



Numerics

802.1x, 343–344

A

A bits, Frame Relay, 286
 ABRs (area border routers), BGP, 234
 abstraction through layering, 35–36
 access layer, routing, 83
 best next hop, 86–87
 dual-homed remotes, 85–86
 single-homed sites, 84
 access lists, 204
 access-list command, 204
 active process, EIGRP, 110–112
 Active state, BGP neighbors, 227
 add/drop multiplexer (ADM) error, 284
 adjacencies
 building, 403–404
 detecting failures, 280–283
 IS-IS, 217, 318
 building, 415–416
 link flaps, 262
 on multiaccess networks, 405
 OSPF, 318
 administrative distance
 BGP, 235
 preventing redistribution routing loops,
 131–132
 advertisements, BGP, 226
 conditional advertisements, 255
 aggregation
 IS-IS, 190
 OSPF, 160–162
 versus summarization, 192
 aggregation layer, summarization, 98
 aging timer (link state), 214
 AH (Authentication Header), 333
 algorithms, BGP, 226
 analyzing redundancy
 MTBF, 23–24
 MTTR, 24–25
 application programming interfaces, 48
 areas, 198, 201–202, 406
 boundaries, IS-IS, 212

AS_PATH length, BGP load sharing, 249
 as-path access-list command, 343
 ASPolicyCerts, BGP, 347
 AS (autonomous systems)
 autosummarization, 137
 BGP, 226, 233
 discontiguous, 138
 EIGRP, 136–139
 assigning IP addresses, 50–53
 ATM (Asynchronous Transfer Mode), NHRP
 case study, 373–375
 attached bits (IS-IS), 198
 attacks
 BGP, 321
 disrupting peering, 318
 flooding, 318
 protocol-level attacks, 318
 transport-level attacks, 318
 disrupting routing domain stability, 324–325
 DoS, 334–335
 preventing via edge filters, 335
 preventing via GTSM, 335, 337
 EIGRP, 320
 falsifying routing information, 323–324
 IS-IS, 318, 320
 OSPF, 318, 320
 protocol-layer attacks, 322
 TCP resets, 321
 AuthCerts, soBGP, 346
 authentication, 311
 MD5, 331–333
 RADIUS servers, 328
 soBGP, 345–346
 transiting trust, 311–313
 versus authorization, 313
 Authentication Header (AH), 333
 authorization, 311
 versus authentication, 313
 RADIUS servers, 328
 soBGP, 346–347
 TACACs servers, 328
 transiting trust, 311–316
 autosummarization, 137, 393

B

bandwidth command, 97
 best next hop, 86–87
 BFD (Bidirectional Forwarding Detection), 283
 BGP (Border Gateway Protocol), 225–226, 233–236, 422
 attacks, 321
 conditional advertisements, 255
 confederations, 240
 core layer, 232–233
 deploying with GR, 304–305
 dividing, 237–238
 dual-homed connections, 247–253
 eBGP, 426
 extranets, 339
 filtering
 with distribution lists, 431
 with prefix lists, 431
 with route maps, 430
 GR, 277–279
 iBGP, 427
 IPSec, 334
 MD5 authentication, 331
 metrics, 423–425
 neighbors, troubleshooting, 227–228, 231
 next hop attribute, 429
 normal restarts, 277
 peers, 227
 route dampening, 255–257
 route reflectors, 242–245
 route servers, 245–247
 scaling, 236–237
 summarization, 432
 synchronization, 431–432
 transport-level attacks, 321
 updates, 239
 bgp dampen command, 257
 bgp dampening command, 340
 bgp graceful-restart command, 279
 bgp graceful-restart stalepath-time seconds command, 279
 bgp graceful-restart-time seconds command, 279
 BGP/MPLS VPNs, 358, 361
 implementing in EIGRP, 361–369
 implementing in OSPF, 369–370
 Bidirectional Forwarding Detection (BFD), 283
 binding EIGRP queries, 393–395
 bit error rate (BER) errors, 284
 black holes, 58, 81, 93

Border Gateway Protocol. *See* BGP
 border routers, BGP, 234
 broadcast interfaces, IS-IS, 210
 broadcast links, IS-IS, 211
 buffer flooding, 318
 building IS-IS adjacencies, 415–416

