

INDEX

Symbols & Numerics

| (pipe), 182

3DES (Data Encryption Standard), 250

10Base2, 21, 91

10Base5, 21, 91

10BaseT, 21, 91

100BaseT, 21, 92

802.1Q, 26

802.11 networks, 88

1000 GE, 21, 92

A

AAA, 228–229

accounting, 231–232

authentication, 230

authorization, 230–231

ABRs (Area Border Routers), 63

access lists, 353–355

extended, 196–198

IP packet debugging, 179–180

standard, 190–195

wildcard masks, 192

accessing Cisco routers, 187

accounting, 228, 231–232

ACKs (acknowledgments), 58

ACS (Cisco Secure Access Control Server).

See Cisco Secure

Active Directory, 135

Active FTP, 116–118

adaptive cut-through switching, 23

adjacencies, 62

administrative distances, 51

AES (Advanced Encryption Standard),

250–251

agents (SNMP), 124

Aggregator attribute (BGP), 73

aggressive mode (IKE), 259

AH, 257–258

alias command, 175

allocating IP addresses, InterNIC, 357

ambiguous test questions, decoding, 628–629

anomaly-based analysis, 386

anomaly-based IDS systems, 305

application layer (OSI model), 18

applications

NetRanger, 309

Director, 311

typical network placement, 309

TFTP, 114

applying access lists to interfaces, 193–195

areas, 62

ARP, 38–39

AS (autonomous systems), 62

AS_Path attribute (BGP), 73

ASA (Adaptive Security Algorithm), 362

ASBRs (Autonomous system boundary

routers), 63

asynchronous communications, 80–81

Atomic Aggregate attribute (BGP), 73

attacks

birthday attacks, 421

CAM overflow, 201–202

chargen, 420

CPU-intensive, 420

DDoS, 420

DHCP starvation, 207–208

DNS poisoning, 420

DoS, 418, 421

E-mail, 420

incident response teams, 415–416

Land.C, 420

MAC spoofing, 205–207

- man in the middle, 421
- methods of, 417
- motivation for, 413
- ping of death, 419
- sacrificial hosts, 419
- smurf, 421
- spoof attacks, 421
- STP manipulation, 204
- TCP SYN flood, 419
- teardrop, 420
- UDP bombs, 420
- VLAN hopping, 202–203

attributes of RADIUS, 234–235

authentication, 228–230

- HTTP, 120
- method lists, 238
- on TACACAS+ servers, 240
- PPP, 78

authoritative time sources

- configuring, 131–132
- stratum, 130–131

authorization, 229–231

- on TACACAS+ servers, 240–241

AVVID (Cisco Architecture for Voice, Video and Integrated Data), 84

- WLAN solutions, 85–88

B

bastion hosts, 419

BECN (backward explicit congestion notification), 79

BGP (Border Gateway Protocol), 71

- attributes, 72–74
- characteristics, 72
- configuring, 74–75
- messages, 71

birthday attacks, 421

bit-flip attacks, 87

Blocking state (spanning tree), 24

bootstrap program, 159

BPDUs (Bridge Protocol Data Units), 24

BRI, 75

bridging, 22

- port states, 24
- transparent, 23

broadcast domains, 23

buffers, 157

C

calculating hosts per subnet, 30–31

CAM tables, 22

- overflow, 199–200
- overflow attacks, 201–202

Catalyst 6500 Series Switch, IDSM-2, 312

CBAC (Content-Based Access Control), 378

- audit trail messages, enabling, 505
- configuring, 380–382

CEP (Certificate Enrollment Protocol), 272

CERT/CC (Computer Emergency Response Team Coordination Center), 413–414

certification exam, objectives, 627

characteristics

- of RIP, 52
- of RIPv1, 52
- of RIPv2, 53

chargen attacks, 420

CIDR (classless inter-domain routing), 32

Cisco 7200 routers, switching methods

- website, 176

Cisco IDS, 422

- RDEP, 138–139
- sensors, 423
- Signature Engines, 423–424
- supported products, 422

