

Numerics

- 10-Mbps Ethernet, 37
- 100-Mbps Ethernet, 37
- 1000-Mbps Ethernet, 37
- 3DES (Triple DES), 208

A

- AAA (authentication, authorization, and accounting), 231
 - Kerberos, 233–234
 - PKI, 234–235
 - RADIUS, 231
 - TACACS+, 232–233
- ABR (Available Bit Rate), 96
- Access Control List Manager (ACLM), 149
- access control lists (ACLs), 39
- access layer, 12
- access patterns, 534
- access points, 401
 - cell coverage, 402–403
 - cell distribution, 404
 - Cisco wireless solutions, 405
 - hot standby redundancy, 413
 - placement and numbers, 410
- ACLM (Access Control List Manager), 149
- ACLs (access control lists), 39
- active monitoring, 150
- addressing, 6
- AES (Advanced Encryption Standard), 208
- AH (Authentication Header), 238
- analyzing network traffic patterns, 31
- antennas, 403
- application layer attacks, 220
- applications
 - Cisco IP Telephony solution, 447
 - IP multicast, 317
 - security, 243
- architectures
 - Cisco content networking solutions, 497
 - Cisco storage-networking solution, 523
 - communication (WLANs), 401
 - access point coverage, 402–403
 - cell distribution, 404
 - network management, 151
- QoS
 - DiffServ, 283
 - IntServ, 282
 - SAFE, 244–245
- ARP spoofing, 426
- ATM, 93–96
- attack signatures, 228
- attacks
 - application layer attacks, 220
 - DDoS, 242
 - DoS attacks, 217
 - IP spoofing, 216
 - man-in-the-middle attacks, 219
 - mitigation
 - EAP authentication, 422–423
 - IPSec, 424–426
 - network reconnaissance, 220–221
 - packet sniffers, 214–215
 - password attacks, 218
 - port redirection attacks, 222
 - trust exploitation, 221
 - unauthorized access attacks, 222
 - viruses and Trojan horses, 222–223
- authentication (VPNs), 353
- Authentication Header (AH), 238
- autonomous solutions, 113
- availability, 6, 132
 - campus networks, 29
 - Campus Network, 16
 - Enterprise Edge, 19, 85
 - parallel, 185
 - server farms, 58
 - storage networks, 535
 - WLANs, 412
- Availability Manager, 145, 159
- AVVID (Cisco Architecture for Voice, Video, and Integrated Data) framework, 3, 141
 - benefits, 9
 - Common Network Infrastructure, 8–9
 - components, 8
 - Intelligent Network Services, 8–10
 - network solutions, 8, 11
 - overview, 7

B

- backups (storage networking), 523
- bandwidth, 89
- best-effort service, 284
- blueprints. *See* SAFE
- branch office WAN, 90
- broadband access VPN design, 378
- broadcast domains, 39
- brute-force attacks, 218
- BSS (Basic Service Set), 401
- Building Access layer, 15
- Building Access submodule, 28
 - high availability, 192
 - QoS, 301
- Building Distribution layer, 15
- Building Distribution submodule, 28, 192
- business continuance, 523

C

- cable, remote access, 107
- cabling, 37
- caching, 495
 - content networks, 498
 - proxy caching, 500
 - reverse proxy caching, 501
 - transparent caching, 499
- call control traffic, 476
- CallManager, 440–441
 - clusters, 448
 - clustering over IP WANs, 467–471
 - deployment guidelines, 449
 - design, 450–451
 - dial plans, 479–480
 - Layer 2 voice transport, 474
 - provisioning, 469
 - voice mail, 457
- Campus Backbone submodule, 15, 28, 192
- Campus Infrastructure module, 15, 28
 - large networks, 256
 - medium networks, 252–253
 - small networks, 248
- Campus Manager, 146
- campus network design, 27
 - analyzing traffic patterns, 31

- Campus Infrastructure module, 32
 - data link and multilayer switching, 41–44
 - hardware and software selection, 45–47
 - IP addressing, 47–49
 - large enterprise design example, 56–57
 - logical campus networks, 33–35
 - medium enterprise design example, 54, 56
 - physical campus networks, 36–40
 - routing protocols, 50–53
 - small enterprise design example, 53
- methodology, 30
- requirement, 29
- server farms, 58
 - infrastructure architecture, 60
 - objectives, 58
 - scalability, 61
 - security, 61
- capacity planning (remote-access VPNs), 378
- CAR (committed access rate), 247
- carrier networks, 187
- case studies
 - content networking, 518–519
 - enterprise network design, 68–77
 - storage networks, 548
 - WLANs, 433–435
- CBR (Constant Bit Rate), 96
- CBWFQ, 290
- CD One (CiscoView), 360
- CDM (Cisco Content Distribution Manager), 505–506, 512
- CDN (Content Delivery Network), 495
- CDP protocol (network management), 140
- cell phones, 107
- Center for Internet Security, 212
- centralized IP Telephony model, 457
- centralized RME design, 158
- CGMP, 332
- Change Audit, 145
- change control policies, 135
- chassis redundancy, 185
- Cisco access routing solutions, 109
- Cisco Architecture for Voice, Video, and Integrated Data framework. *See* AVVID framework
- Cisco Cluster Manager, 137
- Cisco Common Services, 143
- Cisco Content Distribution Manager (CDM), 505–506, 512