C

calculating MTBF, 24
 capability lls command, 273
 case studies, OSPF external routes, 182
 CDP (Cisco Discovery Protocol), 219
 CE routers, 356
 checklist for IP network design, 438
 network operations section, 435–437
 redistribution section, 438
 security section, 438
 topological layout section, 437
 choke points, creating, 48
 Cisco Discovery Protocol (CDP), 219
 CLNS (connectionless network services)
 addressing, 412–413
 IS-IS, 189, 205
 clusters, BGP, 242
 commands
 bgp dampen, 257
 set metric-type internal, 233
 show ip bgp neighbor, 227–228
 common services, EIGRP, 91–93
 community strings, 425
 comparing EIGRP and OSPF, 457
 convergence time, 459–462
 ease of troubleshooting, 458–459
 suitability of network designs, 462–468
 complexity of network management, 25
 layering, 27
 functionality, separating, 32
 hiding information, 28–31
 confederations, 240
 Connect state (BGP neighbors), 227
 connectionless network services. *See* CLNS
 connection-oriented network services (CONS), 189
 connections, BGP dual-homed connections, 247–253
 CONS (connection-oriented network services), 189
 control planes, 265
 GR, 266
 convergence. *See also* fast convergence

- decreasing speed, 296
 - EIGRP feasible successors, 296–299
 - link-state incremental SPF, 300–302
 - link-state partial SPF, 299–300
- false injection attacks, 325
- SONET, 284–285
- core layer
 - BGP, 232–233
 - migration, 233–236
 - summarization, 77, 98
 - summarizing to core, 80
 - summarizing to distribution layer, 77–78
- corruption, packet corruption, 214
- creating choke points, 48
- creating layers, 47
- cryptology, key distribution, 345

D

- dampening,
 - BGP route dampening algorithm, 226
 - event dampening, 293–295
- dampening command, 295
- DBDs (database descriptors), 404
- debouncing, 263
- default routes, BGP load sharing, 248
- default-information originate command, 91
- delay, 9
- denial-of-service attacks. *See* DoS attacks
- dense wavelength division multiplexing networks, SONET, 285
- deploying OSPF
 - on three-layer hierarchy, 146–150
 - on two-layer hierarchy, 152
- dial links, OSPF, 180
- dial-in clients, EIGRP, 94
 - bandwidth issues, 97
 - host routes, 94
- DIS (designated intermediate system), 210–211
- discard routes, 116
- disrupting
 - peering attacks, 318
 - routing domain stability attacks, 324–325
- distance command, 131
- distribute lists, 116
 - BGP filtering, 431
 - preventing redistribution routing loops, 130
- distribution layer, summarizing, 80

- toward core, 80–83
- toward remote sites, 83
- dividing BGP, 237–238
- domains, routing, 326
 - illegitimate devices, thwarting, 330
 - IPSec, 333–334
 - MD5 authentication, 331–333
 - router compromise, avoiding, 326
 - filtering access, 328–330
 - using passwords, 326–328
- DoS (denial-of-service) attacks, 334–335
 - preventing via edge filters, 335
 - preventing via GTSM, 335–337
- down detection. *See* failure detection
- DUAL, 383–384
- dual-homed remotes, 85–86
 - best next hop, 86–87
- DWDM (dense wavelength division multiplexing) networks, SONET, 285
- dynamic multipoint IPSec VPNs, 376–378

E

- eBGP, 426
 - peers, 226
- eBGP-multihop, BGP neighbors, 229
- edge filters, 335
- edges, SPF, 299
- EGPs (External Gateway Protocols), 225, 339
 - BGP. *See* BGP
- EIGRP (Enhanced IGRP), 264
 - active process, 111–112
 - admin distance, 131–132
 - attacks, 320
 - bandwidth, 97
 - BGP/MPLS VPNs, implementing, 361–365
 - common services, 91–93
 - comparing with OSPF, 457–468
 - deploying on three-layer network, 75
 - access layer, 83
 - common services area, 91
 - core layer, 77
 - dial-in clients, 94
 - distribution layer, 80
 - stub routers, 87
 - deploying on two-layer network, 97
 - aggregation layer, 98
 - core layer, 98

