

Numerics

3DES, 110

802.1x, 80

A

A/D(analog to digital conversion), 42

 Nyquist Theorem, 43

 oversampling, 42

 quantization, 43

access layer, 187-188

access methods

 of ISDN, 203

 of SANs, 232

ACF/VTAM (Advanced Communication Facility/Virtual Telecommunication Access Method), 253

active attacks, 85

addressing, DECnet, 248

aggregation layer (data centers), 226

aliasing, 42

anarchists, 86

AppleTalk, 248

application layer, 6

 data centers, 226

 IP telephony systems, 37–39

applications of ECDN infrastructure, 25

APs (access points), 139

 roaming, 140, 142

 rogue, 86

arbitrated loop topology (fiber channel), 232

architecture of MPLS, 217

ATM (Asynchronous Transfer Mode),

 208-209, 212

 asynchronous transmission, 212

 connections, 213

 devices, 212

 fixed cell size, 213

 network interfaces, 212

 virtual channels, 213

AToM (Any Transport over MPLS), 217

attacks, 85

 DoS, 86

authentication, 74

 802.1x, 80

 EAP, 80

 RADIUS, 83

authorization, 74

availability, 153

 content availability, 241

 factors affecting, 156

 five 9s, 153

 measuring, 156

 of carriers, 157

 of software, 157

B

back doors, 86

back-end layer (data centers), 226

backbone, 187

backing up data, 150

bandwidth

 provisioning, 168

 traffic shaping, 171

 voice data compression, 43

Banyan VINES, 249

bastion hosts, 96

BECN (backward explicit congestion notification), 211

best routes, 134

block retrieval, 234

bottlenecks, 240

BPDUs (Bridge Protocol Data Units), 179, 183

BRI (basic rate interface), 199, 203

bridges, 118–120, 123, 129

 wireless, 143

broadband, 199–201

 cable, 202

 cable modems, 199

 DSL, 200-202

 evolution of, 199

 ISDN, 199

broadcast domains, 125
 broadcast storms, 181
 browsers, caching, 244
 building-to-building wireless bridges, 143
 business continuance plans, 147
 backing up data, 150
 restoring primary systems, 150
 risk assessment, 147, 149
 business resiliency, 148

C

cabling, 202
 cable modems, 199
 versus DSL, 200
 CAC (call admission control), 38
 caching, 240, 243
 call centers
 IPCCs, 45–47
 outbound, 46
 ACD, 46
 call flow, 48
 components, 47
 inbound, 45
 IVR, 46
 call processing layer (IP telephony systems), 39–39
 campus network design, 187, 190
 VLANs, 189

carrier availability, 157
 cells, 213
 centralized deployment model, 37
 centralized policy-management tools, 73
 CGMP (Cisco Group Management Protocol), 62
 chromatic distortion, 197
 circuit-switched WANs, 207
 classification, 170
 classifying routing protocols, 135–136
 distance-vector, 136
 link-state, 136
 routing algorithms, 176–177
 clean net, 96
 client layer (IP telephony systems), 35, 39
 CM (call manager), 47
 CMTS (cable modem termination system), 202
 collision domains, 119, 125
 segmentation, 120
 collisions, 124
 comfort noise, 43
 compression of voice data, 43
 congestion notification methods of Frame Relay, 211
 connection-oriented protocols, 14
 connectionless protocols, UDP, 15
 connections, ATM, 213
 content distribution and caching, 26
 content manager, 241
 content networking, 239–240
 caching, 243–244
 content switching, 239–241
 equipment, 240
 mirror sites, 240
 content switching, 239
 control plane (MPLS), 105, 217
 convergence, 157
 benefits of, 53
 RSTP, 183
 core layer, 187–188
 CPR (customer premise equipment), 216
 crackers, 86
 CSU/DSU, 209
 CTI (computer telephony integration) servers, 47
 CWDM, 196