Cisco IOS, 165

- firewall features, 377–379
- intrusion prevention methods
 - core dumps*, 430
 - disabling default services*, 429
 - disabling DHCP*, 427
 - disabling TCP/UDP small servers*, 427
 - enabling sequence numbering*, 428
 - enabling TCP intercept*, 429
 - Nagle algorithm*, 425–426
- modes of operation, 164
- password recovery, 182–187

Cisco IOS SSH, 135–138**Cisco Product Security Incident Response Team, web site, 414****Cisco SDM (Security Device Manager), 328****Cisco Secure, 301**

- AAA features, 302
- features, 301
- test topics, 301

Cisco Secure IDS, 309

- sensors, 309–310

Cisco Secure VPN Client, 326–328**Cisco TFTP, 114****Cisco VPN 3000 Series Concentrators, 314–316, 319–325****classful addressing, 33****classful routing protocols, 33****clear conduit command, 372****clock sources, 131–132**

- NTP configuration, 130–131

Cluster-List attribute (BGP), 73**collisions, jam signals, 20****commands**

- | (pipe) modifier, 182
- alias, 175
- clear conduit, 372
- conduit, options, 372
- copy running-config startup-config, 165
- copy tftp flash, 115
- debug all, 179
- global, options, 368
- HSRP, 43
- ip http authentication, 120
- ip route-cache, 176
- ip subnet-zero, 32
- ip verify unicast reverse-path, 430
- logging console debug, 175

service password-encryption, 189**service tcp-keepalives-in, 426****set vlan, 24****shortcuts, creating, 175****show accounting, 231–232****show debugging, 170****show interface, 163****show interfaces, 171–172****show ip access-lists, 170****show ip arp, 39****show ip route, 48–50, 169–170****show logging, 173****show process, 158–159****show route-map, 174****show startup-config, 185****show version, 162–163, 174****SMTP, 129****snmp-server enable traps config, 126****snmp-server host, 126–127****static, 371****undebg all, 171****write terminal, 157****community access strings, 122****Community attribute (BGP), 73****comparing****HIDS and NIDs, 305****preshared keys and manual keys, 268****RADIUS and TACACS+, 245–246****conduit command, options, 372****configuration files****loading, 165****saving, 165****Configuration mode (IOS), 164****configuration registers, 160–161****modifying, 184****configuring, 54–56, 130–131****CBAC, 380–382****HSRP, 44****IPSec, 264–272****Nagle algorithm, 426****RADIUS, 236–238****SGBP, 81****SNMP support on Cisco routers, 125****SSH on Cisco IOS routers, 136–138****TACACAS+, 241–244****VPDNs, 278–281****VPNs, 385****connectionless protocols, 16**

connection-oriented protocols, 16
 TCP, 34
 header format, 34
 packets, 34–35
 Telnet requests, 36–37

copy running-config startup-config commands, 165

copy tftp flash command, 115

copying IOS images from TFTP servers, 115

core dumps, performing, 430

CPU, 158–159

CPU-intensive attacks, 420

creating
 command shortcuts, 175
 extended access lists, 196–198
 standard access lists, 190–195
 VLANs, 23

crypto map entries, 266

cryptography
 key exchange management, 264–272
 PKI, 382–383

CSA (Cisco Security Agent), 422, 387
 versus pattern-matching, 388

CSACS (Cisco Secure Access Control Server), 239

CSMA/CD, 20

CSS (calling search spaces), 83

CTA (Cisco Trust Agent), 391

CTR (Cisco Threat Response), 391
 IDS requirements, 392
 IOS Authentication 802.1X, 392–393

cut through switching, 23

D

Daemen, Joan, 250

DATA command (SMTP), 129

data encryption, 255–257
 3DES, 250
 AES, 250–251
 DES, 248–250
 Diffie-Hellman, 252–253
 IPSec, 254
 MD5, 251–252
 principles of, 247–248

data link layer. See Layer 2 security

data manipulation, 417

DDOS (Distributed Denial Of Service) attacks, 420

debug all command, 179

debug commands, 175, 182
 options, 177–178

debugging, turning off, 171

default services, disabling, 429

defining
 HTTP port number, 121
 TFTP download directory, 115

deploying NAT, 357

DES (Data Encryption Standard), 248–250

development
 of Ethernet, 20
 of OSI reference model, 14

devices
 asynchronous communication, 80–81
 broadcast domains, 23
 firewalls, 352
 VLANs, creating, 23

