



## Symbols

---

.rhosts file (UNIX), 290  
| (pipe), 174

## Numerics

---

1000 GE, 28  
100BaseT, 28  
10Base2, 28  
10Base5, 28  
10BaseT, 28  
3DES (Data Encryption Standard), 238  
802.1Q, 33

## A

---

AAA, 208–209  
    accounting, 211–212  
    authentication, 210  
    authorization, 210–211  
ABRs (Area Border Routers), 68  
access lists, 250  
    extended, 187–189  
        options, 188–189  
    filtering TCP services, 322, 324  
    IP packet debugging, 171–172  
    standard, 182–187  
    wildcard masks, 184  
accessing  
    Cisco routers, 179  
accounting, 208, 211–212  
ACKs (acknowledgments), 63  
ACS (Cisco Secure Access Control Server)  
    See Cisco Secure  
Active Directory, 133  
Active FTP, 115, 117  
adaptive cut-through switching, 30  
address classes, 36  
Adjacencies, 67  
administrative distances, 56–57  
agents (SNMP), 123  
Aggregator attribute (BGP), 78  
Aggressive mode (IKE), 246  
AH (Authentication Header), 244–246  
alias command, 167  
allocating IP addresses  
    InterNIC, 325  
ambiguous test questions  
    decoding, 572–573  
application layer (OSI model), 25  
applications  
    NetRanger, 300  
        Director, 302  
        sensors, 300  
        supporting platforms, 301  
        typical network placement, 300  
    TFTP, 113  
applying  
    access lists to interfaces, 185–187  
areas, 67  
arguments  
    UNIX commands, 286  
ARP, 45–46  
AS (Autonomous System), 67  
AS\_Path attribute (BGP), 77  
ASA (Adaptive Security Algorithm), 330  
ASBRs (Autonomous system boundary routers), 68  
asynchronous communications, 84–85  
Atomic Aggregate attribute (BGP), 78  
attacks  
    birthday attacks, 372  
    chargen, 371  
    CPU-intensive, 371  
    DDoS, 371  
    DNS poisoning, 371  
    DoS, 370, 372  
    E-mail, 371  
    incident response teams, 367  
    Land.C, 371  
    man in the middle, 372  
    methods of, 369  
    motivation for, 365  
    ping of death, 371  
    sacrificial hosts, 370  
    smurf, 372  
    spoof attacks, 372  
    TCP SYN flood, 371  
    teardrop, 371

- UDP bombs, 371
- attrib command (DOS), 285
- attributes
  - of RADIUS, 214
- attributes (BGP), 77–78
- authentication, 208, 210
  - HTTP, 119
  - Kerberos, 225
  - method lists, 217
  - on TACACAS+ servers, 219
  - PPP, 82
- authoritative time sources
  - configuring, 130–131
  - stratum, 128–129
- authorization, 209–211
  - on TACACAS+ servers, 219–220

## B

---

- backup domain controllers, 290
- bastion hosts, 370
- BECN (backward explicit congestion notification), 83
- BGP, 76
  - attributes, 77–78
  - characteristics, 77
  - configuring, 79
  - messages, 76
- birthday attacks, 372
- Blocking state (spanning tree), 31
- bootstrap program, 153
- BPDUs (Bridge Protocol Data Units), 31
- BRI, 80
- bridging, 28
  - port states, 31
  - transparent, 30
- broadcast domains, 30
- broadcasting, 292
- browsing, 291

## C

---

- calculating
  - hosts per subnet, 37–38
- CAM tables, 29

- CBAC
  - audit trail messages
    - enabling, 451
- CBAC (Content-Based Access Control), 345
  - configuring, 346–347
- cd command (DOS), 284
- cd command (UNIX), 284
- CERT/CC (Computer Emergency Response Team Coordination Center), 366
- certification
  - exam
    - objectives, 4–7
    - preparing for, 3, 7–8
- characteristics
  - of RIP, 57–58
  - of RIPv1, 58
  - of RIPv2, 59
- chargen attacks, 371
- chkdsk command (DOS), 284
- chmod command (UNIX), 289
- CIDR, 39
- CIDS (Cisco Secure Intrusion Detection System)
  - See also NetRanger
- Cisco IDS, 373
  - sensors, 373
  - Signature Engines, 373–374
  - supported products, 373
- Cisco IOS
  - configuration files
    - saving, 158
  - firewall features, 344–345
  - intrusion prevention methods
    - core dumps, 379–380
    - disabling default services, 378
    - disabling DHCP, 377
    - disabling TCP/UDP small servers, 376
    - enabling sequence numbering, 378
    - enabling TCP intercept, 379
    - Nagle algorithm, 375–376
  - modes of operation, 157
  - password recovery, 174, 176–179
- Cisco Product Security Incident Response Team
  - web site, 367
- Cisco Secure, 297, 299
  - AAA features, 298
  - features, 297
  - test topics, 297

