

INDEX

Numerics

- 5-4-3 rule (Ethernet), 291
- 10BASE-T, 85, 89, 104
- 10Gigabit Ethernet
 - IEEE 802.3ae, 41
 - trunk speeds, incrementing 255
- 10-Mbps Ethernet. *See* Ethernet
- 80/20 rule (VLANs), 255
- 100BASE-T, 85, 89
- 100-Mbps Ethernet. *See* Fast Ethernet
- 802.1 specification (IEEE), 39, 109, 147
 - 802.1d, 39, 239
 - 802.1w, 166
 - 802.1q, 39, 188, 193
- 802.3 specification (IEEE), 40–41, 85, 89
- 802.5 specification (IEEE), 42
- 802.11 specification (IEEE), 42–43
- 1000-Mbps Ethernet. *See* Gigabit Ethernet
- 10,000-Mbps Ethernet, 41

A

- AAA (authentication, authorization, and accounting) model, 276
- access control lists (ACLs), 207, 213
- access layer (HDM), 35, 233, 236
- access links, 185
- access methods, 89. *See also specific methods*
- accounting (security), 276
- accounting management, 272–273
- ACLs (access control lists), 207, 213
- Address Resolution Protocol. *See* ARP
- address space, 243
- address-based VLANs, 178–179
- Advanced Television System Committee (ATSC), 36
- alarm group (RMON), 282
- algorithms
 - back-off algorithm, 93
 - spanning-tree algorithm, 39, 109, 147–149
 - root bridges, 149*
 - switch ports, 149*



American National Standards Institute, 37–38

analog repeaters, 53

analog signals, 50–52

converting to digital, 52

ANSI (American National Standards Institute), 37–38

application layer (OSI), 29, 33

application-specific integrated circuits (ASICs), 174, 237

ARP (Address Resolution Protocol), 139, 212, 246

attacks, 212–213

broadcasts, 121

cache (routers), 139

mapping, 139–141

poisoning, 212

segmenting broadcasts, 249

steady-state conditions, 141

tables, 136

ASICs (application-specific integrated circuits), 174, 237

ATM (Asynchronous Transfer Mode), 32

ATSC (Advanced Television System Committee), 36

authentication, 276

authentication, authorization, and accounting (AAA) model, 276

authorization, 276

availability, managing performance, 275

B

backbone switches, 84

back-off algorithm, 93

backups (redundancy/fault management), 253, 267

bandwidth

accounting management, 272

conserving via multicast, 120

contending for, 296

doubling Ethernet bandwidth, 232

Ethernet, 40

flat network topology, 228

hubs, 97

managing, 227, 275

microsegmenting, 247

network designs, 227, 254

network traffic, 296

network management applications, 227

performance management, 275

- routing inter-VLAN traffic, 255
 - sharing, 236
 - STP, 74
 - switches, 104, 220, 237
 - high bandwidth requirements*, 228
 - microsegmenting*, 247
 - twisted-pair cable, 74
 - UTP, 75
- baselines**
- configuration management, 271
 - performance management, 274
- BGP (Border Gateway Protocol), 133**
- billing (accounting management), 272**
- binary conversion (decimal/hexadecimal), 91**
- binary numbering, 91**
- bit buckets, 126**
- bit streams, 32. *See also* signals**
- bits, 50, 53**
- blocking state, 148, 156–157, 166**
- Border Gateway Protocol (BGP), 133**
- BPDU (bridge protocol data unit), 150–153**
- bridges, 150, 165
 - contents of, 152
 - determining superiority, 151
 - electing designated ports, 163
 - network topology changes, 151
 - selecting ports, 153
 - switches, 150
 - transmission rate (default), 162
 - transparent switching, 242
- breaking up. *See* segmenting**
- bridges**
- BPDU, 150, 165
 - data link layer, 32, 63
 - Ethernet, 89, 98–100
 - filtering, 99
 - flooding, 102
 - fragmenting frames, 141
 - functioning as multiport hubs, 63
 - ID components, 151
 - interconnecting switches, 109
 - interface address tables, 103
 - IP routing lookups (versus), 138
 - LAN bridges, 297
 - MAC addresses, 98, 136, 151
 - MAC flooding attack, 211
 - MAC tables, 63
 - multiport bridges (switches), 63
 - network congestion, preventing 97
 - network segmentation, 94
 - operation, 100–102



- port numbers, 29
- priority, 151
- removing loops, 150
- repeaters and hubs (versus), 98
- routers (versus), 109
- STP port states, 155
- transparent bridges, 100, 222
- WAN interfaces, 298

bridging (data-link addresses), 118

broadcast (transmission method), 121

broadcasts, 107, 242–243

- controlling, 248–249
- domains, 172
 - breaking up with routers, 291*
 - distribution layer, 236*
 - flat networks, 222, 228*
 - routers separating, 228*
 - traditional versus VLAN, 225*
 - VLANs, 172, 304*
- filtering, 224
- IPX clients, 248
- radiation, 250
- segmenting, 249–250
- storms, 108, 242–243, 254

C

cabling, 11, 73

- coaxial, 17, 56
- copper, 11, 56, 74
- EMI/RFI, 56
- Ethernet, 74
- Fast Ethernet, 74
- fiber-optic, 11, 17, 56, 75–77
- LAN connections, 73
- LAN versus VLAN infrastructure, 225
- physical layer components, 50
- repeaters, 96
- security, 74–76
- termination, 77
- twisted-pair, 17, 55, 74
 - STP, 56, 74*
 - UTP, 55, 75*
- wall plates/boxes, 79

CAD/CAM (computer-assisted design/computer-assisted manufacturing), 296

CAM (content-addressable memory), 206

campus LANs, 302

- design principles, 254–256
- distributed routing/switching, 259
- introducing switch benefits, 237–238