D

DAD (Duplicate Address Detection), 21
 DARPA (Defense Advanced Research Projects Agency),
 development of Internet protocols, 13

- DAS (directly attached storage), 231–233
JBOD, 231
- data centers**, 223–225
facilities, 227
Internet server farms, 225
layers, 224–226
management services, 227
n-tier model, 226
security, 227
storage methods, 227
- data conferencing**, T.120 protocols, 68
- data link layer**, 6
- data plane (MPLS)**, 105, 217
- data privacy**, 77
- datagrams**, 14
- DCE (data communication equipment)**, 210
- DDoSs (distributed denial-of-service attacks)**, 86
- DDR (dial-on-demand routing)**, 207
- de-encapsulation**, 8
- DECnet**, 248
- delay**, 168–169
- dense mode (PIM)**, 60–62
- depletion of IP addresses**, IPv6 as solution, 20
- deploying fiber-channel topologies**, 232
- deployment models**, IP telephony, 37
- DES (data encryption standard)**, 110
- designing**
campus networks, 187–190
highly available networks, 153
optical networks, 197
- desktop protocols**, 247, 250–251
- development**
of desktop protocols, 247
of Ethernet, 118–119
of new technologies, open versus proprietary systems, 5
- devices**
ATM, 212
bridges, 118–120, 129
 wireless, 143
caching, 244
collision domains, 125
content networking equipment, 240
CSU/DSU, 209
Frame Relay equipment, 210
hot-swappable, 156
hubs, 120
modems, 209
MPLS, 216
repeaters, 120, 123
routers, 120, 130
switches, 129
- dial plans**, 36
- Diffie-Hellman key exchange**, 110
- digital signatures**, 74
- directory gatekeepers**, 69
- disaster recovery**, 147–149
backing up data, 150
business resiliency, 148
preparedness testing, 148
restoring primary systems, 150
risk assessment, 147, 149
- distance accumulation**, 136
- distance limitations of WLANs**, 139
- distance vector routing protocols**, 136, 177
network discovery, 136
- distributed deployment model**, 37
- distribution layer**, 187–188
- distribution trees**, 61
- DLCI (Data Link Connection Identifiers)**, 211
- DMZs (de-militarized zones)**, 96
- DNS (Domain Name System)**, 13
- documentation, network management**, 161–162
- DoS attacks**, 86
- dotted decimal notation**, 17
- DPM (defects per million)**, 156
- DPT (dynamic packet transport)**, 194
- DSL (digital subscriber line)**, 200–202
- DSS (Digital Signature Standard)**, 110
 Diffie-Hellman key exchange, 110

DSSS (Direct Sequence Spread Spectrum), 142
 DTE (Data Termination Equipment), 210
 duplicate frame transmission, handling, 181
 DWDM (Dense Wavelength Division Multiplexing), 196
 dynamic NAT, 21
 dynamic routes, 134
 dynamic routing algorithms, 176

E

e-learning, 25, 27
 content distribution and caching, 26
 ECDNs, 27
 interactive multimedia, 28
 live media streaming, 28
 media on demand, 26
 VC, 26–28, 65, 68
endpoints, 68
H.323, 65, 68
T.120, 68
zones, 69
 versus traditional classroom learning, 25
 EAP (Extensible Authentication Protocol), 80
 ECDNs (Educational Content Delivery Networks), 25–27
 ELSRs (edge label switch routers), 216

encapsulation, 8, 55. *See also MPLS*
 GRE, 54, 104
 encryption, 109–110
 endpoints, 68
 establishing TCP/IP connections, 14
Ethernet, 117, 119
 bridges, 118
 collision domains, 119
 development of, 118–119
 Gigabit Ethernet, 195
 history of, 117
 hubs, 118
 segmentation, 120
 segments, 120
 switched Ethernet, 120
 switching, 123
evolution
 of broadband technologies, 199
 of Ethernet, 118
extranet server farms, 225