- Cisco Customer Response Solution (CRS), 447
- Cisco EAP (LEAP), 421–422
- Cisco Intrusion Detection System Host Sensor, 360
- Cisco IOS, 175
- Cisco IP Telephony solution, 437
 - applications, 447
 - CallManager, 440–441
 - components, 439
 - gateways and control protocols, 441–443
 - network design, 448
 - CallManager clusters, 448–451
 - clustering over IP WANs, 467–471
 - intelligent network services, 480–486
 - multisite solutions with centralized call processing, 457–459
 - multisite solutions with distributed call processing, 460–466
 - network infrastructure, 473–480
 - single-site solutions, 452–456
 - overview, 440
 - transcoders and conferencing, 444
 - hardware support, 444
 - unicast conference bridge, 445
- Cisco LEAP, 418
- Cisco network management strategy, 140–141
- Cisco Product Advisor, 46
- Cisco Secure Policy Manager (CSPM), 360
- Cisco Service Assurance Agent (SAA), 150
- Cisco storage-networking solutions, 521
 - architecture, 523–525
 - FCIP, 531
 - intelligent network services, 532–533
 - iSCSI, 528–529
 - network-attached storage, 526
 - SANs, 526
 - IP access, 534
 - examples, 537
 - identifying needs, 534–536
 - network-attached storage model, 541–543
 - storage over WAN model, 538–539
- Cisco wireless solutions, 405
- CiscoView (CD One), 144, 360
- CiscoWorks, 141
 - Cisco Common Services, 143
 - Common Management Foundation, 143
 - LAN management, 143–147
 - modules, 144–147
 - CiscoWorks IP Telephony Environment Monitor (ITEM), 142
 - CiscoWorks Management Server, 144
 - CiscoWorks RE Availability Manager, 159
 - CiscoWorks Routed WAN (RWAN)
 - management solution, 148–151
 - CiscoWorks Small Network Management Solution (SNMS), 142
 - CiscoWorks VPN/Security Management Solution (VMS), 142, 359
 - class-based shaping, 292
 - classification (QoS), 285
 - client notification policies, 135
 - client software, VPN termination, 357–358
 - clusters (IP WANs), 467–471
 - committed access rate (CAR), 247
 - Common Management Foundation (CiscoWorks), 143
 - Common Network Infrastructure, 8–9
 - companding a law, 446
 - Computer Emergency Response Team, 212
 - concentrators (VPN), 355–356
 - conferencing (Cisco IP Telephony solution), 444
 - hardware support, 444
 - unicast conference bridge, 445
 - congestion
 - avoidance, 287–288
 - management, 288–290
 - connectivity
 - remote access, 107
 - security, 213
 - Content Delivery Network (CDN), 495
 - content networks, 11
 - caching, 498
 - proxy, 500
 - reverse proxy, 501
 - transparent, 499
 - case study, 518–519
 - Cisco content networking products, 516
 - content networking architecture, 497
 - content switching, 501–502
 - designing
 - design considerations, 507–508
 - e-commerce, 510–511
 - streaming media, 512–513
 - Web content delivery, 508–509

- distribution and management of content, 505–506
- intelligent network services
 - integration, 506
- overview, 495
- requirements, 496
- routing, 502
 - direct mode content routing, 503–504
 - WCCP mode content routing, 504
- control protocols (Cisco IP Telephony solution), 443
- core layer, 12
- cost
 - cabling, 37
 - Enterprise Edge, 85
 - service providers, 92
- CQ, 289
- creating DMZs, 225
- CRS (Cisco Customer Response Solution), 447
- CRTP (Compressed Real-Time Transfer Protocol), 294
- cryptology, 234
- CSMA/CA (carrier sense multiple access collision avoidance), 401
- CSPM (Cisco Secure Policy Manager), 360
- CST (Common Spanning Tree) mode, 40

D

- data, network management, 153–154
- data-link protocols, 38
- data link switching, 41
 - medium campus networks, 42–43
 - multilayer switched campus backbone, 44
 - small campus networks, 42
- data rats (WLANs), 407
- DCBWFQ, 290
- dcRTP (Distributed Compressed Real-Time Transfer Protocol), 294
- DDoS attacks, 242
- defining
 - network policies, 134
 - security policies, 206
- delay (enterprise networks), 280
- deploying
 - CallManager clusters, 449
 - IDS, 229–230
 - network management, 155
 - Availability Manager, 159
 - centralized WAN management with LAN management, 158
 - multiple management domains, 157
 - multiserver, 156
 - single server, 156
 - single-site IP Telephony solutions, 454
- DES (Data Encryption Standard), 208
- designing
 - CallManager cluster environment, 450–451
 - content networks, 495
 - architecture, 497
 - caching, 498–501
 - content switching, 501–502
 - design considerations, 507–508
 - distribution and management of content, 505–506
 - e-commerce, 510–511
 - intelligent network services
 - integration, 506
 - requirements, 496
 - routing, 502–504
 - streaming media, 512–513
 - Web content delivery, 508–509
 - Enterprise Campus networks, 189
 - Enterprise Edge, 86
 - enterprise networks
 - high-availability, 188–189
 - IP multicast solutions, 333–337
 - Internet Connectivity module, 111
 - design example, 115–116
 - ISP connectivity solutions, 113–114
 - NAT, 112–113
 - requirements for the Internet, 111
 - multisite IP Telephony solutions with centralized call processing, 457–459
 - multisite IP Telephony solutions with distributed call processing, 460–462
 - example, 463–466
 - WANs, 461
 - network management
 - large site design, 162–164
 - medium site design, 160–161
 - small site design, 159
 - QoS for enterprise networks, 295
 - Building Access submodule, 301

