Numerics

6Bone, 417, 446–447
6DISS, 448
6NET, 448
6PE routers
  forwarding performance, 432–433
  MPLS DiffServ, 191–194
  overview, 135–139
  RSVP-TE, 194–199
  security, 347
6to4 addressing, 128–131
6VPE
  forwarding in, 264–266
  label stack, building, 262, 264
  MP-BGP features, 272
  MPLS DiffServ, 191–194
  next hop, 261–262
  router forwarding performance, 432–433
  routing protocols, 260–261
  RSVP-TE, 194–199
  scaling, 270–271
  virtual routing and forwarding, 267–269

AAA (authentication, authorization, and accounting), 360–361
AAAA records, 105
access
  edge/core, 532–537
  global IA (Internet access), 488–489
  media types, 107–109
  MPLS networks, 462–464
  native access, 109
    bridged, 109–110
    PPP-encapsulated, 110–115
    routed, 109
    virtualized, 115–120
  overview, 530–532
  remote access
    enterprise networks, 589
    IPsec VPNs, 254–255
  tunnels, 120–121
    brokers, 122
ISATAP, 123–124
  manually configured, 121–122
  servers, 122
Teredo, 122–123
  unauthorized, 334–336
  WiFi access points, 443
access control lists. See ACLs
access layer
  media types, 107–109
  native access, 109
    bridged, 109–110
    PPP-encapsulated, 110–115
    routed, 109
    virtualized, 115–120
  overview, 106–107
  QoS for IPv6 deployment, 201
  tunnels, 120
ACLs (access control lists)
  example, 355–356
  extended, 353
  IP packet fragmentation, 354–355
  MIPv6, 303–304
  overview, 352
  stateful filtering, 353–354
  time-based, 354
addressing
  6to4, 128–131
  address-space allocation, 444–447
  anycast, 446
  architecture, 445
  enterprise networks, 577, 592–594
  global multicast, 446
  IPv4, 6–8
  loopback, 445
  MPLS networks, 497–499
  multicast, 208–215
  NAT, 11–14
  overview, 6, 526–528
  policies, 444–447
  public versus private, 8–9
  registration, 444–447
  renumbering, 10–11
  RIRs, 446
  SSM, 543
  static vs. dynamic, 9–10
unicast, 445, 528–530
unspecified, 445
VPNs, 18, 252–253
address-resolution attacks, 341–342
ADVERTISE messages, 94
AF (Assured Forwarding) PHB, 183
AFRINIC, 445
aggregated home networks, 314
AH (Authentication Header), 12
Any Source Multicast. See ASM
anycast addresses, 446
filtering traffic, 335
application layer attacks, 346
application classification, 441–442
architecture
addressing, 445
routers, 423–424
ARIN, 445
ARPNIC, 445
AS_PATH attribute, 162
ASM (Any Source Multicast)
intradomain versus interdomain, 231–232
multicast deployment example, 239–247
SSM, versus, 230–231
Assured Forwarding (AF) PHB, 183
attachment router selection, 324
authentication
AAA, 360–361
CHAP, 112
RADIUS, 112
Authentication Header (AH), 12
autoconfiguration, stateless, 100
autonomous systems, 145

B
backbone networks
6PE, 135–139
6to4, 128–131
GRE, 127–128
IPv4, 127
IPv6, 126
layer 2 circuits, 132–134
MPLS, 131–132
IPv4 tunnels over MPLS, 134
native MPLS, 139–140
overview, 125–126

BE (Best Effort) PHB, 183
Bellman-Ford algorithm, 146
Best Effort (BE) PHB, 183
BGP (Border Gateway Protocol)
configuring, 168–169
next hops, 166–168
overview, 161–165
peering, 165–166
BGP-MPLS VPNs, implementing
basic topology, 274–277
dual stack topology, 278–279
forwarding in, 264–266
hub-and-spoke topology, 280–282
Internet access topology, 282–284
interprovider topology, 285–289
label stack, building, 262–264
MP-BGP features, 272
next hops, 261–262
overview, 255–257
route reflector topology, 279–280
routing protocols, 260–261
routing table segregation, 257–260
scaling, 270–271
virtual routing and forwarding, 267–269
Binding Acknowledgment message, 296
binding databases, 102
Binding Error message, 296
Binding Refresh Request message, 296
Binding Update message, 296
bindings, 294
black hole routes, 100
bootstrap router (BSR)
configuring, 240–241
overview, 226–227
Border Gateway Protocol. See BGP
bridged access, 109–110
broadcast-amplification attacks, 343
brokers, tunnel, 122
BSR (bootstrap router), 226–227
configuring, 240–241
business drivers, enterprise network
deployments, 574–575

