

Numbers

- 802.1p, QoS values, 275–276**
- 802.1q trunking, 66**
- 802.1x networks**
 - dot1x client-based authentication, 306–311
 - protocols, 303–306
 - roles, 302–303

A

- aaa authentication
 - dot1x command, 309
 - network default group radius command, 312
- access control lists (ACLs), 43, 253**
- access layer, 317–318**
 - access switches, 289–293
 - authentication, 293–295
 - client-based Layer 2 authentication, 301–311*
 - clientless authentication, 295–301*
 - definition of, 293*
 - authorization, 293–295
 - hierarchical WAN architecture, 26
 - sample virtualized access layer, 311–316
- access ports, assigning to VLAN, 128–129**
- access switches, 293**
 - CAM, 291
 - enforcing security policies with, 291
 - hierarchical campus design, 19
 - private VLANs, 291
 - QoS deployment, 292
 - stacking, 291
 - VLANs, 290
 - wiring closet deployment, 289–290
- access-distribution blocks, Layer 2 h2h architectures, 126–127**
- access-distribution data path virtualization, Layer 2 h2h architectures, 127–128**
- access-distribution segmentation, Layer 2 h2h architectures, 127**
- ACL (access control lists), 43, 253**
 - h2h architectures, 94
 - Layer 3 h2h architectures, 138–140
- acquisitions, virtualization, 11
- Active Directory (AD), 299**
- AD (Active Directory), 299**
- Address Resolution Protocol (ARP), 291, 295**
- adjacencies (FIBs), 58**
- AF PHB (assured forwarding per-hop behaviors), 275**
- aggregation routers, hierarchical WAN architecture, 26**
- AH headers (IPsec), 69**
- airports, virtualization, 10**
- any-to-any VPN (Virtual Private Networks), unprotected shared services, 212**
- architecture (QoS), 44**
- ARP (Address Resolution Protocol), 291, 295**
- authentication, 47–48, 293–295**
 - authentication failure, 309
 - client-based Layer 2 authentication, 301
 - 802.1x protocols, 303–306*
 - 802.1x roles, 302–303*
 - dot1x implementation, 306–311*
 - clientless authentication
 - centralized dynamic clientless authentication, 297–299*
 - Layer 3 clientless authentication, 299–301*
 - MAC authentication, 295–296*
 - static clientless authentication, 296–297*
 - definition of, 293
 - failure, 309
 - guest access, 7
 - servers (802.1x networks), 302
- authenticators (802.1x networks), 302**
- auth-fail VLANs, 308**
- authorization, 47–48, 294–295**
 - definition of, 293
 - guest access, 7
- auto-discovery, tunnel-based L2VPN architectures, 107**
- auto-provisioning, tunnel-based L2VPN architectures, 107**
- auto-rp feature, 262**
- awareness (VRF), 62**

B – C

bandwidth

BC

MAM, 335–336

RDM, 335

guaranteed bandwidth, 278–279, 335–337

BBSM (Building Broadband Service Manager), 301

BGP (Border Gateway Protocol), 61, 160

BPDU (bridge protocol data unit), 290, 304

branch-end routers, hierarchical WAN architecture, 26

broadcast, compared to multicast, 242

business requirements for virtualization, 14

CAM (content-addressable memory), 291

campuses

hierarchical design, 17

access switches, 19

distribution switches, 19

equal-cost paths, 19

failure-isolation features, 21

failures, effects of, 19

IGP, 19

Layer 2 (switched) connectivity, 19–21

Layer 3 (routed) technologies, 19–21

network layers, collapsing, 21

topology designs, 19

VLAN, 22

modular design, 18

car manufacturers, virtualization, 9

CBR (constraint-based routing)

MPLS-TE, 332

TE, 278

CDP (Cisco Discovery Protocol), 291

CDPv2 (Cisco Discovery Protocol Version 2), 310

CE (customer edge), 76

centralized policies, 37

CHAP (Challenge Handshake Authentication Protocol), 303

Class D addresses, 242

Classification policy mechanism, QoS, 274

client-based Layer 2 authentication, 301

802.1x protocols, 303–306

802.1x roles, 302–303

dot1x implementation, 306–311

clientless authentication

centralized dynamic clientless authentication, 297–299

Layer 3 clientless authentication, 299–301

MAC authentication, 295–296

static clientless authentication, 296–297

collapsing network layers, hierarchical campus design, 21

colleges, virtualization, 12

communication interfaces, virtual enterprise networks, 38

configuration

dot1x client-based authentication, 306–311

GRE, 68–69, 260

IPsec, 71–72

L2TPv3, 73, 75

LSPs, 80–82

mVPN

D1 BGP configuration, 268

MVRF and MDT configuration on

D1, 268

native multicast configuration on

C1, 267

OSPF, 84

per-VRF iBGP configuration, 85

per-VRF RIP configuration, 84

RP, 262

Congestion avoidance policy mechanism, QoS, 274

constrained routing, h2h architectures, 95

consultant access (networks), 8

content-addressable memory (CAM), 291

contractors access (networks), 8

control-plane 41

segmentation, 45–47

virtualization, 41, 83

MTR, 85–86

OSPF, 84

per-VRF iBGP configuration, 85

per-VRF RIP configuration, 84

summary, 86

VRF-aware routing, 84

convergent services, reasons for virtualization, 9

core layer, hierarchical WAN architecture, 26

core links, converting to dot1q trunks, 133–134

crypto isakamp policy command, 71

crypto maps, 71–72

CsC (Carrier supporting Carrier)
 VPN, 116–119
 WAN, VN extensions over, 187–192

CSPE, MPLS-TE, 332

CT (Class-Types)
 BC
 MAM, 335–336
 RDM, 335
 DS-TE, 337
 guaranteed bandwidth, 335

customer edge (CE), 76

D

data MDTs, 264

data-link connection identifiers (DLCIs), 75

data-path virtualization, 41, 66
 802.1q trunking, 66
 GRE, 66–69
 IPsec, 69–72
 L2TPv3, 72–75
 LSPs, 75
 CE, 76
 edge LSRs, 76
 FIBs, 79
 IOS configuration, 80–82
 LDP, 78
 LSRs, 76
 MPLS packet forwarding, 76–77
 summary, 83

