Note to the reader: Throughout this index boldfaced page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

**Symbols and Numbers**

* (asterisk)
  * in show session results, 273
  * in show user results, 274
?
  * (question mark), for help, 173
| (pipe), 197–198
0x, 36, 235
2.4GHz/5GHz (802.11n), 416–417
2.4GHz bands (802.11b), 409, 412–413
2.4GHz bands (802.11g), 413–414, 414
5GHz (802.11a), 414–415
10Base-2, 39, 41
10Base-5, 39
10Base-FX, 42
10Base-T, 40, 41, 42
10GBase-ER, 42
10GBase-EW, 43
10GBase-Extended Range (ER), 41
10GBase-Extra Long Wavelength (EW), 41
10GBase-Long Range (LR), 41
10GBase-Long Wavelength (LW), 41
10GBase-LR, 42
10GBase-LW, 43
10GBase-Short Range (SR), 41
10GBase-Short Wavelength (SW), 41
10GBase-SR, 42
10GBase-SW, 43
10GBase-T, 40, 42
40MHz channels, for 802.11n, 416–417
100Base-FX (IEEE 802.3u), 40, 42
100Base-TX (IEEE 802.3u), 40, 42
900MHz bands, 409
1000Base-CX (IEEE 802.3z), 40, 42
1000Base-LX (IEEE 802.3z), 40, 42
1000Base-SX (IEEE 802.3z), 40, 42
1000Base-T (IEEE 802.3ab), 40, 42

**A**

access lists, 7, 430
access points, 417
Acknowledgment Number field, in TCP header, 77
acknowledgments, 21
active console, listing all, 273
active hub, 27
active processes, list of, 284
AD. See administrative distance (AD)
ad hoc service set (IBSS), 417
address learning, by layer 2 switches, 387, 388–389, 389
Address Resolution Protocol (ARP), 51, 92, 92–93
  broadcast message from, 103
cache, 304, 308–309
  viewing, 306
administrative distance (AD), 329, 342–343
default, 342
  for directly connected routes, 340
advertising
  default route using RIP, 365–367
RIP network, limiting, 354
agencies, governing use of wireless technology, 409
agents, 71
AirSnort, 421
anonymous username, for FTP, 69
antennas, 416
anti-x, 435
Application layer (OSI), 15
coloration profiles, 432
application-specific integrated circuit
(ASIC), 25
arp -a command, 142
ARP (Address Resolution Protocol), 51, 92, 92–93
broadcast message from, 103
cache, 304, 308–309
viewing, 306
ARP request, 312
ARPAnet, 79
asterisk (*)
in show session results, 273
in show user results, 274
asynchronous transfer mode (ATM), 454
attenuation, 39
authentication, 420, 421, 442
in PPP, 461
configuration, 462–463
TACACS server for, 183
authentication login, in FTP, 69
Authentication phase, in PPP session, 461
autodetect mechanism, 32
Automatic Private IP Addressing (APIPA), 74
autonomous system (AS), 341
autorooters, 433
aux parameter, for line command, 183
auxiliary password, 184
auxiliary port, for Cisco router connection, 164

back doors, 433
back up
Cisco Internetwork Operating System
(IOS), 245–246
Cisco router configuration, 252–254
backbone, collapsed, 382
backoff, 31
bandwidth, 456
layer 2 switching and, 386
bandwidth command, 200–201
banners, 180–182
baseline, for SNMP, 71
basic service set (BSS), 418, 418
beaconing, 420
binary numbering, 33–34
IP address format, 96
memorization chart for converting to decimal, 34
binding, 12
bits, 27, 33, 95
in configuration register, 234–236
block acknowledgment, 417
boot field, 236
boot process, for router, 166
boot sequence
in Cisco routers, 233–234
interrupting, 239–240
boot system commands, 242–243
bootloader, 233
bootstrap, 234
in Cisco router, 232
Bootstrap Protocol (BootP), 73
Border Gateway Protocol (BGP), 341
bottlenecks, 18
routers and switches as, 10
Bridge-Group Virtual Interface (BVI), 326
bridges, 8, 8–9, 384
for connecting to mainframe, 382–385
in Data Link layer, 25–27
vs. LAN switching, 387
in OSI model, 14
bridging, 7
broadcast address, 95, 102–103, 144
for Class C subnet, 121, 124, 128
for MAC address, 4
switch response to, 26–27
broadcast domains, 9, 10, 29
   routers for breaking up, 6, 23
   size, and performance, 386
broadcasting routing updates, 345
brute-force attack, 434
BSS (basic service set), 418, 418
buffer, 18
Buffer Full/Source Quench event, 89
BVI (Bridge-Group Virtual Interface), 326
byte, 33, 95
byte-oriented protocols, 458

channel service unit/data service unit
   (CSU/DSU), 27, 451, 456
channels, non-overlapping, 414
CHAP (Challenge Handshake
   Authentication Protocol), 461
character
   in command-line interface, deleting, 176
delimiting, for banner, 181–182
Checksum field
   in TCP header, 77
   in UDP segment, 80
circuit-switched WAN connection type,
   452, 452
Cisco 1841 router, 165, 165, 314
Cisco 2500 router, 193
   changing configuration register on,
   240–241
Cisco 2600 series modular router,
   164, 164
   bringing up, 167–169
Cisco 2800/2900 series modular router,
   164, 165
Cisco 2811 router, 314
Cisco 2950 switch, and connection, 392
Cisco 2960 switch, 392
Cisco 3550 switch, and connection, 392
Cisco 3560 switch, 392
Cisco Adaptive Security Appliance (ASA),
   435, 441
Cisco Catalyst switches, 392–398, 393
   Core switch configuration, 396–398
   S1 configuration, 394–395
   S2 configuration, 395–396
   verifying port security, 439
Cisco Discovery Protocol (CDP),
   258–270
documenting network topology using,
   267, 267–269, 269
status information, 264–266
value of, 266–267
Cisco Hot Standby Router Protocol (HSRP), 95

Cisco Internetwork Operating System (IOS), 162
back up and restoring, 243–252
   back up, 245–246
   restoring or upgrading, 246–247
seeing size, 250
upgrading IOS, 249–252
user interface, 163–169

