

Numerics

802.1x, 230

A

access control list (ACL), 54–55
 address space separation, 48–49
 any to any topology, 159
 ATM/FR security comparisons
 attack resistance, 74–75
 CE-CE visibility, 75
 hiding core infrastructure, 75
 overview, 73, 76
 VPN separation, 74
 VPN spoofing, 75
 attacks
 ATM/FR security comparisons, 74–75
 DoS attacks. *See* DoS attacks
 how an MPLS core can be attacked, 54
 intrusion, 54
 overview, 52
 protection of core, 54–55
 receive traffic, 54
 where an MPLS core can be attacked, 53
 AutoSecure, 155–157

B

BGP Internet routing table from service provider of ISP, 256–259
 BGP maximum-prefix mechanism, 183–184
 BGP PE-CE routing, 179–180
 BGP peering sessions, configuring TTL security check for, 176
 bootp service, 139
 broadcast limiters, applying, 224

C

Carrier's Carrier (CSC)
 design and, 128–130
 how it works, 69–71
 overview, 69
 security of, 71
 case studies
 BGP Internet routing table from service provider of ISP, 256–259
 hybrid model, 260
 Internet access
 BGP Internet routing table from service provider of ISP, 256–259
 via customer-controlled NAT, 252–254
 global routing table, using, 255–256
 hybrid service model, 260
 NAT via common gateways, 245–246
 NAT via single common gateway, 251
 overview, 245
 PE to multiple Internet gateways, 247–250
 registered NAT by CE, 251
 tier 3 ISP connecting to an upstream tier via a service provider, 259
 Layer 2 LAN access, 264–265
 Multi-Lite VRF mechanisms
 configuration example for Internet and VPN service using same CE, 262–264
 overview, 261
 NAT via common gateways, 245–246
 NAT via single common gateway, 251
 overview, 245
 PE to multiple Internet gateways, 247–250
 registered NAT by CE, 251
 tier 3 ISP connecting to an upstream tier via a service provider, 259
 CDP (Cisco Discovery Protocol), 140
 CE devices, secure management of
 management VRF
 IN-Management route-map, 237
 OUT-Management route-map, 238
 overview, 236–237
 overview, 234–235

- CE-CE IPsec
 - overview, 188, 201–203
 - PE-PE IPsec compared, 189
 - CE-CE visibility, ATM/FR security comparisons, 75
 - central services topology, 158
 - CE-PE routing security best practices
 - BGP maximum-prefix mechanism, 183–184
 - BGP PE-CE routing, 179–180
 - dynamic routing, 179
 - EIGRP PE-CE routing, 180–181
 - key chaining, 179
 - nonrecognized neighbors, prevention of routes
 - being accepted by, 182
 - OSPF PE-CE routing, 181
 - overview, 178, 182
 - PE-CE addressing, 178
 - RIPv2 PE-CE routing, 182
 - static routing, 178
 - CE-specific router security
 - data plane security, 160
 - managed CE security considerations, 159
 - overview, 157–158
 - unmanaged CE security considerations, 160
 - Cisco Discovery Protocol (CDP), 140
 - confidentiality, integrity, and availability, 11
 - connection-oriented VPN technologies, 13
 - control plane, 16–18, 118–121
 - CoPP (control plane policing), 148
 - command syntax, 149
 - deployment guidelines, 152–154
 - overview, 154
 - policy, developing, 149–152
 - risk assessment for, 154
 - core network
 - attacks
 - how an MPLS core can be attacked, 54
 - overview, 52
 - protection of core, 54–55
 - receive traffic, 54
 - where an MPLS core can be attacked, 53
 - iACLs, 164–165
 - deployment examples, 169–171
 - developing protection ACL, 167–169
 - examples, 165–166
 - risk assessment, 169
 - techniques, 165
 - management, 239–241
 - overview, 163
 - threats against, 32
 - hierarchical core, 37–39
 - Inter-AS core, 36–37
 - monolithic core, 32–35
 - CSC. See Carrier's Carrier (CSC)
 - customer edge router, 221
 - broadcast limiters, applying, 224
 - CE interconnection service is layer 2 device, 222
 - CE interconnection service is layer 3 device, 221
 - disable/block L2 control traffic, 224–226
 - 802.1x, 230
 - hard-code physical port attributes, 229–230
 - Hijack Management Security, 222
 - MAC address limits and port security, 227–228
 - network reporting, establishing, 230
 - password recovery, disabling, 222–223
 - U-PE STP priority, 223
 - VLANs, 228
 - VTP transparent operation, 226
 - customer network security, 73
- ## D
-
- data confidentiality, integrity, and origin
 - authentication, 72
 - data plane, 18, 121–123
 - defense in depth, 82
 - designs
 - Carrier's Carrier (CsC), 128–130
 - against DoS attacks
 - bandwidth planning, 105
 - device positioning, 105
 - DoS resistant routers, 114
 - overview, 104–106
 - PE routers, 106–108
 - service overprovisioning, 105