DHCP, 40
 disabling, 427
 leases, viewing, 40
 starvation attacks, 207–208

DHCP snooping, 207

Diffie-Hellman protocol, 252–253

disabled state (spanning tree), 24

disabling, 427–429
 DNS lookup on Cisco routers, 112
 mask replies, 431
 proxy ARP, 431
 TCP/UDP small servers, 427
 Telnet login password, 113

displaying
 configured policy routes, 174
 router home page, 119
 routing tables, 48–50
 system log, 173

distance vector protocols
 loop avoidance techniques, 53
 RIP, 52–53
 configuring, 54–56

DLCIs (data-link connection identifiers), 79

DMZ, 351

DNS, 110–111
 disabling lookup on Cisco routers, 112
 enabling lookup on Cisco routers, 113

DNS poisoning, 420

DoS attacks, 418, 421

- double tagging, 203**
- DRs (Designated Routers), 63**
 - election process, disabling, 70
- DSS (digital signatures), 382**
- dynamic crypto map entries, 266**
- Dynamic NAT, 359–360**

E

- EAP (Extensible Authentication Protocol), 85, 272, 275–276**
- EAP-TLS (Extensible Authentication Protocol Transport Layer Security), 272, 275–276**
- eBGP (external BGP), 74**
- EIGRP (Enhanced Interior Gateway Routing Protocol), 57–61**
- election process (DRs), disabling, 70**
- e-mail**
 - attacks, 420
 - SMTP, 128–129
- enable passwords, setting, 188**
- enabling, 428–429**
 - HSRP, 43
 - Nagle algorithm, 426
 - PortFast on Cisco switches, 25
 - SSH support on Cisco routers, 136–138
- encapsulation, 19**
 - HDLC, 76
 - LCP, 78
 - PPP, 77
- encryption technologies, 246–247**
 - 3DES, 250
 - AES, 250–251
 - DES, 248–250
 - Diffie-Hellman, 252–253
 - IPSec, 254
 - AH, 257–258
 - ESP, 255–256
 - MD5, 251–252
 - principles of, 247–248
- error messages, synchronous logging, 178**
- establishing Telnet connections, 187**
- Ethernet**
 - CSMA/CD, 20
 - interfaces, states of, 173
 - media specification, 21, 92
 - spanning tree, 23

- exam**
 - FAQs, 633
 - objectives, 627
 - preparing for, 631
 - study tips, 625–626
- extended access lists, 196–198**
- external links, 63**

F

- FAQs regarding exam, 632–637**
- FC (feasibility condition), 58**
- feasible distance, 58**
- features**
 - of RADIUS, 235
 - of TACACAS+ servers, 241
- FEC (Fast EtherChannel), 25–26**
- FECN (forward explicit congestion notification), 79**
- fields, 34–35, 50**
- filtering TCP services, 353–355**
- firewalls, 352**
 - Cisco IOS features, 377–379
 - PIX, 361, 363–373
- Flags field (TCP packets), 35**
- Flash memory, 157–158**
- Forwarding state (spanning tree), 24**
- Frame Relay, 79**
- frames, 15**
 - BPDU, 24
- framing, ISDN, 76**
- FTP, 47–48**
 - Active mode, 116–118
 - Passive mode, 118

G

- gateways, HSRP, 41**
- generating keepalive packets, 426**
- global command, options, 368**
- gratuitous ARP, 39**

