

Index

Numerics

- 3DES (Triple Data Encryption Standard), 118
- 802.1q protocol, 43
- 802.1x standard, 140
- 802.11i standard, 141

A

- AAA (Authentication, Authorization, and Accounting), 121
- access attacks, 106
- access layer (hierarchical network design), 16–17
 - design considerations, 53–54
- access points
 - autoconfiguration option, 144
 - integrated access points, 135
 - WAPs, 135
- accounting management, 216
- acknowledgments, 322
- address overloading, 63
- addresses, 329
 - BIAs, 329
 - classful, 334
 - IP, 331
 - ANDing*, 63
 - classes*, 332
 - private addresses*, 333
 - subnets, calculating*, 64–66
 - logical, 331
 - network layer, 331
 - physical, 331
- ad-hoc networks, 136
- advanced distance vector routing protocols, BGP neighbors, 93
- AES (Advanced Encryption Standard), 118

- AF (Assured Forwarding) PHB, 158
- AirDefense, 141
- analog signals, digitization, 175
- ANDing IP addresses, 63
- anycast IPv6 addresses, 246
- application layer (TCP/IP protocol suite), 316
- ARP (Address Resolution Protocol), 323
- ASBRs (Autonomous System Boundary Routers), 89
- attacks
 - access attacks, 106
 - DoS attacks, 108–109
 - information disclosure attacks, 107
 - reconnaissance attacks, 106
- authentication, 121
 - shared-key, 139
- authenticity, 120
- autoconfiguration option for WAPs, 144
- AutoQoS, 167–168
- availability, 239–241
 - decreasing downtime, 240
 - five nines, 239

B

- backbone (IS-IS), 91
- BackboneFast, 40
- bandwidth, 79
 - domains, 313
 - of signaling traffic, 188
 - requirements for voice traffic, 185
- base 10 numbers, 343
- base 2 numbers, 345
- BE PHB (best effort per-hop behavior), 158
- bearer traffic, 177

best practices

- for network management, 228
- for network security, 124
 - network management, 124*
 - security policies, implementing, 125*

best-effort service, 149, 177

BGP (Border Gateway Protocol)

neighbors, 93

BHT (busy-hour traffic), 185

- calculating, 186

BIAs (burned-in addresses), 31, 329

binary numbers

- converting to decimal, 345–347
- decimal-to-binary conversion chart, 341
- IP addresses, ANDing, 63

black-box hackers, 104

Blaster worm, 103

blocking state, 38

block-oriented access, 244

Bluetooth, 135

botnets, 110

bottom-up approach to network design, 12

BPDU (bridge protocol data units), 37

- configuration BPDUs, 38

bridges, 29, 313–314

- comparing to switches, 314

broadcast domains, 313

broadcast storm, 35

built-in Catalyst security, 51

business case

- for CN, 197
- for data and voice network convergence, 173–174
- for QoS, 149–151

C

CA (certificate authority), 123

caching, 200

calculating

- available host addresses per subnet, 335
- BHT, 186
- device addresses per subnet, 67
- hosts per subnet, 65–66
- OSPF cost, 90
- subnet addresses, 63–66
- summary routes, 70
- trunk capacity, 186–188
- VLSMs, 72–74

call control traffic, 177

call processing, 176, 181

CAM (content-addressable memory), 31

candidate entries, 48

CAR (committed access rate), 162

case studies, Venti systems, 265–266

- background information and context, 253, 256
- branch office, 270
- e-mail, 283–284
- future considerations, 291
- head office, 267–270
- IP addressing, 281–283
- network management, 289–290
- network requirements, 257–263
- QoS and voice, 284, 288
- remote users, 271
- security, 275–281
- servers, 273
- switching, 273–275
- wireless, 288