- Cisco Secure Scanner
  - See also NetSonar
- Cisco Security Manager
  - See CSPM
- Cisco Security Wheel, 304
- Cisco TFTP, 113
- classes of IP addresses, 36
- classful addressing, 40
- classful routing protocols, 40
- clock sources
  - NTP configuration, 128–131
- Cluster-List attribute (BGP), 78
- collisions
  - jam signals, 27
- command structure
  - UNIX, 285–287
- commands
  - | (pipe) modifier, 174
  - alias, 167
  - copy running-config startup-config, 158
  - copy tftp flash, 114
  - debug all, 171
  - DOS
    - attrib, 285
    - ip helper-address, 292
    - ipconfig, 295–296
    - route, 296
  - ip host, 110
  - ip http authentication, 119
  - ip route-cache, 168
  - ip subnet-zero, 38
  - logging console debug, 168
  - service password-encryption, 181
  - service tcp-keepalives-in, 376
  - set vlan, 30
  - shortcuts, creating, 167
  - show accounting, 211–212
  - show debugging, 163
  - show interface, 156
  - show interfaces, 163–165
  - show ip access-lists, 163
  - show ip arp, 46
  - show ip route, 55–56, 162–163
  - show logging, 166
  - show process, 153
  - show route-map, 166
  - show startup-config, 178
  - show version, 155–156, 166
  - SMTP, 127–128
  - snmp-server enable traps config, 124
  - snmp-server host, 124–126
  - undebug all, 163
  - UNIX
    - correlated DOS commands, 284–285
- community access strings
  - configuring on Cisco routers, 121
- Community attribute (BGP), 78
- comparing
  - preshared keys and manual keys, 255
  - RADIUS and TACACS+, 224–225
- components of Security Wheel, 304
- configuration files
  - loading, 158
  - saving, 158
- Configuration mode (IOS), 157
- configuration registers, 154–156
  - modifying, 177
- configuring
  - BGP, 79
  - CBAC, 346–347
  - Dynamic NAT, 326
  - HSRP, 50–51
  - IKE, 252–253, 255–256, 258–259
  - Kerberos, 228–229
  - Nagle algorithm, 375
  - NTP
    - time sources, 128–131
  - OSPF
    - in a single area, 66, 69
    - in multiple areas, 69–70
  - PIX, 332–337
  - RADIUS, 215–217
  - RIP, 59, 61
  - SGBP, 85
  - SNMP support on Cisco routers, 124
  - TACACS+, 220–223
  - VPDNs, 231–235
  - VPNs, 350–351
- connectionless protocols, 23
- connection-oriented protocols, 23
  - TCP, 40
    - header format, 41
    - packets, 41–42
    - Telnet requests, 42, 45

- copy command (DOS), 284
- copy running-config startup-config commands, 158
- copy tftp flash command, 114
- copying
  - IOS images from TFTP servers, 114
- core dumps
  - performing, 379–380
- cp command (UNIX), 284
- CPU, 152
- CPU-intensive attacks, 371
- creating
  - command shortcuts, 167
  - extended access lists, 187–189
  - standard access lists, 182–187
  - VLANs, 30
- credentials, 227
- crypto map entries, 253
- cryptography
  - key exchange management, 246
    - IKE, 247–250, 252–253, 255–256, 258–259
  - PKI, 348
- CSACS (Cisco Secure Access Control Server), 218
- CSMA/CD, 27
- CSPM, 299
- CSPM (Cisco Secure Policy Manager), 299
- cut through switching, 30

## D

---

- DATA command (SMTP), 128
- data encryption
  - 3DES, 238
  - DES, 237–238
  - Diffie-Hellman, 240–241
  - DSS, 238–239
  - IPSec, 242
    - AH, 244–246
    - ESP, 243–244
  - MD5, 239–240
  - principles of, 235, 237
- data link layer (OSI model), 22
- data manipulation, 369
- DDOS (Distributed Denial Of Service) attacks, 371
- debug all command, 171
- debug commands, 168–174
  - options, 169–170
- debugging
  - turning off, 163
- default services
  - disabling, 378
- defining
  - HTTP port number, 120
  - IP address names, 110
  - TFTP download directory, 114
- del/erase command (DOS), 284
- deploying
  - NAT, 325
- DES (Data Encryption Standard), 237–238
- development
  - of Ethernet, 27
  - of OSI reference model, 21
- development of UNIX operating system, 284
- devices
  - asynchronous communication, 84–85
  - broadcast domains, 30
  - broadcasting, 292
  - firewalls, 320
  - VLANs
    - creating, 30
- Df command (UNIX), 284
- DHCP, 47
  - disabling, 377
- DHCP (Dynamic Host Configuration Protocol), 292
- Diffie-Hellman protocol, 240–241
- dir command (DOS), 284
- directories, 289
- directories (UNIX), 289–290
- disabled state (spanning tree), 31
- disabling
  - default services, 378
  - DHCP, 377
  - DNS lookup on Cisco routers, 112
  - TCP/UDP small servers, 376
  - Telnet login password, 113
- displaying
  - configured policy routes, 166
  - router home page, 118
  - routing tables, 55–56
  - system log, 166
- distance vector protocols
  - loop avoidance techniques, 59
  - RIP, 57–59