- dial-in clients, 94
 - bandwidth issues, 97
 - host routes, 94
- discard routes, 116
- distribute lists, 116, 130
- DUAL, 383–384
- dual-homed remotes, 85
- external clients, 91
- external flags, 132–134
- feasible successors, 296–299
- GR, 267–269
- IP summary addresses, 114–115
- load balancing, 396
- loop detection, 388–390
- MD5 authentication, 331
- metrics, 387–388
- multiple autonomous systems, 136–139
- neighbor relationships, 120, 385–386
 - mismatching primary addresses, 120–122
 - multicast delivery problems, 122–123
- neighbors, querying, 390–391
- network design summary, 98–99
- new features
 - active process enhancements, 110–114
 - enhanced route map support, 104–106
 - route map enhancements, 106–110
 - third-party next hop, 99–104
- normal restart, 267
- polling, 280
- prefix lists, 131
- queries
 - bounding, 393–395
 - propagation, controlling, 116–117
- redistribution, 129–130
 - setting admin distance, 131–132
 - using distribute lists, 130
 - using external flags, 132–134
 - using prefix lists, 131
 - using route maps, 130–131
- route maps, 130–131
- routing, access layer, 83–87
- SIA routes, 124–128, 391–393
- single-homed sites, 84
- SRRT, 121
- stub routing, 87–90, 394–395
- summarization
 - controlling query propagation, 116–117
 - core layer, 77–80
 - distribute lists, 116
 - distribution layer, 80–83
 - IP summary addresses, 114–115
 - multiple topology table entries, 118–119
 - stub routers, 87–90
- timers, 134
 - hold timers, 134–135
 - hold/SIA timer interaction, 135–136
 - SIA timer, 135
- topology tables, 118–119
 - clearing, 390–391
- transport-level attacks, 320
- troubleshooting
 - neighbor relationships, 120–123
 - SIA routes, 124–128
- eigrp log-neighbor-changes command, 120
- emergency network management, 18–20
- enable password, 327
- enable secret password, 327
- Encapsulating Security Payload (ESP), 333
- Enhanced Interior Gateway Routing Protocol.
 - See* EIGRP
- EntityCerts, soBGP, 345
- error checking, 215
- errors
 - ADM, 284
 - BER, 284
 - path errors, 284
 - SONET, 284
- ESP (Encapsulating Security Payload), 333
- Established state (BGP neighbors), 228
- Ethernet, failure detection, 288–289
- event dampening, IP, 293–295
 - default values, 295
 - interface specific, 295
- event reporting, limiting, 264–265
 - GR, 266
 - BGP, 277–279
 - EIGRP, 267–269
 - IS-IS, 274–276
 - OSPF, 270–274
 - NSF, 265
- event-driven notification, detecting link/adjacency failures, 283
- exponential backoff, 291
 - deploying, 305
 - setting SPF timers, 306–307
 - IS-IS, 293
 - link-state generation timer, 291
- OSPF
 - LSAs, 292
 - SPF, 292
- SPF timer, 291
- versus IP event dampening, 293–295

- extended access lists, IS-IS, 204
- Exterior Gateway Protocols (EGPs), 225, 339
- external connections, EIGRP, 91
- external flags, preventing redistribution routing loops, 132–134
- external route
- external routes
 - in OSPF, case study, 182
 - injecting, 407
- extranets, 337–338
 - BGP, 339
 - dampening prefixes, 340
 - filtering routes, 339–340
 - limiting route count, 341
 - using EGPs, 339

F

- failure detection, 280
 - Ethernet, 288–289
 - Frame Relay, 285–288
 - measured responses, 290
 - exponential backoff, 291
 - IP event dampening, 293–295
 - IS-IS exponential backoff, 293
 - link-state exponential backoff, 291
 - OSPF exponential backoff, LSAs, 292
 - OSPF exponential backoff, SPF, 292
 - SONET, 284–285
 - using BFD, 283
 - using Ethernet, 288–289
 - using event-driven notification, 283
 - using Frame Relay, 285–288
 - using polling, 280–283
 - using SONET, 284–285
- falsifying routing information attacks, 323–324
- fast convergence, 261–262
 - deploying
 - exponential backoff, 305–307
 - GR versus fast failure detection, 302–304
 - GR with BGP and an IGP, 304–305
 - detecting failures, 280–289
 - limiting reporting, 264, 271–273, 279
 - network meltdowns, 263
 - avoiding with routing protocol design, 263–264
 - troubleshooting, 263
 - slowing down, 290
- fast hellos, 283