F

fat clients, 247
FCAPS (fault, configuration, accounting, performance, security), 161, 164
FCIP (Fiber Channel over IP), 232

FECN (forward explicit congestion notification), 211
FEC (forward error correction), 217
fiber channel, 232–234
fiber-based metro networks, 193
 DWDM, 194
 SONET, 193
filtering, 126
firewalls, 93, 95
 Bastion hosts, 96
 functionality, 95
 inside filters, 96
 outside filters, 96
five 9s, 153
flat networks, 135, 176
flooding, 123, 126
forwarding state (STP), 180
Frame Relay, 208–210
 congestion notification, 211
 DLCI, 211
 equipment, 210
 LMI, 211
 VCs, 210
PVCs, 211
SVCs, 210
frame transmission modes, 126

frames, 126
handling duplicate transmissions, 181
front-end layer (data centers), 226
full duplex transmission, 118, 124

G

gateways, IP telephony, 36
Gigabit Ethernet, 195-196
GK (gatekeeper), 68
good inbound packets, 95
good outbound packets, 95
GRE (generic route encapsulation), 54, 104

H

H.323, 65, 68
hackers, inside jobs, 86
half duplex Ethernet, 118
hash, 110
hierarchical networks, 135, 176
 layers of, 188
high availability, 156-157, 189
 factors affecting, 156
 five 9s, 153

high-speed Internet access, 199
 cable modems, 199
 DSL, 200-202
history of Ethernet, 117
hit-and-run attacks, 85
host-intelligent routing algorithms, 176
hot-swappable devices, 156
HSSI (High-Speed Serial Interface), 208
HTTP (Hypertext Transfer Protocol), caching, 244
hubs, 118, 120

I

ICM (intelligent contact management), 47
identifying subnet addresses, 18
identity-based security, 73, 76, 81
 PKI, 83
IDSs (intrusion detection systems), 94
IGMP (Interior Gateway Management Protocol), 61
IGMP snooping, 62
IKE (Internet Key Exchange), 102
in-building WLANs, 141
inbound call centers, 45
infrastructure layer (IP telephony systems), 36, 39
inside filters, 96

intelligent rerouting, 217
interactive multimedia, 28
interdomain routing algorithms, 135, 177
interleaving, 168, 171
Internet
 high-speed access, 199
 cable modems, 199
 DSL, 200-202
 security, 74
 server farms, 225
intradomain routing algorithms, 135, 177
intranet server farms, 225
IP addressing, 13, 17
 address classes, 17
 convergence, 53
 DNS, 13
 dotted decimal notation, 17
 IPv6, 20
 address hierarchy, 21
 security features, 21
 stateless autoconfiguration, 21
 versus IPv4, 20
 MAC addresses, 17
 static addresses, 13
 subnet addresses, identifying, 18
 subnet masks, 18
 subnetting, 18

IP multicast, 59–61
 CGMP, 62
 distribution trees, 61
 IGMP, 61
 Layer 2 multicast, 62
 multicast forwarding, 62
 PIM, 59, 62
dense mode, 60
sparse mode, 60

IP telephony, 38
 application layer, 37, 39
 benefits of, 35
 CAC, 38
 call processing layer, 36, 39
 client layer, 35, 39
 deployment models, 37
 dial plans, 36
 gateways, 36
 infrastructure layer, 36, 39
 placing calls, 39
 QoS, 39
 toll bypass, 38
 versus traditional telephony, 38
 voice/data convergence, 35

IPCCs, 45, 47
 ACD, 46
 call flow, 48
 components, 47
 inbound, 45
 IVR, 46
 outbound, 46

IPSec, 105
 IKE, 102
 VPNs, 101
IPv6, 20
 address hierarchy, 21
 DAD, 21
 security features, 21
 stateless autoconfiguration, 21
 versus IPv4, 20
IPX (Internetwork Packet Exchange), 249
ISCSI (Internet Small Computer Systems Interface), 234
ISDN (Integrated Services Digital Network), 203
 access methods, 203
 call establishment, 204
 SPIDs, 204
isolation LANs, 96
IVR (interactive voice response), 46–47