- large switching/minimal routing, 258–259
- scalable switching, 256–257
- capture group (RMON), 283**
- carrier sense multiple access with collision detect. *See* CSMA/CD**
- case studies**
 - bridge-based networks, 297–298
 - hub-based networks, 292–296
 - medium/large switch-based networks, 302–303
 - small switch-based networks, 298–301
 - VLANs, 303–305
- change control, 271**
- checksums, 31**
- ciphertext, 30**
- Cisco IOS interface, 137**
- client mode (VTP), 190**
- coaxial cable, 56**
- collapsed backbone networks, 108**
- collision detection, 93**
- collision domains, 92**
 - breaking up, 291
- collisions, 93–94**
 - Ethernet, 41, 128
 - late, 128
- computer-assisted design/computer-assisted manufacturing (CAD/CAM), 296**
- confidentiality (traffic integrity), 224**
- configuration management, 270–271**
- congestion. *See* network congestion**
- congestion control, 31**
- content-addressable memory (CAM), 206**
- convergence. *See* network convergence**
- converting numbers, 91**
- copper cable, 11, 56, 74**
- core layer (HDM), 35, 233, 236**
- CRC (cyclic redundancy check), 121–123**
 - adding to frame size, 121
 - Ethernet frame sizes, 121
 - multilayer switching, 131
- CSMA/CD (carrier sense multiple access with collision detect)**
 - collisions/collision domains, 92–94
 - Ethernet, 41, 86, 92
 - flat network topology, 228
 - operation, 92–93
 - retransmitting (frames), 41, 94
 - shared environments, 89
 - time slots, 94
- cut-through method (switching), 108**
- cut-through switching, 126–128**
- cyclic redundancy check. *See* CRC**



D

daisy chaining, 295

dark fiber, 49

data, defined, 11

data flow, 4

- bit streams, 32
- broadcast method, 121
- collisions, 93
- en-/decapsulating, 33
- errors, 31
- FDDI, 85
- forwarding, 31, 174
- frames, 12, 54, 61
- full-duplex mode, 14
- half-duplex mode, 13
- high-priority/sensitive traffic, 224
- isolating network traffic, 174
- multicast method, 120
- native VLANs, 202
- NICs, 80
- OSI model, 28, 33
- protocols, 147
- ring topology, 82
- routed versus switched networks, 243
- routers, 67
- routing, 31
- segmenting network traffic, 174
- sensitive/high-priority traffic, 224

- simplex mode, 13

- signal types, 32

- star topology, 80

- switch-based hierarchical design, 301

- switching, 10, 108–109

- Token Ring, 42

- transmission media, 32

- transmission methods, 118–121

- transmission modes, 13–14

- unicast method, 120

- VLANs, 226

data link layer (OSI model),

31–33, 57, 60, 231

- address space, 243

- addresses, 136

- bridges, 63

- fixed-length fields, 136

- flat network topology (switching), 231–232

- fragmenting (frames), 141

- frames, 61–62

- hardware, 63–65

- multilayer switching, 130

- network attacks, 210

- RMON, 283

- switches, 63, 247

- switching methods, 123–129

 - cut-through, 126–128*

- fragment-free*, 128–129
 - store-and-forward*, 123–126
 - VLANs, 174, 208
 - data-link addresses**
 - ARP, 246
 - bridging, 118
 - IP addresses (versus), 139
 - decapsulation**, 34
 - decimal conversion (hexadecimal/binary)**, 91
 - decimal numbering**, 91
 - dedicated-media LANs**, 40
 - delay**. *See also* latency
 - comparing switching methods, 126
 - flat network topology, 228
 - multilayer switching, 131
 - demarcation points**, 6
 - demodulation**, 11
 - dense wavelength-division multiplexing (DWDM)**, 32
 - designated ports**, 152
 - electing, 163
 - MAC addresses, 164
 - designated switches**, 152
 - destination**, defined, 4
 - DHCP (Dynamic Host Configuration Protocol)**, 249
 - Digital Equipment Corporation (DEC)**, 22
 - Digital Equipment Corporation, Intel, Xerox (DIX)**, 22, 28
 - digital repeaters**, 53
 - digital signals**, 50–52
 - converting to analog, 52
 - Digital Subscriber Line (DSL)**, 89
 - distant end**, defined, 9
 - distributed routing/swithing**, 259–260
 - distribution layer (HDM)**, 35, 233, 236, 258
 - DIX (Digital Equipment Corporation, Intel, Xerox)**, 22, 28
 - DSL (Digital Subscriber Line)**, 89
 - DTP (Dynamic Trunking Protocol)**, 207
 - DWDM (dense wavelength-division multiplexing)**, 32
 - Dynamic Host Configuration Protocol (DHCP)**, 249
 - Dynamic Trunking Protocol (DTP)**, 207
- ## E
- EIA/TIA-232 (Electronic Industries Alliance/Telecommunications Industry Alliance)**, 32



**electronic signals (analog/digital),
50–52**

EMI (electromagnetic interference)

sources of, 56

STP, 56, 74

UTP, 56, 75

encapsulation, 33

encryption, 30

error correction, 31

error handling, 31

error recovery, 30

EtherChannel, 255

Ethernet, 41

5-4-3 rule, 291

bandwidth, 40, 232

bridges, 89, 98–100

broadcast domains, 172

cable modems, 89

cabling, 74

collisions, 41, 93–94

CSMA/CD, 41, 92

discarding frames, 124

doubling bandwidth, 232

environments, 89

frames

source/destination addresses, 134

sizes, 121, 245

full-duplex mode, 232

half-duplex mode, 232

hubs, 89, 96–97

IEEE 802.3 specification, 41, 85

interface tables, 89

interfaces, 132

inventors, 22, 28

Layer 2 addresses, 246

MAC addresses, 89

microsegmenting, 219

modes, 40, 232

packet switching, 134

popularity of, 18

port cost, 160

port security, 204

repeaters, 95

RJ connectors, 77

RMON groups, 282

routers, 109, 132

routing tables, 89

segment numbers, 291

shared environment, 89

standards, 40–41, 89

switched environments, 89

switches, 89, 104–106

switching methods, 108–109
 Token Ring (versus), 85
 transfer rates, 41, 85, 89
event group (RMON), 283