DCSPs (differentiated services code points), 86

default MDTs, 264

Dense mode (PIM-DM), 248

device virtualization, 41
 definition of, 56
 network infrastructure requirements, 55
 summary, 65
 VLANs, 56–57
 VRFs
 definition of, 57
 displaying, 58
 FIB, 58–60
 LR, 61
 multiple VRF on routers, 57–58
 RIB, 58–60
 sharing routes between, 58
 VFI, 63–64
 virtual firewall contexts, 64–65
 VRF awareness, 62
 VR, 61

DHCP services
 dedicated services per VPN, 236
 shared services, 237

dialup networks, client-based authentication, 301

differentiated services code points (DSCPs), 44, 86

DiffServ (Differentiated Services), 275–276

digital subscriber line (DSL), client-based authentication, 301

Distance Vector Multicast Routing Protocol (DVMRP), 246

distribution layer, hierarchical WAN architecture, 26

distribution switches, hierarchical campus design, 19

DLCIs (data-link connection identifiers), 75

DMVPN (dynamic multipoint VPN)
 RFC 2547 VPN over (WAN, VN extensions over), 202–205
 VRF interconnections (WAN, VN extensions over), 200–202
 tunnel-based L3VPN architectures, 98–101
 WAN, 178

DNS (Domain Name System), 238, 301

dot1x client-based authentication, 306–311

dot1x guest vlan command, 308

dot1x guest-vlan command, 314

dot1x port-control command, 306

dot1q trunks, converting core links to, 133–134

DSCP (differentiated services code points), 44, 275–276

DSL (digital subscriber line), client-based authentication, 301

DS-TE (DiffServe-aware), 335
 CT, 337
 MPLS QoS, 279, 283

dual-circuit resiliency (WAN), scalable enterprise network design, 27

DVMRP (Distance Vector Multicast Routing Protocol), 246

dynamic groups, 315–316

dynamic NAT, routed firewalls, 232–234

dynamic network membership, 294

dynamic routing protocols, failure detection in GRE tunnel-based L3VPN architectures, 152

E

EAP (Extensible Authentication Protocol), 303–304

EAPOL (Extensible Authentication Protocol over LAN), 303–305

edge LSRs (label switching routers), 76

EF PHB (expedited forwarding per-hop behaviors), 275

EIGRP (Enhanced Interior Gateway Routing Protocol), 137, 291

E-LSP, MPLS QoS, 277

employee access (networks), 8

encapsulation (IPsec), WAN security, 32

encryption

- GRE tunnel-based L3VPN architectures, 155
- Ipsec, WAN security, 32

enterprise networks, 35

- campuses
 - hierarchical design, 17–21*
 - modular design, 18*
 - virtualization, 22*
- centralized policies, 37
- communication interfaces, 38
- functional areas, 38–40
- functionality of, 37
- hub-and-spoke topologies, 24
- VPN, 36–37, 41
- VRF, 40, 45–47
 - definition of, 57*
 - displaying, 58*
 - FIB, 58–60*
 - LR, 61*
 - multiple VRF on routers, 57–58*
 - resource allocation, 60*
 - RIB, 58–59*
 - routing table information, 59*
 - sharing routes between, 58*
 - traffic processing, 60*
 - VRF awareness, 62*
 - VR, 61*

WAN, 22

- aggregation routers, 26*
- branch-end routers, 26*
- dedicating routers at network core, 26–27*
- dual-circuit resiliency, 27*

- hierarchical architecture, 25–26*
- IP service with VPN overlay routing*
 - adjacencies, 30*
- IPsec/GRE, 26–28*
- ISDN backup resiliency, 27*
- multilayer switches, 26*
- point-to-cloud IP service routing*
 - adjacencies, 29–30*
- point-to-point service routing, 31*
- private point-to-cloud connectivity, 25*
- private point-to-point connectivity, 24*
- private spoke-to-spoke connectivity, 24*
- security, 31–32*
- tunnel overlay resiliency, 28*
- virtualization, 32*

equal-cost paths, hierarchical campus design, 19

ESP headers (IPsec), 69

EXCLUDE mode (IGMP), 244

Extensible Authentication Protocol (EAP), 303–304

Extensible Authentication Protocol over LAN (EAPOL), 303–305

Extranet VPN, unprotected shared services, 213

F

failovers, GRE tunnel-based L3VPN architectures, 150

failure detection, GRE tunnel-based L3VPN architectures, 150–152

FEC (Forward Equivalency Classes), 76

FIB (Forwarding Information Bases), 41

- adjacencies, 58

- definition of, 58

- LSP, 79

- output, 59–60

- updating, 59

firewalls, 52

- protected services, 220

- routed firewalls, 222–234*

- transparent firewalls, 222,*

- 234–236*

- routed mode, 252

- transparent mode, 252

- virtual firewall contexts, 64–65

forwarding, 245

- RPF, 245
- shared trees, 247
- source trees, 246
- VRF, 40, 45–47
 - definition of, 57*
 - displaying, 58*
 - FIB, 58–60*
 - LR, 61*
 - multicast, 250–255*
 - multiple VRF on routers, 57–58*
 - resource allocation, 60*
 - RIB, 58–59*
 - routing table information, 59*
 - sharing routes between, 58*
 - traffic processing, 60*
 - VRF awareness, 62*
 - VR, 61*

forwarding plane, 41**FRR (fast reroute)**

- link protection, 279–280
- MPLS, 333

fusion routers, 50**fusion-switch deployment model (MVR), 258****G**

global space, multicast in, 255–259

global tables, leaking traffic (unprotected services), 217–218**globally significant code points, 44****GRE (generic routing encapsulation), 41, 66**

- configuration, 260
- headers, 67
- ISO configuration, 68–69
- mGRE, WAN, 177
- MPLS over (WAN, VN extensions over), 192, 194–195
- P2P GRE, WAN, 176–177
- peer-based L3VPN architectures,
 - RFC 2547bis, 160*
- RP keepalives, 67
- tunnel-based L3VPN architectures, 96–98, 141
 - failovers, 150*
 - failure detection, 150, 152*
 - hub configurations, 143*

hub routes in hub-and-spoke mGRE overlays, 154–155

IGP, 153

load balancing, 149

OSPF, 153–154

overlays, 155, 259–260

resiliency, 149

spoke configurations, 143–144

VRF interconnections (WAN, VN extensions over), 200–202

guaranteed bandwidth, 335–337**guest access (networks), 7–8****guest VLANs, 308–309****H****h2h (hop-to-hop) architectures**