Catalyst switches, 33, 51–53

- hardware security, 53
- native security, 51

- CBWFQ (class-based weighted fair queuing), 165–166**
- CCSs (Centum call seconds), 185**
 - BHT, calculating, 186
- CDNs (content delivery networks), 197**
 - components of, 198
 - content caches, 200–203*
 - content engine, 199–200*
 - content distribution and management, 207–208
 - content routing, 204
 - direct mode, 205*
 - WCCP mode, 206–207*
 - content switching, 208
- CEF (Cisco Express Forwarding), 47–49**
- CGMP (Cisco Group Management Protocol), 236**
- channels, 207**
- CIS (Catalyst integrated security), 50**
- Cisco AutoQoS feature, 167–168**
- Cisco Enterprise Composite Network Model, 15, 18, 125–127**
 - Enterprise Campus Functional Area, 20
 - Enterprise Edge Functional Area, 23
 - Service Provider Edge Functional Area, 24
- Cisco Integrated Wireless Network, 142**
- Cisco IOS traffic policing, 162**
- Cisco IOS traffic shaping, 163**
- Cisco MeetingPlace, 182**
- Cisco NetFlow, 223**
- Cisco Network Assistant, 227**
- Cisco Network Management Framework, 226–227**
- Cisco Personal Assistant, 182**
- Cisco QoS Baseline, traffic classes, 160–161**
- Cisco SAFE Blueprint, 125, 128**
- Cisco Unity, 182**
- CiscoWorks, 225**
- Class A addresses, 333**
- Class C addresses, 333**
- Class D addresses, 333**
- class-based shaping, 163**
- classes of traffic in Cisco QoS Baseline, 160–161**
- classful addressing, 334**
- classful routing protocols, 68, 77**
- classification, 155–156**
- classifying routing protocols, 75**
- classless routing protocols, 77**
- CNs (content networks)**
 - business case for, 197
 - designing
 - for providing live video to corporations, 210–211*
 - for school curricula, 209*
 - on-demand content, 207
 - pre-positioned content, 207
 - services provided by, 198–199
- Code Red worm, 102**
- collapsed backbone, 54**
- collecting management information**
 - Cisco NetFlow, 223
 - RMON, 220–222
 - extensions, 222–223*
- collision domains, 313**
- combo malware, 102**
- commands**
 - directed broadcast, 315
 - ip directed broadcast, 41
- common-use networks, 60**
- comparing**
 - bridges and switches, 314
 - routing protocols, 82–83
- components of MLS, 47**
- compression techniques, 182**
 - cRTP, 184
- concatenating IP addresses, ANDing, 63**
- confidentiality, 117, 120**
- configuration BPDUs, 38**
- configuration management, 216**
- congestion management, 164–166**
- congestion-avoidance techniques, 164**
- connectionless unreliable transport, 307**
- connectivity, devices**
 - bridges, 29, 313–314
 - hubs, 313
 - switches, 29, 313–314
- content caches**
 - nontransparent caching, 201–202
 - reverse proxy caching, 203
 - transparent caching, 200–201
- content distribution and management, 198, 207–208**
- content engines, 198–200**
 - in nontransparent mode, 203
 - pre-positioned content, 207

content filtering, 117
content routing, 198, 204
 direct mode, 205
 WCCP mode, 206–207
content switching, 199, 208
contingency plans for network deployment, 13
control traffic, 177
Controlled Load Service, 154
converged networks, 80, 150, 174
 bandwidth requirements for voice traffic, 185
 digitization, 175
 IP telephony
 call processing, 181
 components of, 179
 infrastructure, 179
 IP phones, 180
 video telephony, 181
 voice applications, 181
 voice gateway, 182
 QoS, 177
 security, 192
 IP telephony issues, 191
 platform security issues, 191
 signaling traffic bandwidth, 188
 trunk capacity, calculating, 186–188
 voice compression, 182–184
 VoIP, components of, 178–179
convergence time, 80
conversation traffic, 177
converting
 binary to decimal, 345–347
 decimal to binary, 341–343, 347
core layer (hierarchical network design), 16–18
 design considerations, 53–54
cost, 37, 80
 calculating, 90
CQ (custom queueing), 165
cracking, 103
cRTP (RTP header compression), 184
CS (Class Selector) PHB, 158
CSA (Cisco Secure Agent), 116