J–K

JBOD (just a bunch of disks), 231, 234
jitter, 168–169

L
labels (MPLS), 216
LANs. *See also WLANs*
 Ethernet, 117
bridges, 118
development of, 118
history of, 117
hubs, 118
segmentation, 120
 switching, 123
 large campus network design, 190
 last mile, 201
Layer 2 multicast, 62
Layer 2 to Layer 3 mapping, 189
layers
 of data centers, 224, 226
 of hierarchical networks, 188
 of OSI model, 6–7
communication between, 8
encapsulation, 8
encryption, 111
 of TCP/IP protocol stack, 14
LDP (Label Distribution Protocol), 216
learning state (STP), 180
legacy networks, IP convergence, 53
LFI (link fragmentation and interleaving), 171
link fragmentation, 168

link-state routing protocols, 136, 177
 listening state (STP), 180
 live media streaming, 28
 LMI (local management interface), 211
 load balancing, content switching, 239
 loop-free topologies
 BPDUs, 179
 STP, 179
 port states, 180
 root port election, 180
 loss, 169
 LSRs (label switch routers), 216

M

MAC addresses, 17
 address learning, 126
 database instability, 182
 mainframes, thin clients, 247
 measuring availability, 156
 media on demand, 26–28
 medium campus network design, 190
 Metcalfe, Robert, 117
 metrics, 134
 path determination, 175–176
 metro optical layer (data centers), 226

metro optical networks, 193–195
 CWDM, 196
 designing, 197
 DWDM, 194–196
 Gigabit Ethernet, 195
 SONET, 193, 196
 migration of SNA networks to IP-based networks, 253–254
 mirror sites, 240
 modems, 209
 monitoring networks, 158
 MPLS (Multiprotocol Label Switching), 105
 architecture, 217
 AToM, 217
 equipment, 216
 FECs, 217
 intelligent rerouting, 217
 labels, 216
 security, 216
 traffic engineering, 215–217
 VPN support, 215
 VPNs, 217
 MST (Multiple Spanning Tree), 179
 multicasting, 59, 61
 CGMP, 62
 distribution trees, 61
 IGMP, 61
 Layer 2 multicast, 62
 multicast forwarding, 62
 PIM, 59–62
 multimode fiber, 197

multipath routing algorithms, 176

multiplexing, 197, 212

multisite deployment model, 37

N

n-tier model, 223, 226
 NAS (network attached storage), 227, 235
 NAT (Network Address Translation), 21
 NetWare, SAP, 249
 network layer, 6
 switching, 130
 network management, 161
 documentation, 161–162
 FCAPS, 161, 164
 protocols, 162
 SNMP, 162
 network uptime, 153
 next hop, 130–131, 175
 nodes (AppleTalk), 248
 NOSs (network operating systems), 247
 AppleTalk, 248
 DECnet, 248
 fat-clients, 247
 Novell NetWare, 249
 XNS, 247
 Novell NetWare, 249
 Nyquist Theorem, 43

O

OAM&P (operation, administration, maintenance, and provisioning), 36
 open systems versus proprietary systems, 5
 optical networks, 193
 DWDM, 194
 CWDM, 196
 designing, 197
 DWDM, 196
 Gigabit Ethernet, 195
 metro optical, 195
 multimode fiber, 197
 single-mode fiber, 197
 SONET, 193, 196
 OSI reference model, 7
 communication between layers, 8
 encapsulation, 8
 ISO, development of OSI model, 5
 layers of, 6
 outbound call centers, 46
 outside filters, 96
 overloading, 21
 oversampling, 42
 oversubscription, 189

