM routers)	Bidir-PIM

Chapter 14

There are three different QoS implementation models:

- **Best effort:** QoS is not enabled for this model. It is used for traffic that does not require any special treatment.
- **Integrated Services (IntServ):** Applications signal the network to make a bandwidth reservation and to indicate that they require special QoS treatment.
- **Differentiated Services (DiffServ):** The network identifies classes that require special QoS treatment.

The following traffic descriptors are typically used for classification:

- **Internal:** QoS groups (locally significant to a router)
- **Layer 1:** Physical interface, subinterface, or port
- **Layer 2:** MAC address and 802.1Q/p class of service (CoS) bits
- **Layer 2.5:** MPLS experimental (EXP) bits
- **Layer 3:** Differentiated Services Code Points (DSCP), IP Precedence (IPP), and source/destination IP address
- **Layer 4:** TCP or UDP ports
- **Layer 7:** Next-Generation Network-Based Application Recognition (NBAR2)

The following traffic descriptors are used for marking traffic:

- **Internal:** QoS groups
- **Layer 2:** 802.1Q/p class of service (CoS) bits

- **Layer 2.5:** MPLS experimental (EXP) bits
- **Layer 3:** Differentiated Services Code Points (DSCP) and IP Precedence (IPP)

The TCI field is a 16-bit field composed of the following three fields:

- Priority Code Point (PCP) field (3 bits)
- Drop Eligible Indicator (DEI) field (1 bit)
- VLAN Identifier (VLAN ID) field (12 bits)

Four PHBs have been defined and characterized for general use:

- **Class Selector (CS) PHB:** The first 3 bits of the DSCP field are used as CS bits. The CS bits make DSCP backward compatible with IP Precedence because IP Precedence uses the same 3 bits to determine class.
- **Default Forwarding (DF) PHB:** Used for best-effort service.
- **Assured Forwarding (AF) PHB:** Used for guaranteed bandwidth service.
- **Expedited Forwarding (EF) PHB:** Used for low-delay service.

Cisco IOS policers and shapers are based on token bucket algorithms. The following list includes definitions that are used to explain how token bucket algorithms operate:

- **Committed Information Rate (CIR):** The policed traffic rate, in bits per second (bps), defined in the traffic contract.
- **Committed Time Interval (Tc):** The time interval, in milliseconds (ms), over which the committed burst (Bc) is sent. Tc can be calculated with the formula $Tc = (Bc \text{ [bits]} / CIR \text{ [bps]}) \times 1000$.
- **Committed Burst Size (Bc):** The maximum size of the CIR token bucket, measured in bytes, and the maximum amount of traffic that can be sent within a Tc. Bc can be calculated with the formula $Bc = CIR (Tc / 1000)$.
- **Token:** A single token represents 1 byte or 8 bits.
- **Token bucket:** A bucket that accumulates tokens until a maximum predefined number of tokens is reached (such as the Bc when using a single token bucket); these tokens are added into the bucket at a fixed rate (the CIR). Each packet is checked for conformance to the defined rate and takes tokens from the bucket equal to its packet size; for example, if the packet size is 1500 bytes, it takes 12,000 bits (1500×8) from the bucket. If there are not enough tokens in the token bucket to send the packet, the traffic conditioning mechanism can take one of the following actions:
 - Buffer the packets while waiting for enough tokens to accumulate in the token bucket (traffic shaping)
 - Drop the packets (traffic policing)
 - Mark down the packets (traffic markdown)

There are different policing algorithms, including the following:

- Single-rate two-color marker/policer
- Single-rate three-color marker/policer (srTCM)
- Two-rate three-color marker/policer (trTCM)

Many queuing algorithms are available, but most of them are not adequate for modern rich-media networks carrying voice and high-definition video traffic because they were designed before these traffic types came to be. The legacy queuing algorithms that predate the MQC architecture include the following:

- **First-in, first-out queuing (FIFO):** FIFO involves a single queue where the first packet to be placed on the output interface queue is the first packet to leave the interface (first come, first served). In FIFO queuing, all traffic belongs to the same class.
- **Round robin:** With round robin, queues are serviced in sequence one after the other, and each queue processes one packet only. No queues starve with round robin because every queue gets an opportunity to send one packet every round. No queue has priority over others, and if the packet sizes from all queues are about the same, the interface bandwidth is shared equally across the round robin queues. A limitation of round robin is that it does not include a mechanism to prioritize traffic.
- **Weighted round robin (WRR):** WRR was developed to provide prioritization capabilities for round robin. It allows a weight to be assigned to each queue, and based on that weight, each queue effectively receives a portion of the interface bandwidth that is not necessarily equal to the other queues' portions.
- **Custom queuing (CQ):** CQ is a Cisco implementation of WRR that involves a set of 16 queues with a round-robin scheduler and FIFO queuing within each queue. Each queue can be customized with a portion of the link bandwidth for each selected traffic type. If a particular type of traffic is not using the bandwidth reserved for it, other traffic types may use the unused bandwidth. CQ causes long delays and also suffers from all the same problems as FIFO within each of the 16 queues that it uses for traffic classification.
- **Priority queuing (PQ):** With PQ, four queues in a set (high, medium, normal, and low) are served in strict-priority order, with FIFO queuing within each queue. The high-priority queue is always serviced first, and lower-priority queues are serviced only when all higher-priority queues are empty. For example, the medium queue is serviced only when the high-priority queue is empty. The normal queue is serviced only when the high and medium queues are empty; finally, the low queue is serviced only when all the other queues are empty. At any point in time, if a packet arrives for a higher queue, the packet from the higher queue is processed before any packets in lower-level queues. For this reason, if the higher-priority queues are continuously being serviced, the lower-priority queues are starved.
- **Weighted fair queuing (WFQ):** The WFQ algorithm automatically divides the interface bandwidth by the number of flows (weighted by IP Precedence) to allocate band-

width fairly among all flows. This method provides better service for high-priority real-time flows but can't provide a fixed-bandwidth guarantee for any particular flow.