Cisco IOS file system (Cisco IFS), 247–252
for managing router configuration, 256–257

Cisco ISR routers, 164, 165
   automatic configuration of clock rate, 322
   command to change bit value, 240
default username and password, 163
erase start command and, 319
interface configuration, 194

Cisco routers, 5
   boot sequence, 233–234
   boot system commands, 242–243
   bringing up, 165–169
configuration, 252–257
   back up, 252–254
   Cisco IFS for managing, 256–257
deleting, 202–203
   erasing, 255
   restoring, 254
   verifying current, 252
connecting to, 163–165
editing and help features, 173–178
   internal components, 232–233
   power-on self-test (POST), 165
   PPP configuration on, 462
proprietary 60-pin serial connector, 456
reloading to run new IOS, 251
   as TFTP server for another router, 247
   web resources, 165
Cisco Unified Wireless Solution, 408
Cisco way of troubleshooting IP addressing, 140
Class A network, 97
   addresses, 99–100
   subetting addresses, 137–140
   practice examples, 137–139
   in your head, 139–140
   valid host IDs, 100
Class B network, 97, 98
   addresses, 100
   subnetting addresses, 130–136
   practice examples, 131–135
   in your head, 136
Class C network, 97, 98
   addresses, 100–101
   subnetting addresses, 120–130
   fast way, 121
   practice examples, 122–127
   in your head, 128
Class D network, 98
Class E network, 98
classful routing, 116, 349
   Cisco routers as, 339
   in RIP version 1, 347
   RIPv2 and, 356
Classless Inter-Domain Routing (CIDR), 118–120
classless routing, 116, 127, 347
   RIPv2 as, 356
clear counters command, 209–210
clear-text passwords, 436
client, 71
   access point support for multiple, 412
   verifying with ipconfig command, 326
client MAC addresses, 421
clock rate command, 199–200
clock rate, setting, 322
clocking, 198–199, 199
closing Telnet sessions, 274
CO (central office), 451
Code Bits/Flags field, in TCP header, 77
code formatting, in Presentation layer, 15
collapsed backbone, 382
collision domains, 7, 10, 28–29, 382
  breaking up, 5
  bridge to increase number of, 8
  switch to break up, 9
collision, on Ethernet LAN, 30
command-line interface (CLI), 162, 169–179
  cursor movement in, 175–176
  entering, 169
  prompts, 170–178
  interfaces, 171
  line commands, 172
  subinterfaces, 172
  for troubleshooting, 140
command.com, viruses attached to, 434
commands
  listing available, 173
  listing parameters for, 174
  negating, 178
communications port, for router or switch, 45
company network, before Internet, 384
confidentiality, encryption and, 442
config net command, 257
config-register command, 237, 240
configuration
  administrative, 182–190
  banners, 180–182
  hostnames, 180
  setting passwords, 182–190
  of Cisco routers, 252–257
  back up, 252–254
  copying to TFTP server, 254
  restoring, 254
  verifying current, 252
  deleting, 202–203
  verifying, 203–213
    in NVRAM, 253
  viewing and changing, 241
configuration mode, viewing configuration and statistics from within, 192
configuration register, 234–243
  bits, 234–236
  changing, 237–238, 240–241
  checking current value, 236
configure terminal command, 170
confreg command, 240
congestion, 18
connection-oriented communication, 16, 17–19, 18, 76
  characteristics of service, 19
  in Transport layer, 50
connectionless communication, 16
connectionless protocol, 79
connections
  to Cisco routers, 163–165
  wide area network (WAN) types, 452–453
console connection, HyperTerminal for, 45–46
console EXEC session, timeout for, 185
console parameter, for line command, 183, 184
console password, 184–185
console port, 163, 164
  for Catalyst switch, 392
copy command, 248, 250
  options, 253–254
copy flash tftp command, 244, 245–246
copy running-config startup-config command, 201–202
copy running-config tftp command, 252, 254
copy startup-config running-config command, 254

copy startup-config tftp command, 252

copy tftp flash command, 246
copy tftp running-config command, 254–255
copying
running-config file to NVRAM, 201
startup-config to running-config file, 241
Corp router configuration
interfaces, 316–318
static routes, 330–331
Counter Mode Cipher Block Chaining-
Message Authentication Code
(CBC-MAC) Protocol (CCMP), 422
counters on interfaces, clearing,
209–210
counting to infinity issue, 346
CPE (customer premises equipment), 451
CPU (central processing unit), utilization
output, 284
CRC (Cyclic Redundancy Check), 38, 51,
305, 306
crossover cable, 44, 44
between switches, 393
crosstalk, 39
CSMA/CA (Carrier Sense Multiple
Access with Collision Avoidance),
412–413, 413
CSMA/CD (Carrier Sense Multiple
Access with Collision Detection),
29–31, 30
CSU/DSU (channel service unit/data
service unit), 27, 451, 456
cursor movement, in command-line
interface, 175–176
customer premises equipment (CPE), 451
cyclic redundancy check (CRC), 38, 51,
305, 306
data communication equipment (DCE),
27, 456–457, 457
serial interface for, 322
data encapsulation, 47–51, 48, 457–458
PPP, 462
verifying, 463–464
Data field, in UDP segment, 80
data frame, 24
data integrity, 17, 442
data link connections, 459
Data Link layer (OSI), 24, 24–27, 304,
306, 307
802.11b and, 412
Ethernet networking at, 32–38
Ethernet addressing, 32–36
Ethernet frames, 36–38
frames in, 48, 51
data links, leasing, 450
data packets, 22
data terminal equipment (DTE), 27, 456–
457, 457
Cisco routers’ serial interfaces as, 198–
199, 199
data transfer, outer layers to define, 14
data translation, in Presentation layer, 15
datagrams, 48
DCE (data communication equipment), 27,
456–457, 457
serial interface for, 322
de-encapsulation, 48
debug all command, 282
debug command, 282–284
debug ip rip command, 283–284, 360–363
troubleshooting with, 361–363
decimal numbering, memorization chart
for converting binary to, 34
dedicated WAN connection type, 452
default administrative distance (AD), 342
default answer — dotted-decimal format for IP address