F

fast convergence, 238

Fast Ethernet, 40. *See also* Ethernet

bandwidth, 40, 232
 cabling, 74
 doubling bandwidth, 232
 IEEE 802.3u, 41
 incrementing trunk speeds, 255
 frame sizes, 245
 microsegmenting, 219
 modes, 40
 port cost, 160
 port security, 204

fault management, 267–270

FCAPS (fault, configuration, accounting, performance, and security) model, 265–278

accounting management, 272–273
 configuration management, 270–271
 fault management, 267–270
 OSI model (versus), 265–267

performance management, 273–275
 security management, 275–278

FDDI (Fiber Distributed Data Interface), 85

ring topology, 82
 transfer rates, 85

fiber-optic cable, 11, 56

copper cable (versus), 75
 modes (MMF/SMF), 76–77

file servers, 18

filter group (RMON), 283

filtering

access layer, 236
 bridges, 99
 Cisco switches enabled for, 244
 nonfiltering switches, 242
 switches, 105
 traffic, 225

firewalls, 225, 238

hub security, 293
 nonsecure side (public), 202
 routing platforms, 224
 secure side (private), 202
 security, 202

flat network topology, 227–230, 241

flooding, 102, 174, 222

flow control, 30

forward delay timer, 156

**forwarding, 31**

- cut-through switching, 126–128
- decisions, 174
- determining next hop, 136
- fragment-free switching, 129
- MTU discovery, 142
- multilayer switching, 131
- routers (ARP cache), 139
- routing protocols, 133
- routing table lookups, 135–136
- store-and-forward method, 126
- store-and-forward switching, 124

forwarding state, 159, 166**fragmentation (frames), 141****fragment-free switching, 128–129****Frame Relay, 297, 304****frame synchronization, 31****frames, 12, 61, 117–118**

- blocking state, 157
- BPDUs, 150
- bridges, 99
- broadcasting, 107
- collisions, 93
- components and functions, 117
- data link layer, 31, 61–62
- disabled state, 159
- errors, 86
- Ethernet, 121, 134, 245

filtering, 106

fragmenting, 141

forwarding state, 159

headers, 12, 61, 99, 117

learning state, 158

listening state, 157

MTUs, 123, 141

multilayer switching, 131

network analyzers, 284

packets (versus), 66–67

payload, 12, 61, 117

random frame-stress attacks, 215

retransmitting, 41, 94

secure ports, 206

sizes, 121–123, 245

STP states, 157–159

switch port costs, 150

switching (multilayer), 131

Token Ring, 42, 85

trailers, 12, 61, 117

transmission methods, 118–121

- broadcast, 121*

- multicast, 120*

- unicast, 119*

VLAN tagging, 186

full-duplex mode, 14, 40

Ethernet, 232

mismatches causing collisions, 128

full-mesh topology, 58

fur-ball networks, 233

G

gateways, 225

GET messages (SNMP), 280

GET NEXT messages (SNMP), 280

GET-RESPONSE messages (SNMP), 280

Gigabit Ethernet, 32, 40

IEEE 802.3z specification, 41

frame sizes, 245

incrementing trunk speeds, 255

microsegmenting, 219

port cost, 160

port security, 204

H

half-duplex mode, 13, 40

Ethernet, 92, 232

mismatches causing collisions, 128

hardware

data link layer, 63–65

network layer, 67–68

physical layer, 53–55

hardware inventory, configuration management, 271

HDM (Hierarchical Design Model), 35

HDTV (High-Definition Television), 36

headers

frames, 12, 61–62, 117

packets, 68

hexadecimal numbering, converting decimal/binary, 91

Hierarchical Design Model (HDM), 35

hierarchical designs (network), 229

hierarchical model, 233, 236

hierachical topology, 232–234

High-Definition Television (HDTV), 36

history group (RMON), 282

host group (RMON), 282

hosts, 142, 282

hub-and-spoke topology, 80. *See also* star topology

hubs, 54, 63

5-4-3 rule (Ethernet), 291

bridges (versus), 98, 106

case study, 292–296

creating VLANs (via switches), 173

daisy chaining, 295



Ethernet, 89, 96–97, 291
home networks, 292–293
multiport hubs, bridges
 functioning as, 63
office networks, 294–296
operation, 97
physical layer, 33
port numbers, 295
scalability, 228
security, 293
shared-media LANs, 40
signal amplification, 96
star topology, 96
switches (versus), 105–106, 173
vendors favoring switches, 293
VLANs, replacing with switches,
 173

I

IBM, 22, 28, 42, 84
**identification numbers (VLANs),
 174**
**IDSs (intrusion detection systems),
 203, 210**
**IEEE (Institute for Electrical and
 Electronics Engineers), 21, 37–38,
 85, 89–90, 147, 160, 193**

802.1, 39, 109, 147
802.1d, 39, 239
802.1q, 39, 188, 193
802.1w, 166
802.3, 40–41, 85, 89
802.5, 42
802.11, 42–43