The current queuing algorithms recommended for rich-media networks (and supported by MQC) combine the best features of the legacy algorithms. These algorithms provide real-time, delay-sensitive traffic bandwidth and delay guarantees while not starving other types of traffic. The recommended queuing algorithms include the following:

- **Class-based weighted fair queuing (CBWFQ):** CBWFQ enables the creation of up to 256 queues, serving up to 256 traffic classes. Each queue is serviced based on the bandwidth assigned to that class. It extends WFQ functionality to provide support for user-defined traffic classes. With CBWFQ, packet classification is done based on traffic descriptors such as QoS markings, protocols, ACLs, and input interfaces. After a packet is classified as belonging to a specific class, it is possible to assign bandwidth, weight, queue limit, and maximum packet limit to it. The bandwidth assigned to a class is the minimum bandwidth delivered to the class during congestion. The queue limit for that class is the maximum number of packets allowed to be buffered in the class queue. After a queue has reached the configured queue limit, excess packets are dropped. CBWFQ by itself does not provide a latency guarantee and is only suitable for non-real-time data traffic.
- **Low-latency queuing (LLQ):** LLQ is CBWFQ combined with priority queuing (PQ), and it was developed to meet the requirements of real-time traffic, such as voice. Traffic assigned to the strict-priority queue is serviced up to its assigned bandwidth before other CBWFQ queues are serviced. All real-time traffic should be configured to be serviced by the priority queue. Multiple classes of real-time traffic can be defined, and separate bandwidth guarantees can be given to each, but a single priority queue schedules all the combined traffic. If a traffic class is not using the bandwidth assigned to it, it is shared among the other classes. This algorithm is suitable for combinations of real-time and non-real-time traffic. It provides both latency and bandwidth guarantees to high-priority real-time traffic. In the event of congestion, real-time traffic that goes beyond the assigned bandwidth guarantee is policed by a congestion-aware policer to ensure that the non-priority traffic is not starved.

Chapter 16

Table 16-3 IPsec Security Services

Security Service	Description	Methods Used
Peer authentication	Verifies the identity of the VPN peer through authentication.	<ul style="list-style-type: none"> ■ Pre-Shared Key (PSK) ■ Digital certificates
Data confidentiality	Protects data from eavesdropping attacks through encryption algorithms. Changes plaintext into encrypted ciphertext.	<ul style="list-style-type: none"> ■ Data Encryption Standard (DES) ■ Triple DES (3DES) ■ Advanced Encryption Standard (AES) <p>The use of DES and 3DES is not recommended.</p>

Security Service	Description	Methods Used
Data integrity	Prevents <i>man-in-the-middle</i> (MitM) attacks by ensuring that data has not been tampered with during its transit across an unsecure network.	Hash Message Authentication Code (HMAC) functions: <ul style="list-style-type: none"> ■ Message Digest 5 (MD5) algorithm ■ Secure Hash Algorithm (SHA-1) The use of MD5 is not recommended.
Replay detection	Prevents MitM attacks where an attacker captures VPN traffic and replays it back to a VPN peer with the intention of building an illegitimate VPN tunnel.	Every packet is marked with a unique sequence number. A VPN device keeps track of the sequence number and does not accept a packet with a sequence number it has already processed.

C

IPsec supports the following encryption, hashing, and keying methods to provide security services:

- **Data Encryption Standard (DES):** A 56-bit symmetric data encryption algorithm that can encrypt the data sent over a VPN. This algorithm is very weak and should be avoided.
- **Triple DES (3DES):** A data encryption algorithm that runs the DES algorithm three times with three different 56-bit keys. Using this algorithm is no longer recommended. The more advanced and more efficient AES should be used instead.
- **Advanced Encryption Standard (AES):** A symmetric encryption algorithm used for data encryption that was developed to replace DES and 3DES. AES supports key lengths of 128 bits, 192 bits, or 256 bits and is based on the Rijndael algorithm.
- **Message Digest 5 (MD5):** A one-way, 128-bit hash algorithm used for data authentication. Cisco devices use MD5 HMAC, which provides an additional level of protection against MitM attacks. Using this algorithm is no longer recommended, and SHA should be used instead.
- **Secure Hash Algorithm (SHA):** A one-way, 160-bit hash algorithm used for data authentication. Cisco devices use the SHA-1 HMAC, which provides additional protection against MitM attacks.
- **Diffie-Hellman (DH):** An asymmetric key exchange protocol that enables two peers to establish a shared secret key used by encryption algorithms such as AES over an unsecure communications channel. A DH group refers to the length of the key (modulus size) to use for a DH key exchange. For example, group 1 uses 768 bits, group 2 uses 1024, and group 5 uses 1536, where the larger the modulus, the more secure it is. The purpose of DH is to generate shared secret symmetric keys that are used by the two VPN peers for symmetrical algorithms, such as AES. The DH exchange itself is asymmetrical and CPU intensive, and the resulting shared secret keys that are generated are symmetrical. Cisco recommends avoiding DH groups 1, 2, and 5 and instead using DH groups 14 and higher.