- ACL, 94
- constrained routing, 95
- IP tunnels, VPN QoS models, 282
- Layer 2 solutions, 92
 - complexity of, 90*
 - scalability of, 91*
 - user groups, 93*
 - VLAN, 90–91, 125–129*
- Layer 3 solutions, 129
 - ACL, 138–140*
 - adding interfaces to VRF, 132*
 - advantages of, 93*
 - complexity, 92*
 - converting core links to dot1q trunks, 133–134*
 - creating VLAN, 132*
 - creating VRF, 131–132*
 - EIGRP address families, 137*
 - hierarchy support, 93*
 - network topologies, 130*
 - PBR, 139–141*
 - routed nodes, 93*
 - scalability, 92*
 - segmented campus networks, 130*
 - static routing, 93*
 - VLAN ID, creating for core data path virtualization, 134–135*
 - VRF, assigning SVI to, 135–137*
 - VRF-lite, 129*

- MTR, 95
 - PBR, 94
 - headers**
 - GRE, 67
 - IPsec, 69
 - hierarchical campus design (scalable enterprise networks), 17**
 - access switches, 19
 - distribution switches, 19
 - equal-cost paths, 19
 - failure-isolation features, 21
 - failures, effects of, 19
 - IGP, 19
 - Layer 2 (switched) connectivity, 19–21
 - Layer 3 (routed) technologies, 19–21
 - network layers, collapsing, 21
 - topology designs, 19
 - VLAN, 22
 - VPN, 22
 - hierarchical QoS (Quality of Service), 284–286**
 - hierarchical WAN architecture, 25–27**
 - HIPAA (Health Insurance Portability and Accountability Act), security controls, 8**
 - hub-and-spoke policy-based segmentation, 44**
 - hub-and-spoke topologies**
 - peer-based L3VPN architectures, 110
 - scalable enterprise network design, 24
 - tunnel-based L3VPN architectures, 96
 - hub-and-spoke VPN, unprotected shared services, 213**
 - peer-based L3VPN architectures, best practices for, 160
 - MPLS-TE, 331–332
 - IKE (Internet Key Exchange), 70–71**
 - importing/exporting routes, unprotected shared services**
 - multiplatform deployment, 210
 - single-platform deployment, 211–212
 - INCLUDE mode (IGMP), 244**
 - inter-autonomous system routing, VPN, 119–120**
 - interface command, 62**
 - interior gateway protocol (IGP), 46, 83**
 - Intermediate System-to-Intermediate System (IS-IS), 61**
 - Internet Services Group (ISG), 301**
 - IntServ (integrated services), QoS, 274**
 - IP addresses, Class D addresses, 242**
 - ip dhcp snooping command, 291**
 - IP multicast, 241–243**
 - applications, 241–242
 - compared to broadcast, 242
 - IGMP, 243–245
 - multicast routing, 245–247
 - PIM, 248–249
 - tree structure, 242–243, 246–247
 - IP Precedence, QoS values, 275–276**
 - IP services**
 - DHCP, 236–237
 - DNS, 238
 - WAN, 173–174
 - ip verify source command, 291**
 - IP VPN, VN extensions over WAN, 185–187**
 - IPsec, 69–72**
 - crypto maps, 71–72
 - encapsulation, WAN security, 32
 - encryption, WAN security, 32
 - headers, 69
 - hierarchical WAN architecture, 26
 - IOS configuration, 71–72
 - SA, 69
 - SPI fields, 69
 - stateful resiliency (WAN), scalable enterprise network design, 28**
 - transform sets, 72
 - transport mode, 70–71
 - tunnel mode, 70
-
- IANA (Internet Assigned Numbers Authority), 67
 - iBGP**
 - configuration, 85
 - multipaths, peer-based L3VPN architectures, 164**
 - IDS (intrusion detection systems), 49**
 - IETF (Internet Engineering Task Force), 248**
 - IGMP (Internet Group Management Protocol), 243–245**
 - IGP (Interior Gateway Protocol), 83, 46**
 - GRE tunnel-based L3VPN architectures, 153
 - hierarchical campus design, 19

ISDN backup resiliency (WAN), scalable enterprise network design, 27
IS-IS (Intermediate System-to-Intermediate System), 61
ISG (Internet Services Group), 301

J – K – L

L2TP access concentrator / L2TP network server (LAC/LNS), 75
l2tp-class command, 74
L2TPv3 (Layer 2 Tunnel Protocol version 3)
 authentication, 326
 compared to GRE, 73
 control channel, 324–327
 cookies, 325
 data channel, 327
 deployment models, 323
 IOS configuration, 73–75
 peer-based L3VPN architectures,
 RFC 2547bis, 159
 session ID, 325
 session setup
 control messages, 325–326
 handshakes, 325
 nonces, 326
 tunnels
 L2VPN architectures, 102–104
 RFC 2547 VPN over (WAN, VN extensions over), 195–200
 tunnel teardown control messages, 325
L2VPN architectures
 peer-based architectures, 165
 Ethernet over MPLS, 166–170
 VPLS, 170–171
 tunnel-based architectures
 auto-discovery, 107
 auto-provisioning, 107
 L2TPv3, 102–104
 MP2MP using MPLS, 106–107
 MPLS, 104–106
 multicast support, 107
L3VPN architectures
 peer-based architectures
 BGP best practices, 160
 hub-and-spoke topologies, 110
 iBGP multipaths, 164