- feasible successors, 460
 - EIGRP, 296–299
- feedback loops, 290
- filtering
 - routes in OSPF, 164
 - with distribution lists, 431
 - with prefix lists, 431
 - with route maps, 430
- flags, external flags, 132–134
- flapping, 262
- flaps, BGP, 340
- flooding
 - attacks, 318
 - IS-IS
 - domains, 197
 - full mesh networks, 206
 - link-state packets, 213–214
 - LSAs, 403
- forwarding planes, 265
- Frame Relay
 - A bits, 286
 - detecting failures, 285–288
 - multipoint configuration, 123
 - point-to-multipoint configuration, 287
 - point-to-point configuration, 287
 - polling, 280
- full mesh networks
 - IS-IS, 205, 208–209
 - flooding, 206
 - mitigating single router failure, 208
 - OSPF, 167, 170–171
 - selecting suitable routing protocols, 465–466
- functionality, separating, 32

G

- Generalized TTL Security Mechanism (GTSM), 335–337
- generation timer, link-state, 291
- goals for network design, 5
 - manageability, 13–14
 - day-to-day maintenance, 14–16
 - emergency management, 18–20
 - reliability, 6
 - and resiliency, 10
 - network failures, defining, 12–13
 - network recovery time, 13
 - of packet delivery, 6–9
 - scalability, 20

GR (graceful restart), 266
 BGP, 277–279
 deploying with BGP and an IGP, 304–305
 EIGRP, 267–269
 high availability, 303
 IS-IS, 274–275
 configuring GR, 276
 signaled GR, 275–276
 lab performance, 302
 mixing with non-GR routers, 304
 OSPF, 270–274
 using link local signaling, 271–272
 using opaque LSAs, 272–273
 graceful restart. *See* GR
 Grace-LSAs, 273
 GRE tunnels, 372
 multipoint GRE tunnels, 376–378
 GTSM (Generalized TTL Security Mechanism), 335–337

H

half-life, BGP route dampening, 256
 HDLC (High-Level Data Link Control), polling, 280
 hello interval, 303, 385
 hello messages
 fast hellos, 282
 IS-IS, 217
 padding, 217
 hello packets, polling, 280
 hiding
 information, 28–31
 layers within layers, 46
 hierarchical network design
 abstraction through layering, 35–36
 choke points, creating, 48
 hiding layers within layers, 46
 horizontal layers, 36
 layer functions, 38
 aggregation of routing information, 39
 controlling traffic, 42
 defining routing policies, 41
 forwarding traffic, 38
 user attachment, 42
 layers, creating, 47
 selecting best design, 45
 three-layer hierarchies, 44–45
 two-layer hierarchies, 43–44
 high availability, 303

hold timers, 134–135, 303
 horizontal network layers, 36
 host names, IS-IS LSPs, 200
 HTML server passwords, 327
 hub-and-spoke topologies, 171–177
 IS-IS, 209
 broadcast interfaces, 210
 point-to-point links, 209
 selecting suitable routing protocols, 463–464

iBGP, 427
 peers, 226
 synchronization, 431–432
 Idle state, BGP neighbors, 227
 ignore-lsp-errors command, 215
 IGP (Interior Gateway Protocols), 225
 deploying with GR, 304–305
 regional, 238
 IGP-to-IGP redistribution, 62–64
 incremental SPF, IS-IS, 302
 incremental time, exponential backoff, 291
 incremental updates, BGP, 239
 incremental-spf command, 302
 initial time, exponential backoff, 291
 interfaces
 debouncing, 263
 null0, 234
 intermediate systems
 DIS election process, 211
 parallel links, 212
 selector bits, 216
 serving as DIS, 215
 Intermediate System-to-Intermediate System protocol. *See* IS-IS
 Interior Gateway Protocols. *See* IGP
 Internet, 226
 Internet connections, 341
 protecting against transit, 342–343
 route dampening, 343
 route filtering, 341
 ip address command, 208
 IP addresses
 assigning, 50–53
 IS-IS, 209
 summarizing, 54, 57
 metrics, 61–62
 suboptimal routing, 59–60