- **RSA signatures:** A public-key (digital certificates) cryptographic system used to mutually authenticate the peers.
- **Pre-Shared Key:** A security mechanism in which a locally configured key is used as a credential to mutually authenticate the peers.

Table 16-4 Allowed Transform Set Combinations

Transform Type	Transform	Description
Authentication header transform (only one allowed)	ah-md5-hmac	Authentication header with the MD5 authentication algorithm (not recommended)
	ah-sha-hmac	Authentication header with the SHA authentication algorithm
	ah-sha256-hmac	Authentication header with the 256-bit SHA authentication algorithm
	ah-sha384-hmac	Authentication header with the 384-bit SHA authentication algorithm
	ah-sha512-hmac	Authentication header with the 512-bit SHA authentication algorithm
ESP encryption transform (only one allowed)	esp-aes	ESP with the 128-bit AES encryption algorithm
	esp-gcm esp-gmac	ESP-GCM—ESP with either a 128-bit (default) or a 256-bit authenticated encryption algorithm ESP-GMAC—ESP with either 128-bit (default) or a 256-bit authentication algorithm without encryption
	esp-aes 192	ESP with the 192-bit AES encryption algorithm
	esp-aes 256	ESP with the 256-bit AES encryption algorithm
	esp-des esp-3des	ESPs with 56-bit and 168-bit DES encryption (no longer recommended)
	esp-null	Null encryption algorithm
	esp-seal	ESP with the 160-bit SEAL encryption algorithm
ESP authentication transform (only one allowed)	esp-md5-hmac	ESP with the MD5 (HMAC variant) authentication algorithm (no longer recommended)
	esp-sha-hmac	ESP with the SHA (HMAC variant) authentication algorithm
IP compression transform	comp-lzs	IP compression with the Lempel-Ziv-Stac (LZS) algorithm

Table 16-5 Major Differences Between IKEv1 and IKEv2

IKEv1	IKEv2
Exchange Modes	
Main mode Aggressive mode Quick mode	IKE Security Association Initialization (SA_INIT) IKE_Auth CREATE_CHILD_SA
Minimum Number of Messages Needed to Establish IPsec SAs	
Nine with main mode Six with aggressive mode	Four
Supported Authentication Methods	
Pre-Shared Key (PSK) Digital RSA Certificate (RSA-SIG) Public key Both peers must use the same authentication method.	Pre-Shared Key Digital RSA Certificate (RSA-SIG) Elliptic Curve Digital Signature Certificate (ECDSA-SIG) Extensible Authentication Protocol (EAP) Asymmetric authentication is supported. Authentication method can be specified during the IKE_AUTH exchange.
Next Generation Encryption (NGE)	
Pre-Shared Key (PSK) Digital RSA Certificate (RSA-SIG) Public key Both peers must use the same authentication method.	AES-GCM (Galois/Counter Mode) mode SHA-256 SHA-384 SHA-512 HMAC-SHA-256 Elliptic Curve Diffie-Hellman (ECDH) ECDH-384 ECDSA-384
Attack Protection	
MitM protection Eavesdropping protection	MitM protection Eavesdropping protection Anti-DoS protection

Table 16-6 Cisco IPsec VPN Solutions

Features and Benefits	Site-to-Site IPsec VPN	Cisco DMVPN	Cisco GET-VPN	FlexVPN	Remote Access VPN
Product interoperability	Multivendor	Cisco only	Cisco only	Cisco only	Cisco only

Features and Benefits	Site-to-Site IPsec VPN	Cisco DMVPN	Cisco GET-VPN	FlexVPN	Remote Access VPN
Key exchange	IKEv1 and IKEv2	IKEv1 and IKEv2 (both optional)	IKEv1 and IKEv2	IKEv2 only	TLS/DTLS and IKEv2
Scale	Low	Thousands for hub-and-spoke; hundreds for partially meshed spoke-to-spoke connections	Thousands	Thousands	Thousands
Topology	Hub-and-spoke; small-scale meshing as manageability allows	Hub-and-spoke; on-demand spoke-to-spoke partial mesh; spoke-to-spoke connections automatically terminated when no traffic present	Hub-and-spoke; any-to-any	Hub-and-spoke; any-to-any and remote access	Remote access
Routing	Not supported	Supported	Supported	Supported	Not supported
QoS	Supported	Supported	Supported	Native support	Supported
Multicast	Not supported	Tunneled	Natively supported across MPLS and private IP networks	Tunneled	Not supported
Non-IP protocols	Not supported	Not supported	Not supported	Not supported	Not supported

Features and Benefits	Site-to-Site IPsec VPN	Cisco DMVPN	Cisco GET-VPN	FlexVPN	Remote Access VPN
Private IP addressing	Supported	Supported	Requires use of GRE or DMVPN with Cisco GET-VPN to support private addresses across the Internet	Supported	Supported
High availability	Stateless failover	Routing	Routing	Routing IKEv2-based dynamic route distribution and server clustering	Not supported
Encapsulation	Tunneled IPsec	Tunneled IPsec	Tunnel-less IPsec	Tunneled IPsec	Tunneled IPsec/TLS
Transport network	Any	Any	Private WAN/MPLS	Any	Any

There are two different ways to encrypt traffic over a GRE tunnel:

- Using crypto maps
- Using tunnel IPsec profiles

Following are the definitions for the LISP architecture components illustrated in Figure 16-5.