- tradeoffs between DoS resistance and network cost, 108–113
- extranet access, 96–99
- firewalls, 100–104
- Inter-AS recommendations and traversing multiple provider trust model issues, 114–116
 - eBGP redistribution of labeled VPN-IPv4 routes, 118–123
 - multihop eBGP distribution of labeled VPN-IPv4 routes with eBGP redistribution of IPv4 routes, 124–128
 - VRF-to-VRF connection on ASBRs, 116–117
- Internet access and
 - DoS attack, 86–87
 - global routing table, 89–94
 - guidelines, 83–87
 - Internet provisioning, 94–96
 - MPLS core without Internet connectivity, 81–83
 - overview, 79–80
 - in VRF, 88–89
- Layer 2 security considerations, 130–132
- multicast VPN security, 132–133
- overview, 79
- DMVPN (dynamic multipoint VPN), 207
- DoS attacks, 54
 - designs against, 104
 - bandwidth planning, 105
 - device positioning, 105
 - DoS resistant routers, 114
 - overview, 86–87, 105–106
 - PE routers, 106–108
 - service overprovisioning, 105
 - tradeoffs between DoS resistance and network cost, 108–113
 - monolithic core, 33–34
 - VPNs, threats against, 30
- dynamic IPsec, 206
- dynamic multipoint VPN (DMVPN), 207
- dynamic routing, 179

E

- eBGP redistribution of labeled VPN-IPv4 routes
 - between source and destination AS, 64–67
 - from AS to neighboring AS, 61–64
 - Inter-AS recommendations and traversing multiple provider trust model issues, 118–123
- edge filtering via infrastructure ACLs, 165
- EIGRP PE-CE routing, 180–181
- encrypted VPN technologies, 14
- end-to-end resource sharing
 - additional security, 186
 - addressing considerations, 187
 - overview, 186
- Ethernet topologies
 - multiple point-to-point connectivity, 213
 - multipoint mesh connectivity, 213
 - single point-to-point connectivity, 212
- extranet access, designs and, 96–99
- extranet sites, threats against, 31

F

- firewalls, 100–104
- flash crowds, 105
- fragmented packets, 146

G

- GDOI (group domain of interpretation), 207
- general router security
 - AutoSecure, 155–157
 - control plane policing, 148
 - command syntax, 149
 - deployment guidelines, 152–154
 - overview, 154
 - policy, developing, 149–152
 - risk assessment for, 154
 - disabling unnecessary services, 139–142
 - IP source address verification, 143
 - overview, 136
 - rACLs, 143–144

- basic template and ACL examples, 144–145
- deployment guidelines, 146–148
- fragmented packets and, 146
- secure access to routers, 136–139
- generalized TTL security mechanism (GTSM), 119, 124
- global routing table, 89–94, 255–256
- GDOI (group domain of interpretation), 207

H

- hard-code physical port attributes, 229–230
- hidden core infrastructure
 - ATM/FR security comparisons, 75
 - overview, 56–57
- hierarchical core, 37–39
- Hijack Management Security, 222
- hop-by-hop routing, 90
- hub and spoke topology, 158
- hybrid service model, 260