IGP best practices, 160
migration recommendations, 164–165
RD, 161–163
RFC 2547 control-plane interaction, 108–111
RFC 2547bis, 112–115, 155–160
RR, 161–163
 tunnel-based architectures
 DMVPN, 98–101
 GRE and IPsec tunnel configuration, 96–98
 GRE tunnels, 141–144, 149–155
 hub-and-spoke topologies, 96
 mGRE tunnels, 144–147
 traffic mapping, 148
Label Distribution Protocol (LDP), 78
label switched paths (LSPs), 46
 CE, 76
 edge LSR, 76
 FIBs, 79
 IOS configuration, 80–82
 LDP, 78
 LSR, 76
 MPLS packet forwarding, 76–77
label switching routers (LSR), 76
LAC/LNS (L2TP access concentrator/L2TP network server), 75
LAN (local-area networks), VPN QoS models, 280–281
Layer 2 (switched) connectivity, hierarchical campus design, 19–21
Layer 2 circuits, WAN, 175, 180–184
Layer 2 client-based authentication, 301
 802.1x
 protocols, 303–306
 roles, 302–303
 dot1x implementation, 306–311
Layer 2 h2h architectures, 92
 complexity of, 90
 scalability of, 91
 user groups, 93
 VLAN, 90–91, 125
 access-distribution blocks, 126–127
 access-distribution data path virtualization, 127–128
 access-distribution segmentation, 127
 assigning access ports, 128–129
 virtual routed interfaces, 128

Layer 3 (routed) technologies, hierarchical campus design, 19, 21**Layer 3 access, 317–318****Layer 3 clientless authentication, 299–301****Layer 3 h2h architectures, 129**

- ACL, 138–140
- advantages of, 93
- complexity, 92
- core links, converting to dot1q trunks, 133–134
- EIGRP address families, 137
- hierarchy support, 93
- network topologies, 130
- PBR, 139–141
- routed nodes, 93
- scalability, 92
- segmented campus networks, 130
- static routing, 93
- VLAN, 132
- VLAN ID, creating for core data path virtualization, 134–135
- VRF
 - adding interfaces to, 132*
 - assigning SVI, 135–137*
 - creating, 131–132*
- VRF-lite, 129

LDP (Label Distribution Protocol), 78**link congestion, MPLS QoS, 278****Link optimization policy mechanism, QoS, 274****link protection**

- FRR, 279–280
- MPLS QoS, 278–279

L-LSP, MPLS QoS, 277**load balancing**

- GRE tunnel-based L3VPN architectures, 149
- MPLS QoS, 278

LR (logical routers), 61–62**LSP (label switched paths), 46, 75**

- CE, 76
- edge LSR, 76
- FIB, 79
- IOS configuration, 80–82
- LDP, 78
- LSR, 76
- MPLS
 - packet forwarding, 76–77*
 - QoS, 277*
- MPLS-TE, link protection, 332

LSR (label switching routers)

- edge LSR, 76
- MPLS QoS, 277

M

MAC addresses, switch MAC table, 56–57

MAC-auth-bypass, 307–308**MAM (maximum allocation model), bandwidth constraints, 335–336****MAN (metro-area networks), 42****Marking policy mechanism, QoS, 274****MDT (multicast distribution trees), 254, 264****memory, CAM, 291****mergers, virtualization, 11****mGRE (multipoint generic routing encapsulation), 259**

- tunnel-based L3VPN architectures, 99, 144
 - hub configurations, 145–146*
 - mapping subnets to VRF, 147*
 - NHRP, 144–147*
 - spoke configurations, 146–147*

WAN, 177

modular campus design (scalable enterprise networks), 18**modular QoS command-line interface (MQC), 48****MP-iBGP (multiprotocol interior Border****Gateway Protocol), 46**

- advertising multiple routes into (routed firewalls), 230–231
- unprotected shared services, 210

MPLS (Multiprotocol Label Switching), 58, 63

- FRR, 333
- GRE over (WAN, VN extensions over), 192–195
- packet forwarding, 76–77
- peer-based L3VPN architectures, *RFC 2547bis campus network/MAN deployment, 155–159*
- MPLS over L2TPv3, 115*
- MPLS over mGRE, 114*
- Multi-VRF CE deployments, 157–158*
- VPN forwarding, 112–113*

QoS

- DS-TE, 279, 283*
- guaranteed bandwidth, 278–279*

- link congestion*, 278
 - link protection*, 278–279
 - load balancing*, 278
 - LSP*, 277
 - LSR*, 277
 - pipe tunnel mode*, 330
 - TE*, 278–280, 283
 - tunnels/pipes*, 277–278
 - uniform tunnel mode*, 329
 - routed firewalls, 233–234
 - tunnel-based L2VPN architectures, 104–107
 - VPN QoS models, 282–283
 - WAN, VN extensions, 180–184
 - MPLS-TE (MPLS traffic engineering)**, 331–332
 - MQC (modular QoS command-line interface)**, 48
 - MTIs (multicast tunnel interfaces)**, 263
 - MTR (Multi-Topology Routing)**, 46, 85–86, 95
 - multi-auth mode**, 307
 - multicast**
 - global space, 255–259
 - IP multicast
 - applications*, 241–242
 - compared to broadcast*, 242
 - IGMP*, 243–245
 - multicast routing*, 245–247
 - PIM*, 248–249
 - shared trees*, 247
 - source trees*, 246
 - mVPN
 - advantages/disadvantages*, 266
 - CE-PE adjacencies*, 265
 - D1 BGP configuration*, 268
 - data MDTs*, 264
 - default MDTs*, 264
 - forwarding*, 265–266
 - MTI*, 263
 - multicast domains*, 263
 - MVRF and MDT configuration on D1*, 268
 - native multicast configuration on C1*, 267
 - provider routers*, 263
 - WAN, 269
 - MVR, 257–259
 - SSM, 244
 - tunnel overlay, 259–262
 - VRF
 - external IP network sources*, 251–254
 - hop-to-hop layer 3 VPNs*, 250–251
 - mVPN extranet*, 254–255
 - mVRFs*, 250
 - WAN, 269–271
 - multicast distribution trees (MDT)**, 254
 - multicast support, tunnel-based L2VPN architectures**, 107
 - multicast tunnel interfaces (MTI)**, 263
 - Multicast VLAN Registration (MVR)**, 257–259
 - multihoming**, 149
 - multi-host mode**, 307
 - multilayer switches, hierarchical WAN architecture**, 26
 - multiple-hop data path virtualization**, 46
 - multiprotocol generic routing encapsulation (mGRE)**, 259
 - multiprotocol interior Border Gateway Protocol (MP-iBGP)**, 46
 - advertising multiple routes into (routed firewalls), 230–231
 - unprotected shared services, 210
 - multitenant enterprises, virtualization**, 11–12
 - Multi-Topology Routing (MTR)**, 46, 85–86
 - Multi-VRF CE**. *See* VRF-lite
 - mVPN (Mobile Virtual Private Networks)**
 - advantages/disadvantages, 266
 - CE-PE adjacencies, 265
 - D1 BGP configuration, 268
 - data MDTs, 264
 - default MDTs, 264
 - extranet, 254–255
 - forwarding, 265–266
 - MTI, 263
 - multicast domains, 263
 - MVRF and MDT configuration on D1, 268
 - native multicast configuration on C1, 267
 - provider routers, 263
 - WAN, 269
 - MVR (Multicast VLAN Registration)**, 257–259
 - mVRFs (multicast VRFs)**, 250
-
- ## N
-
- NAT (Network Address Translation), 50, 301
 - dynamic NAT, routed firewalls, 232–234
 - routed firewalls, 231–234
 - static NAT, routed firewalls, 232–234