H

- hashing algorithms, 251–252**
- HDLC, 76**

- Hello packets**
 - EIGRP, 58
 - OSPF, 62
 - heuristic-based signatures, 386**
 - hiding secret passwords, 189**
 - HIDS, comparing with NIDS, 305**
 - hijacking, 418**
 - holdtime, 58**
 - host IDSs, 422**
 - hosts per subnet, calculating, 30–31**
 - HSRP, 41**
 - configuring, 44–45
 - enabling, 43
 - status, viewing, 45
 - HTTP (Hypertext Transfer Protocol), 119**
 - defining port number, 121
 - SSL, 121
 - user authentication, 120
 - hybrid routing protocols, EIGRP, 57–58**
 - configuration example, 59–61
- I**
- iBGP (internal BGP), 74**
 - iCisco SDM (Security Device Manager), 330**
 - ICMP, 46–47**
 - IDS Device Manager, 311**
 - IDSs (intrusion detection systems), 303**
 - anomoly-based, 305
 - Cisco IDS
 - Signature Engines*, 423–424
 - supported products*, 422
 - Cisco Inline IDS, 311
 - NetRanger, 309
 - Director*, 311
 - typical network placement*, 309
 - network-based, 305–306, 386
 - notification alarms, 303
 - placement, 305–307
 - signature-based, 304
 - tuning, 307–308
 - IETF (Internet Engineering Task Force), 29**
 - web site, 417
 - IKE, 258–259**
 - configuring, 264–272
 - phase I message types, 259–260
 - phase II message types, 260–264
 - images, 157**
 - incident response teams, 415–416**
 - inform requests (SNMP), 124**
 - Initial configuration mode (IOS), 164**
 - inside global addresses, 356**
 - inside local addresses, 356**
 - Interface configuration mode (IOS), 164**
 - interfaces, 163, 193–195**
 - Ethernet states, 173
 - Internet Domain Survey web site, 417**
 - Internet newsgroups, 416–417**
 - InterNic, 357**
 - intruders, methods of attack, 417**
 - IOS images, copying from TFTP servers, 115**
 - IP addressing**
 - address classes, 29
 - ARP, 38–39
 - CIDR, 32
 - classful addressing, 33
 - DHCP, 40
 - DNS, 110–113
 - logical AND operation, 30
 - packets, 27–29
 - RARP, 39
 - subnets, 29–30
 - subnetting, 30–32
 - IP GRE (generic routing encapsulation)**
 - tunnels, configuring, 383–385
 - ip http authentication command, 120**
 - IP multicast, 79**
 - IP packet debugging, 179–180**
 - ip route-cache command, 176**
 - IP source guard, 208**
 - ip subnet-zero command, 32**
 - ip verify unicast reverse-path command, 430**
 - IPSec, 254**
 - configuring, 264–272
 - IKE, 258–259
 - phase I message types*, 259–260
 - phase II message types*, 260–263
 - ISDN (Integrated Services Digital Network), 75**
 - commands, 78
 - framing, 76
 - layer 2 protocols, 76
 - authentication*, 78
 - HDCL*, 76
 - LCP*, 78
 - NCP*, 78
 - PPP*, 77

ISL (Inter-Switch Link), 26
 ISO (International Organization for Standardization), 14
 ISOC (Internet Society) web site, 417