default answer, for configuration question, 202
default gateway, 141, 144, 304, 307 on switches, 398
default routing, 335, 338–341 misconfiguring, 340
RIP for advertising, 365–367
default subnet mask, 118
default variables for ping, changing, 204
delete command, 249, 250
deleting character in command-line interface, 176
configuration, 202–203
startup-config file, 255
delimiting character, for banner, 181–182
demarcation point, 451, 456
demilitarized network (DMZ), 431
Denial-of-Service (DoS) attacks, 433
Department of Defense (DoD), 66. See also DoD model
description command, 190, 191
Destination Address (DA) field, in Ethernet frames, 37
destination hardware address, 50
destination IP address, 304, 309
Destination IP Address field, in IP header, 88
destination MAC address, of frames, 309
Destination Port field
in TCP header, 77
in UDP segment, 80
destination port number, 50
destination unreachable message, 89, 308
DHCP (Dynamic Host Configuration Protocol), 73–74
address conflicts, 75
configuration on router, 326–327
connection, 74
verifying pool, 326
dial-up modems, 452
digital subscriber line access multiplexer (DSLAM), 454
digital subscriber line (DSL), 454
dir command, 248, 249
direct connection for network, C indicator for, 318
Direct Sequence Spread Spectrum (DSSS), 413
directories, changing, 249
disable command, 169
disabling debugging, on router, 283 interfaces, 195
disconnect command, 274
discontiguous networks
RIPv1 and, 352
RIPv2 as, 356–357, 357
Discover message (DHCP), 73
distance-vector routing internetwork with, 344
protocols, 343–347. See also Routing Information Protocol (RIP)
Distributed Denial-of-Service (DDoS) attacks, 433
DMZ (demilitarized network), 431
do command, 192
do show run command, 194–195
documentation, of network topology using CDP, 267, 267–269, 269
DoD model, 66–95
Host-to-Host layer protocols, 75–85
Internet layer protocols, 85–95 vs. OSI model, 67
Process/Application layer protocols, 68–75
domain name, for SSH, 186
Domain Name Service (DNS), 3, 72
ping to test server, 278
DoS (Denial-of-Service) attacks, 433
dotted-decimal format for IP address, 96
DSL (digital subscriber line), 454
DSLAM (digital subscriber line access multiplexer), 454
DSSS (Direct Sequence Spread Spectrum), 413
DTE (data terminal equipment), 27, 456–457, 457
Cisco routers’ serial interfaces as, 198–199, 199
Dynamic Host Configuration Protocol (DHCP), 73–74
address conflicts, 75
configuration on router, 326–327
connection, 74
verifying pool, 326
dynamic NAT, 149
dynamic routing, 301, 341

enable secret password, 182
Encapsulating Security Payload (ESP), 442
capsulation, 47–51, 48, 457–458
PPP, 462
verifying, 463–464
capsulation ? command, 453
encryption
confidentiality and, 442
of passwords, 187–190, 462
encryption keys, for SSH, 187
Enhanced Interior Gateway Routing Protocol (EIGRP), 22, 343
default administrative distance (AD), 342
erase command, 249
erase start command, ISR routers and, 319
erase startup-config command, 202, 255, 316
erasing
Cisco router configuration, 255
line in command-line interface, 176
error messages
destination unreachable, 89, 308
Invalid input detected, 175
request timed out, 308
Serial0/0 is up, line protocol is down, 464
ESP (Encapsulating Security Payload), 442
ESS (extended service set), 417, 419, 419
Ether-Type field, 305
Ethernet II frame format, 37
Ethernet networking, 28–43
broadcast domains, 29
cable types, 41–47
crossover, 44, 44
rolled, 44–47, 45
straight-through, 43, 43–44
collision domains, 28–29
CSMA/CD, 29–31, 30
at Data Link layer, 32–38
Ethernet addressing, 32–36
Ethernet frames, 36–38
half-duplex and full-duplex, 31–32
at Physical layer, 38–43
ETSI (European Telecommunications Standards Institute), 409
European Telecommunications Standards Institute (ETSI), 409
exclusions, for DHCP server, 326
exec banner, 182
eexec process creation banner, 181
EXEC session, 163
eexec-timeout command, 185
exit command, 272, 274
exit interface, 22, 49, 334–335
expiration of passwords, 436
exponent, 117
extended ping, 204
extended service set (ESS), 417, 419, 419
exterior gateway protocols (EGPs), 341
external EIGRP, default administrative distance (AD), 342
extranet VPNs, 441

F

Fast Ethernet, 384
FCS (Frame Check Sequence) field, 305 in Ethernet frames, 38
FDDI (Fiber Distributed Data Interface), 33
Federal Communications Commission (FCC), 409
file prompt command, 248
file systems, Cisco IFS, 247–252
File Transfer Protocol (FTP), 69, 205 as attack risk, 432
real world scenario, 70
filter table, 26
firewall, 431
Flags field, in IP header, 87
flash cards, for ISR routers, 252
flash memory, 165
in Cisco router, 233
loading Cisco IOS from, 234
verifying amount, 244–245
flow control
transmitting segments with, 19
Transport layer for, 17
format command, 249
forward/filter decisions, 389–391
forward/filter table, 387, 388
populating, 389, 390
FQDN (fully qualified domain name), 72, 277
Fragment Offset field, in IP header, 87
Frame Check Sequence (FCS) field, 305 in Ethernet frames, 38
frame filtering, 390
Frame Relay, 453–454
frames, 48, 51, 305, 305, 307
at Data Link layer, 36
destination MAC address of, 309
frequency bands, unlicensed, for public use, 409–410, 410
FTP (File Transfer Protocol), 69, 205 as attack risk, 432
real world scenario, 70
full-duplex mode for communication, 16, 31–32
fully qualified domain name (FQDN), 72, 277

G

G/L bit (global/local bit), 33
gateway of the last resort, 338, 339
configuration, 339
GETBULK, 71
Gigabit Ethernet, 40
Gigabit Media Independent Interface (GMII), 40
global command, 172
global configuration mode, 170, 173
global/local bit (G/L bit), 33
global NAT addresses, 150
GMII (Gigabit Media Independent Interface), 40
graphical user interface (GUI), X Window for, 71
gratuitous ARP, 75
guest-mode line, 326