D

DAS (directly attached storage), 242
data and voice network convergence, business case for, 173–174
data link layer, 305
data networks, 302
 analog signals, digitization, 175
 convergence, 174
 QoS requirements, 152–153
datagrams, 306–307
DDoS attacks, 109
decimal-to-binary conversion, 341–343, 347
decreasing network downtime, 240
definition of design, 5–7
dejitter buffers, 151
delay, 79
dense mode (PIM), 238
deployment planning, 12–13
DES (Data Encryption Standard), 118
design, definition of, 5, 7
designated ports, 37
designing CNs
 for providing live video to corporations, 210–211
 for school curricula, 209
design-related vulnerabilities, 105
developing final network design, 12
device addresses per subnet, calculating, 67
devices
 bridges, 29, 313–314
 comparing to switches, 314
 hubs, 313
 IP phones, 180
 routers, 314–315
 switches, 29, 313–314
 Layer 2, 31–33
 Layer 3, 33
 learning process, 32
 trunks, 42
 wireless client devices, 136
 laptops, 136
 PDA's, 136
 user workstations, 136
 wireless IP phones, 137
 wireless IP phones, design considerations, 145
DiffServ, 154
digitization, 175

- direct mode (content routers), 204**
- directed broadcasts, 40, 315**
- directed-broadcast command, 315**
- directly connected routes, 74, 327**
- distance vector routing protocols, 75**
 - split-horizon rule, 76
- Distribution Coordination Method, 134**
- distribution layer of hierarchical network design, 16–17**
 - design considerations, 53–54
- DNS race processes, 204**
- documentation, maintaining, 13–14**
- domains (IS-IS), 91**
- DoS attacks, 108–109**
- dotted decimal notation, 331, 345–347**
- DSCP (DiffServ Code Point) bits, 159**
- DSP, 183**
- DTS (Distributed Traffic Shaping), 163**
- DUAL (Diffusing Update Algorithm), 86**
- dumb terminals, 301**
- dynamic packet filtering, 113–114**

E

- EBGP (external BGP), 94**
- ECN (explicit congestion notification), 164**
- Edge Distribution module, 22**
- EF (Expedited Forwarding) PHB, 158**
- EGPs (external gateway protocols), BGP neighbors, 93**
- EIGRP, 86–88**
 - DUAL, 86
 - query messages, 87
- email filtering, 117**
- embryonic connections, 109**
- enabler entries, 49**
- encryption, 117**
 - DES, 118
 - encrypted VPNs, 119
 - file encryption, 121
 - hashing, 120
 - SSL, 121
- end-to-end QoS, 153**
- EIGRP (Enhanced Interior Gateway Routing Protocol), 86**
- Enterprise Composite Network Model, 18**
 - Enterprise Campus Functional area, 20
 - Management Module, 230–232*

- Enterprise Edge Functional Area, 23
- Service Provider Edge Functional Area, 24
- equal-cost load balancing, 80**
- Erlangs, 185**
- ES (end systems), 91**
- Ethernet**
 - collision domains, 313
 - routers, 315
- EUI-64 format interface ID, 247**
- expectational acknowledgments, 321**
- extending IP addresses, job aids, 341**
- extensions (RMON), 222–223**
- exterior routing protocols, 75**

F

- false positives, 116**
- Fast Secure Roaming, 143**
- fault management, 216**
- FCAPS (fault, configuration, accounting, performance, and security management), 216**
- FCIP (Fibre Channel IP), 244**
- FIB (Forwarding Information Base), 50**
- fields**
 - in IPv6 header, 245
 - in IP datagrams, 324–325
- file encryption, 121**
- filtering, 32**
- final design, developing, 12**
- five nines availability, 239**
- fixed delays, 150**
- flash updates, 81**
- flat routing protocols, 77**
- forwarding unicast packets, 315**
- forwarding state, 37**
- four-way handshakes, 322**
- FRTS (Frame Relay Traffic Shaping), 163**
- FTP (File Transfer Protocol), data encapsulation/decapsulation, 336–338**