J-K

jam signals, 20

keepalive packets, generating, 426

L

L2F (Layer 2 Forwarding), 276–277

L2TP (Layer 2 Tunneling Protocol), 276–277

lab exam, 633–635

FAQs, 635–637

sample, 639–664

Land.C attacks, 420

Layer 2 security, 15

CAM table overflow, 199–202

DHCP starvation attacks, 207–208

MAC spoofing attacks, 205–207

STP manipulation attacks, 204

VLAN hopping, 202–203

layers of OSI reference model

application layer, 18

data link layer, 15

network layer, 16, 22–23, 27–30

physical layer, 14

presentation layer, 17–18

session layer, 17

transport layer, 17

LCP, 78

LDAP (Lightweight Directory Access Protocol), 135

Learning state (spanning tree), 24

leases (DHCP), viewing, 40

link-state protocols, OSPF, 61–70

media types, 65

Listening state (spanning tree), 24

LLC sublayer, 15

loading configuration files, 165

Local Preference attribute (BGP), 73

log files (PIX Firewall), troubleshooting, 374–375

logging console debug command, 175

loopback interfaces, 431

loop prevention, split horizon, 53

lost passwords, recovering, 182–187

LSAs (link-state advertisements), 63

M

MAC spoofing attacks, 205–207

MAC sublayer, 15

MAIL command (SMTP), 129

main mode (IKE), 259

man in the middle attacks, 421

managed devices, 124

manual keys, comparing with preshared keys, 268

mask replies, disabling, 431

masquerading, 418

MD5 (Message Digest 5), 251–252

MED attribute (BGP), 73

media specifications of Ethernet, 21, 92

memory

NVRAM, 157

RAM, 157

ROM, 159–160

System Flash, 157

method lists, 238

methods of attacks, 417

metrics, administrative distance, 51

MIBs, 123–125

MIC (Message Integrity Check), 275

modes of IOS operation, 164

modifying configuration registers, 184

monitoring NAT, 360

motivation for attacks, 413

multicasting, 79

N

Nagle algorithm, preventing Cisco IOS from attacks, 425–426

Nagle, John, 426

name resolution, DNS, 110–113

NAT (Network Address Translation), 355–356

deploying, 357

Dynamic NAT, configuring, 359

monitoring, 360

operation on Cisco routers, 358

NCP, 78

NetRanger, 309
 Director, 311
 typical network placement, 309

network IDS, 422

network layer
 bridging
 BPDUs, 24
 port states, BPDUs, 24
 ICMP, 46–47
 IP, 27
 address classes, 29
 logical AND operation, 30
 packets, 27–28
 subnets, 29–30
 spanning tree protocol, 23
 subnetting, 31–32
 switching, 22
 CAM tables, 22
 cut through, 23
 store and forward, 23

network layer (OSI model), 16

network management, SNMP, 122
 community access strings, configuring on
 Cisco routers, 122
 configuring on Cisco routers, 125
 examples of, 128
 managed devices, 124
 MIBs, 123–125
 notifications, 123–126

network-based IDS systems, 305–306, 386

newsgroups, reporting security breaches, 416–417

Next Hop attribute (BGP), 73

NMSs (network management systems), 124

NOOP command (SMTP), 129

notification alarms, 303

notifications (SNMP), 123–126

NSSAs (Not-so-stubby areas), 65

NTP (Network Time Protocol), configuring
 clock sources, 130–132

NVRAM (nonvolatile RAM), 157

O

Origin attribute (BGP), 73
Originator ID attribute (BGP), 73

OSI reference model
 application layer, 18
 data link layer, 15
 development of, 14
 network layer, 16, 27
 spanning tree, 23
 switching, 22–23
 peer-to-peer communication, 19
 physical layer, 14
 presentation layer, 17–18
 session layer, 17
 transport layer, 17
 versus TCP/IP model, 18

OSPF (Open Shortest Path First), 61–63
 example configuration, 66–70
 media types, 65
 multiple area configuration, 64–65
 single area configuration, 62–64
 virtual links, 66

outside global addresses, 356

outside local addresses, 356

P

packet filtering, 353
 CBAC, 378
 configuring, 380–382
 extended access lists, 196–198
 standard access lists, 190–195

packets
 EIGRP, Hello, 58
 IP
 debugging, 179–180
 fields, 28–29
 rerouting, 418
 TCP, 34–35

partitioning System Flash, 157

Passive FTP, 118

passive IDS modules, 387

passwords
 authentication, 230
 method lists, 238
 enable passwords, setting, 188
 recovering, 182–187
 virtual terminal passwords, setting, 190