P

packet analyzers, 163
 packet switching, 175, 207
 packets
 flooding, 126
 interleaving, 171
 queuing, 167
 scheduling, 167
 PARC (Palo Alto Research Center), 119
 passive attacks, 85
 PAT (Port Address Translation), overloading, 21
 path determination, 175–176
 PBXs (private branch exchanges), 38
 OAM&P, 36
 performance
 bottlenecks, 240
 QoS, 167–169
 traffic shaping, 171
 perimeter security, 73, 76
 Perlman, Radia, 183
 PG (peripheral gateway), 47
 physical layer, 6
 PIM (Protocol Independent Multicast), 59–62
 dense mode, 60
 sparse mode, 60
 ping, 162

PKI (public-key infrastructure), 83

planning for disaster recovery, 147

point-to-point connections, 102

point-to-point WANs, 207

policy management, 73, 76

port states (STP), 180–182

POTS (plain old telephone service), migration to IP telephony, 35

presentation layer, 6

PRI (primary rate interface), 203

proprietary systems versus open systems, 5

provisioning, 168–170

PSTNs (public-switched telephone networks), 38

PVCs (permanent virtual circuits), 207, 211
 ATM, 213

Q–R

QoS (quality of service), 39, 167–169
 on VoIP networks, 42
 traffic shaping, 171
 quantization, 43
 queuing, 167