- design example, 302–304
- guidelines, 296–300
- Remote Access module, 104
 - access routing solutions, 109
 - design example, 110
 - enterprise need for, 105
 - physical connectivity, 107
 - remote access protocols, 108
 - remote access type and termination, 106
- remote-access VPNs
 - advantages, 376
 - broadband access, 378
 - capacity planning, 378
 - design considerations, 377
 - large remote-access VPN example, 384–385
 - NAT, 379–382
 - requirements, 374–375
 - small remote-access VPN example, 382–383
- server farms, 58
 - infrastructure architecture, 60
 - objectives, 58
 - scalability, 61
 - security, 61
- single-site IP Telephony solutions, 452
 - benefits, 454
 - example, 455–456
- site-to-site VPNs, 360
 - design considerations, 362–363
 - high-availability and resiliency, 364–365
 - IPSec, 368
 - large site-to-site VPN example, 371–373
 - packet fragmentation, 367
 - requirements, 361
 - routing protocols, 365–366
 - small site-to-site VPN example, 369–370
- storage networks, 521
 - Cisco storage-networking architecture, 523–533
 - Cisco storage-networking solution, 521
 - enterprise needs for, 522–523
 - IP access, 534–537
 - network-attached storage model, 541–543
 - storage over WAN model, 538–539
- WANs, 88
 - data link layer, 93
 - design example, 101–103
 - edge routing solutions, 96–98
 - enterprise needs, 88
 - physical layer, 94–95
 - routing protocols and IP addressing, 98–100
 - selecting topology, 89–92
 - service providers, 92
- WLANs, 407
 - access point placement, 410
 - access-point hot standby redundancy, 413
 - availability, 412
 - channel selection, 409
 - client density and throughput, 408
 - coverage, 408
 - data rates, 407–408
 - design considerations, 407
 - enterprise WLAN design model, 427–429
 - inline power, 411
 - IP addressing, 412
 - IP multicast, 414
 - QoS, 415
 - remote-access and telecommuter WLAN design model, 429–430
 - RF environment, 409
 - roaming, 413
 - security, 416–426
 - small office WLAN design model, 426
 - VLANs, 411
- Device Configuration Manager, 145
- Device Fault Manager, 147
- device redundancy, 6
- devices
 - fault tolerance, 177
 - security, 239
 - applications, 243
 - hosts, 241
 - network-wide, 242
 - routers, 240
 - switches, 240
- DHCP servers, 422
- dial plans, 479–480
- dialup, 95
- differentiated service, 284
- DiffServ, 283

dipole antenna, 403
 direct mode content routing, 503–504
 discovery of networks, 143
 Discrepancy Reports, 147
 dish antennas, 403
 distributed traffic shaping (DTS), 292
 distribution layer, 12
 distribution of content (content networks), 505–506
 distribution trees (IP multicast), 321–323
 DMZs (Demilitarized Zone), 224–225
 DoS attacks, 217
 DRAM (dynamic random-access memory), 236
 DSL, 95, 107
 DSniff, 215
 DTS (distributed traffic shaping), 292
 dynamic routing, 50

E

E911 (enhanced 911), 454
 EAP, 418
 ECNM (Enterprise Composite Network Model), 12, 138–139
 campus design, 27
 analyzing traffic patterns, 31
 Campus Infrastructure module, 32–53
 large enterprise design example, 56–57
 medium enterprise design example, 54–56
 methodology, 30
 requirements, 29
 server farms, 58–61
 small enterprise design example, 53
 Enterprise Campus, 14
 Campus Infrastructure module, 15
 Edge Distribution module, 16
 meeting enterprise needs, 16
 Network Management module, 15
 Server Farm module, 15
 Enterprise Edge, 16
 E-commerce module, 17
 Internet Connectivity module, 18
 Remote Access and VPN module, 18–19
 functional area overview, 12
 layers, 12
 routers, 23
 Service Provider Edge, 19
 e-commerce, content network design, 510–511
 E-Commerce module, 17
 Enterprise Edge, 84
 SAFE, 260
 Edge Distribution module, 16, 260
 edge routing solutions (WANs), 96–98
 EIGRP (Enhanced Interior Gateway Routing Protocol), 51, 99
 Encapsulating Security Payload (ESP), 238
 encryption (VPNs), 353–355
 Enterprise Campus, 12–14
 Campus Infrastructure module, 15
 Edge Distribution module, 16
 IP multicast design, 333–334
 meeting enterprise needs, 16
 Network Management module, 15
 Server Farm module, 15
 Enterprise Campus networks, designing, 189
 enterprise data storage. *See* storage networks, 521
 Enterprise Edge, 13, 16
 designing, 83
 Internet Connectivity module, 111–116
 methodology, 86
 remote access, 104–110
 E-Commerce module, 17
 high availability, 190–191
 Internet Connectivity module, 18
 modules, 83–84
 NAT, 112–113
 network traffic patterns, 86–87
 Remote Access and VPN module, 18–19
 requirements, 85
 SAFE
 E-Commerce module, 260
 Internet Connectivity module, 263
 Remote Access and VPN module, 264
 WAN module, 264
 enterprise network design
 campus networks, 27
 analyzing traffic patterns, 31
 Campus infrastructure module, 32
 methodology, 30
 requirements, 29
 data link and multilayer switching, 41
 medium campus networks, 42–43
 multilayer switched campus backbone, 44

- small campus networks, 42
 - hardware and software selection, 45–47
 - IP addressing, 47–49
 - large enterprise design example, 56–57
 - logical campus networks, 33
 - one-VLAN-per-switch model, 34
 - unique-VLAN-per-switch model, 34
 - VLANs-spanning-multiple-access-switches model, 35
 - medium enterprise design example, 54–56
 - physical campus networks
 - cabling, 36
 - Ethernet, 37
 - segmentation strategy, 39
 - STP, 40
 - routing protocols, 50
 - comparison, 53
 - EIGRP, 51
 - IGRP, 51
 - Integrated IS-IS, 52
 - OSPF, 52
 - RIP/RIPv2, 51
 - static vs. dynamic routing, 50
 - small enterprise design example, 53
- enterprise networks
 - case study, 68–77
 - content network requirements, 496
 - designing. *See* enterprise network design
 - high availability, 184
 - best practices for design, 188–189
 - design goals, 188
 - power availability, 187
 - redundancy options, 185
 - software features, 186
 - high-availability, 173–175
 - IP multicast solutions, 333
 - Enterprise Campus, 333–334
 - large campus design, 335–336
 - small campus design, 334
 - WANs, 337
 - QoS, 279, 295
 - Building Access submodule, 301
 - delay, 280
 - design example, 302–304
 - guidelines, 296–300
 - jitter, 281

- switches, 65
 - VPNs, 350
 - WLANs, 399
- enterprise WAN backbone, 92
- enterprise WLAN design model, 427–429
- escalation policies, 134
- ESP (Encapsulating Security Payload), 238
- EtherChannel, 38
- Ethereal, 215
- Ethernet, 37–38
- event driven network management, 135–136