- **Endpoint identifier (EID):** An EID is the IP address of an endpoint within a LISP site. EIDs are the same IP addresses in use today on endpoints (IPv4 or IPv6), and they operate in the same way.
- **LISP site:** This is the name of a site where LISP routers and EIDs reside.
- **Ingress tunnel router (ITR):** ITRs are LISP routers that LISP-encapsulate IP packets coming from EIDs that are destined outside the LISP site.
- **Egress tunnel router (ETR):** ETRs are LISP routers that de-encapsulate LISP-encapsulated IP packets coming from sites outside the LISP site and destined to EIDs within the LISP site.
- **Tunnel router (xTR):** xTR refers to routers that perform ITR and ETR functions (which are most routers).

- **Proxy ITR (PITR):** PITRs are just like ITRs but for non-LISP sites that send traffic to EID destinations.
- **Proxy ETR (PETR):** PETRs act just like ETRs but for EIDs that send traffic to destinations at non-LISP sites.
- **Proxy xTR (PxTR):** PxTR refers to a router that performs PITR and PETR functions.
- **LISP router:** A LISP router is a router that performs the functions of any or all of the following: ITR, ETR, PITR, and/or PETR.
- **Routing locator (RLOC):** An RLOC is an IPv4 or IPv6 address of an ETR that is Internet facing or network core facing.
- **Map server (MS):** This network device (typically a router) learns EID-to-prefix mapping entries from an ETR and stores them in a local EID-to-RLOC mapping database.
- **Map resolver (MR):** This network device (typically a router) receives LISP-encapsulated map requests from an ITR and finds the appropriate ETR to answer those requests by consulting the map server.
- **Map server/map resolver (MS/MR):** When MS and the MR functions are implemented on the same device, the device is referred to as an MS/MR.

To facilitate the discovery of VNIs over the underlay Layer 3 network, *virtual tunnel endpoints (VTEPs)* are used. VTEPs are entities that originate or terminate VXLAN tunnels. They map Layer 2 and Layer 3 packets to the VNI to be used in the overlay network. Each VTEP has two interfaces:

- **Local LAN interfaces:** These interfaces on the local LAN segment provide bridging between local hosts.
- **IP interface:** This is a core-facing network interface for VXLAN. The IP interface's IP address helps identify the VTEP in the network. It is also used for VXLAN traffic encapsulation and de-encapsulation.

The VXLAN standard defines VXLAN as a data plane protocol, but it does not define a VXLAN control plane; it was left open to be used with any control plane. Currently, four different VXLAN control and data planes are supported by Cisco devices:

- VXLAN with Multicast underlay
- VXLAN with static unicast VXLAN tunnels
- VXLAN with MP-BGP EVPN control plane
- VXLAN with LISP control plane

Chapter 17

Table 17-4 A Summary of Common 802.11 Standard Amendments

Standard	2.4 GHz?	5 GHz?	Data Rates Supported	Channel Widths Supported
802.11b	Yes	No	1, 2, 5.5, and 11 Mbps	22 MHz
802.11g	Yes	No	6, 9, 12, 18, 24, 36, 48, and 54 Mbps	22 MHz
802.11a	No	Yes	6, 9, 12, 18, 24, 36, 48, and 54 Mbps	20 MHz
802.11n	Yes	Yes	Up to 150 Mbps* per spatial stream, up to 4 spatial streams	20 or 40 MHz
802.11ac	No	Yes	Up to 866 Mbps per spatial stream, up to 4 spatial streams	20, 40, 80, or 160 MHz
802.11ax	Yes*	Yes*	Up to 1.2 Gbps per spatial stream, up to 8 spatial streams	20, 40, 80, or 160 MHz

* 802.11ax is designed to work on any band from 1 to 7 GHz, provided that the band is approved for use.

Chapter 22

The hierarchical LAN design divides networks or their modular blocks into the following three layers:

- **Access layer:** Gives endpoints and users direct access to the network
- **Distribution layer:** Provides an aggregation point for the access layer and acts as a services and control boundary between the access layer and the core layer
- **Core layer (also referred to as the backbone):** Provides connections between distribution layers for large environments

Chapter 23

With SD-Access, an evolved campus network can be built that addresses the needs of existing campus networks by leveraging the following capabilities, features, and functionalities:

- **Network automation:** SD-Access replaces manual network device configurations with network device management through a single point of automation, orchestration, and management of network functions through the use of Cisco DNA Center. This simplifies network design and provisioning and allows for very fast, lower-risk deployment of network devices and services using best-practice configurations.
- **Network assurance and analytics:** SD-Access enables proactive prediction of network-related and security-related risks by using telemetry to improve the performance of the network, endpoints, and applications, including encrypted traffic.

