

Numerics

802.1AE. *See* IEEE 802.1AE

802.1X. *See* IEEE 802.1X

A

access control, 10

access ports, 68

ACLs (access control lists), 259

configuring, 230–232

HSRP attacks, mitigating, 153–154

ingress perimeter filtering, 262

PACLs, 267

RACLs, 264

VACLs, 265

VRRP attacks, mitigating, 162

wire speed enforcement, 259–260

active router (HSRP), 145

AES-GCM algorithm, 318

agent.circuit-id, 99

anatomy of LAN switches, 188

control plane, 190

vulnerabilities, 192

data plane, 189

vulnerabilities, 192

management plane, 190

vulnerabilities, 193

annualized loss expectancy, 9

applying Smartports macro to interface, 234

ARP (Address Resolution Protocol), 105

gratuitous ARP, 107–108

normal behavior, 105

rate-limiting, 235

requests, 105

vulnerabilities, 108

mitigating, 117

ARP inspection integration, 286

ARP spoofing, 108–110, 154

mitigating, 112, 115

with DAI, 112–115

with IDS, 116–117

tools for performing, 111

dsniff, 111–112

ARPwatch, 116

ASICs (application-specific integrated circuits), 192, 199

asymmetric cryptosystems, 12, 15

authentication, 17–18

confidentiality, 16

digital certificates, 18

X.509, 19

integrity, 17–18

attacks

against cryptosystems, 19

ARP spoofing, 108–110

mitigating, 112–117

tools used to perform, 111–112

CDP flooding attacks, mitigating on Cisco

ME3400 switch, 218–222

DDoS

botnets, 185–186

initiating, 184

zombies, 184–185

DHCP exhaustion, mitigating, 93–96

DHCP rogue server installation, 92–93

DHCP scope exhaustion, 89

DoS

TCP SYN, 187

TCP SYN attacks, 187

IP+MAC spoofing, 101

MAC spoofing, preventing with DHCP

snooping, 100

mitigating on Catalyst 6500 switch, 211

STP attacks, 55–57

Telnet flooding attacks, mitigating on Catalyst

6500 switch, 211–215

TTL expiry attacks, mitigating on Catalyst 6500

switch, 215–218

authentication, 10, 274

802.1X, 287, 310

multihost mode, 289

shadow hosts, 310–312

single-auth mode, 288

HSRP attacks, mitigating, 151–153

in asymmetric cryptosystems, 17–18

MAC address authentication, 293

VRRP attacks, mitigating, 162

Authentication Data field (HSRP packets), 148

authentication servers, 277

INDEX

authentication type field (VRRP packets), 160
authenticator (IEEE 802.1X), 277
authorization, 10, 275
 VLAN assignment, 298–299
availability, 8
 ARP vulnerability, 117

B

backup routers, 157
 VRRP, 159
bidirectional controlled port (802.1X), 281
binary search tries, 267
binding table (DHCP snooping), 98–99
binding tables, 98
bogons, 253
botnets, initiating DDoS attacks, 185–186
BPDUs guard feature (STP), 58–60
BPDUs (bridge protocol data units), 47, 70
 802.1D, 49
 configuration BPDUs, parameters, 48
 Flags field, 50
 hello interval, 49
 IEEE 802.1D, Flag field, 50
 TCN BPDUs, 50
broadcast domains, 26
brute-force attacks, 19
burning attacks, 140–142

C

CA (certification authority), 18
Caesar Code, 6
cain, 111
CAM table entries, 147
Catalyst 6500 switch
 attacks, mitigating, 211
 hardware-based CoPP, configuring, 200–202
 MLS QoS status, displaying, 203
 NetFlow, configuring, 244–245
 Telnet flooding attacks, mitigating, 211–212, 214–215
 TTL expiry attacks, mitigating, 215–218
Catalyst switches, flow mask, 240