I

- iACLs (infrastructure access lists), 164–165
 - deployment examples, 169–171
 - developing protection ACL, 167–169
 - examples, 165–166
 - risk assessment, 169
 - techniques, 165
- ICMP redirect message, 140
- ICMP unreachable, 140
- individual router ACLs, 165
- IN-Management route-map, 237
- Inter-AS connectivity
 - comparison of Inter-AS security considerations, 67–68
 - eBGP redistribution of labeled VPN-IPv4 routes between source and destination AS, 64–67
 - eBGP redistribution of labeled VPN-IPv4 routes from AS to neighboring AS, 61–64
 - overview, 59

- VRF-to-VRF connections at AS border routers, 59–61, 116–117
- Inter-AS core, 36–37
- Inter-AS recommendations and traversing multiple provider trust model issues, 114–116
 - eBGP redistribution of labeled VPN-IPv4 routes, 118–123
 - multihop eBGP distribution of labeled VPN-IPv4 routes with eBGP redistribution of IPv4 routes, 124–128
 - VRF-to-VRF connection on ASBRs, 59–61, 116–117
- internal threats, 34–35
- Internet, threats against, 40–41
- Internet access
 - case studies
 - BGP Internet routing table from service provider of ISP, 256–259
 - hybrid service model, 260
 - NAT via common gateways, 245–246
 - NAT via single common gateway, 251
 - overview, 245
 - PE to multiple Internet gateways, 247–250
 - registered NAT by CE, 251
 - tier 3 ISP connecting to an upstream tier via a service provider, 259
 - using global routing table, 255–256
 - via customer-controlled NAT, 252–254
 - designs and
 - DoS attack, 86–87
 - global routing table, 89–94
 - guidelines, 83–87
 - in VRF, 88–89
 - Internet provisioning, 94–96
 - MPLS core without Internet connectivity, 81–83
 - overview, 79–80
 - security recommendations
 - overview, 185
 - resource sharing, 185–186
- Internet based VPN technologies, 14
- Internet-free MPLS core, 93
- intrusions, 28–30, 33, 54
- IP address spoofing, 58
- IP routing, 119, 125
- IP source address verification, 143

IPsec

- CE-CE IPsec, 201–203
- deployment, 206–207
- dynamic IPsec, 206
- dynamic multipoint VPN (DMVPN), 207
- group domain of interpretation (GDOI), 207
- overview, 197–199
- PE-PE IPsec, 203–205
- remote access IPsec. *See* remote access IPsec
- static IPsec, 206
- termination points
 - CE-CE IPsec, 201–203
 - between CE routers of VPN, 200
 - overview, 200
 - PE-PE IPsec, 203–205
 - between PE routers within MPLS VPN core, 200
 - between point in VPN and PE, 200
 - remote access IPsec into MPLS VPN, 205–206
 - within VPN sites, 200
- transport mode, 198
- tunnel mode, 198

- MAC address limits and port security, 227–228
- network reporting, establishing, 230
- password recovery, disabling, 222–223
- U-PE STP priority, 223
- VLANs, 228
- VTP transparent operation, 226
- Ethernet topologies, 212–213
 - multiple point-to-point connectivity, 213
 - multipoint mesh connectivity, 213
 - single point-to-point connectivity, 212
- Metro Ethernet Architecture, 215–216
- overview, 211
- security considerations, 211–212
- VPLS
 - overview, 214–215
 - security considerations, 217–220
- VPWS
 - overview, 215
 - security considerations, 217–220
- layers of defense, 12
- LDP (Label Distribution Protocol), 62, 174
- least privilege principle, 11
- link encryption, 207
- LSP (label switch path), 18

K–L

key chaining, 179

- L2TPv3, 191
- label distribution protocol (LDP), 62, 174
- label spoofing, 58
- label switch path (LSP), 18
- LAN security, 187
- Layer 2 VPNs
 - customer edge router, 221
 - broadcast limiters, applying, 224
 - CE interconnection service is layer 2 device, 222
 - CE interconnection service is layer 3 device, 221
 - disable/block L2 control traffic, 224–226
 - 802.1x, 230
 - hard-code physical port attributes, 229–230
 - Hijack Management Security, 222