**IETF (Internet Engineering Task
 Force), 21, 278**

**IGMP (Internet Group Multicast
 Protocol), 249**

**IGRP (Interior Gateway Routing
 Protocol), 133**

in-band management ports, 207

**Institute for Electrical and
 Electronics Engineers. *See* IEEE**

**International Telecommunications
 Union (ITU), 37–38**

Intel, 22, 28

interconnections, 6

interface address tables, 102–103

interface tables (Ethernet), 89

**Interior Gateway Routing Protocol
 (IGRP), 133**

**International Business Machines,
 22, 28, 42, 84**

**Internet Engineering Task Force
 (IETF), 21, 278**

Internet Group Multicast Protocol

(IGMP), 249

Internet Protocol. *See* IP

Internet-standard management framework. *See* SNMP

Internetwork Packet Exchange (IPX), 136, 248

interoperability, 21, 193

Inter-Switch Link (ISL), 186

intrusion detection systems (IDSs), 203, 210

inventory configuration management, 271

IP (Internet Protocol), 110, 134

addresses, 134, 136

ARP, 139

data-link addresses (versus), 139

routing, lookup results, 138

television (IPTV), 220

IPTV (Internet Protocol television), 220

IPX (Internetwork Packet Exchange), 136, 248

ISL (Inter-Switch Link), 186

ITU (International Telecommunication Union), 37–38

J–L

Jumbo Ethernet. *See* Gigabit Ethernet

LANs (local-area networks), 17–18, 47–48, 73

cabling, 55

campus LANs, 302

connecting via routers, 67

data link layer, 57–65

differentiating characteristics, 47

distributed routing/switching, 259

Ethernet LANs. *See* Ethernet networks

large switched/minimal routing, 258–259

microsegmenting, 219

mixed-media switching, 245

network layer, 65–68

network topologies, 60

OSI model, 49–68

physical layer, 50–56

hardware, 53–55

media, 55–56

signals, 50–52

routers, 240–246

scalable switching, 256–257

segments, 219–220



switched network design, 237, 240, 255–256

switches, 220, 240–247

transmission methods, 117–121

utilizations, 47

WANs (versus), 48–49

large switched/minimal routing (network design), 258–259

latency. *See also* delay

 comparing switching methods, 126–127

 multilayer switching, 131

Layer 3-based VLANs, 180

Layers 1–7 (OSI model), 29. *See also separate layer names*

leased lines, creating WANS, 48

LEDs (light emitting diodes), 77

link segments (Ethernet), 291

link-management protocols, 39, 147

listening state, 157

LLC (logical link control) layer, 31

load balancing (routers), 239

load sharing (redundancy), 253

logging (security), 278

logical link control (LLC), 31

logical networks, 7–8

long-reach Ethernet (LRE), 47

loops, 148, 241

 bridge loops, 147

 causing broadcast storms, 243

 detecting via BPDUs, 150

 preventing, 147

 STP, 153, 241

LRE (long-reach Ethernet), 47

M

MAC (Media Access Control) addresses, 89–91, 118, 151

 age-time expiration, 206

 assigning, 178

 allocating on a port, 205

 bridges, 98, 63

 converting IP addresses, 139

 electing designated ports, 164

 electing root bridges, 161

 flooding attacks, 211

 MAC tables, 63, 222

 port security, 204

 reading (Token Ring versus Ethernet), 246

 switches

Cisco, 204

MAC tables, 63

total supply, 204

- MAC (Media Access Control) layer, 31**
- management. *See* network management**
- Management Information Bases (MIBs), 279–280**
- man-in-the-middle (MiM) attacks, 212**
- MANs (metropolitan-area networks), 18–19, 60**
- matrix group (RMON), 283**
- MAUs (multistation access units), 82**
- maximum transmission units. *See* MTUs**
- media, 48**
- dependence, 244, 246
 - mixed-media networks, 244
 - network types, 11
 - physical layer, 55–56
 - shared-media networks, 219, 223
 - switches, 223
 - transitions (distribution layer), 236
- Media Access Control addresses. *See* MAC addresses**
- medium, defined, 11**
- metropolitan-area networks (MANs), 18–19, 60**
- MIBs (Management Information Bases), 279–280**
- microsegmentation, 219, 236, 247**
- MiM (man-in-the-middle) attacks, 212**
- mixed-media networks, 244–246**
- MMF (multimode fiber), 77**
- models. *See* network models**
- modulation, 11**
- modules, versus ports, 137**
- MTUs (maximum transmission units), 141**
- discovering, 142
 - fragmenting, 141
 - frames, 123
 - lowest common denominator requirement, 245–246
 - mixed-media networks, 244
- multicast (transmission method), 120**
- control, 248–249
 - protocols, 249
- multicast brute-force attacks, 214**
- multilayer switching, 130, 240**
- multimode fiber (MMF), 77**
- multistation access units (MAUs), 82**