F

- fabric topology, 526
- failure domains, 39
- Fast Ethernet, 37
- fault tolerance, 6, 176
- FCAPS (fault, configuration, accounting, performance, and security management), 133
- FCIP compared to iSCSI, 531
- Fibre Channel, 524
 - storage networks with IP access, 537
- FIFO (first-in, first-out), 288
- firewalls, 267
 - design options, 223
 - DMZs, 224–225
 - filtering rules, 225–226
 - IOS firewall, 227
 - PIX firewall, 226
 - statefull, 213
- fixed network delay, 280
- FR PIPQ (Frame Relay PVC Interface Priority Queuing), 289
- FR/ATM/PPP module, 19
- Frame Relay, 93–94
- Frame Relay IP RTP Priority, 290
- FRTS (Frame Relay traffic shaping), 292
- full-mesh VPN topologies, 363
- functional areas
 - Enterprise Composite Network Model, 12
 - Enterprise Campus, 14–16
 - Enterprise Edge, 16–19
 - Service Provider Edge, 19

G

- gatekeepers, 442
- gateways
 - CallManager servers, 470
 - Cisco IP Telephony solution, 441–443
 - voice, 488
- Gigabit Ethernet, 37
- GTS (generic traffic shaping), 292
- guaranteed service, 284

H

- H.225, 442
- H.245, 442
- H.323, 442
- hardware
 - campus networks, 45–47
 - Common Network Infrastructure, 9
 - redundancy, 178–179
 - VoIP, 488
 - wireless networks, 431
- hardware conference bridge, 446
- HIDS (host-based IDS), 228
- hierarchical VPN topologies, 363
- high availability, 173
 - Cisco IOS high-availability architecture, 175
 - Cisco IP Telephony solutions, 481
 - design example, 191–192
 - Enterprise Campus networks, 189
 - Enterprise Edge, 190–191
 - enterprise networks, 174–175, 184
 - best practices for design, 188–189
 - design goals, 188
 - power availability, 187
 - redundancy options, 185
 - software features, 186
 - fault tolerance, 176
 - hardware redundancy, 178
 - NIC redundancy, 179
 - Route Processor Redundancy (RPR), 178
 - network requirements, 173
 - tools, 10
 - VPNs, 364–365
- host-based IDS (HIDS), 228
- hosts, security, 241

- HP OpenView, 137
- HSRP, 180
- HTTP protocol (network management), 139
- hub-and-spoke VPN topologies, 362

I

- I/O profiles, 534
- identifying IP addressing strategy for campus networks, 47–49
- identity, 214
- IDS (intrusion detection system), 228, 268
 - deploying, 229–230
 - operation, 229
- IEEE 802.11, 404
- IGMP (Internet Group Management Protocol), 330–331
- IGRP (Interior Gateway Routing Protocol), 51
- IKE (Internet Key Exchange), 237
- implementing
 - IPSec (VPNs), 368
 - WLAN security, 420–421
- infrastructure
 - Cisco IP Telephony solution design, 473
 - bandwidth provisioning, 475
 - dial plans, 479–480
 - Layer 2 voice transport, 474
 - traffic engineering, 477
 - voice bearer traffic, 476
 - voice over Frame Relay, 475
 - network management, 151–152
 - server farms, 60
- inline power (WLANs), 411
- Integrated IS-IS (Integrated Intermediate System-to-Intermediate System), 52
- Integration Utility, 144
- Intelligent Network Services, 8
 - Cisco IP Telephony solution design, 480
 - high availability, 481
 - QoS, 484–486
 - voice security, 483
 - content networking, 506
 - storage networking, 532–533
 - tools, 10
- interface queuing, 485
- Interior Gateway Routing Protocol (IGRP), 51

- Internet Connectivity module, 18, 111
 - design example, 115–116
 - ISP connectivity solutions, 113–114
 - NAT, 112–113
 - requirements for the Internet, 111
 - Internet Connectivity module (Enterprise Edge), 84
 - Internet Connectivity module (SAFE)
 - enterprise edge, 263
 - medium networks, 250–252
 - small networks, 246–247
 - Internet Group Management Protocol (IGMP), 330–331
 - Internet Key Exchange (IKE), 237
 - Internet Small Computer System Interface. *See* iSCSI
 - Internetwork Performance Monitor (IPM), 149
 - intracluster communication, 449
 - intrusion detection system. *See* IDS
 - IntServ, 282
 - Inventory Manager, 144
 - IOS firewall, 227
 - IP access
 - storage networking architectures, 534
 - examples, 537
 - identifying needs, 534–536
 - IP addressing
 - campus networks, 47–49
 - NAT, 49
 - WANs, 98–100
 - WLANs, 412
 - IP multicast, 11
 - overview, 316
 - servers, 317
 - WLANs, 414
 - IP multicast services, 315–316
 - Cisco servers, 340
 - control mechanisms, 329
 - CGMP, 332
 - IGMP, 330–331
 - IGMP snooping, 332
 - data-delivery principles, 318
 - enterprise networks, 333
 - Enterprise Campus, 333–334
 - large campus design, 335–336
 - small campus design, 334
 - WANs, 337
 - group membership and distribution trees, 321–323
 - multicast forwarding, 319–321
 - IP phones, 488
 - IP RTP Priority, 290
 - IP spoofing, 216, 426
 - IP Telephony. *See* Cisco IP Telephony solution
 - IPM (Internetwork Performance Monitor), 149
 - IPSec (IP security), 236
 - AH, 238
 - attack mitigation, 424–426
 - ESP, 238
 - IKE, 237
 - VPNs, 352, 368
 - WLAN security, 419
 - iSCSI (Internet Small Computer System Interface), 525, 528–529
 - compared to FCIP, 531
 - protecting traffic, 533
 - ISDN, 95, 107
 - ISP connectivity solutions (Internet Connectivity module), 113–114
 - ISP module, 19
 - ITEM (CiscoWorks IP Telephony Environment Monitor), 142
-
- ## J–L
-
- jitter, 279–281
 - KDC (key distribution center), 233
 - Kerberos, 233–234
 - L2TP (Layer 2 Tunneling Protocol), 213
 - LAN management (CiscoWorks), 143–148
 - large campus networks, IP multicast design, 335–336
 - large enterprise design example, 56–57, 140
 - Layer 2 voice transport, 474
 - Layer 3 redundancy, 180–181
 - layers (ECNModel), 12
 - LEAP (Cisco Wireless EAP), 417
 - leased lines, 95
 - LFI (Link Fragmentation and Interleaving), 293
 - link-efficiency mechanisms (QoS), 293
 - links, redundancy, 6
 - LLQ, 289
 - local failover deployment model, 467