G

- GLBP (Gateway Load Balancing Protocol), 242**
- global unicast addresses, 246**
- GoS (grade of service), 185**
- GTS (Generic Traffic Shaping), 163**
- Guaranteed Rate Service, 153**

H

hackers, 103
 white-hat, 104

half-open connections, 109

hashing, 120

header format of IPv6 packets, 245–246

HIDSs (host-based IDSs), 116

hierarchical IP address design, 67–68

hierarchical network design model, 15
 access layer, 17
 core layer, 18
 design considerations, 53–54
 distribution layer, 17
 limitations of, 18

hierarchical routing protocols, 77

high-complexity codecs, 183

HomeRF, 135

hop count, 79

host addresses, 63
 per subnet, calculating, 65–66, 335

HSRP (Hot Standby Routing Protocol), 241

hubs, 313

hybrid routing protocols, 75

I

I Love You virus, 102

IBGP (internal BGP), 94

ICMP (Internet Control Message Protocol), 323

identity management
 AAA, 121
 NAC, 122
 PKI, 123–124

IDSs (intrusion detection systems)
 AirDefense, 141
 host-based, 116
 network-based, 114
 target-based, 116

IEEE 802.1q protocol, 43

IGMP (Internet Group Management Protocol), 236

IGPs (interior gateway protocols), 75

IGRP (Interior Gateway Routing Protocol), 84–85

implementation-related vulnerabilities, 105

implementing
 MLS, 47
 security policies, 125

increasing network availability, 239–241

information disclosure attacks, 107

inside interfaces, 62

integrated access points, 135

integrity, 120

intelligent network solutions, 10

interior routing protocols, 75

Internet layer (TCP/IP protocol suite), 323
 IP datagrams, 324–325

internetworking, 302
 devices
 bridges, 29, 313–314
 hubs, 313
 switches, 29, 313–314

inter-VLAN routing, 46

Intrusion, 114–116

IntServ, 153–154

IP addresses, 331
 address overloading, 63
 ANDing, 63
 classes, 332
 extending, job aids, 341
 hierarchical design, 67–68
 private, 61, 333
 public, 61
 subnet addresses, 334
 calculating, 63–66
 subnet masks
 prefixes, 335
 VLSMs, 70–74

IP datagrams, 324–325

ip directed-broadcast command, 41

IP multicast, 235
 IGMP, 236
 PIM, 237–238

IP Precedence bits, 157

IP RTP priority queuing, 165

IP SLAs, 229–230

IP telephony, 176

- call processing, 181
- components of, 179
- infrastructure, 179
- IP phones, 180
- multisite design, 189
- multisite distributed design, 190
- security, 191–192
- single-site design, 189
- video telephony, 181
- voice applications, 181
- voice gateway, 182

IPsec, 118–120**IPs (intrusion prevention systems), 116****IPv4, 60, 74, 94****IPv6, 244**

- address types, 246
- header format, 245–246

IS-IS, 90–93

- L1-2 routers, 92
- versus OSPF, 91

iSCSI protocol, 244**ISL (Inter-Switch Link) trunks, 43****ISO (International Organization for Standardization), 303****J–L****jitter, 150, 177****job aids**

- decimal-to-binary conversion chart, 341

L1-2 routers, 92**Land.c attacks, 109****LANs**

- devices
 - bridges, 29, 313–314*
 - hubs, 313*
 - routers, 314*
 - switches, 29, 313–314*
- Ethernet
 - collision domains, 313*
 - routers, 315*

laptops, 136**latency, 79, 150****Layer 2 roaming, 146****Layer 2 switching, 31–33**