H
half-duplex mode for communication, 16, 31–32, 408
hardware address, 3–4, 25, 32, 86. See also MAC (Media Access Control) addresses
hardware broadcasts, 103
HDLC (High-Level Data-Link Control), 454, 457–459
frame format, 458
in PPP, 460
Header Checksum field, in IP header, 88
Header Length field
in IP header, 87
in TCP header, 77
help, global configuration mode for, 186
hertz, 456
hexadecimal addressing, 35–36, 96, 235
High-Level Data-Link Control (HDLC), 454, 457–459
frame format, 458
in PPP, 460
HMAC-SHA-1 algorithm, 442
holddown, 347
holddown timer, 348
hop, 343
hop count, 22, 200, 342, 344
incrementing, 353
maximum, 346
RIP use of, 347
Hops/Time Exceeded event, 90
host address, 96
host table, 275–277
vs. DNS server, 279
removing hostname from, 277
Host-to-Host layer (DoD), 67
protocols, 75–85
key concepts, 80–81
Transmission Control Protocol (TCP), 76–78
User Datagram Protocol (UDP), 78–79
hostname command, 180, 186, 462
hostname resolution, 72, 274–278
host table, 275–277
hostnames
removing from host table, 277
show sessions for displaying, 276
for SSH, 186
Hot Standby Router Protocol (HSRP), 95
HTTP (Hypertext Transfer Protocol), 205
as attack risk, 432
HTTPS server, sending data to, 310
hub network, 382
hubs, 3, 9, 28, 384
as layer 2 switches, 388
in OSI model, 14
at Physical layer, 27–28
vs. switches, 27
hybrid protocols, 343
HyperTerminal
for console connection, 45–46
Ctrl+Break to interrupt boot sequence, 239
IBSS (independent basic service set), 417, 418

ICMP. See Internet Control Message Protocol (ICMP)

ICMP echo request, 90–91

Identification field, in IP header, 87

IDSs (intrusion detection systems), 435

IEEE (Institute of Electrical and Electronics Engineers), 409

802.1AB for Station and Media Access Control Connectivity Discovery, 270

specifications, 24

IEEE 802.1AB for Station and Media Access Control Connectivity Discovery (IEEE), 270

IEEE 802.3 Ethernet, 31

frame format, 37

IEEE 802.3 standards, 39–41

IEEE 802.3u (Fast Ethernet), 40

IEEE 802.11

committees and subcommittees, 411–412

specifications, 409, 410–417

comparing 802.11a, b, and g, 415

product certification for interoperability, 410

IEEE 802.11a standard, 414

IEEE 802.11b standard, 412

disabling, 416

IEEE 802.11g standard, 412, 413–414, 414

IEEE 802.11i standard, 422

IEEE 802.11n standard, 416–417

IGRP (Interior Gateway Routing Protocol), default administrative distance (AD), 342

IMAP, 71

in-band, 164

incoming terminal line banner, 181, 182

independent basic service set (IBSS), 417, 418

Industrial, Scientific, and Medical (ISM) bands, 409

inside global address, 150

int serial command, 193

Integrated Services Router (ISR), 164, 165

automatic configuration of clock rate, 322

calendar command to change bit value, 240

default username and password, 163

erase start command and, 319

interface configuration, 194

interface command, 171

interface configuration mode, 171

interface ethernet command, 193

interfaces, 171

bringing up, 195–196

checking status, 195

central configuration on router, 320

configuring IP address on, 196–197

disabling, 195

enabling, with no shutdown command, 255

gathering traffic information, 264

output modifier (|; pipe), 197–198

overview for router, 210–211

of routers, 192–201

in routing table, 22

setting descriptions, 190–192

verifying statistics, 205

interference, 802.11a/g immunity to, 414

interior gateway protocols (IGPs), 341

Interior Gateway Routing Protocol (IGRP), default administrative distance (AD), 342
International Organization for Standardization (ISO), 11
Internetworking basics, 2–10
addressing, 3–10
devices, 8
with distance-vector routing, 344
models, 11–12
router in, 23
routers for creating, 6
Internetwork Packet Exchange (IPX), 22
intranet VPNs, 441
intrusion detection systems (IDSs), 435
intrusion prevention systems (IPSs), 435, 436
“Invalid input detected” error message, 175
invalid timer, 348
IOS. See Internetwork Operating System (IOS)
IP, 22
ip address command, 196
IP addressing, 86
assigning to hosts, 73
basic IP routing using, 311
configuring on interface, 316–318
domain name and, 72
hierarchical scheme, 96–101
terminology, 95
domain name lookup, 277
domain-name command, 72, 186, 277
ip host command, 275
IP (Internet Protocol), 22, 86–87, 303–304
header, 86, 87
Internetwork Packet Exchange (IPX), 22
ip classless command, 338, 339
ip default-gateway command, for managing switches, 398
ip default-network command, 339, 340, 341, 367
ip domain-lookup command, 277
ip domain-name command, 72, 186, 277
ip host command, 275
IP (Internet Protocol), 22, 86–87, 303–304
header, 86, 87
ip name-server command, 277
ip route command, syntax, 328
IP routing, 300, 303, 303–327
configuration
default, 335, 338–341
of DHCP, 326–327
interfaces for Corp router, 316–318
network addresses, 315
R1 router configuration, 318–322
R2 router configuration, 322–324
R3 router configuration, 325–326
RIP, 348–351
verifying, 336–337, 358–367
corporation in network, 327–343
Corp router static routes, 330–331
R1 router static routes, 331–332
R2 router static routes, 332–333
R3 router static routes, 334–335
static routing, 327–337
configuring, 313–327, 314
testing understanding of, 309–313
IP spoofing, 433
IP stack failure, 140
ip subnet-zero command, 115–116
ipconfig /all command, 142
ipconfig command, 337
verifying client with, 326
IPsec, 442
IPSs (intrusion prevention systems),
435, 436
IPv4, address types, 102–104
IPv6, 22
IPX (Internetwork Packet Exchange), 22
ISDN, 452
in PPP, 460
ISM (Industrial, Scientific, and Medical)
bands, 409
ISO (International Organization for
Standardization), 11
ISR routers, 164, 165
automatic configuration of clock
rate, 322
command to change bit value, 240
default username and password, 163
erase start command and, 319
interface configuration, 194