- ip default-network command, 91
- ip eigrp hold-time command, 136
- IP event dampening, 293–295
 - default values, 295
 - interface specific, 295
- ip hello-interval eigrp command, 282
- ip hold-time eigrp command, 282
- ip ospf dead-interval minimal hello-multiplier command, 281
- ip ospf resynch-timeout command, 273
- ip router isis command, 208
- IP routes, IS-IS, 205
- IP summary addresses, 114–115
- IPSec, 333–334, 370
 - AH, 333
 - dynamic multipoint IPSec VPNs, 376–378
 - ESP, 333
 - transport mode, 333
 - tunnel mode, 333
- IS-IS (Intermediate System-to-Intermediate System), 189–190, 412
 - adjacencies, building, 318, 415–416
 - aggregation, 190
 - versus summarization, 192–193
 - aging timer, 214
 - attacks, 318, 320
 - blocked interfaces, 207
 - CDP, 219
 - Cisco router default adjacencies, 220
 - CLNS, 189, 205
 - configuring summarization, 204
 - CONS, 189
 - data transport, 318
 - deploying on three layers, 190
 - core as L2 domain, 193–194
 - merging core and distribution in L2, 194–195
 - mixing/overlapping L1/L2 border, 195–197
 - single routing domain, 190, 193
 - deploying on two layers, 197–198
 - DIS election process, 210–211
 - error checking, 215
 - exponential backoff, 293
 - flooding, 206–208
 - domains, 197
 - Frame Relay, 209
 - full mesh networks, 205, 208–209
 - GR, 274–275
 - configuring GR, 276
 - signaled GR, 275–276
 - hub-and-spoke networks, 209
 - broadcast interfaces, 210
 - point-to-point links, 209
 - incremental SPF, 302
 - IP address space, 209
 - IP integration, 417
 - IP routes, 205
 - links parallel to area boundaries, 212
 - link-state flooding, 213–214
 - LSP corruption, 214–215
 - LSP flooding, 416
 - mesh groups, 206
 - metrics, 213, 415
 - MPLS traffic engineering, 213
 - multiple net statements, configuring, 418
 - neighbor adjacencies
 - correcting, 220
 - different subnets, 218
 - misconfigured NSAPs, 217
 - neighbor loss, 417
 - normal restart, 274
 - NSAPs, 215
 - path costs, 213
 - point-to-point broadcast links, 211
 - PRC, 293
 - prefix-driven routing installation, 216
 - pseudonode LSPs, 215–216
 - redistribution, 204–205
 - refresh interval, 214
 - route leaking, 203
 - route maps, 205
 - route tags, 205
 - router isis configuration mode, 201
 - routing, 413–414
 - routing areas, 198–202
 - aggregating routes, 204
 - leaking routes into L1 routing domain, 203–204
 - routing domains, 190
 - L1 versus L2, 198
 - splitting single into multiple, 190
 - routing loops, 205
 - routing tables, 216–217
 - selector bits, 216
 - SPF
 - calculation time, 306
 - trees, 213

- standards track RFCs, 411
- static routes, 205
- subinterfaces, 209
- summarization, 190
 - versus aggregation, 192–193
- suppressing hello padding, 217
- tagging routes, 205
- timers, 264
- transport-level attacks, 318–320
- wide metrics, 213
- isis hello-interval minimal command, 282
- isis hello-multiplier command, 282
- isis link-type level-1-2 command, 212
- isis mesh-group blocked command, 208
- isis mesh-group command, 208
- isis network point-to-point command, 211
- isis priority command, 210
- ispf command, 302
- is-type level-1 command, 201

J-K-L

- jitter, 9
- key distribution, 345
- layer functions, 27, 38
 - aggregation of routing information, 39
 - controlling traffic, 42
 - defining routing policies, 41
 - forwarding traffic, 38
 - hiding information, 28–31
 - separating, 32
 - user attachment, 42
- layered network designs, selecting suitable routing protocols, 466–468
- leaking routes (IS-IS), 204
- leaves (SPF), 299
- link flaps, 262
- link local signaling, 271–272
- links, detecting failures, 280–283
- link-state advertisements. *See* LSAs
- link-state exponential backoff, 291–292
- link-state flooding, 213–214
- link-state generation timer, 291
- link-state incremental SPF, 300–302
- link-state packets. *See* LSPs
- link-state partial SPF, 299–300
- link-state protocols