CatOS, configuring DAI, 115
CDP (Cisco Discovery Protocol), 165
 attacks, mitigating on Cisco ME3400 switches, 218–222
 disabling, 169
 packet fields, 166–167
 risk analysis, 167–169
 risk mitigation, 169
CGAs (cryptographically generated addresses), 131
CIA (confidentiality, integrity, availability), 5
cipher text, 11
Cisco Catalyst 3750, applying Smartports macro to interface, 234
Cisco DTP (Dynamic Trunking Protocol), 76–79
 DTP attacks, mitigating, 80
Cisco IOS Software, configuring DAI, 113–114
Cisco ISL (Inter-Switch Link), 67
Cisco ME3400 switch
 control plane security, configuring, 203–206
 CPD flooding attacks, mitigating, 218–222
Cisco prestandard PoE detection mechanism, 136
Cisco QinQ, 71
Cisco switches, bridging table capacity, 27
Cisco VTP (VLAN Trunking Protocol), 80–81
clear text, 11
coexistence of LinkSec with other technologies, 317–318
collection architecture of NetFlow, 243
combining VACLs and RACLs, 266
commands
 dot1q tag native, 76
 macro apply, 235
 mls rate-limit, 202
 show platform policer, 205
 show policy-map control-plane, 209
 tcpdump, 161
compact notation, 107
comparing
 data and control plane, 226–227
 DDoS and DoS attacks, 183
 End-to-End and Hop-by-Hop cryptographic protection, 318–320
 stateful and stateless devices, 261
confidentiality, 6–7
 in asymmetric cryptosystems, 16

configuration BPDUs

- flooding attacks, 60–61
 - mitigating with BPDU filtering*, 62
 - mitigating with Layer 2 PDU rate limiter*, 63
- parameters, 48

Configuration Revision Number, 172**configuring**

- 802.1X, Guest-VLAN functionality, 292–293
- ACLs, 230–232
- control plane security on Cisco ME3400, 203–206
- DAI
 - on CatOS*, 115
 - on Cisco IOS*, 113–114
- hardware-based CoPP on Catalyst 6500 switch, 200–202
- IPsec/L2TPv3 combination, 325
 - full configuration, debugging*, 328–329
 - IKE authentication*, 327
 - IPsec crypto maps*, 326–327
 - xconnect*, 326
- NetFlow on Catalyst 6500, 244–245
- port security, 37
- software-based CoPP, 206–211
- STP, BPDU guard, 59–60
- unicast flood protection, 39

control plane, 190, 225

- ARP, rate-limiting, 235
- best practices, 236
- comparing to data plane, 226–227
- DTP, disabling, 228
- HSRP, disabling, 228
- ICMP messages, generating, 232–233
- link aggregation protocols, disabling, 228
- management protocols, disabling, 229
- routing protocols, disabling, 229–230
- securing, 198
- services, 198
- STP, disabling, 227
- VRRP, disabling, 229
- VTP, disabling, 228
- vulnerabilities, 192, 307

controlled port (802.1X), 280**CoPP (control plane policing), 197–198**

- hardware-based, configuring on Catalyst 6500, 200–202
- software-based, configuring, 206–211

crypto analysis, 19**crypto maps, configuring for IPsec/L2TPv3 combination, 326–327****cryptographic protection, 7****cryptology, 11–12**

- asymmetric cryptosystems, 15
 - authentication*, 17–18
 - confidentiality*, 16
 - digital certificates*, 18–19
 - integrity*, 17–18
- symmetric cryptosystems, 13
 - hashing functions*, 13
 - HMAC*, 14–15
 - symmetric encryption*, 13

cryptosystems, 12

- attacks against, 19

CS-MARS, 247–249**D****DAD (disclosure, alteration, disruption), 8****DAD (duplicate address detection), 127****DAI (Dynamic ARP inspection), mitigating ARP spoofing attacks, 112–115****data plane, 189**

- 802.1X, 280
- comparing to control plane, 226–227
- vulnerabilities, 192, 306

data-origin validation, 12**DDoS attacks**

- botnets, 185–186
- initiating, 184
- mitigating, 187–188
- versus DoS attacks, 183
- zombies, 184–185

debugging IPsec/L2TPv3 configuration

- full configuration, 328–329
- L2TP tunnels, 327

decryption, 11**defense in depth, 259****depletion of IPv4 addresses, 121****deploying DHCP snooping, 99****designated bridge, 47****detecting active worms**

- with ISPs, 252–253
- with MRTG, 254

detection mechanism for PoE, 136–137

DHCP (Dynamic Host Configuration Protocol), 85

- binding tables, 98
- exhaustion attacks, 89, 93–96
- IPv6 stateless configuration mode, 127–129
- lease time, 85
- packet fields, 88
- rogue server installation attacks, 92–93