C
Care-of Test Init message, 296
Care-of Test message, 296
CBTS (COS-based TE tunnel selection), 198–199
CE (customer edge)-based VPNs
   IPsec VPNs, implementing, 254
      deploying, 255
      example, 273–274
      remote access, 254–255
      routing protocols, 255
      tunnel alternatives, 255
      overview, 251–252
      security, 253–254, 347–348
centralized forwarding routers, 424
CHAP (Challenge Handshake Authentication Protocol), 112
CIDR (Classless Inter-Domain Routing), 7
Cisco HSRP protocol, 599–601
Cisco IOS Firewall, 357–359
Cisco Learning Connection (CLC), 449
Cisco Network Registrar (CNR), 93
Cisco SAFE Blueprint, 20
classification, 176
Classless Inter-Domain Routing (CIDR), 7
CNR (Cisco Network Registrar), 93
communities of interest, 321, 519–520
Compressed Real Time Protocol (cRTP), 181
cost analysis
   applications, 441–442
   hosts, 440–442
   network elements, 442–443
   operations, 443–444
   overview, 439
cRTP (Compressed Real Time Protocol), 181
customer edge-based VPNs
   IPsec VPNs, implementing
      deploying, 255
      example, 273–274
      remote access, 254–255
      routing protocols, 255
      tunnel alternatives, 255
      overview, 251–252
      security, 253–254, 347–348
customer interfaces, 545, 547
d data plane, 419–420
Default Router Preferences (DRP), 597
delegating routers, 101–102
deployment
   addressing, 526–532
   edge core, 528–537
   content distribution, 541–551
   content hosting/storage, 538
   design, 520–521
   design options
      dual stack, 523–525
      PPP/L2TP, 521–523
DNS, 538
Internet access, 539–541
network environment, 509–515
plans, 515–516
QoS, 551–555
service rollout, 537–538
targeted services
   communities of interest, 519–520
   content delivery, 518
   content hosting/storage, 517
   DNS services, 517
   Internet access, 517
   mail services, 517
   MIPv6, 519–520
unicast connectivity, 516
VoIP, 517–518
unicast, 89
design goals
dual stack options, 523–525
overview, 520–521
PPP/L2TP options, 521–523
destination option, 297
DHAAD (Dynamic Home Agent Address Discovery), 295–298, 303
DHCP (Dynamic Host Configuration Protocol), 9, 94–95
binding databases, 102
DHCP-PD, 96–98
DUID (DHCP Unique Identifier), 97
prefix pools, 101–102
protocol description, 96–98
provisioning, 93
RRs (Requesting Routers), 98–101
stateless, 103–104
dialup, 509
DiffServ (differentiated services), 15, 176, 181–194
diffusing update algorithm (DUAL), 150
distance vector routing protocol, 146–147
distributed forwarding routers, 424
distributed home networks, 316–317
DNS (Domain Name System)
AAAA records, 105
deployment, 538
enterprise networks, 583–584
ip6.arpa domain, 105
overview, 11, 103–104
query messages, 105–106
Resource Records, 105
Doors protocol, 318
DoS attacks, 343
DRP (Default Router Preferences), 597
DSL (Digital Subscriber Line), 9
DUAL (diffusing update algorithm), 150
dual stack, 523–525
dual-stack networks
enterprise networks, 594–595
managing, 605
overview, 103
VPNs, 278–279
DUID (DHCP Unique Identifier), 97
Duplicate Address Detection (DAD), 94, 296
Dynamic Home Agent Address Discovery (DHAAD), 295–298, 303
Dynamic Host Configuration Protocol.
See DHCP