- logical campus networks, 33
 - one-VLAN-per-switch model, 34
 - unique-VLAN-per-switch model, 34
 - VLANs-spanning-multiple-access-switches model, 35
- loop topology, 526
- LRE (Long-Range Ethernet), 37

M

- Malware, 223
- management tools
 - Cisco Cluster Manager, 137
 - HP OpenView, 137
- managing
 - congestion, 288–290
 - content (content networks), 505–506
 - Enterprise Edge, 85
 - enterprise networks and devices, 141
 - IP multicast, 329
 - CGMP, 332
 - IGMP, 330–331
 - IGMP snooping, 332
 - LANs (CiscoWorks), 143–147
 - networks. *See* network management
 - security risks, 209
 - server farms, 59–61
 - VPNs, 358
 - CiscoWorks VPN/Security Management Solution, 359
 - considerations, 359
- man-in-the-middle attacks, 219
- many-to-one translation, 380
- marking (QoS), 285
- MD5 (Message Data 5), 205
- MDRR (Modified Deficit Round Robin), 290
- media resource group lists (MRGLs), 470
- media resource groups (MRGs), 470
- medium campus networks, data link and multilayer switching, 42–43
- medium enterprise design example, 54–56
- Message Data 5 (MD5), 205
- MGCP, 442
- MHSRP (multi-group HSRP), 180
- mitigation
 - IDS, 230

- man-in-the-middle attacks, 219
- unauthorized access attacks, 222
- m-law, 627
- module redundancy, 185
- modules (Enterprise Edge), 83–84
- monitoring
 - performance, 132
 - policies, 134
- MPLS, 94
- MRGLs (media resource group lists), 470
- MRGs (media resource groups), 470
- MSFC (Multilayer Switch Feature Card), 179
- MST (Multiple Spanning Tree) protocol, 40, 183
- multicast forwarding, 319–321
- multi-group HSRP (MHSRP), 180
- multi-homed enterprise, 114
- Multilayer Switch Feature Card (MSFC), 179
- multilayer switching, 41
 - medium campus networks, 42–43
 - multilayer switched campus backbone, 44
 - small campus networks, 42
- multimode fiber, 36
- multiple management domains, 157
- multiserver network management, 156

N

- NAT (Network Address Translation), 49
 - Internet Connectivity module, 112–113
 - remote-access VPN design, 379–382
- NAT Traversal (NAT-T), 380
- Nessus, 212
- network-attached storage, 526
- network-attached storage model, 541–543
- network availability. *See* high availability
- network-based IDS (NIDS), 228
- network capacity design, 6
- network design
 - Cisco IP Telephony, 448
 - CallManager clusters, 448–451
 - clustering over IP WANs, 467–471
 - intelligent network services, 480–486
 - multisite solutions with centralized call processing, 457–459
 - multisite solutions with distributed call processing, 460–466

- network infrastructure, 473–480
 - single-site solutions, 452–456
- Enterprise Edge, 83
- Internet connectivity, 111
 - design example, 115–116
 - ISP connectivity solutions, 113–114
 - NAT, 112–113
 - requirements for the Internet, 111
- remote access, 104
 - access routing solutions, 109
 - design example, 110
 - enterprise need for, 105
 - physical connectivity, 107
 - remote access protocols, 108
 - remote access type and termination, 106
- WANs, 88
 - data link layer, 93
 - design example, 101–103
 - edge routing solutions, 96–98
 - enterprise needs, 88
 - physical layer, 94–95
 - routing protocols and IP addressing, 98–100
 - selecting topology, 89–92
 - service providers, 92
- network management, 132
 - active monitoring, 150
 - architectures, 151
 - Cisco strategy, 140–141
 - data collection, 153–154
 - deployment recommendations, 155
 - Availability Manager, 159
 - centralized WAN management with LAN management, 158
 - multiple management domains, 157
 - multiserver, 156
 - single server, 156
 - designing
 - large site design, 162–164
 - medium site design, 160–161
 - small site design, 159
 - evolution of, 132
 - infrastructure considerations, 151–152
 - LANs, 147–148
 - methods, 135–136
 - module functions, 138–140
 - policies and procedures, 134–135
 - protocols, 139–140
 - reactive, 135
 - resources, 155
 - RWAN, 148–151
 - software, 166
 - station sizing, 155
 - strategy process, 136–137
- Network Management module, 15, 257–258
- network solutions, 8, 11
- networks
 - discovery, 143
 - performance, 3
 - availability, 6
 - responsiveness, 4
 - scalability, 5–6
 - throughput, 4
 - utilization, 4
 - reconnaissance, 220–221
 - security
 - AAA, 231–235
 - applications, 243
 - attacks, 214–222
 - defining policies, 134, 206
 - device, 239–242
 - evaluating policies, 203–205
 - firewalls, 223–226
 - IDS, 228–230
 - IPSec, 236–238
 - key elements, 213
 - maintaining security, 207–208
 - network reconnaissance, 220–221
 - PIX firewall, 226–227
 - risk assessment and management, 209–211
 - SAFE, 244–264
 - trust exploitation, 221
 - viruses and Trojan horses, 222–223
 - traffic patterns (Enterprise Edge), 86–87
 - wireless. *See* WLANs
- nGenius Real-Time Monitor, 147
- NICs, redundancy, 179
- NIDS (network-based IDS), 228
- non-overlapping channels (WLANs), 409
- NRT-VBR (Non Real-Time Variable Bit Rate), 96
- Nyquist theorem, 439

O

- omnidirectional antennas, 403
- one-to-one translation, 380
- one-VLAN-per-switch model, 34
- OSPF (Open Shortest Path First), 52, 99
- OTP (one-time password), 218
- outline, network management strategy process, 136–137
- overrun, 281