N

NAT (network address translation), 132

native VLANs, 202

National Television Standards Committee (NTSC), 36

NBAR (Network-Based Application Recognition), 210

network, defined, 3

network adapters, 90

network address translation (NAT), 132

network addresses, 31, 90, 118

network analyzers, 284–286

network attacks, 210

ARP, 212–213

data link layer, 210

MAC flooding, 211

multicast brute-force, 214

private VLAN, 213–214

random frame-stress, 215

spanning-tree, 215

Network-Based Application Recognition (NBAR), 210

network congestion, 97

broadcast domains, 173

controlling, 31

flat networks, 223

preventing, 97

reducing

shared-media environments, 223

switches, 231

network contention, 94, 104

network convergence, 159, 164–166, 242

fast convergence, 238

STP, 239

network designs

bandwidth, 227

common

CPU adjacencies, 234

distributed routing/switching, 259

flat network topology, 227–230

fur-ball networks, 233

general principles, 253–254

hierarchical designs, 229

hierarchical topology, 232–234

Layer 2 switching, 231–232

Layer 3 switching, 237

large switched/minimal routing, 258–259

network management tools, 227

routers, 223

routing inter-VLAN traffic, 255

scalable switching, 256–257

security, 244

- software infrastructures, 224–225
- switched LANs, 237, 240
 - principles*, 254–256
 - routers/switches*, 240–246
- switched network components, 220, 223
- VLANs, 225–226, 250–253
- network infrastructure, 7**
- network interface cards. *See* NICs**
- network interface ports, 73**
- network latency, 128**
- network layer (OSI model), 65–68**
 - address space, 243
 - addresses, host identifiers, 138
 - CSMA/CD, 86
 - fragmenting packets, 142
 - hardware, 67–68
 - hierarchical topology, 237
 - interfaces (security), 203
 - multilayer switching, 130
 - packet switching, 134–135
 - ARP mapping*, 139–141
 - routing table lookup*, 135–136, 139
 - packets, 33, 66–67
 - routers, 67, 248
 - routers versus switches, 132, 135
 - switching methods, 129, 131–134
 - VLANs, 174, 180–181
- network management, 271–273**
 - configuration management, 270–271
 - fault management, 267–270
 - FCAPS model, 266
 - hierarchical topology, 234
 - inventories (software/hardware), 271
 - NOCs, 270
 - performance management, 273–275
 - port mirroring/monitoring, 284–286
 - principles, 265
 - protocols, 278
 - RMON*, 281, 284
 - SNMP*, 250, 278
 - security management, 275–278
 - SPAN, 284–286
 - tools/applications, 227
 - troubleshooting, 270
 - VLANs, 252
- network media types, 11. *See also specific types***
- network models, 21–22, 27**
 - HDM, 35
 - OSI, 21, 23, 28
- network modularity, hierarchical topology, 234**



network operations centers (NOCs), 270

network segmentation, 94

network signal carriers, physical media, 32

network standards, 21–22, 27, 36

ANSI, 37–38

de facto standards (versus), 36

E1, 38

Ethernet, 40, 89

Europe, 38

IEEE. *See* IEEE

IETF, 21

interoperability, 21

ISL, 186

ITU, 37

LANs/MANs, 39

North America, 38

proprietary features (versus), 22, 27

T1, 38

telecommunications, 37–38

Token Ring, 41, 84

VLAN tagging, 186

wireless networks, 42

network topologies, 47, 80

flat, 227–232

full-mesh, 58

hierarchical, 232–237

physical versus logical, 69, 80

ring, 60, 82

star, 59, 80–81

Token Ring, 60

tree, 60, 83–84

network types, 15–17

network utilization, performance management, 274–275

networking protocols, 48

networking rules, defined, 27

NICs (network interface cards), 73

data flow, 80

jack connections, 78

physical layer components, 50

routers, 129

VLAN interoperability, 193

NOCs (network operations centers), 270

nodes, 18

5-4-3 rule (Ethernet), 291

assigning end nodes, 174

broadcast radiation, 250

as design parameter, 228

Token Ring, 85

VLAN limitations, 174

nonblocking service, switches, 219

NTSC (National Television Standards Committee), 36

numbering systems, 91

O

object identifiers (OIDs), 280

off mode (VTP), 191

OIDs (object identifiers), 280

Open System Interconnection model. *See* OSI model

Open Shortest Path First Protocol (OSPF), 133

organizational unique identifiers (OUIs), 90, 118

originator, defined, 4

OSI (Open System Interconnection) model, 21, 23, 28

- application layer, 29, 33
- bridges, 32
- data link layer. *See* data link layer (OSI model)
- Ethernet hubs, 89
- FCAPS model (versus), 265–267
- interface tables, 89
- LANs, 49–68
- layers, 29
- network layer. *See* network layer (OSI model)
- physical layer, 32–33, 50–56
- presentation layer, 30, 33
- session layer, 30, 33

- switches, 32
- topologies, 60
- transport layer, 30, 33

OSPF (Open Shortest Path First), 133

OUI (organizational unit identifiers), 90, 118

out-of-band management ports, 207

P

packets, 66–67

- fragmenting, 142
- frames (versus), 66–67
- missing ARP entries, 141
- sequencing, 31
- switching, 134–135
 - ARP mapping, 139–141*
 - routing table lookup, 135–136, 139*

path redundancy (STP), 148

payload (frames), 12, 61–62, 117

performance management, 273–275

physical layer (OSI model), 50

- bits, 33



components

hardware, 53–55

media, 55–56

signals, 50–53

converting digital/analog signals, 52

physical media (network signal carriers), 32

physical networks, 7–8

PIM (Protocol Independent Multicast), 249

plaintext, defined, 30

point-to-point links, 97

Point-to-Point Protocol (PPP), 141

policy-based connectivity, 35

poll/response model (SNMP), 280

port-based VLANs, 177–178

ports

allocating MAC addresses, 205

configuring for ISL, 187

costs, 160

IEEE default costs, 160

switch ports, 151–152

dedicated bandwidth, 221

designated ports, 163

disabling DTP on untrusted ports,
207

inoperability (not all vendors use)
137

MAC address number limitations,
204

microsegmenting (switch ports), 247

mirroring/monitoring, 284–286

numbers of, 137, 295

port-based VLANs, 177–178

repeaters, 63

restrictive mode, 206

root switch ports, 149

security, 204–206

shutdown mode, 206

specifying age time, 205

states

blocking, 156

disabled, 159

forwarding, 159

learning, 158

listening, 157

RSTP, 166

STP, 154–160

transitioning times, 154

STP, 149

switch ports, 149–150

VLANs

managing, 207

tagging, 187

PPP (Point-to-Point Protocol), 141

presentation layer (OSI model),
30, 33

print servers, 18

private VLAN attacks, 213–214

promiscuous ports (security), 213

proprietary features, 22, 27

protocol, defined, 17

protocol delay timer, 156

Protocol Independent Multicast (PIM), 249

protocol translation, 225

protocols, 48. *See also specific protocols*

PSTN (Public Switched Telephone Network), 48

Q–R

QoS (quality of service), 127
store-and-forward switching, 127
switches, 220, 237