- MAC addresses, 32–33
- redundancy, 35

Layer 3 switching, 33**Layer 4 switching, 34****learning process, 32****learning state, 39****limitations of hierarchical network design model, 18****link-local unicast addresses, 247****link-specific tools, 166–167****link-state routing protocols, 75****live video, providing via CNs, 210–211****LLC sublayer, 306****LLQ (low-latency queuing), 166****load balancing**

- content switches, 208
- equal-cost load balancing, 80

logical addresses, 331**logical ANDing, 64****LSAs (link-state updates), 89****M****MAC (Media Access Control) addresses, 32–33**

- address table, 31
- verifying, 139

MAC sublayer, 306**maintaining design documentation, 13–14****malware, 102****managed devices, 217****management agents, 217****management information, 217**

- Cisco NetFlow, 223
- MIBs, 218–220
- RMON, 220–222
 - extensions, 222–223*

Management Module (Enterprise Campus functional area), 21, 230

- security features, 232

manifest files, 208**marking, 155–157**

- DSCP markings, 159
- PHB classes, 158

measuring network performance with IP SLAs, 229–230**medium-complexity codecs, 183**

Melissa virus, 102
message digest, 120
messages, SNMP, 218
metrics, 79, 328
MIBs (Management Information Bases), 218–220
MISTP (Multiple-Instance STP), 44
MLS (Multilayer Switching), 47–49
MLS-SE (MLS Switching Engine), 47
modular network design, 14–15
 Cisco Enterprise Composite Network Model, 18
 Enterprise Campus Functional Area, 20
 Enterprise Edge Functional Area, 23
 Service Provider Edge Functional Area, 24
 hierarchical network design model, 15
 access layer, 17
 core layer, 18
 distribution layer, 17
 limitations of, 18
modules, 14
MTBF (mean time between failure), 239
MTTR (mean time to repair), 239
MTU (maximum transmission unit), 84
multicast groups, 236
multicast IPv6 addresses, 246
multicast OSPF, 237
multiplexing, 307
multisite distributed IP telephony design, 190
multisite IP telephony design, 189

N

NAC (Network Admission Control), 122
NAD (network access device), 122
NAS (network-attached storage), 243–244
NAT (Network Address Translation), 62, 333
native Catalyst security, 51
NBAR (Network-Based Application Recognition), 227
neighbors, BGP, 93
networks, baselining, 13
network analysis tools, Optiview Series II Integrated Network Analyzer, 227
Network Assistant, 227

network design

CNs
 CDNs, 197–208
 for providing live video to corporations, 210–211
 for school curricula, 209
 design, definition of, 5–7
 preliminary design, preparing, 12
network flows, 47, 223
network interface layer (TCP/IP protocol suite), 317
network layer, 306, 331
 private IP addresses, 333
network management, 124, 217
 Cisco Network Management Framework, 226–227
 CiscoWorks, 225
 design considerations, 230, 232
 FCAPS, 216
 management information
 Cisco NetFlow, 223
 RMON, 220–223
 NBAR, 227
 on wireless networks, 141–143
 SLAs, 229–230
 SNMP, 218
 strategies for, 228
 syslog, 224
network devices
 bridges, 29, 313–314
 hubs, 313
 routers, 314
 switches, 29, 313–314
NIDSs (network-based IDSs), 114
Nimda worm, 103
NMSs (network management systems), 217
nondesignated ports, 38
nonroot bridges, 37
nontransparent caching, 201–202
NSF (Nonstop Forwarding), 242
Nyquist theorem, 175

O

octets, 318
on-demand content, 207
OptiView Series II Integrated Network Analyzer, 227

OSI (Open System Interconnection) model, 15, 88, 303

- data link layer, 305
- network layer, 306
- physical layer, 305
- protocols, 304
- transport layer, 307
- upper layers, 304

OSPF (Open Shortest Path First), 88–89

- cost, calculating, 90
- LSAs, 89
- totally stubby areas, 89
- versus IS-IS, 91

OTP (one-time password), 122**OUI (Organizational Unique Identifier), 37, 330****outside interfaces, 62****overlapping channels in wireless networks, 144****P****packet filtering, 113–114****packetization delay, 150****packetization of voice traffic, 176–177****packets**