E

ECN (explicit congestion notification), 183
edge policies
MPLS service provider networks
overview, 468–478
PE router design, 470–471
PE-CE interface design, 471–473
PE-CE routing design, 473–476
PE-PE routing design, 477–478
overview, 202
edge/aggregation layer, 201
edge/core access, 532–537
education, 447–449
EF (Expedited Forwarding) PHB, 183
EGPs (exterior gateway protocols), 145
EIGRP (Enhanced Interior Gateway Protocol)
configuring, 152–153
IPv6 support, 151–152
overview, 150–151
embedded RP, 227–229, 244–247
Encapsulating Security Payload (ESP), 12
encryption, 442
Enhanced Interior Gateway Protocol. See EIGRP
enterprise networks, IPv6 deployments
addressing, 577, 592–594
business drivers, 574–575
default router, configuring, 597–598
DNS, 583–584
dual-stack approach, 594–595
equipment overview, 576
first-hop router redundancy, 596–601
future evolutions, 610–613
host configuration, 580–581
infrastructure, 571–574
Internet-to-campus connectivity, 587–589
IP Mobility, 606–609
ISATAP router configuration, 584–586
managing, 605
market expansion, 612–613
moving IPv6 to production, 590–591
multicast services, 602–605
QoS, 609–610
remote site configuration, 589
routing protocols, 595
security, 601–602, 611–612
troubleshooting, 610
ESP (Encapsulating Security Payload), 12
Ethernet MPLS, 133
Euro6IX, 448
Expedited Forwarding (EF) PHB, 183
explicit congestion notification (ECN), 183
extended home networks, 313–314
extension headers, 179
exterior gateway protocols (EGPs), 145
faster roaming, 323
filtering
stateful, 353–354
traffic, 334–335
firewalls
Cisco IOS Firewall, 357–359
overview, 356, 442
PIX Firewall, 359–360
fish problem, 195
fleet in motion, 309–310
flooding attacks, 343, 346
flow label, 179
forwarding
in BGP-MPLS IPv6 VPNs, 264–266
multicast, 215–225
router performance, measuring
6PE/6VPE environments, 432–433
black-box testing, 420–422
centralized versus distributed forwarding, 424
control plane, 417–419
data plane, 419–420
evaluation checklist, 433–435
high-end routers, 429–432
low-end routers, 425–426
mid-range routers, 426–429
overview, 415–417
software versus hardware forwarding, 423
fragmentation, IP packets, 337–338, 354–355
GARP (Generic Attribute Registration Protocol), 214
general prefixes, 98
global addresses, 253
global IA (Internet access), 488–489
global multicast, 446
GRE (Generic Routing Encapsulation), 127–128
group multicast addresses, 209–215
hardware forwarding routers, 423
upgrade costs, 441
headers
AH (Authentication Header), 12
extension, 179
Mobility, 295–297
security threats, 336–337
high-end router forwarding performance, 429–432
home gateways, 306
home networks, 313
Home Test Init message, 296
Home Test message, 296
host-initialization attacks, 341–342
hosts
cost analysis, 440–442
deployment, 300–304
mobility
destination option, 297
DHAAD, 297–298
Mobility header, 295–297
overview, 292–295
route optimization, 298
security, 299–300
hotspots, 305
hub-and-spoke topology, PE-based VPNs, 280–282
IANA, 446
IA-PD (Identity Association Prefix Delegation), 97
ICMP
 traffic filtering and, 335–336
IGMP (Internet Group Management Protocol), 209
IGPs (interior gateway protocols), 145, 148
EIGRP
 configuring, 152–153
 IPv6 support, 151–152
 overview, 150–151
IS-IS
 configuring, 159–161
 IPv6 support, 158–159
 overview, 157
OSPFv3
 configuring, 155–157
 IPv6 support, 154–155
 overview, 153–154
RIPng
 configuring, 149–150
 IPv6 support, 148–149
 overview, 148
integrated services (IntServ)
 IPv4, 176
 overview, 15, 189–190
interdomain routing
 BGP next hop, 166–168
 BGP peering, 165–166
 overview, 164–165
interior gateway protocols. See IGPs
Intermediate System-to-Intermediate System. See IS-IS
Internet Group Management Protocol (IGMP), 209
Internet-enabled cars, 307–308
interprovider VPNs, 285–289
Intra-Site automatic Tunnel Addressing Protocol (ISATAP), 123–124
Integrated Digital Services Network (ISDN), 9, 509
IntServ (integrated services), 189–190
 IPv4, 176
(IP Mobility, 606–609
ip6.arpa domain, 105
IPsec
 communication, securing, 348–352
VPNs, implementing
 deploying, 255
 example, 273–274
 remote access, 254–255
 routing protocols, 255
tunnel alternatives, 255
IPSs, 442
IPv4
 addressing, 6–8
coeexistence with IPv6, 204–205
mobility, 293
multicast, 17
QoS, 15, 179–181
services, 509–515
IPv6
coeexistence with IPv4, 204–205
EIGRP support, 151–152
IS-IS support, 158–159
OSPFv3 support, 154–155
RIPng support, 148–149
See also MIPv6
IPv6 Form, 447
IPv6 Task Force, 448
ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), 123–124
configuring routers for enterprise networks, 584–586
ISDN (Integrated Digital Services Network), 9, 509
IS-IS (Intermediate System-to-Intermediate System)
 configuring, 159–161
 IPv6 support, 158–159
 overview, 157
L2TP networks, 521–523
 access aggregation, 116–120
label stack, building for 6VPE, 262–264
LACNIC, 445
layer 2
  circuits, 132–134
  multicast protocols, 214
  QoS, 180
layer 3
  QoX, 179–180
  spoofing attacks, 338–341
layer 4 spoofing attacks, 338–341
LFI (link fragmentation and interleaving), 181
link-efficiency mechanisms, 180–181
link-local addresses, 498
link-state vector routing protocol, 147–148
load balancing servers, 322
load sharing, 169–170
Local Mobility Management (LMM), 301
loopback addresses, 445
low-end router forwarding performance, 425–426