network device virtualization. See device virtualization, 55**networks**

- acquisitions/mergers, integrating into, 11
- consolidating, reasons for virtualization, 10–11
- contractors access, 8
- dynamic membership, 294
- employee access, 8
- guest access, 7–8
 - authentication/authorization, 7*
 - physical access locations, 7*
- partner access, 8
- perimeters, 35, 49
 - common services positioning, 50–51*
 - firewalls, 52*
 - fusion routers, 50*
 - IDS, 49*
 - unprotected services, 51–52*
- layers, collapsing** (hierarchical campus design), 21
- quarantine VN segments, 7
- security controls, 8–9
- static membership, 294
- topologies**, Layer 3 h2h architectures, 130
- NHRP (Next Hop Resolution Protocol)**
 - GRE tunnel based L3VPN architectures, 153
 - mGRE tunnel-based L3VPN architectures, 144
 - hub configurations, 145–146*
 - spoke configurations, 147*
- nonces, L2TPv3, 326**

O – P**OSPF (Open Shortest Path First), 84, 153–154, 291****overlay networks**

- advantages/disadvantages, 259
- GRE configuration, 260
- GRE tunnel overlay, 259–260
- mGRE, 259
- multicast configuration, 261
- RP configuration, 262

p2p (point-to-point), QoS, 274**P2P GRE, WAN, 176–177****packets**

- forwarding, 245
 - MPLS networks, 76–77*
 - shared trees, 247*
 - source trees, 246*
- IGMP (Internet Group Management Protocol), 245
- PAP (Password Authentication Protocol), 303**
- partner access (networks), 8**
- PBR (policy-based routing), 300**
 - failure detection in GRE tunnel-based L3VPN architectures, 152
 - h2h architectures, 94
 - Layer 3 h2h architectures, 139–141
 - tunnel-based L3VPN architectures, *traffic mapping, 148*
- PE (provider edges), 63, 76, 254**
- peer-based L2VPN architectures, 165**
 - Ethernet over MPLS, 166–170
 - VPLS, 170–171
- peer-based L3VPN architectures**
 - BGP best practices, 160
 - hub-and-spoke topologies, 110
 - iBGP multipaths, 164
 - IGP best practices, 160
 - migration recommendations, 164–165
 - RD, 161, 163
 - RFC 2547 control-plane interaction, 108–111
 - RFC 2547bis
 - GRE, 160*
 - L2TPv3, 159*
 - MPLS, 112–115, 155–159*
 - RR, 161, 163
- penultimate hop popping (PHP), 77**
- Per VLAN Spanning Tree (PVST), 83**
- Per VLAN Spanning Tree Plus (PVST+), 289**
- per-VRF iBGP configuration, 85**
- per-VRF RIP configuration, 84**
- PE (provider edges), 63, 76, 254**
- PHB (per-hop behaviors), 44**
 - AF PHB, 275
 - class selectors, 275
 - default, 275
 - EF PHB, 275
 - pipe tunnel mode (MPLS networks), 330
 - QoS values, 275–276

PHP (penultimate hop popping), 77, 330
PIM (Protocol Independent Multicast), 248–249

pipes

MPLS QoS, 277–278
 tunnel mode (MPLS networks), 330

planes (control/forwarding), 41

point-to-cloud connectivity, WAN, 25

point-to-point connectivity, WAN, 24

policies

centralized policies, 37
 PBR, 300
failure detection in GRE tunnel-based L3VPN architectures, 152
h2h architectures, 94
Layer 3 h2h architectures, 139–141
tunnel-based L3VPN architectures, traffic mapping, 148
 security policies, enforcing with access switches, 291

Policing policy mechanism, QoS, 274

segmentation, 43–45

ports

security, static clientless authentication, 296–297
 VLAN ID (PVID), 307

PPPoE (PPP over Ethernet), 302

private services, WAN, 24–25

private VLANs, 291

protected services, 218–220

routed firewalls
advertising multiple routes into MP-iBGP, 230–231
asymmetric return paths, 231
multiple common services/internet edge site deployments, 224–229
NAT, 231–234
single common services/ internet edge site deployments, 222–224
 shared services, 207–208
 transparent firewalls, 222, 234–236