- **Host mobility:** SD-Access provides host mobility for both wired and wireless clients.
- **Identity services:** *Cisco Identity Services Engine (ISE)* identifies users and devices connecting to the network and provides the contextual information required for users and devices to implement security policies for network access control and network segmentation.
- **Policy enforcement:** Traditional access control lists (ACLs) can be difficult to deploy, maintain, and scale because they rely on IP addresses and subnets. Creating access and application policies based on group-based policies using Security Group Access Control Lists (SGACLs) provides a much simpler and more scalable form of policy enforcement based on identity instead of an IP address.
- **Secure segmentation:** With SD-Access, it is easier to segment the network to support guest, corporate, facilities, and IoT-enabled infrastructure.
- **Network virtualization:** SD-Access makes it possible to leverage a single physical infrastructure to support multiple virtual routing and forwarding (VRF) instances, referred to as *virtual networks (VNs)*, each with a distinct set of access policies.

There are three basic planes of operation in the SD-Access fabric:

- Control plane, based on Locator/ID Separation Protocol (LISP)
- Data plane, based on Virtual Extensible LAN (VXLAN)
- Policy plane, based on Cisco TrustSec

There are five basic device roles in the fabric overlay:

- **Control plane node:** This node contains the settings, protocols, and mapping tables to provide the endpoint-to-location (EID-to-RLOC) mapping system for the fabric overlay.
- **Fabric border node:** This fabric device (for example, core layer device) connects external Layer 3 networks to the SDA fabric.
- **Fabric edge node:** This fabric device (for example, access or distribution layer device) connects wired endpoints to the SDA fabric.
- **Fabric WLAN controller (WLC):** This fabric device connects APs and wireless endpoints to the SDA fabric.
- **Intermediate nodes:** These intermediate routers or extended switches do not provide any sort of SD-Access fabric role other than underlay services.

There are three types of border nodes:

- **Internal border (rest of company):** Connects only to the known areas of the organization (for example, WLC, firewall, data center).
- **Default border (outside):** Connects only to unknown areas outside the organization. This border node is configured with a default route to reach external unknown net-

works such as the Internet or the public cloud that are not known to the control plane nodes.

- **Internal + default border (anywhere):** Connects transit areas as well as known areas of the company. This is basically a border that combines internal and default border functionality into a single node.

The Cisco SD-WAN solution has four main components and an optional analytics service:

- **SD-WAN edge devices:** These physical or virtual devices forward traffic across transports (i.e., WAN circuits/media) between locations.
- **vManage Network Management System (NMS):** This SD-WAN controller persona provides a single pane of glass (GUI) for managing and monitoring the SD-WAN solution.
- **vSmart controller:** This SD-WAN controller persona is responsible for advertising routes and data policies to edge devices.
- **vBond orchestrator:** This SD-WAN controller persona authenticates and orchestrates connectivity between edge devices, vManage, and vSmart controllers.
- **vAnalytics:** This is an optional analytics and assurance service.

Chapter 25

In addition to providing standard firewall functionality, a *next-generation firewall* (NGFW) can block threats such as advanced malware and application-layer attacks. According to Gartner, Inc.'s definition, an NGFW firewall must include

- Standard firewall capabilities such as stateful inspection
- An integrated IPS
- Application-level inspection (to block malicious or risky apps)
- The ability to leverage external security intelligence to address evolving security threats

At the core of Cisco Secure Network Analytics are the following components:

- **Cisco Secure Network Analytics Manager, formerly Stealthwatch Management Console (SMC):** The Network Analytics Manager is the control center for Cisco Secure Network Analytics. It aggregates, organizes, and presents analysis from up to 25 Flow Collectors, Cisco ISE, and other sources. It offers a powerful yet simple-to-use web console that provides graphical representations of network traffic, identity information, customized summary reports, and integrated security and network intelligence for comprehensive analysis. The Network Analytics Manager is available as a hardware appliance or a virtual machine.
- **Cisco Secure Network Analytics Flow Collectors:** The Flow Collectors collect and analyze enterprise telemetry data such as NetFlow, IP Flow Information Export (IPFIX), and other types of flow data from routers, switches, firewalls, endpoints, and other network devices. The Flow Collectors can also collect telemetry from proxy data

sources, which can be analyzed by Global Threat Analytics, formerly Cognitive Threat Analytics. It can also pinpoint malicious patterns in encrypted traffic using Encrypted Traffic Analytics (ETA), without having to decrypt it, to identify threats and accelerate response. Flow Collectors are available as hardware appliances and as virtual machines.

- **Cisco Secure Network Analytics Flow Rate License:** The Flow Rate License is required for the collection, management, and analysis of flow telemetry data and aggregates flows at the Network Analytics Manager as well as to define the volume of flows that can be collected.

Cisco Secure Cloud Analytics supports two deployment models:

- Cisco Secure Cloud Analytics Public Cloud Monitoring, formerly Stealthwatch Cloud Public Cloud Monitoring
- Cisco Secure Network Analytics SaaS, formerly Stealthwatch Cloud Private Network Monitoring

802.1x comprises the following components:

- **Extensible Authentication Protocol (EAP):** This message format and framework defined by RFC 4187 provides an encapsulated transport for authentication parameters.
- **EAP method (also referred to as EAP type):** Different authentication methods can be used with EAP.
- **EAP over LAN (EAPoL):** This Layer 2 encapsulation protocol is defined by 802.1x for the transport of EAP messages over IEEE 802 wired and wireless networks.
- **RADIUS protocol:** This is the AAA protocol used by EAP.