- directed broadcasts, 40
- network flows, 47
- unicast forwarding, 315

PAM (pulse amplitude modulation), 175**PBXs, 176****PCM (pulse code modulation), 175****PDAs, 136****PDIOO (Plan-Design-Implement-Operate-Optimize), 7–9**

- baselining network statistics, 13
- design documentation, maintaining, 13–14
- planning phase of network deployment, 12–13

peers, 93**people-related security vulnerabilities, 105****performance management, 216****performing site surveys for wireless networks, 143–144****personal area networks, 135****PHB classes, 158****phishing, 107****physical addresses, 331****physical layer (OSI model), 305****PIM (Protocol Independent Multicast), 237–238****PKI (Public Key Infrastructure), 123–124****planning network deployment, 12–13****point-to-point bridging, 145****policies, 125****policing, 162****political layer (OSI model), 303****port numbers, 319****PortFast, 40****ports, nondesignated, 38****PQ (priority queuing), 165****prefixes (subnet masks), 335****preliminary design, preparing, 12****pre-positioned content, 207****private addresses, 61, 333****propagation delay, 150****protocols, 304**

- routing protocols. *See* routing protocols
- TCP/IP

Internet layer, 323–325

TCP, 320–322

transport layer, 317–319

proxies, 202**public addresses, 61****PVST (per-VLAN Spanning Tree), 44****Q****QoS (quality of service), 149**

AutoQoS, 167–168

business case for, 149–151

Cisco QoS Baseline, traffic classes, 160–161

classification, 155–156

congestion avoidance, 164

congestion management, 164–166

design guidelines, 168–169

DiffServ, 154

DSCP markings, 159

end-to-end, 153

IntServ, 153–154

link-specific tools, 166–167

marking, 155–157

on converged networks, 177

on data networks, requirements, 152–153

on voice networks, requirements, 152–153

- PHB classes, 158
- policing, 162
- traffic shaping, 163
- trust boundaries, 155

query messages (EIGRP), 87
queuing techniques, 165

R

- reconnaissance attacks, 106**
- redistribution, 95**
- redundancy, 241**
 - in Layer 2 switched networks, 35
- registered IP address translation, 333**
- registered port numbers, 319**
- reliability, 80**
- reliable transport, 307**
- religious layer (OSI model), 303**
- reverse proxy caching, 203**
- RIPv1, 83–84**
- RIPv2, 83–84**
- RMON, 220–222**
 - extensions, 222–223
- roaming**
 - Layer 2 roaming, 146
 - point-to-point bridging, 145
- root bridge, 37**
- root content engines, 208**
- root port, 37**
- router on a stick, 46**
- routing, 63, 75, 314–315**
 - inter-VLAN routing, 46
 - TCP/IP protocol, 332
- routing protocols, 74, 329**
 - BGP4, 93
 - classful, 77
 - classless, 77
 - comparing, 82–83
 - distance vector, 75
 - EIGRP, 86–88
 - exterior, 75
 - flat, 77
 - hierarchical, 77
 - IGRP, 84–85
 - interior, 75
 - IS-IS, 90–93
 - link-state, 75

- metrics, 79
- OSPF, 88–89
 - cost, calculating, 90
 - LSAs, 89
 - totally stubby areas, 89
- RIPv1/RIPv2, 83–84
- suites, 304

routing tables, 327–328
RPF (Reverse Path Forwarding), 238
RPs (rendezvous points), 238
RSTP (Rapid STP), 40
RTP (Real-Time Transport Protocol), 184