- IS-IS, 412
 - adjacencies, building, 415–416
 - IP integration, 417
 - LSP flooding, 416
 - metrics, 415
 - neighbor loss, 417
 - routing, 413–414
 - OSPF, comparing with EIGRP, 457–468
- load balancing, 396
- load sharing, BGP, 249–252
- loops, 310
 - detecting, 388–390
 - discard route, 116
 - redistribution routing loops, 129
 - TTL, 336
- LSAs (link-state advertisements), 399–402
 - adjacencies
 - building, 403–404
 - on multiaccess networks, 405
 - age parameter, 402
 - generation time, 461
 - Grace-LSAs, 273
 - opaque LSAs, 272–273
 - OSPF exponential backoff, 292
 - reliable flooding, 403
 - throttling, 292
- lsp-gen-interval command, 293
- lsp-refresh-interval command, 214
- LSPs (link-state packets)
 - attached bits, 198
 - error checking, 215
 - flooding, 213, 416
 - host names, 200
 - reflood storms, 215

M

- manageability of networks, 13–14
 - day-to-day maintenance, 14–16
 - emergency management, 18–20
- MARP (Multiaccess Reachability Protocol), 289
- maximum time, exponential backoff, 291
- max-lsp-lifetime command, 214
- MD5 (Message Digest 5) authentication, 331–333
- MED (Multi-Exit Discriminator), 251, 424
- meltdowns, network, 263
 - avoiding via routing protocol design, 263–264
 - troubleshooting, 263
- mesh groups, 206

- metrics, 387–388
 - BGP, 423–425
 - IS-IS, 213, 415
 - OSPF external route metrics, 164–167
- metric-style transition command, 213
- metric-style wide command, 213
- MPLS (Multiprotocol Label Switching), 213, 353–355
 - BGP/MPLS VPNs, 358, 361
 - implementing in EIGRP, 361–369
 - implementing in OSPF, 369–370
 - overlying routing, 356–357
 - peer-to-peer routing over, 357
- MTBF (mean time between failures), 23–24
- MTTR (mean time to repair), 24–25
- multiaccess networks, OSPF adjacencies, 405
- Multiaccess Reachability Protocol. *See* MARP
- multicast addresses, EIGRP, 122–123
- multiple points of redistribution, 66
 - filters, 67–69
 - tags, 69–71
- multipoint GRE tunnels, 376–378

N

- narrow metrics, 415
- neighbor adjacencies
 - IS-IS, misconfigured NSAPs, 217
 - OSPF, troubleshooting, 184–187
- neighbor relationships
 - BGP, 226, 240
 - troubleshooting, 227–231
 - eBGP, 426–427
 - EIGRP, 385–386
 - hello interval, 385
- net command, 210
- network design goals, 5
 - manageability, 13–14
 - day-to-day maintenance, 14–16
 - emergency management, 18–20
 - reliability, 6
 - and resiliency, 10
 - network failures, defining, 12–13
 - network recovery time, 13
 - of packet delivery, 6–9
 - scalability, 20
- network failures
 - defining, 12–13

- MTBF, 23–24
- MTTR, 24–25
- network layer functions, 38
 - aggregation of routing information, 39
 - controlling traffic, 42
 - defining routing policies, 41
 - forwarding traffic, 38
 - user attachment, 42
- network management, complexity of, 25–32
- network recovery time, 13
- network service access points. *See* NSAPs
- next hop attribute (BGP), 429
- NHRP (Next Hop Routing Protocol), 372–373
 - ATM network implementation, case study, 373–375
- no ip next-hop-self command, 104
- no ip next-hop-self eigrp command, 101
- no ip peer host-route command, 94
- no isis hello-padding command, 217
- nodes, SPF, 299
- Non-Stop Forwarding (NSF), 265
- notification, event-driven, 283
- NSAPs (network service access points), 412–413
 - misconfigured, 217
 - versus IP addresses, 413
- NSAPs (network service access points), 215
- NSF (Non-Stop Forwarding), 265
- NSSAs (Not-So-Stubby Areas), 157–158
- nsf command, 273
- null0 interface, 234

O

- opaque LSAs, 272–273
- OpenConfirm state, BGP neighbors, 228
- OpenSent state, BGP neighbors, 227
- OSPF (Open Shortest Path First)
 - adjacency formation, 318
 - areas, 406
 - attacks, 318–320
 - comparing with EIGRP, 457–468
 - data transport, 318
 - deploying
 - on three-layer hierarchy, 146–150
 - on two-layer hierarchy, 152
 - dial links, 180
 - exponential backoff, 292
 - external routes