P

- packet sniffers, 214–215
- packetization delay, 280
- packets
 - loss, 281
 - minimizing fragmentation (VPNs), 367
 - priority classifications (enterprise network QoS), 297
 - tunneling, 351
- packets per second (pps), 3
- parallel availability, 185
- password attacks, 218, 426
- patch antennas, 403
- Path Analysis, 146
- performance, 3
 - availability, 6
 - Campus Network, 16
 - campus networks, 29
 - Enterprise Edge, 19, 85
 - IP multicast, 318, 414
 - monitoring, 132
 - responsiveness, 4
 - scalability, 5–6
 - server farms, 58
 - storage networks, 535
 - throughput, 4
 - utilization, 4
- perimeter LANs, 224–225
- perimeter security, 213
 - IOS firewall, 227
 - PIX firewall, 226
- per-VLAN spanning tree (PVST), 182

- physical campus networks
 - cabling, 36
 - Ethernet, 37
 - segmentation strategy, 39
 - STP, 40
- PIM-DM (PIM dense mode), 324, 329
- PIM-SM (PIM sparse mode), 325, 329
 - source registration, 326
 - SPT switchover, 328
- PIMv1 (Protocol Independent Multicast version 1), 324
- PIX firewall, 226–267
- PKI (public key infrastructure), 234–235
- policies
 - network management, 134
 - security
 - defining, 206
 - maintaining network security, 207–208
 - risk assessment and management, 209–211
- policy domains, 39
- polling network management, 136
- port redirection attacks, 222
- PortFast, 184
- power availability, 187
- PPP, 93–94, 108
- PPPoA, 108
- PPPoE, 108
- pps (packets per second), 3
- PQ, 289
- proactive network management, 136
- Product Advisor, 46
- propagation delay, 281
- Protocol Independent Multicast version 1 (PIMv1), 324
- protocols
 - Cisco IP Telephony solution, 442
 - data link layer, 93
 - network management, 139–140
 - remote access, 108
 - resiliency, 6
 - routing (WAN design), 98–100
- provisioning
 - call control traffic, 476
 - voice bearer traffic, 476
- proxy caching, 500
- PSTN gateway, 439

PSTN module, 19
 public key infrastructure (PKI), 234–235
 PVST (per-VLAN spanning tree), 182

Q

QoS (quality of service), 10, 279
 architecture
 DiffServ, 283
 IntServ, 282
 AVVID, 10
 Cisco IP Telephony solutions, 484–486
 classification and marking, 285
 congestion avoidance, 287–288
 congestion management, 288–290
 enterprise networks, 279, 295
 Building Access submodule, 301
 delay, 280
 design example, 302–304
 guidelines, 296–300
 jitter, 281
 key Cisco QoS categories and features, 294
 link-efficiency mechanisms, 293
 network storage, 533
 service levels, 284–285
 signaling, 293
 switches, 307
 traffic conditioning, 290–292
 WLANs, 415

R

RADIUS, 231
 RADIUS servers, 422
 Rapid Spanning Tree (RSTP), 183
 RAS, 443
 reachability, 132
 reactive network management, 135–136
 reconnaissance (network), 220–221
 RED (random early detection), 287
 redundancy
 enterprise networks, 185
 hardware (high-availability networks), 178
 Layer 3, 180–181
 NICs, 179

RPR, 178
 STP, 182–184
 regional office WAN, 91
 Remote Access and VPN module, 18–19
 Enterprise Edge, 84
 SAFE, 264
 Remote Access module, 104
 access routing solutions, 109
 design example, 110
 enterprise need for, 105
 physical connectivity, 107
 protocols, 108
 selecting remote access type and termination, 106
 remote-access VPNs, 351
 designing
 advantages, 376
 broadband access, 378
 capacity planning, 378
 design considerations, 377
 large remote-access VPN
 example, 384–385
 NAT, 379–382
 requirements, 374–375
 small remote-access VPN example,
 382–383
 routers, 120
 remote-access WLAN design model, 429–430
 remote failover deployment model,
 470–473
 requirements (Enterprise Edge), 85
 resiliency (VPNs), 364–365
 Resource manager Essentials (RME), 360
 resources
 network management, 155
 QoS, 280
 responsiveness, 4
 reverse proxy caching, 501
 RIP (Routing Information Protocol), 51
 IPv2, 51, 99
 risk assessment, 209–211
 RME (Resource Manager Essentials), 360
 RMON protocol (network
 management), 140
 roaming (WLANs), 413
 Route Processor Redundancy (RPR), 178

routers

- content networking, 516
- ECNM, 23
- ISCSI, 529
- redundant power supply, 195
- remote access, 120
- security, 240
- storage networks, 545
- WAN aggregation routers, 119
- routing (content), 502
 - direct mode, 503–504
 - WCCP mode, 504
- Routing Information Protocol (RIP), 51
- routing protocols, 6
 - campus networks, 50
 - comparison, 53
 - EIGRP, 51
 - IGRP, 51
 - Integrated IS-IS, 52
 - OSPF, 52
 - RIP/RIPv2, 51
 - static vs. dynamic, 50
 - VPNs, 365–366
- RPR (Route Processor Redundancy), 178
- RSTP (Rapid Spanning Tree), 183
- RT-VBR (Real-Time Variable Bit Rate), 96
- RWAN management solution, 148–151