M

- MAC address limits and port security, 227–228
- management network security, 233
- management plane, 19–21
- management VRF
 - IN-Management route-map, 237
 - OUT-Management route-map, 238
 - overview, 236–237
- MD5 (Message-Digest 5 authentication), 174
- Metro Ethernet Architecture, 215–216
- Metro Ethernet Model, 220
- misconfiguration or operational mistakes, protection against, 72
- monolithic core, 32
 - DoS attacks, 33–34
 - internal threats, 34–35
 - intrusions, 33

- MPLS architecture
 - customer network security, 73
 - data confidentiality, integrity, and origin authentication, 72
 - misconfiguration or operational mistakes, protection against, 72
 - MPLS backbone, attacks from Internet through, 73
 - security issues not addressed by, 72–73
- MPLS VPNs
 - nomenclature of, 15–16
 - overview, 15
 - planes of
 - control plane, 16–18
 - data plane, 18
 - management plane, 19–21
 - overview, 16
 - security implications of connectionless VPNs, 21–22
 - security reference model, 22–24
- multicast VPN security, 132–133
- multihop BGP peering sessions, configuring TTL security check for, 177
- multihop eBGP distribution of labeled VPN-IPv4 routes with eBGP redistribution of IP4 routes, 124–128
- Multi-Lite VRF mechanisms
 - case studies, 261
 - configuration example for Internet and VPN service using same CE, 262–264
- Multi-Protocol Border Gateway Protocol (MP-BGP), 17

N

- NAT
 - via common gateways, 245–246
 - customer-controlled NAT, Internet access via, 252–254
 - registered NAT by CE, 251
 - via single common gateway, 251
- neighbor router authentication, 172–174
- network operations center (NOC)
 - overview, 19
 - threats against, 39–40

- network reporting, establishing, 230
- Network Time Protocol (NTP), 140
- no service finger, 139
- no service pad, 139
- nomenclature, 15–16
- nonrecognized neighbors, prevention of routes being accepted by, 182

O–P

- 100 percent security, impossibility of, 8
- OSPF PE-CE routing, 181
- OUT-Management route-map, 238
- password recovery, disabling, 222–223
- PE data plane security, 162
- PE routers and DoS attacks, 106–108
- PE to multiple Internet gateways, 247–250
- PE-CE addressing, 178
- PE-CE connectivity security issues, 163
- peer authentication with MD5, 118, 124
- PE-PE IPsec, 189, 203–205
- PE-specific router security, 161–162
- point of presence (PoP), 19
- policy-based routing (PBR), 111
- prefix filtering, 119, 125
- prefix flooding, 119, 125
- pseudowire, 214
- P-specific router security, 163

R

- rACLs (receive ACLs), 143–144
 - basic template and ACL examples, 144–145
 - deployment guidelines, 146–148
 - fragmented packets and, 146
- receive traffic, 54
- reconnaissance attacks, 42–43
- remote access IPsec, 205–206
- resource sharing, 185–186
- RIPv2 PE-CE routing, 182
- route distinguisher (RD), 17
- route flap damping, 118, 124

- route targets (RTs), 17
 - exports, 97
 - filtering, 119, 125
 - imports, 97
- routing security
 - configuring TTL security check for BGP peering sessions, 176
 - configuring TTL security check for multihop BGP peering sessions, 177
 - MD5 for Label Distribution Protocol, 174
 - neighbor router authentication, 172–174
 - overview, 172
 - TTL security check, configuring, 177
 - TTL security mechanism for BGP, 175–176
- routing/forwarding instance (VRF), 17
 - BGP PE-CE routing, 179–180
 - dynamic routing, 179
 - EIGRP PE-CE routing, 180–181
 - key chaining, 179
 - nonrecognized neighbors, prevention of routes being accepted by, 182
 - OSPF PE-CE routing, 181
 - overview, 178, 182
 - PE-CE addressing, 178
 - RIPv2 PE-CE routing, 182
 - static routing, 178
- CE-specific router security
 - data plane security, 160
 - managed CE security considerations, 159
 - overview, 157–158
 - unmanaged CE security considerations, 160
- checklist, 192–193
- core
 - iACLs, 164–171
 - overview, 163
- end-to-end resource sharing
 - additional security, 186
 - addressing considerations, 187
 - overview, 186
- general router security
 - AutoSecure, 155–157
 - control plane policing, 148–154
 - disabling unnecessary services, 139–142
 - IP source address verification, 143
 - overview, 136
 - rACLs, 143–148
 - secure access to routers, 136–139
- Internet access
 - overview, 185
 - resource sharing, 185–186
- LAN security
 - LAN factors for peering constructs, 187
 - overview, 187
- MPLS over IP operational considerations, 189–190
- MPLS over L2TPv3, 191
- overview, 135–136
- PE data plane security, 162
- PE-CE connectivity security issues, 163
- PE-specific router security, 161–162