DHCP snooping, 95–96

- binding table, 98–99
- deploying, 99
- on unsupported switches, 100
- security features
 - DHCP option 82*, 99
 - message validation*, 97–98
 - rate-limiting DHCP messages per port*, 97

DHCP spoofing attacks, 129**DHCP-snooping integration, 286****dictionary attacks, 19****digital certificates, 18–19****disabling**

- CDP, 169
- control plane protocols
 - HSRP*, 228
 - link aggregation protocols*, 228
 - management protocols*, 229
 - routing protocols*, 229–230
 - STP*, 227
 - VRRP*, 229
 - VTP*, 228
- ICMP message generation, 233

displaying MLS QoS status on Catalyst 6500, 203**DLSw, 324****domains (VTP), 171****don't care bits, 268****DoS attacks, 20**

- HSRP vulnerabilities, 149–150
- versus DDoS attacks, 183
- VRRP vulnerabilities, 161–162

dot1q tag native command, 76**double-nested VLAN attack, 71–74****dsniff, 111–112****DTP (Dynamic Trunking Protocol)**

- attacks, mitigating, 80
- disabling, 228

dual-homed switch simulation attacks, 63–64**dynamic mode (port security), 37****E****EAP (Extensible Authentication Protocol), selecting type of, 277****EAP-FAST, 276****EAP-MD5, 276****EAP-MSCHAPv2, 276****EAPOL, 275****EAP-TLS, 276****electronic circuits, TCAMs, 268–269****enabling**

- BPDU-Filter, 282
- BPDU-Guard, 282
- NetFlow on Catalyst 6500, 244–245

encryption, 11**End-to-End cryptographic protection, 318–320****enrollment, 18****EtherChannel, 174****Ethernet switches**

- ACLs, configuring, 230, 232
- control plane, 225
 - best practices*, 236
 - DTP, disabling*, 228
 - HSRP, disabling*, 228
 - ICMP messages, generating*, 232–233
 - IEEE 802.1X, rate limiting*, 234
 - link aggregation protocols, disabling*, 228
 - management protocols, disabling*, 229
 - routing protocols, disabling*, 229–230
 - STP, disabling*, 227
 - VRRP, disabling*, 229
 - VTP, disabling*, 228

frames, 23

EthernetV2 versus IEEE 802.3, 24**Ethertypes, 24, 68****ettercap, 111****exploits, DTP, 78–80****F****fields**

- of CDP packets, 166–167
- of DHCP packets, 88

filtering IP traffic with IP Source Guard, 102–103**fingerprinting flows, 241****Flag field (IEEE 802.1D BPDUs), 50**

Flexible NetFlow, 244**flooding, 44**

- attacks, preventing, 36–39
- config BPDU flooding, 60–61
 - mitigating with BPDU filtering, 62*
 - mitigating with Layer 2 PDDU rate limiter, 63*
- consequences of, 26
- effect on NetFlow cache, 246–247
- forced, 28–33
- preventing, 39–40
- TCP SYN attacks, 187
- unicast flood protection, preventing, 39

flow mask, 240**flows**

- fingerprinting, 241
- Netflow cache entry expiry, 244

forced flooding, 28–29

- macof, 30–33

forward delay timer (STP), 48**forwarding table, 25****framing format (EAPOL), 275****G****GCM (Galois/Counter Mode), 309****generating ICMP messages, 232–233****Gobbler, 90–92****gratuitous ARP, 107–108****group number (HSRP), 147****group number (VRRP), 158****Guest-VLAN functionality (802.1X), 290–293****H****hardware-based CoPP, 199**

- configuring on Catalyst 6500, 200
- rate-limiters, configuring on Catalyst 6500, 201–202

hashing functions, 13**header chaining, 124****hello interval, 49****Hello timer (STP), 48****help menu (Gobbler), 91–92****hexadecimal notation of IPv6 addresses, 125****history of WANs, 307–308****HMAC, 14–15**

- VTP authentication, 172

Hop-by-Hop cryptographic protection, 318–320**HSRP (Hot Standby Routing Protocol)**