radio frequency interference (RFI), 56

RADIUS (Remote Authentication Dial-In User Service), 203

random frame-stress attacks, 215

Rapid Spanning Tree Protocol (RSTP), 166, 239

RARP (Reverse Address Resolution Protocol), 247

receivers, 4

reduced instruction set computing (RISC), 174

redundancy, 39
avoiding single points of failure, 253
fault management, 267
FDDI, 85
path redundancy, 147–148
ring topology, 60, 82
routers, 239
STP/RSTP, 239

regenerators, 53

Remote Authentication Dial-In User Service (RADIUS), 203

Remote Monitoring. *See* RMON

repeaters, 53, 96
5-4-3 rule (Ethernet), 291
analog versus digital, 53
bridges (versus), 98
Ethernet, 95
operation, 96
physical layer, 33
ports, 63
ring topology, 82

response times, performance management, 275

restrictive mode (ports), 206



RFI (radio frequency interference),
56

ring topology, 60, 82

RIP (Routing Information Protocol),
133

**RISC (reduced instruction set
computing), 174**

RJ (registered jack) connectors, 77

RMON (Remote Monitoring),
281–284

agents (probes)/clients, 281

groups, 282

RMON2, 284

root bridges, 149

electing, 152

priority values, 152

root ports, costs of, 160

root switches, 150

routers, 67, 110, 132, 240

address resolution, 246

ARP tables, 136

benefits, 248–250

breaking up broadcast domains, 291

bridges, 109, 242–243

broadcast control, 248–249

broadcast domains, separating 228

broadcast segmentation, 249–250

broadcast storms, 108, 243

connecting via outside networks,
109

convergence, 242

defining broadcast domain
boundaries, 172

defining VLAN boundaries, 172

deploying in network backbones,
223

determining next hop, 136

DHCP services, providing, 249

enabling WAN connections, 298

Ethernet, 109, 132

load balancing, 239

loops, 241

MAC addresses, 139

media dependence, 244–246

MTU discovery, 142

multicast control, 248–249

network designs, 223

network layer

benefits, 248

switches (versus), 132

network segmentation, 94

NICs, 129

operation, 110–111

redundancy, 239

routing platforms, 223–224

routing protocols, 133

- routing tables, 68
- security, 239, 244
- separating broadcast domains, 228
- steady-state conditions, 141
- subnetting, 243–244
- switches (versus), 109
- table lookups, 135
- versus bridges/switches, 129
- VLANs (required for), 181, 226

routes, 5

routing, 31

- forwarding decisions, 174
- tables, 68, 111
 - ARP mapping (Layer 3 switching), 139–141*
 - lookup (Layer 3 switching), 35–139*
 - routers, 135*
 - switches, 135*
- switching (versus), 174

Routing Information Protocol (RIP), 133

routing maps, maintaining, 242

routing mechanisms (VLANs), 176

routing platforms, 223–224

RSTP (Rapid Spanning Tree Protocol), 166, 239

runtless switching, 128

S

satellites, creating WANs, 48

scalability

- hierarchical topology, 235
- switches versus hubs, 228
- VLAN-based networks, 223

scalable switching (network design), 256–257

security

- AAA model, 276
- access levels, 278
- accounting, 276
- ACLs, 213
- ARP attacks, 212
- authentication, 276
- authority, 277
- authorization, 276
- basic rules, 200–203
- CAM entries, 206
- components, managing, 277
- disabling DTP, 207
- encryption, 30
- exceptions, 278
- fiber-optic cable, 76
- firewalls, 202, 225
- hubs, 293
- IDSs, 203



- limiting device connectivity, 211
- logging, 278
- MAC flooding attacks, 211
- managing, 275, 278
- message-level, 279
- MiM attacks, 212
- NBAR, 210
- network designs, 244
- network layer interfaces, 203
- physical security guidelines, 207
- policies, 277
- port security, 203–206
 - promiscuous ports*, 213
 - switch ports*, 203
 - SPAN ports*, 206
 - trunk ports*, 206
- private VLAN attacks, 213
- RADIUS, 203
- routers, 239, 244
- SNMPv2, 278
- SNMPv3, 279
- STP cable, 74
- switched networks, 275–278
- switched VLANs, 200
- switches, 210, 244
- TACACS+, 203
- tools, 203
- user sets, 275
- VLANs, 200–203, 207, 251
 - management ports*, 207
 - precautions*, 208–209
 - private VLANs*, 215
 - trunking*, 202
 - trusted versus untrusted ports*, 209–210
- VTP, 209
- WLANs, 43
- segmenting, 94**
 - bandwidth, 300
 - broadcasts, 249–250
 - network-intensive applications, 296
- segments (network)**
 - as design parameter, 228
 - broadcast storms, 243
 - Ethernet networks, 291
 - microsegmentation, 219, 247
 - ports, 221
- sender, defined, 4**
- serial numbers (network adapters), 90**
- server farms, 84, 255**
- server mode (VTP), 190**
- service level agreements (SLAs), 274**
- session layer (OSI model), 30, 33**
- SET messages (SNMP), 280**