K
keepalives, 208
kernel, 163
keystroke loggers, 434

L
LAN. See local area network (LAN)
laptop, Ethernet port directly connected
to router interface, 244
large files, FTP for sending, 70
last-resort parameter, for enable
password, 183
latency, 25
Layer 2 broadcasts, 103
layer 2 switching, 25, 382
address learning by, 388–389, 389
features, 386
functions, 387–392
limitations, 386–387
networks before, 382–385, 383
port security, 391–392
Layer 3 broadcasts, 103
layer 3 switches, routers as, 7
layered approach to internetworking
models, 11–12
layers, seeing status of each interface, 211
LCP (Link Control Protocol), 459
in PPP, 460
leased lines, 452
leasing data links, 450
Length field
in Ethernet frames, 38
in UDP segment, 80
line-activation (exec) banner, 182
line command, 172, 183
line console command, 172
line in command-line interface, erasing, 176
Line Printer Daemon (LPD), 71
line vty command, 185
Link Control Protocol (LCP), 459 in PPP, 460
Link Establishment phase, in PPP session, 461
Link Layer Discovery Protocol (LLDP), 270
link-state protocols, 343
local area network (LAN), 3. See also virtual LANs (VLANs)
assign server and router IP addresses, 145
bridging vs. switching, 387
first switched, 384
open access mode for wireless products, 420
switching vs. hub-centered implementations, 27
local device, ending session from, 274
local loop, 451
DSL connections in, 454
local NAT addresses, 150
logging synchronous command, 185
logical addressing, 48, 50, 86
logical interfaces, 206
Logical Link Control (LLC) 802.2 sublayer, 25
login banner, 181, 182
login command, 184
login, disabling accounts after unsuccessful attempts, 436
logout command, 169
longest match rule, 301–302
loop avoidance, 387
loopback address, 140
loopback tests, 98, 99
loops, default routing on, 338

M
MAC database, 387
MAC frame format, 37
MAC (Media Access Control) addresses assigning to switch port, 391
basic IP routing using, 311
client, 421
in filtering table, 388
security, 438–440
MAC (Media Access Control) authentication, 420
mainframes, bridges for connecting to, 382–385
major command, 172
man-in-the-middle WLAN attacks, 421, 434
management interface, 395
maximum hop count, 346
maximum transmission time (MTU), 207
MD5 hash function, 461
Media Access Control (MAC) 802.3 sublayer, 25
Ethernet addressing using, 32
Media Access Control (MAC) address, 3–4
Media Access Control (MAC) authentication, 420
Media Independent Interface (MII), 40
memorization, slash notation (/), 129–130
message of the day (MOTD) banner, 181
metric, in routing table, 22
microsegmentation, 385
MII (Media Independent Interface), 40
MIMO (multiple-input multiple-output), 416
mini-IOS, in Cisco router, 233
mkdir command, 249
mobile devices, as security risk, 432
modems, dial-up, 452
more command, 248
MOTD (message of the day) banner, 181
MTU (maximum transmission time), 207
multicast address, 98, 103, 104
multilayer switches, security features, 431
multiple-input multiple-output (MIMO), 416, 417
multiplexing, spatial, 417
multiport bridges, 7
layer 2 switch as, 385

N
name, for routers, 180
name resolution, 3
troubleshooting, 142
native VLAN, 395
NCP (Network Control Protocol), 459, 461
in PPP, 460
negating command, 178
neighbor
gathering information, 259–264
IOS version of, 262
Network layer address, 203
neighbor routers, 301
NetWare servers, 383
Network Access layer (DoD), 68
Network Address Translation (NAT), 101, 148, 148–152
advantages and disadvantages, 149
global addresses, 150
how it works, 150–152
types of, 149
network addresses, 95, 96–99
in routing table, 22
network analyzer, output for name resolution process, 4
network command, 348

Network Control Protocol (NCP), 459, 461
in PPP, 460
Network File System (NFS), 70
network interface card (NIC), troubleshooting, 141
Network layer (OSI), 22–24, 48, 306
address of neighbor, 203
logical addressing, 50
Network Layer Protocol phase, in PPP session, 461
network loops, and redundancy, 387
network reconnaissance, 434
networks
best design, 10
documenting topology using CDP, 267, 267–269, 269
before layer 2 switching, 382–385, 383
segmentation, 4
switched design, 385
troubleshooting connectivity, 279–285
debugging, 282–284
with ping command, 280
with show processes command, 284–285
with traceroute command, 280–282
next-hop router, 338
NFS (Network File System), 70
nibble, 33, 35, 234
NIC (network interface card), troubleshooting, 141
no auto-summary command, 358
no cdp enable command, 265
no cdp run command, 259, 264
no debug all command, 283
no ip domain-lookup command, 277
no ip host command, 277
no login command, 184, 186
no shutdown command, 195–196, 208, 315
to enable port, 392
for enabling interface, 255
node address, 96
non-ISR router, bringing up, 167–169
non-overlapping channels, 414
“not ready” indicator, 19
Novell, 383
numbering system, conversion, 35–36
NVRAM (nonvolatile RAM), 165, 233
in Cisco router, 233
seeing contents, 256
verifying configuration, 253

O

o/r command, 240
octet, 95, 96
OFDM (Orthogonal Frequency Division Multiplexing) modulation, 413
open access mode, for wireless LAN products, 420
open authentication, 421
Open Shortest Path First (OSPF), 22, 356
default administrative distance (AD), 342
Open Systems Internconnection (OSI)
reference model, 11–28
advantages, 12
Application layer, 15
Data Link layer, 24, 24–27
vs. DoD model, 67
layer functions, 14
lower layers, 14
Network layer, 22–24
Physical layer, 27–28
PPP stack vs., 460
Presentation layer, 15–16
Session layer, 16
Transport layer, 16–21
upper layers, 13
Options field
in IP header, 88
in TCP header, 78

organizationally unique identifier (OUI), 32–33
Orthogonal Frequency Division Multiplexing (OFDM) modulation, 413
OSI. See Open Systems Internconnection (OSI) reference model
OSPF (Open Shortest Path First), 22, 356
default administrative distance (AD), 342
out-of-band, 164
output modifier (|; pipe), 197–198
overhead, 17
overloading, 149, 151