- active router, 145
- attacks
 - DoS attacks, susceptibility to, 149–150*
 - mitigating, 151–154*
- disabling, 228
- group number, 147
- information leakage attacks, susceptibility to, 151
- link local scope, 146
- MAC addresses, 147
- message authentication, 152
- MITM attacks, susceptibility to, 150
- packets, 148
- standby routers, 145
 - becoming active, 148*

I**IBNS (Identity-Based Networking Service)**

- authentication, 274
- authorization, 275
- identification, 274

ICMP (Internet Control Message Protocol), 262

- messages, generating, 232–233

identification, 274**identity management, 10–11****IDS (Intrusion Detection Systems), mitigating**

- ARP spoofing attacks, 116–117**

IEEE 802.1AE

- AES-GCM algorithm, 318
- versus L2TPv3/IPsec combination, 325

IEEE 802.1D STP, 46

- BPDUs, 49–50

IEEE 802.1Q, 67

- backward-compatible specifications, 69
- Ethertype values, 68
- input classification, 69
- tags, stacking, 71

IEEE 802.1Q STP, 46**IEEE 802.1w Multiple STP, 47****IEEE 802.1w Rapid STP, 46**

IEEE 802.1X, 310

- ARP inspection integration, 286
- authentication, 287
 - shadow hosts, 310–312*
- bidirectional controlled port, 281
- controlled port, 280
- data plane, 280
- DHCP-snooping integration, 286
- extending with LinkSec, 312
 - authentication, 313*
 - data confidentiality, 314*
 - encryption modes, 316*
 - frame format, 314–316*
 - integrity, 314*
 - key distribution, 313*
- Guest-VLAN functionality, 290–292
 - configuring, 292–293*
- MAB operation, 293–294, 297–298
- multihost mode, 289
- port security integration, 285–286
- port-based access control, 277–278
- rate limiting, 234
- security, 279
- single-auth mode, 288
- STP considerations, 281–282
 - BPDU-Filter, enabling, 282*
 - BPDU-Guard, enabling, 282*
 - information leaks, 283–284*
 - trunking, 283*
- supplicant, 277

unsupported devices, 289**IEEE 802.11 vulnerabilities, 12****IEEE 802.3af PoE detection mechanism, 137****IEEE 802.3 versus EthernetV2, 24****IKE authentication, configuring for IPsec/
L2TPv3 combination, 327****impetus for IPv6, 121****in-band key distribution, 13****information leakage attacks, vulnerability to**

- ARP, 117
- HSRP, 151

ingress perimeter filtering ACLs, 262**initiating DDoS attacks, 184**

- botnets, 185–186
- zombies, 184–185

innocent bystanders, 101**input classification, 69****integrity, 7**

- in asymmetric cryptosystems, 17–18

interface ID, 125–126**inter-frame gap, 260****IP ACLs, configuring, 232****IP addresses**

- bogons, 253
- compact notation, 107

IP Source Guard, IP traffic filtering, 102–103**IP spoofing attacks, 101****IP+MAC spoofing attacks, 101****IPsec/L2TPv3**

- debugging, 328–329
- IKE authentication, configuring, 327
- IPsec crypto maps, configuring, 326–327
- pseudowires, configuring, 325
- versus IEEE 802.1AE, 325
- xconnect, configuring, 326

IPv4

- address depletion, 121
- comparing with IPv6, 122–124

IPv6

- differences with IPv4, 122–124
- header fields, 123–124
- hexadecimal notation, 125
- impetus for, 121
- interface ID, 125–126
- link local address, 125
- ND, 126
 - attacks, mitigating, 130*
 - DAD, 127*
 - SEND, 131–133*
- packets, 124
- rate limiting, 233
- stateless configuration mode, 127, 129
- vulnerability to attacks, 129

**IRPAS (Internet Routing Protocol Attack Suite),
173****ISPs, detecting active worms, 252–253**

J-K-L**key distribution, 13****key rollovers, 152****L2TPv3, 323**

- xconnect mode, 324

L2TPv3/IPsec integration

- debugging, 328–329
- IKE authentication, configuring, 327
- IPsec crypto maps, configuring, 326–327
- pseudowires, configuring, 325
- xconnect, configuring, 326

LACP (Link Aggregation Control Protocol), 174, 176

- risk analysis, 176–177
- risk mitigation, 177

Layer 2 security, MACSec, 309**lease time, 85****link aggregation protocols, 174–176**