Protocol Independent Multicast (PIM), 248–249

provider edges (PE), 63, 76, 254

pseudowire command, 74

Pseudowire topologies, peer-based L2VPN architectures, 168–170

pseudowire-class command, 74

PVID (port VLAN ID), 307

PVST (Per VLAN Spanning Tree), 83

PVST+ (Per VLAN Spanning Tree Plus), 289

Q

QoS (Quality of Service), 316

architecture, 44

Classification policy mechanism, 274

Congestion avoidance policy mechanism, 274

dedicated protocol fields, 273

deployment, 292

DiffServ, 274

802.1p values, 275–276

DSCP values, 275–276

IP Precedence values, 275–276

PHB, 275–276

Internet deployment models, 274

IntServ, 274

Link optimization policy mechanism, 274

Marking policy mechanism, 274

MPLS, 277

DS-TE, 279, 283

guaranteed bandwidth, 278–279

link congestion, 278

link protection, 278–279

load balancing, 278

LSP, 277

LSR, 277

TE, 278–280, 283

tunnels/pipes, 277–278

MPLS networks

pipe tunnel mode, 330

uniform tunnel mode, 329

p2p, 274

Policing policy mechanism, 274

policy mechanisms, summary of, 274

Queuing/scheduling policy mechanism, 274

Resource reservation policy mechanism, 274

RSVP, 274

VPN models

h2h IP tunnels, 282

hierarchical QoS, 284–286

LAN rules, 280–281

MPLS VPN, 282–283

multiple policies per group, 282, 285

one policy per group, 280–283

point-to-cloud models, 282

point-to-service models, 282
WAN rules, 280–281

quarantine VN segments, 7
queries (IGMP), 243–244
Queuing/scheduling policy mechanism, QoS, 274

R

R103 routers
 GRE configuration, 68
 LSP configuration, 80–81
Rapid Spanning Tree Protocol (RSTP), 289
RD (route distinguishers), 161–163, 210
RDM (Russian dolls model), bandwidth constraints, 335
receiver mVRFs, 254
receiver provider edge (PE), 254
regulatory compliance, reasons for virtualization, 9
Remote Switched Port Analyzer (RSPAN), 306
reports (IGMP), 243–244
requests (DNS), 301
resiliency
 GRE tunnel-based L3VPN architectures, 149
 WAN, scalable enterprise network design, 27–28
Resource reservation policy mechanism, QoS, 274
RESV messages, MPLS-TE, 332
reverse path forwarding (RPF), 245
RFC 2547 VPN
 over DMVPN (WAN, VN extensions over), 202–205
 over L2TPv3 tunnels (WAN, VN extensions over), 195–200
RIB (Routing Information Bases), 41, 58–59
RIP configuration, 84
routed core virtualization
 control-plane-based segmentation, 45–47
 policy-based segmentation, 43–45
routed firewalls, 252
 deploying
advertising multiple routes into MP-iBGP, 230–231
asymmetric return paths, 231
multiple common services/internet edge site deployments, 224–229

single common services/internet edge site deployments, 222–224

NAT, 231–234

routers
 aggregation, hierarchical WAN architecture, 26
 brand-end, hierarchical WAN architecture, 26
 dedicating at network core, hierarchical WAN architecture, 26–27
 edge LSR, 76
 fusion routers, 50
 IPsec/GRE headend, hierarchical WAN architecture, 26
 LR, 61–62
 LSR, 76
 PE routers, 76
 VR, 61–62
 WAN, scalable enterprise network design, 29–31
routing
 GRE, 66
headers, 67
ISO configuration, 68–69
RP keepalives, 67
 MTR, 46, 85–86
 multicast routing. *See* multicast
 PBR, 300
 VRF, 40, 45–47
definition of, 57
displaying, 58
FIB, 58–60
LR, 61
multicast, 250–255
multiple VRFs on routers, 57–58
resource allocation, 60
RIB, 58–59
routing table information, 59
sharing routes between, 58
traffic processing, 60
VRF awareness, 62
VR, 61
Routing Information Bases (RIB), 41, 58–59
RP (rendezvous points), 247
RP (Route processor)
 configuration, 262
 keepalives, 67
RPF (reverse path forwarding), 245
RR (route reflectors), peer-based L3VPN architectures, 161–163

RSPAN (Remote Switched Port Analyzer), 306
RSTP (Rapid Spanning Tree Protocol), 289
RSVP (Resource Reservation Protocol)
 MPLS-TE, 332
 QoS, 274
RT (route targets), 210

S

Sarbanes-Oxley Act, security controls, 8–9

SA (security associations), 69

scalability, VLANs, 42–43

scalable enterprise networks

campuses

hierarchical design, 17–21

modular design, 18

virtualization, 22

hub-and-spoke topologies, 24

WAN, 22

aggregation routers, 26

branch-end routers, 26

dedicating routers at network core, 26–27

dual-circuit resiliency, 27

hierarchical architecture, 25–26

IP service with VPN overlay routing

adjacencies, 30

IPsec/GRE headend routers, 26

IPsec/GRE stateful resiliency, 28

ISDN backup resiliency, 27

multilayer switches, 26

point-to-cloud IP service routing

adjacencies, 29–30

point-to-point service routing, 31

private point-to-cloud connectivity, 25

private point-to-point connectivity, 24

private spoke-to-spoke connectivity, 24

security, 31–32

tunnel overlay resiliency, 28

virtualization, 32

secure service areas (convergent services), 9

security

controls, 8–9

firewalls, 52, 252

network perimeters, 35, 49–50

common services positioning, 50–51

firewalls, 52

fusion routers, 50

IDS, 49

unprotected services, 51–52

policies, enforcing with access switches, 291

ports, static clientless authentication, 296–297

WAN, scalable enterprise network design,
31–32

security associations (SA), 69

Security Parameter Index (SPI) fields, 69

segmentation

control-plane-based, 45–47

policy-based, 45

code points, 43

hub-and-spoke policy-based

segmentation, 44

servers

authentication servers (802.1x networks), 302

server farms, virtualization, 11–12

services

common services positioning, 50–51

firewalls, 52

shared services

DHCP services, 237

protected services, firewalls, 207–208,

218–234

unprotected services, 51–52, 207–218

shared trees, 247

short pipes, MPLS QoS, 277

show ip cef forwarding vrf name detail

command, 59

show ip route command, 81

show ip route vrf command, 59

single-hop data path virtualization, 46

source mVRFs, 254

source provider edge (PE), 254

source trees, 246

Source-Specific Multicast (SSM), 244

Sparse mode (PIM-SM), 248

SPF (shortest path first)

CSPF, 332

MPLS-TE, 331

SPI (Security Parameter Index) fields, 69

spoke-to-spoke connectivity, WAN, 24

SP (service providers), 63

SSM (Source-Specific Multicast), 244

stacking access switches, 291

static NAT, routed firewalls, 232, 234

static network membership, 294

static routing, Layer 3 h2h architectures, 93

supplicants (802.1x networks), 302
SVI (switch virtual interfaces), 47
 VLAN, h2h architectures, 128
 VRF, assigning to, 135–137
switches, MAC table, 56–57