- configuring, 59, 61
- DLCIs (data-link connection identifiers), 83
- DMZ, 320
- DNS, 110–111
  - disabling lookup on Cisco routers, 112
  - enabling lookup on Cisco routers, 112
- DNS poisoning, 371
- domains, 290
  - trust relationships, 294
  - trusted domains, 292
- domains (Windows NT)
  - scalability, 292
- DOS
  - commands
    - attrib, 285
    - correlated UNIX commands, 284–285
    - ipconfig, 295–296
    - route, 296
- DoS attacks, 370, 372
- DR (Designated Router), 68
- DRs
  - election process
    - disabling, 75
- DSS (Data Signature Standard), 238–239
- DSS (digital signatures), 348
- dynamic crypto map entries, 254
- Dynamic NAT
  - configuring, 326
- dynamic NAT, 327

## E

- EBGP (external BGP), 78
- EIGRP, 62–63
  - example configuration, 64, 66
- election process (DRs)
  - disabling, 75
- e-mail
  - SMTP, 127
    - commands, 127–128
- E-mail attacks, 371
- enable passwords
  - setting, 180
- enabling
  - DNS lookup on Cisco routers, 112
  - FastEther Channel, 31

- HSRP, 49
  - Nagle algorithm, 376
  - portfast on Cisco switches, 31
  - sequence numbering, 378
  - TCP intercept, 379
- encapsulation, 26
  - HDLC, 80
  - LCP, 82
  - PPP, 81
- encrypting passwords, 181
- encryption technologies, 235
  - 3DES, 238
  - DES, 237–238
  - Diffie-Hellman, 240–241
  - DSS, 238–239
  - IPSec, 242
    - AH, 244–246
    - ESP, 243–244
  - MD5, 239–240
  - principles of, 235, 237
- ESP (Encapsulation Security Payload), 243–244
- establishing
  - Telnet connections, 179
- Ethernet
  - bridge port states, 31
  - CSMA/CD, 27
  - FEC, 31
  - interfaces, states of, 165
  - media specification, 27–28
  - spanning tree, 30
- exam
  - FAQs, 576
  - objectives, 4–7
  - preparing for, 3, 7–8, 575
  - study tips, 569–570
- example configurations
  - EIGRP, 64, 66
- extended access lists, 187–189
  - options, 188–189
- external links, 68

## F

- FAQs regarding exam, 576
- FAQs regarding lab exam, 578–580
- FAQs regarding qualification exam, 576–577

- FC (feasibility condition), 63
- feasible distance, 63
- features
  - of RADIUS, 215
  - of TACACAS+ servers, 220
- FEC (FastEther Channel), 31
- FECN (forward explicit congestion notification), 83
- fields
  - of IP packets, 34–35
  - of show ip route command output, 56
  - of TCP packets, 41–42
- file systems
  - NTFS, 293
  - UNIX, 289
    - directories, 289–290
- files
  - attributes
    - modifying, 285
- filtering TCP services, 322, 324
- firewalls, 320
  - Cisco IOS features, 344–345
  - CSPM, 299
  - PIX, 328
    - commands, 339–341
    - configuring, 332–337
    - DMZs, 330
    - stateful packet screening, 330–331
    - static routing, 337–338
- flags
  - chmod command, 289
  - UNIX commands, 286
- Flags field
  - TCP packets, 42
- Flash memory, 151
- Forwarding state (spanning tree), 31
- Frame Relay, 83
- frames, 22
  - BPDUs, 31
- framing
  - ISDN, 80
- FTP, 53
  - Active mode, 115, 117
  - Passive mode, 117–118
- functionality
  - of NetBIOS, 291

## G

---

- gateways
  - HSRP, 47
    - configuring, 50–51
    - enabling, 49
- generating
  - keepalive packets, 376
- Global, 293
- Global domain model, 293
- global groups, 294
- gratuitous ARP, 46
- grep command (UNIX), 287