S

- SAFE blueprint, 125–128**
 - Cisco Enterprise Composite Network Model, 18
 - Enterprise Campus Functional Area, 20
 - Enterprise Edge Functional Area, 23
 - Service Provider Edge Functional Area, 24
- SAN (storage area networking), 243–244**
- script-kiddies, 104**
- security**
 - 802.1x standard, 138–140
 - assessing, 124
 - attacks
 - access attacks, 106
 - DoS attacks, 108–109
 - information disclosure attacks, 107
 - reconnaissance attacks, 106
 - best practices, 124
 - network management, 124
 - security policies, implementing, 125
 - Catalyst hardware security, 53
 - Catalyst native security, 51
 - CIS, 50
 - on voice networks, 191–192
 - on wireless networks
 - 802.11i standard, 141
 - AirDefense, 141
 - Fast Secure Roaming, 143
 - MAC address verification, 139
 - SSIDs, 139
 - threat mitigation, 138
 - WEP, 139

- policies, implementing, 125
 - vulnerabilities, 104–105
 - WPA, 140–141
- security management, 216**
- segments, 307**
- self-defending networks, 128**
- sequencing, 321**
- serialization delay, 150**
- Server module, 22**
- services provided by CN, 198–199**
- shaping traffic, 163**
- shared trees, 238**
- shared-key authentication, 139**
- signaling traffic bandwidth, 188**
- single-site IP telephony design, 189**
- site surveys for wireless networks, 143–144**
- site-local unicast addresses, 247**
- Slammer worm, 103**
- SLAs (service-level agreements), 229–230**
- SLB (Server Load Balancing), 242**
- snapshot routing, 84**
- sniffing, 138**
- SNMP (Simple Network Management Protocol), 218**
- SoBig.F worm, 103**
- social engineering, 107**
- source trees, 238**
- sparse mode (PIM), 238**
- split-horizon rule, 76**
- SSIDs (Service Set Identifiers), 138–139**
- SSL (secure sockets layer), 121**
- SSO (Stateful Switchover), 242**
- stacks, 304**
- stateless autoconfiguration process (IPv6), 247**
- stateful firewalling, 113**
- static packet filtering, 113**
- static port membership, 42**
- static routes, 74, 327**
- sticky-learning addresses, 33**
- storage networking, 242**
- storage networking models, 243–244**
- STP (Spanning Tree Protocol), 34, 44, 241**
 - blocking state, 38
 - learning state, 39
 - link cost, 37
 - PVST, 44
 - RSTP, 40
- strategies for network management, 228**
- strong authentication, 122**
- subnet addresses, 334**
 - available host addresses, calculating, 65–66, 335
 - calculating, 63–66
 - device addresses, calculating, 67
 - summary routes, calculating, 70
- subnet masks, 334**
 - prefixes, 335
 - VLSMs, 70–71
 - calculating, 72–74*
- summarization, 81**
- summary routes, calculating, 70**
- SWAN (Cisco Structured Wireless-Aware Network), 142**
- switches, 29, 313–314**
- switching, 50, 53**
 - comparing to bridging, 314
 - Layer 2, 31
 - MAC addresses, 32–33*
 - redundancy, 35*
 - Layer 3, 33
 - learning process, 32
 - versus STP learning state, 39*
 - MLS, 47–49
 - security, 50
 - trunks, VTP, 45–46
 - VLANs
 - membership, 42*
 - PVST, 44*
 - trunks, 42*
- switching the packet, 34**
- SYN requests, 109**
- syslog, 224**

T

- tail drops, 164**
- target-based IDSs, 116**
- TCP, 317**
 - acknowledgments, 322
 - embryonic connections, 109
 - four-way handshakes, 322
 - segment fields, 317
 - sequencing, 321
 - three-way handshakes, 320
 - windowing, 321–322