P

packet filtering, 7
Packet Internet Grouper (Ping). See ping (Packet Internet Grouper)
packet sniffers, 434
packet-switched WAN connection type, 452
packet switching, 7, 453
packets, 48, 50, 303, 312
destination IP address of, 309
PAP (PasswordAuthentication Protocol), 461
parallel transmission, 455
passive-interface command, 354
passphrase, 421
password attacks, 434
Password Authentication Protocol (PAP), 461
passwords, 163, 182–190
auxiliary, 184
clear-text, 436
console, 184–185
encryption of, 187–190, 462
mitigating security threats, 436–437
in plain-text configuration file, 437
recovery, 235, 238–239
strong, 436
user-mode, for Telnet, 185
VTY, 270–271
performance
  broadcast domain size and, 386
  of routers, debug all command and, 282, 284
physical interfaces, 206
  displaying information about, 211
Physical layer (OSI), 27–28, 51, 305
  Ethernet networking at, 38–43, 39
  output from problem, 208
physical star network, 28
ping of death attacks, 433
ping (Packet Internet Grouper), 72, 90, 91, 396
  for DHCP conflicts, 75
  extended, 204
  to test connectivity, 279, 280
  to test DNS server, 278
TFTP device from router console, 245
  for troubleshooting, 140
unreachable network and, 362
  to verify configuration, 203, 336
pinhole congestion, 344, 344
pipe (|), 197–198
PoE (Power over Ethernet), 392
point of presence (POP), 451
point-to-point connection, 452
Point-to-Point Protocol (PPP), 454, 458, 459–464
  authentication, 461
  configuration on Cisco router, 462
  configuring authentication, 462–463
  session establishment, 460–461, 461
  stack vs. OSI layer, 460
  verifying encapsulation, 463–464
poison reverse, 347
populating forward/filter table, 389, 390
Port Address Translation (PAT), 149, 150, 151
port numbers, for TCP and UDP, 81–85, 82
port redirection attacks, 434
port security, 391–392, 437–438
ports
  gathering information, 264–266
  numbers at Transport layer, 50
  security for unused, 440
  setting for rolled cable connection, 46
  positive acknowledgment with retransmission, 21
Post Office Protocol version 3 (POP3), 71
POST (power-on self-test), 232
  in boot sequence, 233
  power-on self-test (POST), 232
  for Cisco switch, 392
Power over Ethernet (PoE), 392
Powers of 2, 117
PPP (Point-to-Point Protocol), 454, 458, 459–464
  authentication, 461
  configuration on Cisco router, 462
  configuring authentication, 462–463
  session establishment, 460–461, 461
  verifying encapsulation, 463–464
Pre-Shared Key (PSK), 421
Preamble field, in Ethernet frames, 37
prefix routing, 347
Presentation layer (OSI), 15–16
printer sharing, Line Printer Daemon for, 71
printing, working directory, 249
Priority field, in IP header, 87
private IP addresses, 101–102
privileged EXEC mode, 172
privileged mode, 168, 169
  entering, 241
  for ping, 280
  Telnet and, 272
Process/Application layer (DoD), 67
Process/Application layer (DoD) protocols, 68–75
Automatic Private IP Addressing (APIPA), 74
Domain Name Service (DNS), 3, 72
Dynamic Host Configuration Protocol (DHCP), 73–74
address conflicts, 75
configuration on router, 326–327
connection, 74
verifying pool, 326
File Transfer Protocol (FTP), 69, 205
as attack risk, 432
real world scenario, 70
Line Printer Daemon (LPD), 71
Network File System (NFS), 70
Secure Shell (SSH), 72
setting up, 186–187
Simple Mail Transfer Protocol (SMTP), 70–71
Simple Network Management Protocol, 71
Simple Network Management Protocol (SNMP), 79
Telnet, 69, 142, 205, 270–274
checking connections, 273
checking users, 273–274
for Cisco router connection, 164
closing sessions, 274
ending connection, 272
into multiple devices simultaneously, 272
user-mode passwords for, 185
Trivial File Transfer Protocol (TFTP), 69–70
routers booting from host, 242
X Window, 71
promiscuous mode, 434
propagation, holding down RIP, 354–355
proprietary HDLC implementation, 458
Protocol Data Units (PDUs), 47
and layer addressing, 49
Protocol field, in IP header, 87, 88
Proxy Address Resolution Protocol (Proxy ARP), 94
public IP addresses, NAT to decrease, 148
public use, unlicensed frequency bands for, 409–410, 410
pwd command, 249
question mark (?), for help, 173
RAM (random access memory)
in Cisco router, 233
seeing contents, 256
range command, 440
rate shifting, 412
read-only memory (ROM), in Cisco router, 233
recovery, of passwords, 235, 238–239
redistribution, 355
redundancy, and network loops, 387
reference model, 11
software developers use of, 12
registered jack (RJ) connector, 39
Registry (Windows), 307
reliable networking, 16
reloading, routers, 202, 241
remote access VPNS, 441
remote device
ending session from, 274
telnet into, 272
remote network, computing distance for, 22
removing hostname, from host table, 277
repeaters, 27
in OSI model, 14
router console, pinging TFTP device from, 245
router modes, overview, 170
Router# prompt, 169
Router> prompt, 169
router prompt, 248
router rip command, 348
router rip global command, 360
routers, 5, 8
administrative configurations, 179–182
banners, 180–182
hostnames, 180
setting passwords, 182–190
advantages, 6
characteristics, 23–24
defining terms, 172–173
interfaces, 192–201
mitigating security threats, 436–437
need for inter-VLAN communication, 9
network locations and, 25
in OSI model, 14, 22
reloading, 202, 241
routing basics, 301–303
gathering basic information, 178–179, 301
routing by rumor, 343
Routing Information Protocol (RIP), 22, 341, 347–357
advertising default route using, 365–367
configuring routing, 348–351
example 2, 353, 353–354
default administrative distance (AD), 342
and discontiguous networks, 352
holding down propagation, 354–355
timers, 348
verifying routing tables, 351–353
version 2, 355–357
enabling, 363–367
v1 vs., 356
resolving hostnames. See hostname resolution
restoring
Cisco IOS, 246–247
Cisco router configuration, 254
retransmission delay, after collision, 31
retransmission, positive acknowledgment with, 21
Reverse Address Resolution Protocol (RARP), 93–94, 94
reverse Telnet, banner for terminals connected to, 182
RF spectrum, unlicensed bands in, 410
RIP version 2 (RIPv2), 22
RJ-45 connector, 163
rmdir command, 249
rolled cable, 44–47, 45
port setting for connection, 46
ROM monitor, in Cisco router, 233
ROM monitor mode, 240
ROM (read-only memory), in Cisco router, 233
rootkit, 433
route flush timer, 348
route poisoning, 347
route update packets, 22
routed protocols, 22, 300
router-command history, reviewing, 176–177
Router (config-if)# prompt, 171
Router (config-line)# prompt, 172
Router (config-subif)# prompt, 172
Request for Comments (RFC), 79
768, on UDP, 79
791, on IP, 86
1661, on PPP, 458
3232, on port numbers, 81, 82
request timed out message, 308
request to send, clear to send (RTS/CTS), 413
reserved IP addresses, 98–99, 101
resolver.
routing loops, 345–347, 346
routing protocols, 22, 300
basics, 341–343
administrative distance (AD), 329, 340, 342–343
classes, 343
distance-vector, 343–347
and dynamic routing, 341
routing table, 7, 23, 301, 311
codes for, 318
converged, 345
manually adding routes, 327
verifying, 351–353
viewing, 318
RSA algorithm, 442
running-config file, 167, 234
  copying startup-config to, 241
  copying to NVRAM, 201
  viewing output, 194–195
RXBOOT, 233