## H

---

- hashing, 238–239
- hashing algorithms
  - MD5, 239–240
  - SHA, 239–240
- HDLC, 80
- Hello packets
  - EIGRP, 63
- Hello packets (OSPF), 67
- HELO command (SMTP), 127
- help command (DOS), 284
- hiding
  - secret passwords, 181
- hijacking, 369
- holdtime, 63
- host IDSs, 372
- hosts per subnet
  - calculating, 37–38
- HSRP, 47
  - configuring, 50–51
  - enabling, 49
- HTTP
  - defining port number, 120
  - security
    - SSL, 121
    - user authentication, 119
- HTTP (Hypertext Transfer Protocol), 118
- hybrid routing protocols
  - EIGRP, 62–63
    - configuration example, 64, 66

- 
- I**
- IBGP (internal BGP), 78
  - ICMP, 52–53
  - IDSs, 372
    - Cisco IDS
      - Signature Engines, 373–374
      - supported products, 373
  - IDSs (intrusion detection systems)
    - NetRanger, 300
      - Director, 302
      - sensors, 300
      - supporting platforms, 301
      - typical network placement, 300
  - IETF (Internet Engineering Task Force) web site, 368
  - ifconfig command (UNIX), 287
  - IKE, 246
    - configuring, 252–253, 255–256, 258–259
    - phase I, 247
    - phase II, 248–250, 252
  - in, 53
  - incident response teams, 367
  - inform requests (SNMP), 122
  - Initial configuration mode (IOS), 157
  - inside global addresses, 324
  - inside local addresses, 324
  - instances, 227
  - Interface configuration mode (IOS), 157
  - interfaces, 156
    - access lists, applying, 185–187
    - Ethernet
      - states, 165
  - Internet Domain Survey web site, 368
  - Internet newsgroups, 368
  - InterNic, 325
  - intruders
    - methods of attack, 369
  - IOS images
    - copying from TFTP servers, 114
  - IP, 33
    - address classes, 36
    - packets, 34–35
    - subnets, 36
  - IP addressing
    - ARP, 45–46
    - CIDR, 39
    - classful addressing, 40
    - DHCP, 47
    - DNS, 110–111
      - enabling lookup on Cisco routers, 112
    - logical AND operation, 37
    - name resolution on Windows NT systems, 292
    - RARP, 46
    - subnets, 36
    - subnetting
      - calculating hosts per subnet, 37–38
      - VLSM, 38–39
  - IP GRE (generic routing encapsulation) tunnels
    - configuring, 349–351
  - ip helper-address command, 292
  - ip host command, 110
  - ip http authentication command, 119
  - IP multicast, 83
  - IP packet debugging, 171–172
  - ip route-cache command, 168
  - ip subnet-zero command, 38
  - ipconfig command, 295–296
  - IPSec, 242
    - AH, 244–246
    - ESP, 243–244
  - is, 223
  - ISDN
    - commands, 82
    - layer 2 protocols, 80
      - authentication, 82
      - HDCL, 80
      - LCP, 82
      - NCP, 82
      - PPP, 81
  - ISDN (Integrated Services Digital Network), 79
    - framing, 80
  - ISL (Inter-Switch Link), 33
  - ISO (Organization for Standardization), 21
  - ISOC (Internet Society) web site, 368
- 
- J**
- jam signals, 27



## K

---

- KDC (Key Distribution Center), 228
- KDC (key distribution center), 225
- keepalive packets
  - generating, 376
- Kerberos, 225
  - configuring, 228–229
- Kerberos realm, 227
- key exchange management
  - IKE, 246
    - configuring, 252–253, 255–256, 258–259
    - phase I, 247
    - phase II, 248–250, 252

## L

---

- L2F, 229
  - VPDNs, 231
- L2TP, 229
  - VPDNs, 231
- lab
  - See self-study lab
- lab exam, 577–578
  - FAQs, 578–580
  - sample, 583–584, 586–597
- Land.C attacks, 371
- lastlog file (UNIX), 290
- Layer 2
  - See also network layer
- layer of OSI reference model
  - network layer
    - spanning tree, 30
    - switching, 28–30
- layers of OSI reference model
  - application layer, 25
  - data link layer, 22
  - network layer, 23
    - IP, 33–37
  - physical layer, 21
  - presentation layer, 24
  - session layer, 24
  - transport layer, 24
- LCP, 82
- LDAP (Lightweight Directory Access Protocol), 133
- Learning state (spanning tree), 31