- disabling, 228
- EtherChannel, 174
- risk analysis, 176–177
- risk mitigation, 177

link local address, 125**link local scope (HSRP), 146****LinkSec, coexistence with other technologies, 317–318****LinkSec security model, 312**

- authentication, 313
- data confidentiality, 314
- encryption modes, 316
- frame format, 314–316
- integrity, 314
- key distribution, 313

LLDP (Link Layer Discovery Protocol), risk analysis, 169–170**loss expectancy, 9****M****MAB (MAC Authentication Bypass), 293–294, 297–298****MAC addresses, 25**

- compact notation, 107
- HSRP, 147
- of VRRP virtual routers, 158
- security on 802.11 addresses, 308
- spoof attacks, 34–36
- spoofing, 34, 36

MAC authentication, 293**MAC spoofing attacks, 100****macof, 28–33****macro apply command, 235****macros, applying Smartports macro to interface, 234****MACSec (Media Access Control Security), 309****Management Domains, 171****management plane, 190**

- vulnerabilities, 193, 307

management protocols, disabling, 229**master routers, 157**

- VRRP, 159

Max age timer (STP), 48**McGrew, Dr. David, 309****MD5 key chain, HSRP message authentication, 152****message age, 48****migration from IPv6 to IPv4, motivation for, 121****mitigating**

- ARP spoofing attacks, 112, 115
 - with DAI, 112–115*
 - with IDS, 116–117*
- attack on Catalyst 6500 switch
- attacks on Catalyst 6500 switch
 - Telnet flooding attacks, 211–212, 214–215*
 - TTL expiry attacks, 215–218*
- attacks on Cisco ME3400 switch, CPD flooding attacks, 218–219, 221–222
- BPDU flooding attacks with BPDU filtering, 62
- BPDU flooding attacks with Layer 2 PDU rate limiter, 63
- CDP risks, 169
- DDoS attacks, 187–188
- DHCP exhaustion attacks, 93–94
 - with port security, 94–96*
- DTP attacks, 80
- HSRP attacks, 151
 - with ACLs, 153–154*
 - with authentication, 151–153*
- IPv6 attacks, 130
- link aggregation protocol risks, 177
- PoE attacks, 140
 - burning attacks, 142*
 - power gobbling, 140–141*
 - power-changing, 141*
 - shutdown attacks, 141*
- VRRP attacks, 161
 - with ACLs, 162*
 - with strong authentication, 162*
- VTP risks, 173–174

MITM (man-in-the-middle) attacks, 20

- burning attacks, 140–142
- HSRP vulnerability to, 150
- preventing, 20
- VRRP vulnerabilities, 161–162

MLS QoS, displaying status on Catalyst 6500, 203**mls rate-limit command, 202****MRTG (Multirouter Traffic Grapher), detecting active worms, 254****multicast, 32****multihost mode (802.1X), 289****Multiple STP, 47****N****NAM (Cisco Network Analysis Module), 249–251**

- SPAN configuration, 250

NAT (network address translation), 122**native VLANs, 70–71****ND (Neighbor Discovery), 126**

- attacks, mitigating, 130
- DAD, 127
- SEND, 131–133
- spoofing attacks, 129

NetFlow

- cache entry expiry, 244
- collection architecture, 243
- CS-MARS, 247–249
- enabling on Catalyst 6500, 244–245
- versions, 241–242

NetStumbler, 308**network baseline, 246–247****NNI (Network Node Interface), 203****no authentication vulnerability (ARP), 117****normal ARP behavior, 105****O-P****Option 82, 99****out of band key distribution, 13****packets**

- CDP, fields, 166–167
- DHCP, fields, 88

HSRP, 148**innocent bystanders, 101****IPv6, 124****VRRP, 159**

authentication type field, 160

Priority field, 160

VTP, 171**PACLs (port-based ACLs), 263, 267****PAGP (Port Aggregation Protocol), 174–175****risk analysis, 176–177****risk mitigation, 177****parasite6, 130****PDU (Protocol Data Units), LACP, 175****PEAP, 276****per port configuration (VTP), 172****phantom circuits, 138****PKI (public key infrastructure), 18****PoE (Power over Ethernet)**