TCP/IP protocol suite, 16, 317
 Internet layer, 323
 IP datagrams, 324–325
 IP addressing, 63, 332
 routing protocols, 329
 TCP
 acknowledgments, 322
 sequencing, 321
 three-way handshakes, 320
 windowing, 321–322
 transport layer, 317–319

threat defense, 111
 traffic filtering, 112
 dynamic packet filtering, 113–114
 static packet filtering, 113
 virus protection, 112

three-ways handshakes, 320

tokens, 122

top-down approach to network design, 12

topology table, 81

totally stubby areas, 89

traffic filtering, 112
 dynamic packet filtering, 113–114
 static packet filtering, 113

traffic shaping, FRTS, 163

translating registered IP addresses to private addresses, 333

transparent caching, 200–201

transport layer (OSI model), 307

transport layer (TCP/IP protocol suite), 317–319
 port numbers, 319
 TCP
 acknowledgments, 322
 four-way handshakes, 322
 sequencing, 321
 three-way handshakes, 320
 windowing, 321–322

triggered updates, 81

Trojan horse attacks, 102

trunk capacity, calculating, 186–188

trunks, 41–42
 VTP, 45–46

trust boundaries, 155, 285

trust management
 AAA, 121
 NAC, 122
 PKI, 123–124

TTL (time to live), 325

U

UDP segment fields, 317

unicast IPv6 addresses, 246

unicast packets, forwarding, 315

unicast routing protocols, 237

unreliable transport, 307

UplinkFast, 40

URL filtering, 117

user workstations, 136

V

VAD (voice activity detection), 184

Venti systems case study, 265–266
 background information and context,
 253, 256
 branch office, 270
 email, 283–284
 future considerations, 291
 head office, 267–270
 IP addressing, 281
 branch-office IP addressing, 282–283
 head office IP addressing, 281–282
 remote user IP addressing, 283
 network management, 289–290
 network requirements, 257–263
 QoS and voice, 284, 288
 remote users, 271
 security, 275–277
 branch office security, 281
 head office security, 278–280
 servers, 273
 switching, 273
 branch-office switching, 275
 head-office switching, 274
 remote user switching, 275
 wireless, 288

video telephony, 181

viruses, 101, 112
 I Love You, 102
 Melissa, 102

VLANs (virtual LANs), 40
 inter-VLAN routing, 46
 membership, 42
 PVST, 44
 static port membership, 42
 trunks, 41–42
 VTP, 45–46

VLSMs (variable-length subnet masks), 60, 70–71

- calculating, 72–74

VMPS (VLAN Management Policy Server), 42**voice applications, 181****voice compression, 182–184****voice gateway, 178, 182****voice networks**

- convergence, 174
- conversation traffic, 177
- IP telephony, 176
- packetization, 176–177
- QoS, 177

- requirements, 152–153*

VoIP (Voice over IP), components of, 178–179**VPN tunnels, 53****VRRP (Virtual Router Redundancy Protocol), 241****VTP (VLAN Trunking Protocol), 45–46****vulnerabilities, 104**

- design-related, 105
- implementation-related issues, 105

wireless networks

- Bluetooth, 135
- HomeRF, 135
- site surveys, 143–144
- network management, 141–143
- nonoverlapping channels, 144
- security, Fast Secure Roaming, 143

wireless PDAs, 136**wireless security**

- 802.11i standard, 141
- 802.1x standard, 138–140
- AirDefense, 141
- MAC address verification, 139
- SSIDs, 139
- threat mitigation, 138
- WEP, 139
- WPA, 140–141

WLANs

- ad-hoc networks, 136
- point-to-point bridging, 145

WPA (Wi-Fi protected access), 140–141**WRED (weighted random early detection), 164**

W

walk-by hacking, 138**WAN devices**

- routers, 314
- hubs, 313

WAPs (wireless access points), 135

- autoconfiguration option, 144
- SSIDs, 138

war driving, 138**WCCP (Web Cache Communication Protocol), 200****WCCP mode (content routing), 206–207****WDS (Wireless Domain Services), 142****WEP (Wired Equivalent Privacy), 139****WFQ (weighted fair queuing), 165****wireless client devices, 136**

- laptops, 136
- PDAs, 136
- user workstations, 136
- wireless IP phones, 137

wireless IP phones, 137

- design considerations, 145