S

- secure failure, 12
- Secure Sockets Layer (SSL), 207
- security
 - components of, 8–9
 - confidentiality, integrity, and availability, 11
 - connectionless VPNs, security implications of, 21–22
 - defined, 7–8
 - layers of defense, 12
 - least privilege principle, 11
 - 100 percent security, impossibility of, 8
 - other technologies, security differing from, 5–6
 - overview, 5
 - recommendations. *See* security recommendations
 - secure failure, 12
 - security policy, 7
 - threat model, 7
 - weakest link principle, 10
 - zones of trust, 24
- security policy, 7
- security recommendations
 - CE-CE IPsec
 - overview, 188
 - PE-PE IPsec compared, 189
 - CE-PE routing security best practices
 - BGP maximum-prefix mechanism, 183–184

- P-specific router security, 163
- routing security
 - MD5 for Label Distribution Protocol, 174
 - neighbor router authentication, 172–174
 - overview, 172
 - TTL security check, configuring, 177
 - TTL security mechanism for BGP, 175–176
- security reference model, 22–24
- shared access line, 109
- small TCP and UDP servers, 139
- spoofing
 - IP address spoofing, 58
 - label spoofing, 58
 - overview, 58–59
 - VPN spoofing, 75
- SSL (Secure Sockets Layer), 207
- standard router security, 119, 125
- static IPsec, 206
- static routing, 178

T

- tag distribution protocol (TDP), 62
- threat model, 7, 27
- threats
 - against core network
 - hierarchical core, 37, 39
 - Inter-AS core, 36–37
 - monolithic core, 32–35
 - overview, 32
 - against extranet sites, 31
 - against Internet, 40–41
 - against NOC, 39–40
 - reconnaissance attacks, 42–43
 - against VPNs
 - DoS (denial of service), 30
 - intrusions, 28–30
 - overview, 27–28
 - against zone of trust, 41
- tier 3 ISP connecting to an upstream tier via a service provider, 259
- traffic separation, 50–52
- TTL security check, configuring, 177
- TTL security mechanism for BGP, 175–176

U–V

- U-PE STP priority, 223
- VLAN trunking protocol (VTP) transparent operation, 226
- VLANS
 - controlling reserved, 228
 - removing unused, 228
- VPLS (Virtual Private LAN Service), 214–215
 - security considerations, 217–218
 - Metro Ethernet Model, 220
 - physical interconnection option, 219
 - SP interconnect models, 219–220
- VPN separation
 - address space separation, 48–49
 - ATM/FR security comparisons, 74
 - non-VRF interface, 51
 - overview, 47
 - traffic separation, 50–52
 - VRF interface, 51
- VPN spoofing, 75
- VPN technologies
 - connection-oriented, 13
 - encrypted, 14
 - Internet based, 14
 - overview, 12–14
- VPWS, 215
 - security considerations, 217–218
 - Metro Ethernet Model, 220
 - physical interconnection option, 219
 - SP interconnect models, 219–220
- VRF designs and Internet access, 88–89
- VRF Lite, 111
- VRF-to-VRF connection on ASBRs, 59–61, 116–117

W–Z

- weakest link principle, 10
- zone of trust
 - overview, 24, 100
 - threats against, 41