PAT (Port Address Translation), 355

path vector protocols, BGP, 71–75

pattern matching, 386

PEAP (Protected EAP), 272–276
peer-to-peer communication, 19
perimeter routers, 353
physical layer (OSI model), 14
ping of death attacks, 419
ping requests, test characters, 46–47
PIX (Private Internet Exchange), 361
 commands, 371–373
 configuring, 364–368
 DMZs, 361
 software features, 376–377
 stateful packet screening, 362–363
 static routing, 368–369

PIX Firewall
 log files, troubleshooting, 374–375
 NAT support, 363

PKI (Public Key Infrastructure), 382–383
placement of IDS systems, 305–307
Poison Reverse updates, 53
policy routes, displaying, 174
PortFast, enabling, 25
PPP (Point-to-Point Protocol), 77
preparing for exam, 631
 FAQs, 633
 objectives, 627
 sample lab, 639–664

preparing for qualification exam, 629–630
presentation layer (OSI model), 17–18
presheared keys, comparing with manual keys, 268, 506
preventing Cisco IOS from attacks
 disabling default services, 429
 disabling DHCP, 427
 disabling TCP/UDP small servers, 427
 enabling sequence numbering, 428
 enabling TCP intercept, 429
 Nagle algorithm, 425–426
 performing core dumps, 430

PRI, 75
privilege levels, authorization, 230–231
Privileged EXEC mode (IOS), 164
protocol decode-based analysis, 386
proxy ARP, disabling, 431
proxy servers, 352

Q

qualification exam
 FAQs, 632–633
 preparing for, 629–630
 study tips, 626–627
decoding ambiguity, 628–629

QUIT command (SMTP), 129

R

RADIUS, 232
 attributes, 234–235
 configuring, 236–238
 features, 235
 security protocol support, 234
 versus TACACAS+, 245–246

RAM, 157
 NVRAM, 157
 System Flash, 157–158

RARP, 39
RCPT command (SMTP), 129
RDEP (Remote Data Exchange Protocol), 138–139
read command (SNMP), 125
recovering lost or unknown passwords, 182–187
redundancy, HSRP, 41–45
remote access VPDNs, 276–277
 configuring, 278–281
remote router access, 187
reporting security breaches, Internet newsgroups, 416–417
rerouting packets, 418
resolving IP addresses to MAC addresses, ARP, 38–39
Rijmen, Vincent, 250
ROM (read-only memory), 159–160
ROM boot mode (IOS), 164
root bridge elections, 24
root bridges, 24
router hardware
 configuration registers, 160–161
 CPU, 158
 interfaces, 163
 NVRAM, 157

- RAM, 157
- ROM, 159–160
- System Flash, 157
- routers, remote access, 187**
- routing protocols, 48**
 - BGP, 71
 - attributes*, 72–74
 - configuring*, 74–75
 - messages*, 71
 - default administrative distances, 51
 - EIGRP, 57–58
 - example configuration*, 59–61
 - OSPF, 61–63
 - example configuration*, 66–70
 - multiple area configuration*, 64–65
 - single area configuration*, 62–64
 - virtual links*, 66
 - RIP, 52–53
 - configuring*, 54–56
- routing tables, viewing, 48–50**
- RSET command (SMTP), 129**
- RTO (Retransmission Timeout), 58**

S

- sacrificial hosts, 419**
- SAFE blueprints, security best practices, 208–209**
- SAML command (SMTP), 129**
- sample lab. See self-study lab**
- SAs (security associations), 254–259**
- saving configuration files, 165**
- sCSA (Cisco Security Agent), 387**
- SDM (Security Device Manager), 328–330**
- secret passwords, hiding, 189**
- security, 353, 380–382**
 - AAA, 228–229
 - accounting*, 231–232
 - authentication*, 230
 - authorization*, 230–231
 - Cisco IOS SSH, 135–138
 - encryption technologies, 246–247
 - 3DES*, 250
 - AES*, 250–251
 - DES*, 248–250
 - Diffie-Hellman*, 252–253
 - IPSec*, 254–258
 - MD5*, 251–252
 - principles of*, 247–248