S
scallopy, RIP v1 vs. v2, 356
scrolling, in command-line interface, 176
SDLC (Synchronous Data Link Control), 454
secondary parameter, for ip address command, 196
secret parameter, for enable password, 183
Secure Shell (SSH), 72
  setting up, 186–187
SecureCRT, 239
security
basics, 430–435, 431
  common attack profiles, 432–435
  recognizing threats, 431–432
MAC addresses, 438–440
mitigating threats, 435–440
for unused ports, 440
for wireless technology, 419–422
segment, 47
segmentation, 384
sendmail, as attack risk, 432
Sequence Number field, in TCP header, 77
serial interface commands, 198–201
  indication of problem, 208
  for WAN connections, 6
serial transmission, for WAN connections, 455–456
Serial0/0 is up, line protocol is down message, 464
service password-encryption command, 188–189, 190, 437, 462
Service Set ID (SSID), 417, 420
  setting access points to same, 419
Session layer (OSI), 16
setup command, 168
setup mode, 173, 203, 316
  for router configuration, 168
shared-key authentication, 421
shortest-path-first protocols, 343
show cdp command, 258–259
show cdp entry * command, 262–264
show cdp entry * protocol command, 203, 263
show cdp entry * version command, 263
show cdp interface command, 264–266
show cdp neighbor command, 259, 269
  output, 259–260
show cdp neighbor detail command, 260–262, 267
show cdp traffic command, 264
show controllers command, 200, 211–213, 212
  displaying clock rate, 322
show file command, 248, 250, 251, 256
show flash command, 238, 244, 250
show history command, 176
show hosts command, 275–276, 278
show interface command, 179, 190, 196, 205–210, 459
  for verifying PPP configuration, 463–464
show interface fastethernet command, 206–207
show interfaces command, 195
show ip arp command, 142, 306
show ip dhcp binding command, 326
show ip interface brief command, 179, 210–211, 360
  to verify switch configuration, 398
show ip interface command, 210, 212
show ip protocols command, 358–360, 364–365
  troubleshooting with, 359–360
show ip route command, 302–303, 311, 318, 321, 330–331
  output, 323
  for troubleshooting, 279
show mac address-table command, 390–391
show port-security command, 439
show processes command, 284–285
show protocols command, 211
show run command, 462
show running-config command, 190, 195, 196, 202
  for documenting network topology, 267–268
  password visibility, 188
  to verify configuration, 252, 398
  for viewing interface description, 190
show sessions command, 273, 276
show startup-config command, 202
show terminal command, 177
show users command, 273
show version command, 178–179, 236, 237–238, 245
shutdown command, 195, 440
Simple Mail Transfer Protocol (SMTP), 70–71
Simple Network Management Protocol (SNMP), 71, 79
simplex mode for communication, 16
site-to-site VPNs, 441
slash notation (/), 118, 129
sniffer, 434
software address, 86
software, configuration meanings, 235
Source Address (SA) field, in Ethernet frames, 37
Source IP Address field, in IP header, 88
Source Port field
  in TCP header, 77
  in UDP segment, 80
source port, numbers for multiple hosts communicating to server, 309
spanning-tree, 392
Spanning Tree Protocol (STP), 387
spatial multiplexing, 417
special purpose IP address, 98–99
specific configuration mode, 173
split horizon, to solve routing loop problem, 346–347
squeeze command, 249
SSID (Service Set ID), 417
configuration, 326
Stacheldraht attack, 433
Start Frame Delimiter (SFD)/Sync field, in Ethernet frames, 37
startup-config file, 167, 168, 201, 234
copying to running-config file, 241
deleting, 202
state transitions, 27
static IP addressing, 75
static NAT, 149
static routing, 301, 327–337
benefits, 327
configuration
Corp router, 330–331
R1 router, 331–332
R2 router, 332–333
R3 router, 334–335
default administrative distance (AD), 342
disadvantages, 328
sticky command, 392
straight-through cable, 43, 43–44
strong passwords, 436
stub networks, default routing on, 338
stub routers, 335
subinterfaces, 172
subnet masks, 116, 117–118
as starting point in troubleshooting, 147
subnets
basics, 114–140
benefits, 115
Class A addresses, 137–140
practice examples, 137–139
in your head, 139–140
Class B addresses, 130–136
practice examples, 131–135
in your head, 136
Class C addresses, 120–130
fast way, 121
practice examples, 122–127
in your head, 128
creating, 116
routing protocol and, 349
switch card configuration, 316
switch port, setup to allow only one host per port, 391
switched network, 393
switched network design, 385
switches, 4, 5, 8. See also Cisco Catalyst switches
administrative configurations, 179–182
banners, 180–182
hostnames, 180
setting passwords, 182–190
crossover cable between, 393
in Data Link layer, 25–27
vs. hubs, 27
in internetwork, 9, 26
mitigating security threats, 436–437
multilayer, security features, 431
in OSI model, 14
port security, 437–438
and routing, 310
troubleshooting port LED alternating green and amber, 392
switching services, 385–387
switchport port-security command, 391, 438
syn packet, 84
synchronization, for connection-oriented communication, 17
Synchronous Data Link Control (SDLC), 454