- leases (DHCP)
  - viewing, 47
- links, 289
- link-state protocols
  - OSPF, 66, 68
    - example configuration, 71, 73, 75
    - media types, 70
    - multiple area configuration, 69–70
    - single area configuration, 66, 69
    - virtual links, 71
- Listening state (spanning tree), 31
- LLC sublayer, 22
- LMhosts file, 292
- loading
  - configuration files, 158
- local groups, 294
- Local Preference attribute (BGP), 77
- logging console debug command, 168
- logical AND operation, 37
- loops
  - spanning tree, 30
    - bridge port states, 31
    - split horizon, 58
- lost passwords
  - recovering, 174, 176–179
- ls command (UNIX), 284
- LSAs (link-state advertisements), 68

## M

---

- MAC sublayer, 22
- MAIL command (SMTP), 128
- man command (UNIX), 284, 287
- man in the middle attacks, 372
- managed devices, 123
- manual keys
  - versus preshared keys, 255
- masquerading, 369
- master domain model, 293
- MD5 (Message Digest 5), 239–240
- MED attribute (BGP), 77
- media specifications of Ethernet, 27–28
- memory
  - NVRAM, 151
  - RAM, 151
  - ROM, 153

- System Flash, 151
- messages
  - BGP, 76
- method lists, 217
- methods of attacks, 369
- metrics
  - administrative distance, 56–57
- MIBs, 122, 124
- modes of IOS operation, 157
- modifying
  - configuration registers, 177
  - UNIX permissions, 289
- monitoring NAT, 327
- motivation for attacks, 365
- multicasting, 83
- multiple master domain model, 293
- mv command (UNIX), 284, 287

## N

---

- Nagle algorithm
  - preventing Cisco IOS from attacks, 375–376
- Nagle, John, 375
- name resolution
  - DNS, 110–111
    - enabling lookup on Cisco routers, 112
  - on Windows NT, 292
- NAT, 324
  - deploying, 325
  - Dynamic NAT
    - configuring, 326
  - monitoring, 327
  - operation on Cisco routers, 326
- NCP, 82
- NetBEUI, 290
- NetBIOS (Network Basic Input/Output System), 290
- NetBT, 291
- NetRanger, 300
  - Director, 302
  - sensors, 300
  - supporting platforms, 301
  - typical network placement, 300
- NetSonar, 302, 304
  - See also Cisco Secure Scanner
- netstat command (UNIX), 287
- network IDS, 372
- network layer
  - bridging
    - BPDU, 31
    - port states
      - BPDU, 31
  - ICMP, 52–53
  - IP, 33
    - address classes, 36
    - logical AND operation, 37
    - packets, 34–35
    - subnets, 36
  - spanning tree protocol, 30
  - subnetting
    - VLSM, 38–39
  - switching, 28–29
    - CAM tables, 29
    - cut through, 30
    - store and forward, 30
- network layer (OSI model), 23
- network management
  - SNMP, 121
    - community access strings, configuring on
      - Cisco routers, 121
    - configuring on Cisco routers, 124
    - examples of, 126
    - managed devices, 123
    - MIBs, 122, 124
    - notifications, 122, 124
- Network Neighborhood, 291
- newsgroups
  - reporting security breaches, 368
- Next Hop attribute (BGP), 77
- NMSs (network management systems), 123
- NOOP command (SMTP), 128
- normal files, 289
- notifications (SNMP), 122, 124
- NSSAs (Not-so-stubby areas), 70
- NTFS (New Technology File System), 293
- NTP
  - configuring clock sources, 128–131
- NVRAM (nonvolatile RAM), 151
- NWLink, 291

**O**

- operating systems
  - UNIX
    - command structure, 285–287
    - commands, 284–285
    - development of, 284
    - file systems, 289–290
    - permissions, 288–289
  - Windows NT, 290
    - browsing, 291
    - domains, 290
    - global groups, 294
    - local groups, 294
    - name resolution, 292
    - permissions, 293–294
    - SAM, 293
    - scalability, 292
    - trust relationships, 294
    - workgroups, 290
- Origin attribute (BGP), 77
- Originator ID attribute (BGP), 78
- OSI reference model
  - application layer, 25
  - data link layer, 22
  - development of, 21
  - network layer, 23
    - IP, 33–37
    - spanning tree, 30
    - switching, 28–30
  - peer-to-peer communication, 26
  - physical layer, 21
  - presentation layer, 24
  - session layer, 24
  - transport layer, 24
  - versus TCP/IP model, 25
- OSPF, 66, 68
  - example configuration, 71, 73, 75
  - media types, 70
  - multiple area configuration, 69–70
  - single area configuration, 66, 69
  - virtual links, 71
- outside global addresses, 324
- outside local addresses, 324