- shared-media networks, 40, 86, 89, 219**
 - design parameters, 228
 - growing to switched networks, 237
 - switches, 223
- shielded twisted-pair (STP) cabling, 56, 74**
- shutdown mode (ports), 206**
- signals**
 - analog signals, 50
 - converting analog/digital, 52
 - digital signals, 51
 - physical layer, 50, 53
 - types, 32
- Simple Network Management Protocol. *See* SNMP**
- simplex mode, 13**
- single-mode fiber (SMF), 77**
- single-switch LANs, 81**
- SLAs (service level agreements), 274**
- slots, versus ports, 137**
- SMF (single-mode fiber), 77**
- SNMP (Simple Network Management Protocol)**
 - broadcast segmentation, 250
 - limitations, 280
 - manager/agent model, 279
 - messages, 280
 - poll/response model, 280
 - RMON MIBs, 278
 - versions, 278
- software inventory, 271**
- SONET (Synchronous Optical Network), 32**
- source, defined, 4**
- SPAN (Switched Port Analyzer)**
 - network management, 284–286
 - port security, 206
- Spanning Tree Protocol (STP), 39, 74, 147**
 - blocking state, 156–157
 - bridge priority values, 152
 - BPDU, 150
 - configuration, 154
 - convergence, 159, 239
 - disabled state, 159
 - forwarding state, 159
 - learning state, 158
 - listening state, 157
 - loops, 241
 - operation, 160
 - path redundancy, 148
 - port states, 154, 156–160
 - preventing loops, 153
 - root bridge, 149



- root switches, 150
- selecting ports, 153
- spanning-tree attacks, 215
- states, 156–159
- switches, bridge priority values, 152
- VLANs, 226
- spanning-tree algorithm, 39, 109, 147–149**
 - port-state transitions, 156
 - preventing loops, 241
 - root bridges, 149
 - switch ports, 149
- spanning-tree attacks, 215**
- standards. See network standards**
- standby state (paths), 148**
- star topology, 59, 80–81**
 - full-mesh (versus), 59
 - hubs, 96
- statistics group (RMON), 282**
- steady-state conditions, 141**
- store-and-forward method (switching), 108, 123–126, 130**
- STP (shielded twisted-pair) cabling, 56, 74**
- subnetting, 243–246**
- switch ports**
 - determining cost of, 150
 - disabling, 155
 - electing, 152
 - microsegmentation, 247
 - monitoring traffic, 284
 - security, 203
 - SPAN, 284
 - STP (port states), 155,
 - trunking, disabling 203
- switched networks**
 - addresses, reading (Layer 2 versus Layer 3), 237
 - components, 220
 - common software infrastructures, 224–225*
 - management tools, 227*
 - physical switch platforms, 223*
 - routing platform, 223*
 - VLANs, 225–226*
 - distributed routing/switching, 259
 - large switched/minimal routing, 258–259
 - managing, 265–275
 - accounting, 272–273*
 - configuration, 270–271*
 - faults, 267, 270*
 - performance, 273–275*
 - security, 275*
 - network analyzers, 284
 - network design, 237, 240, 254–256

- protocols, 278
 - RMON*, 281–284
 - RMON2*, 284
 - SMNP*, 278–281
- scalable switching, 256–257
- security, 275–278
- SPAN, 284
- topologies, 151, 154
- Switched Port Analyzer (SPAN), 206**
- switches, 8–10, 132, 240**
 - address-based VLANs, 179
 - ARP attacks, 212
 - ASICs, 237
 - backbone switches, 83
 - bandwidth, 104, 228, 237
 - benefits, 247
 - BPDUs messages, 165
 - breaking up collision domains, 291
 - broadcasts, 107, 242–243
 - campus LAN benefits, 237–238
 - collapsed backbone networks, 108
 - collision domains, breaking up, 291
 - convergence, 159, 242
 - cut-through method, 108
 - cut-through switches, 126–127
 - data link layer, 32, 63, 247
 - dedicated-media LANs, 40
 - designated ports/switches, 152
 - Ethernet, 89, 104–108
 - extending VLANs across, 184
 - filtering, 105
 - firewalls, 202, 210
 - forwarding method, 123
 - fragment-free switches, 129
 - functioning as
 - firewalls*, 202
 - multiport bridges*, 63
 - high bandwidth requirements (preferable for), 228
 - hubs (versus), 105
 - identifiers, 151
 - IDS modules, 210
 - interconnecting bridges, 109
 - LAN traffic benefits, 220
 - Layer 3 switches, 183
 - loops, 241, 150
 - MAC addresses, total supply, 204
 - MAC flooding attack, 211
 - MAC tables, 63
 - MAUs (versus), 82
 - media dependence, 244–246
 - multilayer switching, 240
 - multiport bridges, 63
 - multiswitch LANs, 83
 - network contention, 104
 - network latency, 128



- network layer
 - identifying host locations, 237*
 - routers (versus), 132*
 - network segmentation, 94
 - network topology changes, determining, 151
 - nonblocking service, 219
 - operation, 105–108
 - port costs, 152, 160
 - port numbers (multiples of two), 295
 - port security enabled on, 204
 - port states, 154
 - potential vulnerabilities, 214
 - protocols, 147
 - QoS, 220, 237
 - recomputing network topology, 159
 - removing loops, 150
 - replacing (in large networks), 234
 - RMON groups (Cisco supported), 283
 - root ports, 160
 - root switches, 150
 - routers (versus), 109
 - scalability, 228
 - scaling network growth, 301
 - security, 203, 210, 244
 - segmenting, 296
 - segmenting networks, 300
 - shared-media networks, 223
 - single-switch LANs, 81
 - star topology, 81
 - store-and-forward method, 108
 - store-and-forward switches, 124–126
 - STP, bridge priority values, 152
 - subnetting, 243–244
 - table lookups, 135
 - transparent bridges, working like, 222
 - vendors favoring over hubs, 293
 - VLANs, 247
 - communication, 176*
 - interoperability, 193*
 - management ports, 207*
 - VTP management domains, 188
 - VTP modes, 190
 - wire-speed switches, 129
 - working like transparent bridges, 222
- switching, 4**
- campus LAN benefits, 237–238
 - case studies, 291
 - bridge-based networks, 297–298*
 - hub-based networks, 292–296*