T

TACACS server, for authentication, 183
TCP SYN flood attacks, 433
Telecommunications Industry Alliance (EIA/TIA), 39
telecommuters, 441
Telnet, 69, 142, 205, 270–274
checking connections, 273
checking users, 273–274
for Cisco router connection, 164
closing sessions, 274
ending connection, 272
into multiple devices simultaneously, 272
user-mode passwords for, 185
terminal emulation, 69
terminal history size command, 177, 178
terminal monitor command, 284, 360
TFTP (Trivial File Transfer Protocol), 69–70
routers booting from host, 242
TFTP host
copying IOS to, 243
router search for, 319
routers booting from, 242
TFTP server
back up Cisco IOS to, 245
copying configuration to, 254
tftp-server flash:ios_name command, 247
thicknet, 39
thin protocol, 78
thinnet, 39
threats to security, recognizing, 431–432
three-way handshake, 17, 18, 18
Time to Live field, in IP header, 87
timers, RIP, 348
Token Ring (TR), 33
toll network, 451
Total Length field, in IP header, 87
trace command, 280
traceroute command, 90, 142, 204, 279, 280–282
tracert command, 142, 281–282, 337
Transmission Control Layer (TCP), 16
Transmission Control Protocol (TCP), 76–78
destination port, 83–84
key features, 81
key protocols using, 84–85
segment format, 76–78, 77
source port, 82–83
syn packet acknowledgment, 84–85
Transmission Control Protocol/Internet Protocol (TCP/IP), 66, 68
transparent bridging, 26
Transport layer (OSI), 16–21
header, 47
port numbers at, 50
reliable delivery, 21
trap, 71
tribe flood network 2000 (TFN2K), 433
tribe flood network (TFN), 433
Trivial File Transfer Protocol (TFTP), 69–70. See also TFTP (Trivial File Transfer Protocol)
Trojan horse, 433, 434
troubleshooting
with debug ip rip command, 361–363
description command and, 191
IP addressing, 140–148
network connectivity, 279–285
debugging, 282–284
with ping command, 280
with show processes command, 284–285
with traceroute command, 280–282
with show ip protocols command, 359–360
switch port LED alternating green and amber, 392
trust exploitation attacks, 435
trusted network, 431
trustworthiness of routing information, 342
tunneling protocols, 442
Type of Service field, in IP header, 87

U

U/L bit (universal/local bit), 33
UDP. See User Datagram Protocol (UDP)
undebug all command, 283
Unicast address, 103–104
universal/local bit (U/L bit), 33
Unlicensed National Information Infrastructure (UNII) band, 409–410
unreachable network, ping and, 362
unreliable protocol, 79
unshielded twisted-pair (UTP) cabling, 39
untrusted network, 431
unused ports, security for, 440
update timer, 348
upgrading Cisco IOS, 246–247
Urgent field, in TCP header, 78
URLs, for file system, 248
use-tacacs parameter, for enable password, 183
user accounts, disabling after unsuccessful login attempts, 436
User Datagram Protocol (UDP), 16, 78–79
DHCP use of, 73
key features, 81
key protocols using, 84–85
segment format, 79–80, 80
user EXEC mode, 169, 172
for ping, 280
user interface, for IOS, 163–169
user-mode passwords, 183–184
encryption of, 187–190
for Telnet, 185
users for Telnet, checking, 273–274

V
V.24 standard, in PPP, 460
V.35 standard, in PPP, 460
valid host IDs
  in Class A network, 100
  in Class B network, 100
  in Class C network, 101
  for Class C subnet, 121, 124
verifying
  Cisco router configuration, 252
  configuration, 203–213
  IP routing configuration, 336–337, 358–367
version 2 command, 358
Version field, in IP header, 87
video over IP, 76
virtual circuit, 76
virtual LANs (VLANs), 9, 385, 386, 431
  native, 395
  router for connections between, 10
virtual private networks (VPNs), 440–442, 441
viruses, 434
voice over IP (VOIP), 76
vty parameter, for line command, 183
VTY password, 270–271
VTY ports, 270
  listing all, 273

W
well-known port numbers, 81, 82
Wi-Fi Alliance, 409, 410
Wi-Fi Protected Access (WPA), 421–422
wide area network (WAN)
  basics, 450–455
  cabling for, 455–457
  Cisco support, 453–454
  connection types, 452–453
  router for connections to, 6
  subnet masks, 127
  terminology, 451, 451–452
wildcards, for configuring default route, 338
Window field, in TCP header, 77
windowing, 20, 20–21
Windows Registry, 96, 307
Wired Equivalency Protocol (WEP), 420
wireless LANs (WLANs)
  radio frequencies, 408
  as security risk, 432
wireless technology
  agencies governing use, 409
  basic service sets, 417–419
  basics, 408–410
  connection for WAN services, 455
  interface configuration, 326
  security, 419–422
witless user ignorance (WUI), 432
WLAN Association (WLANA), 409
working directory, printing, 249
workstation, Ethernet port directly
  connected to router interface, 244
WPA (Wi-Fi Protected Access), 421–422
WUI (witless user ignorance), 432

X

X Window, 71
X.25 protocol, 453

Y

Yeager, William, 163