T

TE (traffic engineering)
 CBR, 278
 MPLS QoS, 278–280, 283
Time To Live (TTL), 245
topologies
 design, 19
 hierarchical campus design, 19
 hub-and-spoke
peer-based L3VPN architectures, 110
scalable enterprise network design, 24
tunnel-based L3VPN architectures, 96
 network topologies, Layer 3 h2h
 architectures, 130
 Pseudowire, peer-based L2VPN architectures,
 168–170
transform sets (IPsec), 72
transparent firewalls, 222, 234–236
transparent mode (firewalls), 252
transport mode (IPsec), 70–71
transport virtualization, 40
 control plane, 41
 control-plane-based segmentation, 45–47
 data-path virtualization, 41
 device virtualization, 41
 forwarding plane, 41
 levels of virtualization, 41
 policy-based segmentation, 43–45
 scalability, 42–43
 VLANs, 42–43
tree structure (IP multicast), 242–243
 shared trees, 247
 source trees, 246
tunnel mode (IPsec), 70
tunnel overlay
 advantages/disadvantages, 259
 GRE configuration, 260
 GRE tunnel overlay, 259–260
 mGRE, 259
 multicast configuration, 261

resiliency (WAN), scalable enterprise network
 design, 28
 RP configuration, 262
tunnel-based L2VPN architectures
 auto-discovery, 107
 auto-provisioning, 107
 L2TPv3, 102–104
 MP2MP using MPLS, 106–107
 MPLS, 104–106
 multicast support, 107
tunnel-based L3VPN architectures
 DMVPN, 98–101
 GRE tunnels, 96–98, 141
failovers, 150
failure detection, 150–152
hub configurations, 143
hub routes in hub-and-spoke mGRE
overlays, 154–155
IGP, 153
load balancing, 149
OSPF, 153–154
overlay encryption, 155
resiliency, 149
spoke configurations, 143–144
 hub-and-spoke topologies, 96
 IPsec tunnel configuration, 96–98
 mGRE tunnels, 144
hub configurations, 146
hubconfigurations, 145
mapping subnets to VRF, 147
NHRP, 144–147
spoke configurations, 146–147
 traffic mapping, 148
tunnels
 h2h IP tunnels, VPN QoS models, 282
 MPLS QoS, 277–278

U – V

uniform tunnel mode (MPLS networks), 329
universities, virtualization, 12
unprotected shared services, 51–52, 207–208
 any-to-any VPN, 212
 Extranet VPN, 213
 global tables, leaking traffic, 217–218
 hub-and-spoke VPN, 213

- importing/exporting routes
 - multiplatform deployment*, 210
 - single-platform deployment*, 211–212
- localized inter-VPN communication, 214–215
- MP-iBGP, 210
- URT (User Registration Tool)**, 299
- user groups, Layer 2 h2h architectures**, 93
- VFI (Virtual Forwarding Instances)**, 63–65
- virtual firewall contexts**, 64–65
- virtual project environments**, 12–13
- virtual routed interfaces, Layer 2 h2h architectures**, 128
- virtual teams**, 12–13
- virtualization**
 - acquisitions/mergers, 11
 - benefits of, 5–6
 - business requirements, 14
 - covergent services, 9
 - multitenant enterprises, 11–12
 - networks
 - restricting access*, 7–8
 - consolidation*, 10–11
 - reasons for, 5–6
 - regulatory compliance, 9
 - secure service areas, 9
 - server farms, 11–12
 - virtual project environments, 12–13
 - WAN, scalable enterprise network design, 32
- viruses, quarantine VN segments**, 7
- visitor access (networks)**, 7–8
- VLAN (Virtual Local Area Networks)**, 42
 - access switches, 290
 - device virtualization, 56–57
 - guest VLANs, 308–309
 - hierarchical campus design, 19, 22
 - Layer 2 h2h architectures, 90–91, 125
 - access-distribution blocks*, 126–127
 - access-distribution data path virtualization*, 127–128
 - access-distribution segmentation*, 127
 - assigning access ports*, 128–129
 - virtual routed interfaces*, 128
 - Layer 3 h2h architectures, *creating VLAN*, 132
 - private VLANs, 291
 - scalability, 42–43
 - SVI, h2h architectures, 128
 - switch MAC table, 56–57
 - VLAN ID, creating for core data path virtualization, 134–135
- VMPS (VLAN Management Project Servers)**, 297–299
- VNs (virtual networks)**, 35, 55
 - authentication, 47–48
 - authorization, 47–48
 - control-plane virtualization, 83
 - MTR*, 85–86
 - OSPF*, 84
 - per-VRF iBGP configuration*, 85
 - per-VRF RIP configuration*, 84
 - summary*, 86
 - VRF-aware routing*, 84
 - data-path virtualization
 - 802.1q trunking*, 66
 - GRE*, 66–69
 - IPsec*, 69–72
 - L2TPv3*, 72–75
 - LSP*, 75–82
 - summary*, 83
 - device virtualization
 - definition of*, 56
 - network infrastructure requirements*, 55
 - summary*, 65
 - VFIs*, 63–65
 - virtual firewall contexts*, 64–65
 - VLAN*, 56–57
 - VRF*, 57–62
 - enterprise networks
 - centralized policies*, 37
 - communication interfaces*, 38
 - functional areas*, 38–40
 - functional blocks*, 35
 - functionality of*, 37
 - VRF*, 40, 45–47
 - network perimeters, 35
 - common services positioning*, 50–51
 - firewalls*, 52
 - fusion routers*, 50
 - IDS*, 49
 - unprotected services*, 51–52
 - transport virtualization, 40
 - control plane*, 41
 - control-plane-based segmentation*, 45–47
 - data-path virtualization*, 41
 - device virtualization*, 41