RADIUS (Remote Authentication Dial-In User Service), 83

RAID (redundant array of inexpensive disks), 234

reducing security threats, 93

redundancy, 189

cost of, 157

of servers, 158

STP, 179, 181

BPDUs, 183

path recalculation, 183

port states, 182

remote attacks, 85

remote-access VPNs, 103

repeaters, 120, 123

retrieving stored data, 234

RFCs (requests for comments), 13

risk assessment, 147–149

roaming, 140–142

rogue APs, 86

root port election (STP), 180

router-intelligent routing algorithms, 176

routers, 120, 130

routing

AppleTalk traffic, 248

best routes, 134

content routing, 241

interdomain versus intradomain, 135

metrics, 134

next hop, 130–131

updates, 130

routing protocols

distance-vector, 136

link-state, 136

metrics, path determination, 175–176

packet switching, 175

routing tables, 175

RP (rendezvous point), 60

RSTP (Rapid Spanning Tree Protocol), 179, 183

RTMP (Routing Table Maintenance Protocol), 248

S

sampling, 42

Nyquist Theorem, 43

SANs (storage area networks), 227, 231–235

access methods, 232

JBOD, 231, 234

tunnels, 232

SAP (Service Advertising Protocol), 249

scheduling, 170

scheduling packets, 167

script kiddies, 86

SCSI (small computer system interface), 234

security

802.1x, 80

attacks, 85–86

authentication, 74

EAP, 80

RADIUS, 83

authorization, 74

data privacy, 77

encryption, 109

DES, 110

DSS, 110

features of IPv6, 21

firewalls, 93–95

hackers, 85

identity-based, 76, 81

PKI, 83

IDSs, 94

inside jobs, 86

Internet, 74

IPSec, 105

VPNs, 101

monitoring, 73

MPLS, 216

of data farms, 227

on wireless networks, 74

perimeter security, 76

policy management, 73

- potential threats, 73
rogue APs, 86
threats to, 77
back doors, 86
reducing, 93
tunneling, 54
versus trust, 76
- segments, 120
- serialization delay, 213
- server farms, 223–225
facilities, 227
layers, 224
management services, 227
n-tier model, 226
security, 227
storage methods, 227
- servers
cache servers, 243
redundancy, 158
- session layer, 6
- shared trees, 61
- single-mode fiber, 197
- single-path routing algorithms, 176
- single-site deployment model, 37
- site-to-site VPNs, 103
- small campus network design, 190
- SNA (Systems Network Architecture), 253–254
sniffing, 86
- SNMP (Simple Network Management Protocol), 162
- software availability, 157
- SONET (Synchronous Optical Network), 193, 196
- source trees, 61
- sparse mode (PIM), 60–62
- SPIDs (service provider identifiers), 204
- spoofing, 86
- stateless autoconfiguration (IPv6), 21
- static, comfort noise, 43
- static IP addressing, 13
- static NAT, 21
- static routes, 134
- static routing algorithms, 176
- storage layer (data centers), 226
- storage networking, 233
fiber channel, 234
iSCSI, 234
JBOD, 231, 234
NAS, 235
RAID, 234
retrieval methods, 234
SANs, 231, 235
SCSI, 234
- STP (Spanning Tree Protocol), 179–181
BPDUs, 179, 183
functionality, 182
MSTP, 179
path recalculation, 183
port states, 180–182
root port election, 180
- subnet addresses, identifying, 18
- subnet masks, 18
- subnetting, 18
- SVCs (switched virtual circuits), 207, 210
ATM, 213
- switch fabric topology, 232
- switched Ethernet, 120
- switching, 123, 129–130
address learning process, 126
broadcast domains, 125
content switching, 239, 241
filtering, 126
flooding, 126
frame transmission modes, 126
VLANs, 124, 127
- synchronous data mirroring, 150
- synchronous transmission, 208

T

T.120 protocols, 68

TCP (Transmission Control Protocol)

- port numbers, 15
- sniffing, 86

TCP/IP, 14

- connection establishment, 14

- datagrams, 14

- IP addressing, 13, 17

 - address classes*, 17

 - convergence*, 53

 - subnetting*, 18

- TCP windowing, 15

- UDP, 14-15

TDM (time-division multiplexing), 194, 197, 212

thin clients, 247, 251

threats to security, 73, 77

- back doors, 86

- hackers, 85

- inside jobs, 86

- reducing, 93

- rogue APs, 86

- trojan horses, 86

- viruses, 86

- worms, 86

toll bypass, 38

ToS (type of service), 167

traffic engineering, 215-217

traffic shaping, 171

training, importance of, 158

translational bridging, 118

transmission paths, 213

transport layer, 6

traps (SNMP), 162

trojan horses, 86

trust versus security, 76

tunneling, 53-55, 103

- GRE, 54, 104

- IP-based SAN tunnels, 232

- security benefits, 54

video on demand, 28

virtual channels, 213

virtual paths, 213

viruses, 86

VLANs (virtual LANs), 124, 127, 189

VoIP (Voice over IP)

A/D

- oversampling*, 42

- quantization*, 43

- aliasing, 42

- comfort noise, 43

- IPCCs, 45

 - outbound*, 46

 - ACD, 46

 - inbound*, 45

 - IVR, 46

- QoS standards, 42

- voice compression, 43

VPNs (virtual private networks), 103

- benefits of, 103

- IPSec-based, 101

 - connectivity*, 101

 - MPLS, 105, 215

 - remote-access, 103

 - site-to-site, 103

 - tunneling, 103

U-V

UDP (user datagram protocol), 14-15

updates, 130

VC (videoconferencing), 26-28, 65, 68

- endpoints, 68

- H.323, 65, 68

- T.120, 68

- zones, 69

VCs (virtual circuits), 210

- DLCI, 211

- PVCs, 211

- SVCs, 210

W**WANs**

ATM, 208-209, 212
asynchronous transmission, 212
connections, 213
devices, 212
fixed cell size, 213
network interface, 212
virtual channels, 213
dialup services, 207
Frame Relay, 208, 210
congestion notification, 211
DLCI, 211
equipment, 210
LMI, 211
VCs, 210-211
HSSI, 208
transport types, 207

WDM (wave-division multiplexing), 194, 197**web pages, caching**, 244**well-known port numbers**, 15**windowing**, 15**wireless networks**

bridges, 143
rogue access points, 86
security, 74

WLANs (wireless LANs), 139–141

APs, 139
benefits of, 139
distance limitations, 139
DSS, 142
in-building, 141
roaming, 140, 142
security issues, 143

worms, 86**X-Z****XNS (Xerox Network Systems)**, 247**zones**, 69