**P**

- packet filtering, 321
  - CBAC, 345
    - configuring, 346–347
  - extended access lists, 187–189
    - options, 188–189
  - standard access lists, 182–187
- packets
  - AH, 245–246
  - Hello
    - EIGRP, 63
  - IP, 34–35
    - debugging, 171–172
  - rerouting, 369
  - TCP, 41–42
- partitioning System Flash, 151
- Passive FTP, 117–118
- passwd file (UNIX), 290
- password recovery, 174, 176–179
- passwords
  - authentication, 210
    - method lists, 217
  - enable passwords, setting, 180
  - encrypting, 181
  - virtual terminal passwords, setting, 182
- PAT, 324
- path vector protocols
  - BGP, 76
    - attributes, 77–78
    - configuring, 79
    - messages, 76
- PDM (PIX Device Manager), 299
- peer-to-peer communication, 26
- performing
  - core dumps, 379–380
- perimeter routers, 321
- permissions
  - UNIX, 288–289
  - Windows NT, 293–294
- PFS (perfect forward secrecy), 249
- physical layer (OSI model), 21
- ping command (DOS), 285
- ping command (UNIX), 285
- ping of death attack, 371
- ping requests
  - test characters, 52–53

PIX  
 stateful packet screening, 330

PIX (Private Internet Exchange), 328  
 commands, 339–341  
 configuring, 332–337  
 DMZs, 330  
 software features, 342–344  
 stateful packet screening, 330–331  
 static routing, 337–338

PKI (Public Key Infrastructure), 348

Poison Reverse updates, 59

policy routes  
 displaying, 166

portfast  
 enabling, 31

PPP, 81

preparing for exam, 3, 7–8, 575  
 FAQs, 576  
 objectives, 4–7

preparing for lab exam  
 sample lab, 583–584, 586–597

preparing for qualification exam, 573–574

presentation layer (OSI model), 24

pre-shared keys  
 versus manual keys, 453

presared keys  
 versus manual keys, 255

preventing Cisco IOS from attacks  
 disabling default services, 378  
 disabling DHCP, 377  
 disabling TCP/UDP small servers, 376  
 enabling sequence numbering, 378  
 enabling TCP intercept, 379  
 Nagle algorithm, 375–376  
 performing core dumps, 379–380

PRI, 80

primary domain controllers, 290

principal (Kerberos), 228

privilege levels  
 authorization, 210–211

Privileged EXEC mode (IOS), 158

proxy servers, 321

## Q

qualification exam

FAQs, 576–577

qualification exam  
 preparing for, 573–574  
 See also lab exam  
 study tips, 570–571  
 decoding ambiguity, 572–573

QUIT command (SMTP), 128

## R

RADIUS, 212  
 attributes, 214  
 configuring, 215–217  
 features, 215  
 security protocol support, 214  
 versus TACACAS+, 224–225

RAM, 151

RARP, 46

RCPT command (SMTP), 128

read command (SNMP), 123

recovering lost or unknown passwords, 174, 176–179

redundancy  
 HSRP, 47  
 configuring, 50–51  
 enabling, 49

remote access  
 VPDNs, 229, 231  
 configuring, 231–235

remote router access, 179

rename command (DOS), 284

reporting security breaches  
 Internet newsgroups, 368

rerouting packets, 369

resolving  
 IP addresses to MAC addresses  
 ARP, 45–46

rm command (UNIX), 284

rmdir command (UNIX), 287

ROM (read-only memory), 153

ROM boot mode (IOS), 157

root bridge elections, 30

root bridges, 31

route command, 296

router hardware  
 configuration registers, 154–156

- CPU, 152
- interfaces, 156
- NVRAM, 151
- RAM, 151
- ROM, 153
- System Flash, 151
- routers
  - remote access, 179
- routing protocols, 53, 55
  - BGP, 76
    - attributes, 77–78
    - configuring, 79
    - messages, 76
  - default administrative distances, 56–57
  - EIGRP, 62–63
    - example configuration, 64, 66
  - OSPF, 66, 68
    - example configuration, 71, 73, 75
    - multiple area configuration, 69–70
    - single area configuration, 66, 69
    - virtual links, 71
  - RIP, 57–59
    - configuring, 59, 61
- routing tables
  - viewing, 55–56
- RSET command (SMTP), 128
- RTO (Retransmission Timeout), 63