- forwarding plane*, 41
- levels of virtualization*, 41
- policy-based segmentation*, 43–45
- scalability*, 42–43
- VLAN*, 42–43
- VPN, 36–37, 41
- VRF
 - definition of*, 57
 - displaying*, 58
 - FIB*, 58–60
 - LR*, 61
 - multiple VRF on routers*, 57–58
 - resource allocation*, 60
 - RIB*, 58–59
 - routing table information*, 59
 - sharing routes between*, 58
 - traffic processing*, 60
 - VRF awareness*, 62
 - VR*, 61
- WAN, extensions over
 - contracting multiple IP VPN*, 185–187
 - CsC*, 187–192
 - MPLS over GRE*, 192–195
 - MPLS over Layer 2 circuits*, 180–184
 - RFC 2547 VPN over DMVPN*, 202–205
 - RFC 2547 VPN over L2TPv3 tunnels*, 195–200
 - VRF interconnected by GRE or DMVPN overlay*, 200–202
- voice virtual LAN (VVLAN)**, 307
- VoIP (Voice-over Internet Protocol)**, 310
- VPLS (Virtual Private LAN Services)**, 63, 170–171
- VPN (Virtual Private Networks)**
 - any-to-any VPN, unprotected shared services, 212
 - compared to VN, 41
 - CsC, 116–119
 - dedicated DHCP services, 236
 - DMVPN, WAN, 178
 - Extranet VPN, unprotected shared services, 213
 - h2h architectures, 90
 - ACL*, 94
 - constrained routing*, 95
 - Layer 2 solutions*, 90–92, 125–129
 - Layer 3 solutions*, 92–93, 129–141
 - MTR*, 95
 - PBR*, 94
 - hierarchical campus design, 22
 - hub-and-spoke VPN, unprotected shared services, 213
 - inter-autonomous system routing, 119–120
 - localized inter-VPN communication, unprotected shared services, 214–215
 - peer-based L2VPN architectures, 165
 - Ethernet over MPLS*, 166–170
 - VPLS*, 170–171
 - peer-based L3VPN architectures
 - BGP best practices*, 160
 - hub-and-spoke topologies*, 110
 - iBGP multipaths*, 164
 - IGP best practices*, 160
 - migration recommendations*, 164–165
 - RD*, 161–163
 - RFC 2547 control-plane interaction*, 108–111
 - RFC 2547bis*, 112–115, 155–160
 - RR*, 161, 163
- QoS models
 - h2h IP tunnels*, 282
 - hierarchical QoS*, 284–286
 - LAN rules*, 280–281
 - MPLS VPN*, 282–283
 - multiple policies per group*, 282, 285
 - one policy per group*, 280–283
 - point-to-cloud models*, 282
 - point-to-service models*, 282
 - WAN rules*, 280–281
- RFC 2547 VPN
 - over DMVPN (WAN, VN extensions over)*, 202–205
 - over L2TPv3 (WAN, VN extensions over)*, 195–200
- tunnel-based L2VPN architectures
 - auto-discovery*, 107
 - auto-provisioning*, 107
 - L2TPv3*, 102–104
 - MP2MP using MPLS*, 106–107
 - MPLS*, 104–106
 - multicast support*, 107
- tunnel-based L3VPN architectures
 - DMVPN*, 98–101
 - GRE and IPsec tunnel configuration*, 96–98
 - GRE tunnels*, 141–144, 149–155
 - hub-and-spoke topologies*, 96

- mGRE tunnels, 144–147*
- traffic mapping, 148*
- WAN, VN extensions over, 185–187
- VR (virtual routers), 61–62**
- VRF (VPN routing and forwarding), 40, 45–47, 57**
 - definition of, 57
 - displaying, 58
 - FIB, 58–60
 - global tables, leaking traffic (unprotected services), 217–218
 - Layer 3 h2h architectures, 92
 - adding interfaces to VRF, 132*
 - assigning SVI to, 135–137*
 - creating VRF, 131–132*
 - network topologies, 130*
 - segmented campus networks, 130*
 - VRF-lite, 129*
 - LR, 61–62
 - mGRE tunnel-based L3VPN architectures, mapping subnets to VRF, 147
 - multicast
 - external IP network sources, 251–254*
 - hop-to-hop layer 3 VPNs, 250–251*
 - mVPN extranet, 254–255*
 - mVRFs, 250*
 - multiple VRFs on routers, 57–58
 - resource allocation, 60
 - RIB, 58–59
 - routing table information, 59
 - sharing routes between, 58
 - traffic processing, 60
 - tunnel-based L3VPN architectures, *traffic mapping, 148*
 - VRF awareness, 62
 - VR, 61–62
- VRF-lite**
 - L3VPN architecture deployments, 157–158
 - Layer 3 h2h architectures, 129
- VSA (vendor-specific attribute), 309**
- VSI (virtual switched interfaces), 63**
- VVLAN (voice virtual LAN), 307**
- Layer 2 circuits, 175, 180–184
- mGRE, 177
- multicast, 269–271
- P2P GRE, 176–177
- scalable enterprise network design, 22
 - aggregation routers, 26*
 - branch-end routers, 26*
 - dedicating routers at network core, 26–27*
 - dual-circuit resiliency, 27*
 - hierarchical architecture, 25–26*
 - IP service with VPN overlay routing adjacencies, 30*
 - IPSec/GRE, 26–28*
 - ISDN backup resiliency, 27*
 - multilayer switches, 26*
 - point-to-cloud IP service routing adjacencies, 29–30*
 - point-to-point service routing, 31*
 - private point-to-cloud connectivity, 25*
 - private point-to-point connectivity, 24*
 - security, 31–32*
 - spoke-to-spoke connectivity, 24*
 - tunnel overlay resiliency, 28*
 - virtualization, 32*
- segmentation, 179
- VN extensions
 - contracting multiple IP VPN, 185–187*
 - CsC, 187–192*
 - MPLS over GRE, 192–195*
 - MPLS over Layer 2 circuits, 180–184*
 - RFC 2547 VPN over DMVPN, 202–205*
 - RFC 2547 VPN over L2TPv3tunnels, 195–200*
 - VRF interconnected by GRE or DMVPN overlay, 200–202*
- VPN QoS models, 280–281
- Web clients, Layer 3 clientless authentication, 299–301**
- wireless access, 48**

W

- WANs (wide-area networks)
 - DMVPN, 178
 - IP services, 173–174

X – Y – Z

- X over Y solutions, 66**
- xconnect command, 74**