- firewalls, 352
 - Cisco IOS features*, 377–379
- HTTP, 119–120
- IKE
 - configuring*, 264–272
 - phase II*, 264
- NAT, 355–356
 - configuring Dynamic NAT*, 359
 - deploying*, 357
 - monitoring*, 360
 - operation on Cisco routers*, 358
- packet filtering, TCP services, 353–355
- PAT, 355
- PIX, 361
 - commands*, 371–373
 - configuring*, 364–368
 - DMZs*, 361
 - software features*, 376–377
 - stateful packet screening*, 362–363
 - static routing*, 368–369
- PKI, 382–383
- RADIUS, 232
 - attributes*, 234–235
 - configuring*, 236–238
 - features*, 235
 - security protocol support*, 234
- SSH, 133–135
- SSL, 121
- TACACS+, 239
 - authentication*, 240
 - authorization*, 240–241
 - configuring*, 241–244
 - features*, 241
 - versus RADIUS*, 245–246
- VPDNs, 276–277
 - configuring*, 278–281
- VPNs, 383
 - configuring*, 385
- security server protocols, 232**
- self-study lab**
 - ACS configuration, 514–524
 - advanced PIX configuration, 511–514
 - BGP routing configuration, 491–495
 - Catalyst Ethernet switch setup, 457–464
 - DHCP configuration, 490
 - dynamic ACL/lock and key feature configuration, 501–502
 - final configurations, 538–558
 - Frame Relay setup, 450–456

- IDS configuration, 525, 530, 538
- IGP routing, 470–475
 - OSPF configuration*, 475–484
- IOS firewall configuration, 505
- IP access list configuration, 495–497
- IPSec configuration, 505–511
- ISDN configuration, 484–490
- local IP host address configuration, 464–466
- physical connectivity, 456
- PIX configuration, 465–470
- setup, 445–448
 - communications server*, 448–449
- TCP intercept configuration, 497–499
- time-based access list configuration, 499–500
- SEND command (SMTP), 129**
- Sendmail, 129**
- sensors, Cisco IDSs, 309–310, 423
- sequence numbering, enabling, 428
- servers, RADIUS, 232
- service password-encryption command, 189
- service tcp-keepalive command, enabling
 - Nagle algorithm, 426
- service tcp-keepalives-in command, 426
- session hijacking, 418
- session layer (OSI model), 17
- session replay, 418
- set vlan command, 24
- SGBP (Stack Group Bidding Protocol), 81
- SHA (Secure Hash Algorithm), 251–252
- show accounting command, 231–232
- show commands, 166–168
- show debugging command, 170
- show interface command, 163
- show interfaces command, 171–172
- show ip access-lists command, 170
- show ip arp command, 39
- show ip route command, 48, 50, 169–170
- show logging command, 173
- show process command, 158–159
- show route-map command, 174
- show startup-config command, 185
- show version command, 162–163, 174
- SIA (Stuck in Active), 58
- Signature Engines, 423–424
- signature-based IDS systems, 304
- signatures, 386
- sliding windows, 37
- SMTP (Simple Mail Transfer Protocol), 128–129**
- smurf attacks, 421**
- SNMP (Simple Network Management Protocol), 122**
 - community access strings, configuring on Cisco routers, 122
 - configuring on Cisco routers, 125
 - examples of, 128
 - managed devices, 124
 - MIBs, 123–125
 - notifications, 123–126
- snmp-server enable traps config command, 126**
- snmp-server host command, 126–127**
- social engineering, 414**
- software**
 - Cisco Secure, 301
 - AAA features*, 302
 - features*, 301
 - test topics*, 301
 - PIX, features of, 376–377
- SOML command (SMTP), 129**
- spanning tree, 23–24**
- SPI (Security Parameters Index), 256**
- split horizon, 53**
- spoof attacks, 421**
- spoofing, 203**
 - MAC spoofing attacks, 205–207
- SRTT (Smooth Route Trip Time), 58**
- SSH (Secure Shell), 133–135**
- SSL (Secure Socket Layer), 121**
- standard access lists, 190–195**
- standard IP access lists, 191–192**
- standards bodies, CERT/CC, 413–414**
- startup config, viewing, 185**
- stateful pattern matching, 386**
- stateful security, 362**
- states of Ethernet interfaces, 173**
- static command, 371**
- static NAT, 360**
- store and forward switching, 23**
- STP manipulation attacks, 204**
- stratum, 130–132**
- stubby areas, 65**
- study tips for exam, 625–631**
- subnetting**
 - calculating host per subnet, 30–31
 - CIDR, 32–33
 - VLSM, 31–32