medium/large switch-based networks, 302–303
small switch-based networks, 298–301
VLANs, 303–305
 CRC, 123
 data link layer, 231–232
 data-link addresses, 118
 distributed routing/switching routing, 259
 distribution layer considerations, 258
 flat network topology (Layer 2), 231–232
 forwarding decisions, 124, 174
 fragmenting frames/packets, 141
 hierarchical topology (Layer 3), 237
 Layer 2 methods, 123–129
 Layer 3 methods, 129–135
 large switched/minimal routing, 258–259
 mixed-media LANs, 245
 multilayer switching, 130
 multiport bridges, 63
 network layer, 237
 packet switching, 134–135
 ARP mapping, 139–141
 routing table lookup, 135–136, 139

routing (versus), 174
 scalable switching, 256–257
 security, 200
 store-and-forward method, 130
 translation functions, 246
 transparent switching, 242
 trunk links, 184

Synchronous Optical Network (SONET), 32

T

T1 lines, 77

TACACS+ (Terminal Access Controller Access Control System Plus), 203

Telecommunications Industry Alliance (TIA), 75

Terminal Access Controller Access Control System (TACACS+), 203

throughput, performance management, 275

Token Ring, 84

Ethernet (versus), 41, 85
 frame sizes, 245
 interfaces, 132
 inventor, 22, 28
 Layer 2 addresses, reading 246



- logical topology, 61
- nodes, 85
- packet switching, 134
- physical topology, 61
- ring topology, 82
- RJ connectors, 78
- RMON groups, 282
- transfer rates, 85
- UTP cabling, 85

Token Ring group (RMON), 283

tokens, 41–42, 85

topologies. *See* network topologies

topology, defined, 16

traffic filtering, 225

traffic flow. *See* data flow

traffic integrity, maintaining, 224

trailers (frames), 12, 61–62, 117

transceivers, 11

transfer rates

- Ethernet, 41, 85, 89
- FDDI, 85
- Token Ring, 85

translation functions, 246

transmission

- media, 32
- methods, 118–121
- modes, 13–14

transmitters, 53

- transparent bridges (switches), 222**
- transparent mode (VTP), 190**
- transparent switching, 242**
- transport layer (OSI), 30, 33**
- TRAP messages (SNMP), 280**
- traps, fault management, 269**
- tree topology, 60, 83–84, 109**
- troubleshooting**
 - network analyzers, 284
 - network management, 270
- trunk links, 184–185**
- trunk ports (security), 206**
- twisted-pair cable, 17, 74**
 - STP, 56, 74
 - UDP, 56, 75

U

- unicast (transmission method), 119**
- unshielded twisted-pair. *See* UTP**
- user segments (Ethernet), 291**
- user sets (security), 275**
- utilization (network), 275**
- UTP (unshielded twisted-pair), 22, 75**
 - EMI/RFI, 56
 - transmission rates, 75

V

vendor-assigned addresses (MAC), 90, 118

virtual circuits, 31

virtual LANs. *See* VLANs

VLAN Trunking Protocol. *See* VTP

VLANs (virtual LANs), 225–226

80/20 rule, 255

address-based VLANs, 178–181

advantages of, 174

assigning end nodes, 174

assigning network devices, 177

benefits, 251

broadcast control, 251

broadcast domains, 172

campus networks, 303

case study, 303–305

communicating with other VLANs, 176

designing, 250–252

differentiating, 253

Ethernet, 40

extending, 184–185

hubs, replacing with switches, 173

identification numbers, 174

IEEE 802.1q, 193

implementing, 252–253

infrastructure, 225

inter-VLAN communication, 181, 184

inter-VLAN traffic, routing 255

Layer 3-based VLANs, 180

limiting node numbers, 174

logical hierarchy, 259

membership, 177–179, 181

network management, 252

node numbers, limiting 174

operation, 177–187

overview, 172–174

performance, 251

port-based VLANs, 177–178, 252

routers (required), 181, 226

routing inter-VLAN traffic, 255

routing mechanisms, 176

scalability, 223

security, 200–203, 207–215, 251

ARP attacks, 212–213

MAC flooding attacks, 211

multicast brute-force attacks, 214

private VLAN attacks, 213–215

random frame-stress attacks, 215

spanning-tree attacks, 215

trunking security, 202

segment-based VLANs, 252

segmenting, 296, 304

server farms, 225



STP, 226

switches, 247

- designated switches*, 152
- management ports*, 207
- replacing hubs with*, 173

tagging, 186–187

topology, 175–176

trunk links, 184

types, 177–180

user communities, segmenting 304

virtual-subnet VLANs, 252

well-behaved VLANs, 255

voice over IP (VoIP), 220

voluntary standardization (ANSI), 38

VTP (VLAN Trunking Protocol), 188–190

- advantages, 190
- advertisements, 192
- exchanging VLAN information, 226
- modes, 190–191
- pruning, 192, 208
- security, 209
- switches, 188

W–X

wall plates/boxes, 79

WANs (wide-area networks), 19, 48

- bridges versus routers, 298
- connecting LANs, 297
- dark fiber, 49
- LANs (versus), 48–49
- serial interfaces (required), 132
- routers, 67

WAPs (wireless access points), 305

wave-division multiplexing (WDM), 47, 60

websites

- ANSI, 45
- IEEE, 45
- ITU-T, 44

wide-area networks. See WANs

wireless access points (WAPs), 305

wireless networks, 11, 17, 42–43

- media, 55
- security, 43
- WAPs, 305

Xerox, 22, 28