M
  mail services, 517
  man-in-the-middle attacks, 346
  marking, 176
  MBGP (Multiprotocol BGP), 217–218
  MDTs (multicast distribution trees), 215–216
  MFIB (Multicast Forwarding Information Base), 225
  mid-range router forwarding performance, 426–429
  MIP (Mobile IP), 21–22, 292
  MIPv4, 293
  MIPv6, 21–22, 294–295, 519–520
  deployment, 300–304
  destination option, 297
  DHAAD, 297–298
  Mobility header, 295–297
  route optimization, 298
  security, 299–300
  MLD (Multicast Listener Discovery) protocol, 209–214
  mobile ad-hoc networking, 324
  mobile home networks, 314–316
  mobile network node (MNN), 311
  mobile nodes, 292
  mobile routers, 311
  mobility
    deployment, 300–304
    future
      attachment router selection, 324
      faster roaming, 323
      integration with mobile ad-hoc networking, 324
      movement detection, 323
      multihoming, 325
      route optimization for NEMO, 325–326
    hosts
      destination option, 297
      DHAAD, 297–298
      Mobility header, 295–297
      overview, 292–295
      route optimization, 298
      security, 299–300
    IPv4, 293
    NEMO, 22
    network
      aggregated home networks, 314
      distributed home networks, 316–317
      enterprises on the move, 305
      extended home networks, 313–314
      fleet in motion, 309–310
      home gateways, 306
      home networks, 313
      Internet-enabled cars, 307–308
      mobile home networks, 314–316
      object model, 311
      operations, 311–313
      PANs, 306–307
      sensor networks, 308–309
      terminology, 311
      virtual home networks, 317
    nonmobile scenarios
      community of interest, 321
      IPv4 to IPv6 transitioning, 318
      route projection, 321–322
      overview, 317–318
      server load balancing, 322
      topology hiding, 319–321
    Mobility header, 295–297
    mobiquity, 291, 327
    Moonv6, 448
    More-Specific Routes (MSR), 598
    movement detection, 323
    MP_REACH_NLRI attribute, 166
**MP-BGP (multiprotocol BGP) extensions**
- next hop, 166–168
- overview, 164–165
- peering, 165–166
  - VPNv6 features, 272