802.1x network devices have the following roles:

- **Supplicant:** Software on the endpoint communicates and provides identity credentials through EAPoL with the authenticator. Common 802.1x supplicants include Windows and macOS native supplicants as well as Cisco Secure Client. All these supplicants support 802.1x machine and user authentication.
- **Authenticator:** A network access device (NAD) such as a switch or wireless LAN controller (WLC) controls access to the network based on the authentication status of the user or endpoint. The authenticator acts as the liaison, taking Layer 2 EAP-encapsulated packets from the supplicant and encapsulating them into RADIUS packets for delivery to the authentication server.
- **Authentication server:** A RADIUS server performs authentication of the client. The authentication server validates the identity of the endpoint and provides the authenticator with an authorization result, such as accept or deny.

There are two methods available for propagating an SGT tag: inline tagging (also referred to as *native tagging*) and the Cisco-created protocol SGT Exchange Protocol (SXP):

- **Inline tagging:** With inline tagging, a switch inserts the SGT tag inside a frame to allow upstream devices to read and apply policy. Native tagging is completely independent of any Layer 3 protocol (IPv4 or IPv6), so the frame or packet can preserve the

SGT tag throughout the network infrastructure (routers, switches, firewalls, and so on) until it reaches the egress point. The downside to native tagging is that it is supported only by Cisco network devices with ASIC support for TrustSec. If a tagged frame is received by a device that does not support native tagging in hardware, the frame is dropped. Figure 25-9 illustrates a Layer 2 frame with a 16-bit SGT value.

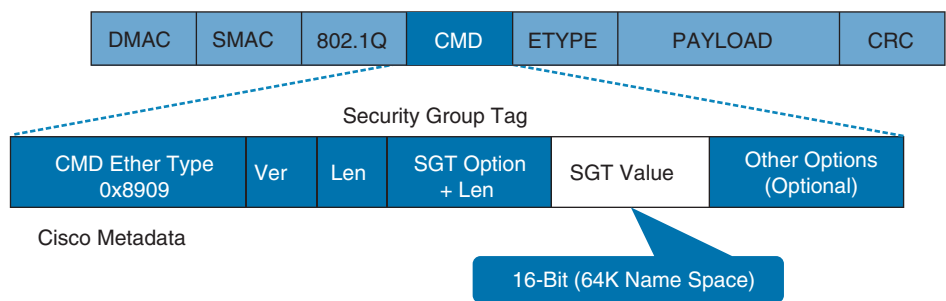


Figure 25-9 Layer 2 Ethernet Frame with an SGT Tag

- **SXP propagation:** SXP is a TCP-based peer-to-peer protocol used for network devices that do not support SGT inline tagging in hardware. Using SXP, IP-to-SGT mappings can be communicated between non-inline tagging switches and other network devices. Non-inline tagging switches also have an SGT mapping database to check packets against and enforce policy. The SXP peer that sends IP-to-SGT bindings is called a *speaker*. The IP-to-SGT binding receiver is called a *listener*. SXP connections can be single-hop or multi-hop, as shown in Figure 25-10.

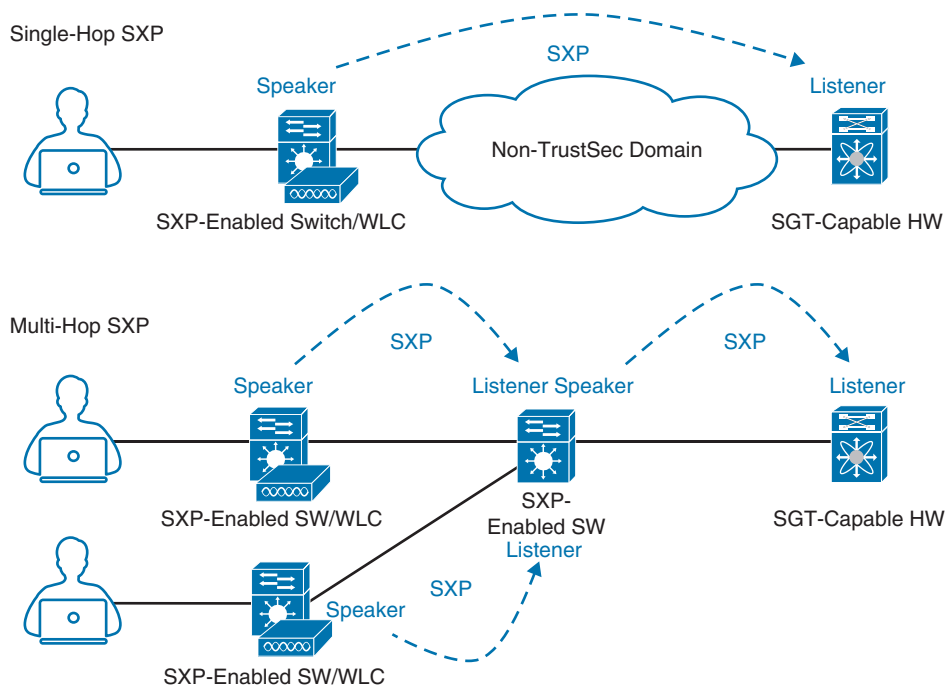


Figure 25-10 Single-Hop and Multi-Hop SXP Connections

Chapter 26

While many different kinds of ACLs can be used for packet filtering, only the following types are covered in this chapter:

- **Numbered standard ACLs:** These ACLs define packets based solely on the source network, and they use the numbered entries 1–99 and 1300–1999.
- **Numbered extended ACLs:** These ACLs define packets based on source, destination, protocol, port, or a combination of other packet attributes, and they use the numbered entries 100–199 and 2000–2699.
- **Named ACLs:** These ACLs allow standard and extended ACLs to be given names instead of numbers and are generally preferred because the name can be correlated to the functionality of the ACL.
- **Port ACLs (PACLs):** These ACLs can use standard, extended, named, and named extended MAC ACLs to filter traffic on Layer 2 switch ports.
- **VLAN ACLs (VACLs):** These ACLs can use standard, extended, named, and named extended MAC ACLs to filter traffic on VLANs.