- burning attacks, mitigating, 142
- detection mechanism, 136–137
- power gobbling attacks, mitigating, 140–141
- power-changing attacks, mitigating, 141
- powering mechanism, 138
- requirements for use, 135
- risk analysis, 139–140
- shutdown attacks, mitigating, 141

port security

- dynamic mode, 37
- effect on CPU utilization, 39
- integration, 285–286
- mitigating DHCP exhaustion attacks, 94–96
- preventing, 37
- preventing MAC spoofing attacks, 37–39

Portfast, 60**ports, cost, 47****power gobbling attacks, 139**

- mitigating, 140–141

power-changing attacks, mitigating, 141**powering mechanism of PoE, 138****preshared keys, key rollovers, 152****preventing**

- flooding attacks, 39–40
- MAC spoofing attacks, 36
- with port security, 37–39*
- MITM attacks, 20

Priority field**HSRP packets, 148****VRRP packets, 160**

private keys, 16
 protective containers, 7
 pseudowires, 324–325
 PSIRT (Product Security Incident Report Team), 9
 public key, 16
 PVST+ (per-VLAN spanning tree plus), 52–53

R

RA spoofing attacks, 129
 RACLs (router ACLs), 263–264
 combining with VACLs, 266
 Rapid STP, 46
 RAs (Router Advertisements), 128
 rate-limiters, configuring for hardware-based CoPP, 201–202
 rate-limiting IPv6 traffic, 233
 relay agents, 85
 renewal of digital certificates, 18
 repudiation, 17
 requests (ARP), 105
 requirements for PoE, 135
 reverse random-access memory, 268
 reverse security triad, 8
 revocation of key pair, 18
 risk analysis, 9
 for VRRP, 161
 for CDP, 167–169
 for link aggregation protocols, 176–177
 for LLDP, 169–170
 for PoE, 139–140
 for VTP, 170–173
 risk management, 8
 risk analysis, 9
 risk control, 10
 risk mitigation
 of link aggregation protocols, 177
 of VTP, 173–174
 RMON (Remote Monitoring), 239, 249
 rogue DHCP server installation, 92–93
 root bridge election (STP), 47
 root guard feature (STP), 58–59
 root ownership attacks, 57–58
 routing protocols, disabling, 229–230

S

Sasser worm, 248
 securing control plane, 198
 on Cisco ME3400, 203–206
 security
 "bandage" analogy, 305
 Layer 2, MACSec, 309
 security triad, 5
 availability, 8
 confidentiality, 6–7
 integrity, 7
 selecting EAP type, 277
 SEND (Secure Neighbor Discovery), 131–132
 future implementation of, 133
 services on control plane, 198
 shadow hosts, 310–312
 shared key, 13
 show platform policer command, 205
 show policy-map control-plane command, 209
 shutdown attacks, mitigating, 141
 signatures, 17
 single-auth mode (802.1X), 288
 sink hole routers, 253
 Smartports macro, applying to interface, 234–235
 SNAP (Subnetwork Access Protocol), 165
 software-based CoPP, 199
 configuring, 206–211
 Song, Dug, 28
 SPAN (Switched Port Analyzer), 250
 spoofing attacks
 MAC address spoofing, 34–36
 preventing, 36
 with port security, 37–39
 stacking IEEE 802.1Q tags, 71
 standby routers (HSRP), 145
 becoming active, 148
 stateful versus stateless devices, 261
 stateless configuration mode (IPv6), 127–129
 sticky port security, 285
 STP (Spanning Tree Protocol), 43–45
 and 802.1X, 281–282
 BPDU-Filter, enabling, 282
 BPDU-Guard, enabling, 282
 information leaks, 283–284
 trunking, 283