S

- SAA (Cisco Service Assurance Agent), 150
- SAFE (Security Architecture for Enterprise), 244
 - architecture, 244–245
 - enterprise edge
 - E-Commerce module, 260
 - Internet Connectivity module, 263
 - Remote Access and VPN module, 264
 - WAN module, 264
 - large networks
 - Campus Infrastructure module, 256
 - Edge Distribution module, 260
 - Network Management module, 257–258
 - Server Farm module, 259
 - medium networks
 - Campus Infrastructure module, 252–253
 - Internet Connectivity module, 250–252
 - WAN module, 255

small networks

- Campus Infrastructure module, 248
- Internet Connectivity module, 246–247
- SANs, storage networks, 526
- satellite, 107
- scalability, 5
 - Campus Network, 16
 - campus networks, 29
 - Enterprise Edge, 19, 85
 - influences on, 6
 - server farms, 58, 61
- SCCP (Signaling Connection Control Part), 476
- security
 - AAA
 - Kerberos, 233–234
 - PKI, 234–235
 - RADIUS, 231
 - TACACS+, 232–233
 - attacks
 - application layer attacks, 220
 - DoS attacks, 217
 - IP spoofing, 216
 - man-in-the-middle attacks, 219
 - network reconnaissance, 220–221
 - packet sniffers, 214–215
 - password attacks, 218
 - port redirection attacks, 222
 - trust exploitation, 221
 - unauthorized access attacks, 222
 - viruses and Trojan horses, 222–223
- AVVID, 10
- Center for Internet Security, 212
- device, 239
 - applications, 243
 - hosts, 241
 - network-wide, 242
 - routers, 240
 - switches, 240
- evaluating policies, 203
 - defining policies, 206
 - maintaining security, 207–208
 - risk assessment and management, 209–211
 - vulnerabilities, 204–205
- firewalls, 223
 - filtering rules, 225–226
 - implementing a DMZ, 224–225

- IOS firewall, 227
- PIX firewall, 226
- IDS, 228
 - deploying, 229–230
 - operation, 229
- IPSec, 236
 - AH, 238
 - ESP, 238
 - IKE, 237
- key elements, 213
- matrix, 211
- network storage, 533
- policies, 134
- SAFE, 244
 - architecture, 244–245
 - enterprise edge, 260, 263–264
 - large network Campus Infrastructure module, 256
 - large network Edge Distribution module, 260
 - large network Network Management module, 257–258
 - large network Server Farm module, 259
 - medium network Campus Infrastructure module, 252–253
 - medium network Internet Connectivity module, 250–252
 - medium network WAN module, 255
 - small network Campus Infrastructure module, 248
 - small network Internet Connectivity module, 246–247
- server farms, 59–61
- voice, 483
- VPNs
 - encryption, 353–355
 - IPSec, 352
 - user authentication, 353
- WLANs, 416–417
 - attack mitigation (EAP Authentication), 422–423
 - attack mitigation (IPSec), 424–426
 - Cisco EAP, 421–422
 - EAP, 418
 - implementation comparison, 420–421
 - IPSec, 419
 - WLAN static WEP, 419
- Security Parameter Index (SPI), 355
- segmentation strategies (physical networks), 39
- selecting
 - data link layer (WANs), 93
 - data link or multilayer switching, 41
 - medium campus networks, 42–43
 - multilayer switched campus backbone, 44
 - small campus networks, 42
 - edge routing solutions (WANs), 96–98
 - hardware and software for campus networks, 45–47
 - physical layer (WANs), 94–95
 - physical network segmentation strategy, 39
 - routing protocols for campus networks, 50
 - comparison, 53
 - EIGRP, 51
 - IGRP, 51
 - Integrated IS-IS, 52
 - OSPF, 52
 - RIP/RIPv2, 51
 - static vs. dynamic, 50
 - service providers, 92
 - STP, 40
- serialization delay, 281
- Server Farm module, 15, 259
- server farms
 - designing, 58
 - infrastructure architecture, 60
 - objectives, 58
 - scalability, 61
 - security, 61
 - switches, 66
- servers
 - IP multicast, 340
 - multicast, 317
 - voice, 489
- service levels (QoS), 284–285
- Service Provider Edge, 13, 19
- service providers, selecting, 93
- Service Set ID (SSID), 401
- SGCP (Simple Gateway Control Protocol), 442
- shaping traffic, 292
- shared trees, 322
- signaling (QoS), 293
- Signaling Connection Control Part (SCCP), 476
- Simple Gateway Control Protocol (SGCP), 442
- single server network management, 156

- single-homed site, 114
- single-mode optical fiber, 36
- SIP, 443
- site-to-site VPNs, 351
 - designing, 360
 - design considerations, 362–363
 - high-availability and resiliency, 364–365
 - IPSec, 368
 - large site-to-site VPN example, 371–373
 - packet fragmentation, 367
 - requirements, 361
 - routing protocols, 365–366
 - small site-to-site VPN example, 369–370
- site-to-site WAN network design example, 103
- small campus networks
 - data link and multilayer switching, 42
 - IP multicast design, 334
- small enterprise design example, 53
- small office WLAN design model, 426
- SNMP protocol (network management), 140
- SNMS (CiscoWorks Small Network Management Solution), 142
- snooping (IP multicast), 414
- software
 - campus networks, 45–47
 - Malware, 223
 - network management, 166
 - VPN termination, 357–358
- software conference bridge, 446
- Software Image Manager, 145
- SONET/SDH, 95
- source trees, 321
- SPAN (Switched Port Analyzer), 229
- Spanning Tree Protocol. *See* STP
- SPI (Security Parameter Index), 355
- split-tunnel communication (VPNs), 381
- SPT switchover (PIM-SM), 328
- SSH protocol (network management), 139, 154
- SSID (Service Set ID), 401
- SSL protocol (network management), 139
- SSL-based VPNs, 392
- stateful firewalls, 213
- static routing, 50
- station sizing, 155
- storage consolidation, 522
- storage networks, 11
 - case study, 548
- Cisco storage-networking
 - architecture, 523–525
 - FCIP, 531
 - intelligent network services, 532–533
 - iSCSI, 528–529
 - network-attached storage, 526
 - SANs, 526
 - Cisco storage-networking solution, 521
 - designing, 521
 - enterprise needs for, 522
 - business continuance and backup, 523
 - storage consolidation, 522
 - IP access, 534
 - examples, 537
 - identifying needs, 534–536
 - network-attached storage model, 541–543
 - storage over WAN model, 538–539
 - STP (Spanning Tree Protocol), 40, 182–184
 - streaming media, 512–513
 - SVCs (switched virtual circuits), 292
 - switches
 - content networking, 516
 - enterprise networks, 65
 - QoS, 307
 - redundancy, 195
 - security, 240
 - server farms, 66
 - storage networks, 545
 - switching
 - content switching, 501–502
 - data link, 41
 - medium campus networks, 42–43
 - multilayer switched campus backbone, 44
 - small campus networks, 42
 - multilayer, 41
 - medium campus networks, 42–43
 - multilayer switched campus backbone, 44
 - small campus networks, 42
 - Syslog Analyzer, 145
 - Syslog protocol (network management), 140