The Cisco IOS XE CLI by default includes three privilege levels, each of which defines what commands are available to a user:

- **Privilege level 0:** Includes the **disable**, **enable**, **exit**, **help**, and **logout** commands.
- **Privilege level 1:** Also known as User EXEC mode. The command prompt in this mode includes a greater-than sign (R1>). From this mode it is not possible to make configuration changes; in other words, the command **configure terminal** is not available.
- **Privilege level 15:** Also known as Privileged EXEC mode. This is the highest privilege level, where all CLI commands are available. The command prompt in this mode includes a hash sign (R1#).

AAA is an architectural framework for enabling a set of three independent security functions:

- **Authentication:** Enables a user to be identified and verified prior to being granted access to a network device and/or network services.
- **Authorization:** Defines the access privileges and restrictions to be enforced for an authenticated user.
- **Accounting:** Provides the ability to track and log user access, including user identities, start and stop times, executed commands (that is, CLI commands), and so on. In other words, it maintains a security log of events.

Chapter 27

There are two types of hypervisors, as illustrated in Figure 27-2:

- **Type 1:** This type of hypervisor runs directly on the system hardware. It is commonly referred to as “bare metal” or “native.”
- **Type 2:** This type of hypervisor (for example, VMware Fusion) requires a host OS to run. This is the type of hypervisor that is typically used by client devices.

Cisco ENFV delivers a virtualized solution for network and application services for branch offices. It consists of four main components that are based on the ETSI NFV architectural framework:

- **Management and Orchestration (MANO):** Cisco DNA Center provides the VNF management and NFV orchestration capabilities. It allows for easy automation of the deployment of virtualized network services, consisting of multiple VNFs.
- **VNFs:** VNFs provide the desired virtual networking functions.
- **Network Functions Virtualization Infrastructure Software (NFVIS):** An operating system that provides virtualization capabilities and facilitates the deployment and operation of VNFs and hardware components.
- **Hardware resources:** x86-based compute resources that provide the CPU, memory, and storage required to deploy and operate VNFs and run applications.

Chapter 28

Table 28-3 HTTP Functions and Use Cases

HTTP Function	Action	Use Case
GET	Requests data from a destination	Viewing a website
POST	Submits data to a specific destination	Submitting login credentials
PUT	Replaces data in a specific destination	Updating an NTP server
PATCH	Appends data to a specific destination	Adding an NTP server
DELETE	Removes data from a specific destination	Removing an NTP server

Table 28-4 CRUD Functions and Use Cases

CRUD Function	Action	Use Case
CREATE	Inserts data in a database or application	Updating a customer's home address in a database
READ	Retrieves data from a database or application	Pulling up a customer's home address from a database
UPDATE	Modifies or replaces data in a database or application	Changing a street address stored in a database
DELETE	Removes data from a database or application	Removing a customer from a database

Table 28-5 HTTP Status Codes

HTTP Status Code	Result	Common Reason for Response Code
200	OK	Using GET or POST to exchange data with an API
201	Created	Creating resources by using a REST API call
400	Bad Request	Request failed due to client-side issue
401	Unauthorized	Client not authenticated to access site or API call
403	Forbidden	Access not granted based on supplied credentials
404	Not Found	Page at HTTP URL location does not exist or is hidden

This page intentionally left blank

Appendix D

Study Planner

Practice Test	Reading	Task

Element	Task	Goal Date	First Date Completed	Second Date Completed (Optional)	Notes
Introduction	Read Introduction				
1. Packet Forwarding	Read Foundation Topics				
1. Packet Forwarding	Review Key Topics				
1. Packet Forwarding	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 1 in practice test software				
2. Spanning Tree Protocol	Read Foundation Topics				
2. Spanning Tree Protocol	Review Key Topics				
2. Spanning Tree Protocol	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 2 in practice test software				
3. Advanced STP Tuning	Read Foundation Topics				
3. Advanced STP Tuning	Review Key Topics				
3. Advanced STP Tuning	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 3 in practice test software				
4. Multiple Spanning Tree Protocol	Read Foundation Topics				
4. Multiple Spanning Tree Protocol	Review Key Topics				
4. Multiple Spanning Tree Protocol	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 4 in practice test software				
5. VLAN Trunks and EtherChannel Bundles	Read Foundation Topics				
5. VLAN Trunks and EtherChannel Bundles	Review Key Topics				
5. VLAN Trunks and EtherChannel Bundles	Define Key Terms				

Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 5 in practice test software				
6. IP Routing Essentials	Read Foundation Topics				
6. IP Routing Essentials	Review Key Topics				
6. IP Routing Essentials	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 6 in practice test software				
7. EIGRP	Read Foundation Topics				
7. EIGRP	Review Key Topics				
7. EIGRP	Define Key Terms				
7. EIGRP	Review Memory Tables				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 7 in practice test software				
8. OSPF	Read Foundation Topics				
8. OSPF	Review Key Topics				
8. OSPF	Define Key Terms				
8. OSPF	Review Memory Tables				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 8 in practice test software				
9. Advanced OSPF	Read Foundation Topics				
9. Advanced OSPF	Review Key Topics				
9. Advanced OSPF	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 9 in practice test software				
10. OSPFv3	Read Foundation Topics				
10. OSPFv3	Review Key Topics				
10. OSPFv3	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 10 in practice test software				
11. BGP	Read Foundation Topics				
11. BGP	Review Key Topics				
11. BGP	Define Key Terms				

Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 11 in practice test software				
12. Advanced BGP	Read Foundation Topics				
12. Advanced BGP	Review Key Topics				
12. Advanced BGP	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 12 in practice test software				
13. Multicast	Read Foundation Topics				
13. Multicast	Review Key Topics				
13. Multicast	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 13 in practice test software				
14. Quality of Service (QoS)	Read Foundation Topics				
14. Quality of Service (QoS)	Review Key Topics				
14. Quality of Service (QoS)	Define Key Terms				
14. Quality of Service (QoS)	Review Memory Tables				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 14 in practice test software				
15. IP Services	Read Foundation Topics				
15. IP Services	Review Key Topics				
15. IP Services	Define Key Terms				
15. IP Services	Review Memory Tables				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 15 in practice test software				
16. Overlay Tunnels	Read Foundation Topics				
16. Overlay Tunnels	Review Key Topics				
16. Overlay Tunnels	Define Key Terms				
16. Overlay Tunnels	Review Memory Tables				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 16 in practice test software				
17. Wireless Signals and Modulation	Read Foundation Topics				
17. Wireless Signals and Modulation	Review Key Topics				
17. Wireless Signals and Modulation	Define Key Terms				

17. Wireless Signals and Modulation	Review Memory Tables				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 17 in practice test software				
18. Wireless Infrastructure	Read Foundation Topics				
18. Wireless Infrastructure	Review Key Topics				
18. Wireless Infrastructure	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 18 in practice test software				
19. Understanding Wireless Roaming and Location Services	Read Foundation Topics				
19. Understanding Wireless Roaming and Location Services	Review Key Topics				
19. Understanding Wireless Roaming and Location Services	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 19 in practice test software				
20. Authenticating Wireless Clients	Read Foundation Topics				
20. Authenticating Wireless Clients	Review Key Topics				
20. Authenticating Wireless Clients	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 20 in practice test software				
21. Troubleshooting Wireless Connectivity	Read Foundation Topics				
21. Troubleshooting Wireless Connectivity	Review Key Topics				
21. Troubleshooting Wireless Connectivity	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 21 in practice test software				
22. Enterprise Network Architecture	Read Foundation Topics				
22. Enterprise Network Architecture	Review Key Topics				
22. Enterprise Network Architecture	Define Key Terms				
22. Enterprise Network Architecture	Review Memory Tables				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 22 in practice test software				
23. Fabric Technologies	Read Foundation Topics				
23. Fabric Technologies	Review Key Topics				
23. Fabric Technologies	Define Key Terms				
23. Fabric Technologies	Review Memory Tables				

Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 23 in practice test software				
24. Network Assurance	Read Foundation Topics				
24. Network Assurance	Review Key Topics				
24. Network Assurance	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 24 in practice test software				
25. Secure Network Access Control	Read Foundation Topics				
25. Secure Network Access Control	Review Key Topics				
25. Secure Network Access Control	Define Key Terms				
25. Secure Network Access Control	Review Memory Tables				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 25 in practice test software				
26. Network Device Access Control and Infrastructure Security	Read Foundation Topics				
26. Network Device Access Control and Infrastructure Security	Review Key Topics				
26. Network Device Access Control and Infrastructure Security	Define Key Terms				
26. Network Device Access Control and Infrastructure Security	Review Memory Tables				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 26 in practice test software				
27. Virtualization	Read Foundation Topics				
27. Virtualization	Review Key Topics				
27. Virtualization	Define Key Terms				
27. Virtualization	Review Memory Tables				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 27 in practice test software				
28. Foundational Network Programmability Concepts	Read Foundation Topics				
28. Foundational Network Programmability Concepts	Review Key Topics				
28. Foundational Network Programmability Concepts	Define Key Terms				
28. Foundational Network Programmability Concepts	Review Memory Tables				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 28 in practice test software				

29. Introduction to Automation Tools	Read Foundation Topics				
29. Introduction to Automation Tools	Review Key Topics				
29. Introduction to Automation Tools	Define Key Terms				
Practice Test	Take practice test in study mode using Exam Bank 1 questions for Chapter 29 in practice test software				
30. Final Preparation	Read Chapter				
30. Final Preparation	Take practice test in study mode for all book questions in practice test software				
30. Final Preparation	Review Exam Essentials for each chapter on the PDF from book page				
30. Final Preparation	Review all Key Topics in all chapters				
30. Final Preparation	Complete all memory tables from the book page				
30. Final Preparation	Take practice test in practice exam mode using Exam Bank #1 questions for all chapters				
30. Final Preparation	Review Exam Essentials for each chapter on the PDF from the book page				
30. Final Preparation	Take practice test in practice exam mode using Exam Bank #2 questions for all chapters				

This page intentionally left blank