successors (EIGRP), 58
summary links, 63
switching, enabling PortFast, 25
synchronous logging, 178
System Flash, 157–158
system log, displaying, 173

T

TACACS+, 239
 authentication, 240
 authorization, 240–241
 configuring, 241–244
 features, 241
 versus RADIUS, 245–246

TCP, 34
 ARP, 38–39
 DHCP, 40
 FTP, 47–48
 header format, 34
 HSRP, 41
 configuring, 44–45
 enabling, 43
 ICMP, 46–47
 packets, 34–35
 RARP, 39
 services, filtering, 353–355
 Telnet, 36–37, 47
 TFTP, 47–48

TCP half close, 37
TCP intercept, enabling, 429
TCP load distribution, 360
TCP SYN Flood attacks, 419
TCP three-way handshake, 37
TCP/IP
 FTP protocol
 Active mode, 116–118
 Passive mode, 118
 vulnerabilities of, 417–418

TCP/IP model, comparing with OSI reference model, 18
teardrop attacks, 420

Telnet, 47
 connections, establishing, 187
 disabling login password, 113
 requests, 36–37

test characters (ping), 46–47

TFTP, 47–48, 114
 defining download directory, 115

time sources (NTP)
 configuring, 131–132
 stratum, 130–131

TKIP (Temporal Key Integrity Protocol), 272, 275–276

topology table (EIGRP), 58

Totally stubby areas, 65

transform sets (IKE), defining, 266

transparent bridging, 23

transport layer (OSI model), 17

Transport mode (IPSec), 254

trap command (SNMP), 125

traps (SNMP), 124

triggered updates, 53

troubleshooting PIX Firewall log files, 374–375

trunks, 26

tuning IDS systems, 307–308

Tunnel mode (IPSec), 254

tunneling
 IP GRE, 383–385
 VPDNs, 276–277
 configuring, 278–281

turning off debugging, 171

U

UDP bombs, 420
undebug all command, 171
unknown passwords, recovering, 182–187
UOS (Intrusion Prevention System), 311
user authentication, HTTP, 120
User EXEC mode (IOS), 164

V

versions of SNMP, 122

viewing
 configuration register, 162
 DHCP leases, 40
 home pages, 119
 HSRP status, 45
 interfaces, 163
 routing tables, 48–50
 startup config, 185

virtual terminal passwords, setting, 190

- VLAN hopping, 202–203**
- VLANs (virtual LANs), creating, 23**
- VLSM (Variable-Length Subnet Masking), 31–32**
- VMS (CiscoWorks VPN/Security Management Solution), 313–314**
- VPDNs, 276–277**
 - configuring, 278–281
- VPNs, 383**
 - configuring, 385
- VRFY command (SMTP), 129**
- vulnerabilities of TCP/IP, 417–418**

W

- web sites**
 - Cisco Product Security Incident Response Team, 414
 - IETF, 417
 - Internet Domain Survey, 417
 - ISOC, 417
- Weight attribute (BGP), 73**
- wildcard masks, 192**
- Windows Active Directory, 135**
- wireless networks, 84–85**
 - deploying, best practices, 86–88
- write command (SNMP), 125**
- write terminal command, 157**