## S

---

- SA (Security Association), 242
- sacrificial hosts, 370
- SAM (Security Accounts Manager), 293
- SAML command (SMTP), 128
- sample lab exam, 583–584, 586–597
- saving
  - configuration files, 158
- scalability
  - Windows NT, 292
- secret passwords
  - hiding, 181
- security, 321
  - AAA, 208–209
    - accounting, 211–212
    - authentication, 210
    - authorization, 210–211
  - CBAC
    - configuring, 346–347
  - encryption technologies, 235
    - 3DES, 238
    - DES, 237–238
    - Diffie-Hellman, 240–241
    - DSS, 238–239
    - IPSec, 242–246
    - MD5, 239–240
    - principles of, 235, 237
  - firewalls, 320
    - Cisco IOS features, 344–345
  - HTTP, 118
    - authentication, 119
  - IKE, 246
    - configuring, 252–253, 255–256, 258–259
    - phase I, 247
    - phase II, 248–250, 252
  - Kerberos, 225
    - configuring, 228–229
  - NAT, 324
    - configuring Dynamic NAT, 326
    - deploying, 325
    - monitoring, 327
    - operation on Cisco routers, 326
  - packet filtering
    - TCP services, 322, 324
  - PAT, 324
  - PIX, 328
    - commands, 339–341
    - configuring, 332–337
    - DMZs, 330
    - software features, 342–344
    - stateful packet screening, 330–331
    - static routing, 337–338
  - PKI, 348
  - RADIUS, 212
    - attributes, 214
    - configuring, 215–217
    - features, 215
    - security protocol support, 214
  - SSH, 132–133
  - SSL, 121
  - TACACS+, 218
    - authentication, 219
    - authorization, 219–220
    - configuring, 220–223

- features, 220
  - versus RADIUS, 224–225
- VPDNs, 229, 231
  - configuring, 231–235
- VPNs, 349
  - configuring, 350–351
- security server protocols, 212
- Security Wheel, 304
- self-study lab
  - ACS configuration, 461–464, 466, 468, 470
  - advanced PIX configuration, 458–460
  - BGP routing configuration, 438, 440–442
  - Catalyst Ethernet switch setup, 403, 405–409, 411–413
  - DHCP configuration, 438
  - dynamic ACL/lock and key feature configuration, 448–449
  - final configurations, 470–471, 473–475, 477–480, 482–485
  - Frame Relay setup, 397–399, 401–402
  - IGP routing, 419–423
    - OSPF configuration, 423, 425–429, 431–432
  - IOS firewall configuration, 450–451
  - IP access list configuration, 442–444
  - IPSec configuration, 452–454, 456–457
  - ISDN configuration, 432–437
  - local IP host address configuration, 414
  - physical connectivity, 403
  - PIX configuration, 414, 416–418
  - setup, 393–395
    - communications server, 396–397
    - TCP intercept configuration, 444, 446
    - time-based access list configuration, 446, 448
- SEND, 128
- SEND command (SMTP), 128
- Sendmail, 127
- sensors
  - Cisco IDSs, 373
- sequence numbering
  - enabling, 378
- servers
  - RADIUS, 212
- service password-encryption command, 181
- service tcp keepalive command
  - enabling Nagle algorithm, 376
- service tcp-keepalives-in command, 376
- session hijacking, 369
- session layer (OSI model), 24
- session replay, 369
- set vlan command, 30
- SGBP, 86
  - configuring, 85
- SGBP (Stack Group Bidding Protocol), 85
- SHA (Secure Hash Algorithm), 239–240
- shadow file (UNIX), 290
- show accounting command, 211–212
- show commands, 160–161
- show debugging command, 163
- show interface command, 156
- show interfaces command, 163–165
- show ip access-lists command, 163
- show ip arp command, 46
- show ip route command, 55–56, 162–163
- show logging command, 166
- show process command, 153
- show route-map command, 166
- show startup-config command, 178
- show version command, 155–156, 166
- SIA (Stuck in Active), 63
- Signature Engines, 373–374
- single domain model, 293
- single logon, 226
- sliding windows, 44
- SMTP
  - commands, 127–128
- SMTP (Simple Mail Transfer Protocol), 127
- smurf attacks, 372
- SNMP, 121
  - community access strings
    - configuring on Cisco routers, 121
  - configuring on Cisco routers, 124
  - examples of, 126
  - managed devices, 123
  - MIBs, 122, 124
  - notifications, 122, 124
- snmp-server community command (SNMP), 124
- snmp-server enable traps config command, 124
- snmp-server host command, 124–126
- social engineering, 367
- software
  - Cisco Secure, 297, 299
  - AAA features, 298
  - features, 297