attacks
 config BPDU flooding, 60–63
 dual-homed switch simulation, 63–64

BPDU guard feature, 58–59
 configuring, 59–60

BPDUs, hello interval, 49

designated bridge, 47

disabling, 227

EtherChannel, 174

IEEE 802.12, 46

IEEE 802.1D, 46

IEEE 802.1Q, 46

IEEE 802.1s, 47

port cost, 47

Portfast, 60

PVST+ (per-VLAN spanning tree plus), 52–53

root bridge election, 47

root guard feature, 58–59

root ownership attacks, 57–58

timers, 48

Yersinia attacks, 55–57

supplicants, 277

SVIs (switch virtual interfaces), 264

switches

ACLs, configuring, 230, 232

anatomy of, 188
 control plane, 190
 data plane, 189
 management plane, 190

ASICs, 199

bridge table capacities, 27

CAM table entries, 147

control plane, 225
 ARP, rate-limiting, 235
 best practices, 236
 DTP, disabling, 228
 HSRP, disabling, 228
 ICMP messages, generating, 232–233
 IEEE 802.1X, rate limiting, 234
 link aggregation protocols, disabling, 228
 management protocols, disabling, 229
 routing protocols, disabling, 229–230
 STP, disabling, 227
 VRRP, disabling, 229
 VTP, disabling, 228
 vulnerabilities, 192

data plane vulnerabilities, 192

DHCP snooping support, 100

forwarding table, 25

management plane vulnerabilities, 193

trunking
 Cisco DTP, 76–80
 Cisco VTP, 80–81

trunks, 69
 traffic, tagging, 74–76

symmetric cryptosystems, 12–13

hashing functions, 13

HMAC, 14–15

symmetric encryption, 13

symmetric encryption, 13

T

tagging trunk traffic, 74–76

TCAM (ternary content-addressable memory), 268–269

TCN BPDUs, 50

TCP SYN attacks, 187

tcpdump command, 161

Telnet flooding attacks, mitigating on Catalyst 6500 switches, 211–215

timers, STP, 48

TLVs (LLDP), 170

tools for performing ARP attacks, 111–112

traffic classes for software-based CoPP, defining, 207

tries, 267

trunk ports, 68

trunking

 Cisco DTP, 76–80

 Cisco VTP, 80–81

 input classification, 69

 traffic, tagging, 74–76

trust

 control plane vulnerabilities, 307

 data plane vulnerabilities, 306

 management plane vulnerabilities, 307

TTL (time-to-live) expiry attacks, mitigating on Catalyst 6500 switches, 215–218

tunneling, DLSw, 324

U-V

UNI (User-Network Interface), 203

unicast flooding protection, 39–40

unknown unicast flooding, 26

consequences of, 26

preventing, 39–40

VACLs (VLAN ACLs), 263–265

advantages over port mirroring, 266

combining with RACLs, 266

versions of NetFlow, 241–242

Viega, John, 309

virtual routers (VRRP), MAC addresses, 158

virtualized bridging table, 29

Vitek, Ian, 28

VLAN ACLs, 130

VLAN assignment, 298–299

VLANs, 67

double-nested VLAN attacks, 71–74

IEEE 802.1Q

tags, stacking, 71

native, 70–71

VRRP (Virtual Router Redundancy Protocol), 157–159

disabling, 229

group number, 158

packets, 159

authentication type field, 160

Priority field, 160

risk analysis, 161

virtual routers, MAC addresses, 158

vulnerability to DoS attacks, 161

mitigating, 161–162

vulnerability to MITM attacks, 161

mitigating, 161–162

VTP (VLAN Trunking Protocol)

disabling, 228

packet format, 171

risk analysis, 170–173

risk mitigation, 173–174

vulnerabilities

of ARP, 108, 117

of CDP, 167–169

mitigating, 169

of Cisco VTP, 81

of cryptosystems, 19

of LAN switches

on control plane, 192

on data plane, 192

on management plane, 193

of link aggregation protocols

mitigating, 177

of LLDP, 169–170

of VTP, 170–174

on control plane, 307

on data plane, 306

on management plane, 307

W-X-Y-Z

WANs, history of, 307–308

wire speed ACL enforcement, 259–260

WLANs

802.11, MAC address security, 308

history of, 307–308

worms

detecting

with ISPs, 252–253

with MRTG, 254

Sasser, 248

WPA (Wi-Fi Protected Access), 308

X.509 digital certificates, 19

xconnect mode (L2TPv3), 324–326

Yersinia, 89, 167

DoS attacks, launching against HSRP, 149–150

double nested VLAN attacks, 73–74

DTP attacks, 79–80

manual page, 53–54

STP attacks, 55, 57

BPDU flooding attacks, 60–63

dual-homed switch simulation, 63–64

zombies, initiating DDoS attacks, 184–185