T

- TACACS+, 232–233
- TCP synchronization attacks, 217
- telecommuter WLAN design model, 429–430

Telnet protocol (network management), 139, 154

termination

- remote access, 106
- VPNs
 - client software, 357–358
 - concentrators, 355–356

testing security, 208

TFTP protocol (network management), 140

throughput, 4

topologies, 6

- fabric, 526
- loop, 526
- WAN design, 89
 - branch office WAN, 90
 - enterprise WAN backbone, 92
 - regional office WAN, 91

Topology Services, 146

TPS (transactions per second), 507

traffic

- analyzing patterns, 31
- call control traffic, 476
- conditioning, 290–292
- congestion avoidance, 287–288
- congestion management, 288–290
- Enterprise Edge, 86–87
- signaling, 293
- unicast vs. multicast, 318
- voice bearer traffic, 476

traffic engineering, 477

transcoding, 439, 444

transmission media

- cabling, 36
- selection example, 38

transparent caching, 499

Triple DES (3DES), 208

Trojan horses, 222–223

troubleshooting, minimizing packet fragmentation (VPNs), 367

trust exploitation, 221

tunneling (VPNs), 351

twisted-pair cabling, 36

U

UBR (Unspecified Bit Rate), 96

unauthorized access attacks, 222

underrun, 281

unicast, 316

unicast conference bridge, 445

unique-VLAN-per-switch model, 34

unshielded twisted-pair (UTP) cabling, 36

untrusted networks, 424

UplinkFast, 184

user authentication (VPNs), 353

User Tracking, 146

utilization, 4

UTP (unshielded twisted-pair) cabling, 36

V

variable network delay, 280

video conferencing, 299–300

Virtual Private networks. *See* VPNs

viruses, 222–223

VLAN Port Assignment, 146

VLANs

- logical campus networks, 33
- STP, 40
- switches as security devices, 241
- WLANs, 411

VLANs-spanning-multiple-access-switches model, 35

VMS (CiscoWorks VPN/Security Management Solution), 142

voice

- digitization, 439
- gateways, 488
- intelligent network services, 480–483
- QoS, 299
- security, 483
- servers, 489

voice bearer traffic, 476

voice over ATM, 475

VoIP

- Cisco products, 488
- QoS, 415

VPN Monitor, 359

VPNs (virtual private networks), 11, 213, 349

- Cisco Systems products, 388
- enterprise requirements, 350
- managing, 358–359
- remote-access

- advantages, 376
- broadband access, 378
- capacity planning, 378
- design considerations, 377
- large remote-access VPN design example, 384–385
- NAT, 379–382
- requirements, 374–375
- small remote-access VPN design example, 382–383
- security, 269–270
 - encryption, 353–355
 - IPSec, 352
 - user authentication, 353
- site-to-site, 360
 - design considerations, 362–363
 - high-availability and resiliency, 364–365
 - IPSec, 368
 - large site-to-site design example, 371–373
 - packet fragmentation, 367
 - requirements, 361
 - routing protocols, 365–366
 - small site-to-site design example, 369–370
- SSL-based VPNs, 392
- termination
 - client software, 357–358
 - concentrators, 355–356
- tunneling, 351
- VRRP (Virtual Router Redundancy Protocol), 180–181
- vulnerabilities, countermeasures, 204–205
- design example, 101–103
- edge routing solutions, 96–98
- enterprise needs, 88
- physical layer, 94–95
- routing protocols and IP addressing, 98–100
- selecting topology, 89–92
- service providers, 92
- edge routing solutions, 96–98
- enterprise WAN backbone, 92
- IP multicast design, 337
- multisite with distributed call processing, 461
- physical layer, 94–95
- regional office WAN, 91
- routers, 119
- routing protocols and IP addressing, 98–100
- service providers, 92
- storage over WAN model, 538–539
- WCCP mode content routing, 504
- Web content delivery (content network design), 508–509
- websites
 - Center for Internet Security, 212
 - Malware, 223
- WFQ, 288
- wireless bridges, 406
- wireless technology, 11, 399. *See also* WLANs
- WLAN static WEP, 419
- WLANs (Wireless Local Area Networks), 399
 - 802.11 standards, 404
 - antennas, 403
 - case study, 433–435
 - Cisco wireless solutions, 405
 - communication architecture, 401
 - access point coverage, 402–403
 - cell distribution, 404
 - enterprise WLAN design, 407
 - access point hot standby redundancy, 413
 - access point placement, 410
 - availability, 412
 - channel selection, 409
 - client density and throughput, 408
 - coverage, 408
 - data rates, 407–408
 - design considerations, 407
 - inline power, 411
 - IP addressing, 412

W

- WAN module
 - Enterprise Edge, 84
 - SAFE
 - enterprise edge, 264
 - medium networks, 255
- WANs
 - branch office WAN, 90
 - data link layer, 93
 - design example, 101–103
 - designing, 88
 - data link layer, 93

- IP multicast, 414
- QoS, 415
- RF environment, 409
- roaming, 413
- VLANs, 411
- enterprise WLAN design model, 427–429
- remote-access and telecommuter
 - WLAN design models, 429–430
- security, 416–417
 - attack mitigation (EAP authentication), 422–423
 - attack mitigation (IPSec), 424–426
 - Cisco EAP, 421–422
 - EAP, 418
 - implementation comparison, 420–421
 - IPSec, 419
 - WLAN static WEP, 419
- small office WLAN design model, 426
- wireless enterprise needs, 399
- workgroup bridges, 406
- WRED, 287

X–Z

X.25, 94

yagi antenna, 403