- test topics, 297
  - NetSonar, 302, 304
- software features of PIX, 342–344
- SOML command (SMTP), 128
- spanning tree, 30
  - bridge port states, 31
- special files, 289
- SPI (Security Parameters Index), 243
- split horizon, 58
- spoof attacks, 372
- SRTT (Smooth Route Trip Time), 63
- SSH (Secure Shell), 132–133
- SSL (Secure Socket Layer), 121
- standard access lists, 182–187
- standard IP access lists, 183
  - wildcard masks, 184
- standards bodies
  - CERT/CC, 366
- startup config
  - viewing, 178
- stateful packet screening
  - PIX, 330–331
- stateful security, 330
- states of Ethernet interfaces, 165
- static NAT, 327
- static routing
  - PIX configuration, 337–338
- store and forward switching, 30
- stratum, 128–129
  - configuring NTP time sources, 130–131
- Stubby areas, 70
- study tips for exam, 569–570, 575
- study tips for qualification exam, 570–571
  - decoding ambiguity, 572–573
- subnets, 36
- subnetting, 36
  - calculating host per subnet, 37–38
  - CIDR, 39–40
  - VLSM, 38–39
- successors (EIGRP), 63
- Summary, 574
- summary links, 68
- switching, 28–29
  - CAM tables, 29
  - cut through, 30
  - portfast
    - enabling, 31

- store and forward, 30
- trunks, 31
- System Flash, 151
- system log
  - displaying, 166

## T

---

- TACACS+, 218
  - authentication, 219
  - authorization, 219–220
  - configuring, 220–223
  - features, 220
  - versus RADIUS, 224–225
- TCP, 40
  - ARP, 45–46
  - DHCP, 47
  - FTP, 53
  - header format, 41
  - HSRP, 47
    - configuring, 50–51
    - enabling, 49
  - ICMP, 52–53
  - packets, 41–42
  - RARP, 46
  - services
    - filtering, 322, 324
  - Telnet, 53
  - Telnet requests, 42, 45
  - TFTP, 53
- TCP half close, 44
- TCP intercept
  - enabling, 379
- TCP load distribution, 328
- TCP SYN Flood attacks, 371
- TCP three-way handshake, 44
- TCP/IP
  - FTP protocol
    - Active mode, 115, 117
    - Passive mode, 117–118
  - vulnerabilities, 369–370
- TCP/IP model
  - versus OSI reference model, 25
- teardrop attacks, 371
- Telnet, 53
  - disabling login password, 113

Telnet connections  
 establishing, 179

Telnet requests, 42, 45

test characters (ping), 52–53

TFTP, 53, 113  
 defining download directory, 114

TGT (Ticket Granting Ticket), 228

time sources  
 stratum, 128–129

time sources (NTP)  
 configuring, 130–131

timestamps, 226

topology table (EIGRP), 63

Totally stubby areas, 70

traceroute command (UNIX), 285

tracert command (DOS), 285

transform sets (IKE)  
 defining, 253

transparent bridging, 30

transport layer (OSI model), 24

Transport mode (IPSec), 242

trap command (SNMP), 123

traps (SNMP), 122

triggered updates, 59

trunks, 31

trusted domains, 292

trusting domains, 294

Tunnel mode (IPSec), 242

tunneling  
 IP GRE, 349–351  
 VPDNs, 229, 231  
 configuring, 231–235

turning off debugging, 163

## U

---

UDP bombs, 371

undebg all command, 163

UNIX  
 command structure, 285–287  
 commands  
 correlated DOS commands, 284–285  
 development of, 284  
 file systems, 289  
 directories, 289–290  
 permissions, 288–289

unknown passwords  
 recovering, 174, 176–179

URLs  
 Cisco security products, 304

user accounts  
 UNIX  
 permissions, 288–289  
 Windows NT  
 permissions, 293–294

user authentication  
 HTTP, 119

User EXEC mode (IOS), 158

## V

---

versions  
 of SNMP, 121

viewing  
 configuration register, 155  
 DHCP leases, 47  
 home pages, 118  
 interfaces, 156  
 routing tables, 55–56  
 startup config, 178

virtual links, 71

virtual terminal passwords  
 setting, 182

VLANs (virtual LANs)  
 creating, 30

VLSM, 38–39

VPDNs, 229, 231  
 configuring, 231–235

VPNs, 349  
 configuring, 350–351

VRFY command (SMTP), 128

vulnerabilities  
 of TCP/IP, 369–370

vulnerable network systems  
 investigating with NetSonar, 302, 304

## W

---

web sites  
 Cisco Product Security Incident Response  
 Team, 367



- IETF, 368
- Internet Domain Survey, 368
- ISOC, 368
- Weight attribute (BGP), 78
- wildcard masks, 184
- Windows, 291
- Windows Active Directory, 133
- Windows NT, 290
  - browsing, 291
  - domains, 290
    - trust relationships, 294
  - global groups, 294
  - local groups, 294
  - name resolution, 292
  - permissions, 293–294
  - SAM, 293
  - scalability, 292
  - workgroups, 290
- WINS (Windows Internet Naming Services), 292
- workgroups, 290
- write command (SNMP), 123
- wtmp file (UNIX), 290

## **X**

---

- xcopy command (DOS), 284