**MPLS (Multiprotocol Label Switching), 131–132**
- DiffServ, 190–194
- Ethernet, 133
- forwarder, 138
- IPv4 tunnels, 134
- multicast deployments, 233–234
- overview, 17, 139–140
- service provider deployments
  - access design, 462–464
  - addressing, 497–499
  - core design, 465–468
  - Cs-C-CE configuration, 493
  - design objectives, 453–460
  - edge design, 468–478
  - global Internet access design and implementation, 488–489
  - inter-AS design, 484–487
  - MTU discovery, 500
  - POP design, 464–465
  - QoS design, 493–496
  - route reflector design, 479–481
  - security, 500–501
  - troubleshooting, 502–507
  - VPN IA service design and implementation, 490–492
  - VPN service design and implementation, 489–490
  - VRF design, 482–484
  - traffic engineering, 195
- MPLS-TE, 190
- MSR (More-Specific Routes), 598
- MTU discovery, 500
- multicast distribution trees (MDTs), 215–216
- Multicast Forwarding Information Base (MFIB), 225
- Multicast Listener Discover (MLD) protocol, 209–214
- multicast services, 16–17, 207–208
  - addressing, 208–215
  - deployment, 225
    - ASM model, 230–232, 239–247
    - domain control, 225–226
    - enterprise networks, 602–605
  - MPLS infrastructures, 233–234
  - RP mapping and redundancy, 226–229
  - service models, 229–232
  - SSM model, 213, 230–239
  - tunneling mechanisms, 232
  - filtering traffic, 336
  - implementation, 547–551
  - IPv4, 17
  - layer 2 protocols, 214–215
  - routing and forwarding, 215–225, 563–565
- multicast VPN (MVPN), 17, 233
- multihoming
  - MPLS networks, 499
  - overview, 169–170, 325
- multiprotocol BGP extensions (MP-BGP)
  - next hop, 166–168
  - overview, 217–218, 164–165
  - peering, 165–166

**Neighbor Discovery (ND), 291, 596**
- Neighbor Solicitation messages, 596
- Neighbor Unreachability Detection (NUD), 596–597
- NEMO (NEtwork MObility) standards, 22, 304
- neighbor access. See access
- Network Architecture Protocol (NAP), 12, 304
- network mobility
  - aggregated home networks, 314
  - distributed home networks, 316–317
  - enterprises on the move, 305
  - extended home networks, 313–314
  - fleet in motion, 309–310
  - home gateways, 306
  - home networks, 313
  - Internet-enabled cars, 307–308
  - mobile home networks, 314–316
operations, 311–313
PANs, 306–307
sensor networks, 308–309
terminology, 311
virtual home networks, 317
NETwork MObility (NEMO), 22, 304
next hops
6VPE, 261–262
BGP, 166–168
BGP-MPLS, 261–262
NEXT_HOP attribute, 162
NUD (Neighbor Unreachability Detection), 596–597
operating systems, 440–441
operations cost analysis, 443–444
ORF (outbound route filtering), 270
OSPFv3 (Open Shortest Path First version 3)
configuring, 155–157
IPv6 support, 154–155
overview, 153–154
outbound route filtering (ORF), 270
PANs (personal-area networks), 306–307
Partner e-Learning Connection (PEC), 449
path vector routing protocol, 147
PE (provider edge)-based VPNs
BGP-MPLS VPNs, implementing
basic topology, 274–277
dual stack topology, 278–279
forwarding in, 264–266
hub-and-spoke topology, 280–282
Internet access topology, 282–284
interprovider topology, 285–289
label stack, building, 262–264
MP-BGP features, 272
next hops, 261–262
overview, 255–257
route reflector topology, 279–280
routing protocols, 260–261
routing table segregation, 257–260
scaling, 270–271
VRF (virtual routing and forwarding), 267–269
overview, 252
security, 253–254, 347–348
peering, BGP, 165–166
penultimate hop popping (PHP), 137, 266
performance, router forwarding
6PE/6VPE environments, 432–433
centralized versus distributed forwarding, 424
data plane, 419–420
evaluation checklist, 433–435
high-end routers, 429–432
low-end routers, 425–426
measuring, 420–422
mid-range routers, 426–429
overview, 415–417
software versus hardware forwarding, 423
PHP (penultimate hop popping), 137, 266
PIM traffic forwarding, 243–244
PIM-Bidir, 220, 225
PIM-SM, 220–229
PIM-SSM, 220, 224–225
Ping command, 581
PIX Firewall, 359–360
policy function, 176
POP design, 464–465
PP (Point-to-Point Protocol), 521–523
PPP over ATM (PPPoA), 111–113
PPP over Ethernet (PPPoE), 113–115
PPP-encapsulated access
overview, 110
PPPoA, 111–113
PPPoE, 113–115
PPVPN (provider-provisioned VPNs), 251
prefixes, 445
delegation, 95–103
genereal, 98
pools, 101–102
RIR, 446
private addresses
public addresses, versus, 8–9
VPN IPv4 sites, 253
protocols
multicast, 207–208
routing
BGP-MPLS VPNs, 260–261
enterprise networks, 595
IPsec VPNs, 255
See also specific protocols
provider edge (PE)-based VPNs. See PE
(provider edge)-based VPNs
provider-provisioned VPNs (PPVPN), 251
provisioning, 91, 559–561
host addresses, 91–93
prefix delegation
Delegating Routers, 101–102
overview, 95–96
protocol description, 96–98
RRs, 98–101
stateful DHCP, 93–95
public addresses, 8–9
remote access
enterprise networks, 589
IPsec VPNs, 254–255
rendezvous points. See RPs
renumbering
addresses, 10–11
VPNs, 18
REPLY messages, 94
Requesting Routers (RRs), 96
resolvers, 104
Resource Records, 104–105
return on investment (ROI)
hosts, 440–442
network elements, 442–443
operations, 443–444
overview, 439
reverse routability, 298
reverse-path forwarding (RPF), 216–219
RGMP (Routing Group Management Protocol), 214
RIBs (Routing Information Bases), 149
RIPE, 445
RIPng
configuring, 149–150
IPv6 support, 148–149
RIRs (Regional Registries), 445
roaming, 323
rogue devices, 346
rollout, service, 537–538
route flapping, 343
route optimization, 295, 298
route optimization for NEMO, 325–326
route projection, 321–322
route reflectors
MPLS networks, 479–481
PE-based VPNs, 270–271, 279–280
route refresh, PE-based VPNs, 270–271
routed access, 109
Routed Bridged Encapsulation (RBE)
feature, 109
Router Group Management Protocol (RGMP), 214
routers, 442
architecture, 423–424
first-hop redundancy, 596–601
forwarding performance
6PE/6VPE environments, 432–433
centralized versus distributed forwarding, 424
control plane, 417–419
data plane, 419–420
evaluation checklist, 433–435
high-end routers, 429–432
low-end routers, 425–426
measuring, 420–422
mid-range routers, 426–429
overview, 415–417
software versus hardware forwarding, 423
mobile, 311
VRF-aware commands, 269
routing, 14
attacks, 343–344
multicast, 215–225
Routing Information Bases (RIBs), 149
Delegating Routers, 102
routing protocols, 145
BGP-MPLS VPNs, 260–261
deploying
network access, 172–173
network core, 170–172
network distribution/edge, 172
distance vector routing, 146–147
enterprise networks, 595
IPv6 VPNs, 255
link-state vector routing protocol, 147–148
path vector routing protocol, 147
See also specific protocols
RPs (rendezvous points), 215
embedded RP, 227–229, 244–247
PIM-Bidir, 225
PIM-SM, 224
PIM-SSM, 224–225
RPF (reverse-pathforwarding), 216–219
RPs (Rendezvous Points), 17
RRs (Requesting Routers), 96–101
RSVP-TE, 194–199
RTP (Real Time Protocol), 181

security
6PE, 347
access, 556–558
best practices, 364–365
Cisco SAFE Blueprint, 20
data center, 558–559
data plane, 419–420
data plane, 420–422
data center, 558–559
data center, 558–559
enterprise network deployments, 601–602, 611–612
MIPv6, 21, 299–300, 345
MPLS, 500–501
NAT, 12
overview, 20–21, 329–332
threats
address-resolution attacks, 341–342
application layer attacks, 346
broadcast-amplification attacks, 343
flooding attacks, 346
header manipulation, 336–337
host-initialization attacks, 341–342
man-in-the-middle attacks, 346
reconnaissance, 332–334
rogue devices, 346
routing attacks, 343–344
sniffing, 346
spoofing, 338–341
transition-mechanism attacks, 344–345
unauthorized access, 334–336
viruses, 344
worms, 344
tools
AAA (authentication, authorization, and accounting), 360–361
ACLs (access control lists), 352–356
firewalls, 356–360
IPsec, 348–352
overview, 348
trafﬁc rate limiting, 363–364
uRPF (Unicast Reverse Path Forwarding), 344, 361–363
VPNs, 19, 253–254, 347–348
sensor networks, 308–309
server load balancing, 322
service level agreements, 15
service provider deployments (MPLS)
access design, 462–464
addressing, 497–499
core design, 465–468
CsC-CE configuration, 493
design objectives, 453–460
design, 468–478
global Internet access design and implementation, 488–489
inter-AS design, 484–487
MTU discovery, 500
POP design, 464–465
QoS design, 493–496
route reflector design, 479–481
security, 500–501
troubleshooting, 502–507
VPN IA service design and implementation, 490–492
VPN service design and implementation, 489–490
VRF design, 482–484

service providers, 16

services
advanced, 541–542
multicast, 542–551
rollout, 537–538
targeted, 516–520

shaping function, 176
shortest path trees (SPTs), 215–216
SIP (Session Initiation Protocol), 12
smurf attacks, 343
sniffing, 346
software
forwarding routers, 423
upgrade costs, 441
SOLICIT messages, 94
Source Specific Multicast. See SSM
spoofing attacks, 338–341
uRPF (Unicast Reverse Path Forwarding), 341, 361–363
SPTs (shortest path trees), 215–216
SSM (Source Specific Multicast)
ASM, versus, 230–231
overview, 543
SSM mapping for MLDv1, 213
SSM mapping for MLDv2, 234–239
Start Here manual, 442
stateful DHCP, 91–95
stateful filtering, 353–354
stateless autoconfiguration
address renumbering, 92–93
operation, 92
stateless DHCP, 103–104
static addresses, 9–10
storage, 443
switches, 442

T

TACACS+ (Terminal Access Controller Access Control System Plus), 361
targeted services
communities of interest, 519–520
content delivery, 518
content hosting/storage, 517
DNS services, 517
Internet access, 517
mail services, 517
MIPv6, 519–520
overview, 516
unicast connectivity, 516
VoIP, 517–518
Teredo tunnels, 122–123
TIB (Tree Information Base), 219
topology hiding, 319–321
Traceroute command, 581
traffic conditioning, 176
traffic engineering, 195
traffic filtering, 334–335
traffic forwarding, PIM, 243–244
traffic rate limiting, 363–364
training, 447–449
transitioning, 318
transition-mechanism attacks, 344–345
translation mechanisms, 140–143
Tree Information Base (TIB), 219
troubleshooting
troubleshooting
enterprise network deployments, 610
MPLS service provider networks, 502–507
multicast routing/forwarding, 563–565
overview, 555
provisioning, 559–561
secure networks
access, 556–558
data center, 558–559
edge, 558
overview, 555–556
unicast routing/forwarding, 561–563
tunnels
6to4, 128–131
brokers, 122
GRE, 127–128
IPsec VPNs, 255
IPv4, 127, 134
ISATAP, 123–124
layer 2 circuits, 132–134
manually configured, 121–122
multicast deployments, 232
overview, 120–121
servers, 122
Teredo, 122–123

ULAs (unique local addresses), 253, 498–499
unauthorized access, 334–336
unicast, 6
access layer
media types, 107–109
native access, 109–115
virtualized, 115–120
address space, 445
addressing
IPv4, 6–8
NAT, 11–14
public vs. private, 8–9
renumbering, 10–11
static vs. dynamic, 9–10
connectivity, 516, 528–530
deployment mechanisms, 89
routing, 14, 561–563
forwarding, 561–563
service rollout, 537
tunnels
brokers, 122
ISATAP, 123–124
manually configured, 121–122
servers, 122
Teredo, 122–123
Unicast Reverse Path Forwarding (uRPF), 341, 361–363
unicast routing/forwarding, 561–563
unique local addresses (ULAs), 253, 498–499
unspecified addresses, 445
upgrade costs
hosts, 440–441
network elements, 442–443
operations, 443–444
overview, 439–442
uRPF (Unicast Reverse Path Forwarding), 341, 361–363

V
vendor-specific attributes (VSAs), 360–361
virtual home networks, 317
virtual routing and forwarding. See VRF
virtualized access layer
L2TPv2 access aggregation, 116–119
L2TPv3 access aggregation, 119–120
overview, 115
viruses, 344
VLSM (variable-length subnet mask), 7
VoIP, 517–518
VPNs (virtual private networks)
addressing, 18, 252–253
benefits, 18
cost savings, 18
extended connectivity, 18
overview, 18–19, 249–251
privacy, 19
renumbering, 18
security, 19, 253–254, 347–348
services, 18
VRF (virtual routing and forwarding)
associating to an interface, 269
configuring, 268
MPLS networks case study, 482–484
overview, 267
VRF-aware router commands, 269
VSAs (vendor router commands), 360–361

W
websites, 449
WiFi access points, 443
worms, 344