- case study, 182
- injecting, 407
- metrics, 164–167
- selecting at ABRs, 167
- full mesh topologies, 167, 170–171
- GR, 270–274
 - using link local signaling, 271–272
 - using opaque LSAs, 272–273
- hello packets, 270
- hub-and-spoke topologies, 171–177
- implementing BGP/MPLS VPNs, 369–370
- incremental SPF, 302
- LSAs, 400–402
 - adjacencies, building, 403–405
 - age parameter, 402
 - reliable flooding, 403
 - throttling, 292
- MD5 authentication, 331
- neighbor adjacencies, troubleshooting, 184–187
- normal restart, 270
- point-to-point broadcast links, 181–182
- polling, 280
- PRC, 293
- restart signaling, 271
- route aggregation, 160–162
- route filtering, 164
- route selection between processes, 167
- router IDs, 399
- SPF
 - calculation time, 306
 - throttling, 292
- stub areas, flooding reduction, 153–155, 160
- summarization, 144–145
- timers, 264
- transport-level attacks, 318–320
- virtual links, 408
- out-of-band resynchronization, OSPF, 271
- output, BGP neighbors, 227
- overlying routing onto MPLS VPNs, 356–357

P

- packet corruption, 214
- packet filtering, 329–330
- packet flooding, 318
- partial route calculation (PRC), 293
- passwords
 - configuration mode access, 327

- console, 327
- enable, 327
- enable secret, 327
- HTML server, 327
- router access, 326
- SSH, 326
- Telnet, 326
- virtual terminal, 326
- path costs, IS-IS, 213
- path errors, 284
- path vector protocols, BGP. *See* BGP
- PE (provider edge) routers, 356
- peer groups, BGP, 239
- peers, BGP, 226–227
- peer-to-peer routing over MPLS VPNs, 357
- point-to-point broadcast links, OSPF, 181–182
- policies, BGP, 225
- polling, detecting link/adjacency failures, 280–283
- port flooding, 318
- pos delay triggers command, 284
- pos threshold command, 284
- PRC (partial route calculation), 293
- pre-interval command, 293
- prefix lists
 - BGP filtering, 431
 - preventing redistribution routing loops, 131
- prefix-driven routing installation (IS-IS), 216
- PrefixPolicyCerts, soBGP, 347
- protocol-level attacks, 318, 322
- pseudonodes, IS-IS, 215–216

Q

- queries
 - controlling propagation, 116–117
 - EIGRP neighbors, 390–391
 - binding, 393–395
 - stub routers, 88

R

- reachability information, 310
- reaction times to failures, 290
- redistribute static ip command, 205
- redistributed next hop, EIGRP, 102–104
- redistribution, 129–130
 - and connected routes, 65

- BGP, 233–235
 - distribute lists, 130
 - external flags, 132–134
 - IGP-to-IGP, 62–64
 - into OSPF, 164–167
 - IS-IS, 204–205
 - multiple points of, 66
 - filters, 67–69
 - tags, 69–71
 - prefix lists, 131
 - route maps, 130–131
 - setting admin distance, 131–132
 - setting admin tags, 133
 - tag filtering, applying, 134
- redistribution command, 204
- redundancy
 - BGP, route reflectors, 244
 - network manageability, effect on , 25
 - resiliency, effect on, 21–22
 - scalability, effect on, 26–27
 - MTBF, 23–24
 - MTTR, 24–25
 - versus resiliency, 6
- reflood storms, 215
- regional IGPs, 238
- reliability, 6
 - and resiliency, 10
 - network failures
 - defining, 12–13
 - recovery time, 13
 - of packet delivery, 6–7
 - delay and jitter budgets, 9
- reporting, limiting, 264–265
 - GR, 266
 - BGP, 277–279
 - EIGRP, 267–269
 - IS-IS, 274–276
 - OSPF, 270–274
 - NSF, 265
- resiliency, 11
 - and redundancy, 6, 21–22
- restart acknowledgment (RA) bit, 275
- restart request (RS) bit, 275
- Restart TLV, 275
- restarts
 - BGP
 - GR, 278
 - normal, 277
 - EIGRP
 - GR, 268
 - normal, 267
 - IS-IS
 - GR, 275
 - normal, 274
 - OSPF GR
 - using link local signaling, 271
 - using opaque LSAs, 272
 - OSPF normal, 270
- reuse limit, BGP route dampening, 257
- route calculation, decreasing convergence speed, 296
 - EIGRP feasible successors, 296–299
 - link-state incremental SPF, 300–302
 - link-state partial SPF, 299–300
- route dampening algorithm, BGP, 226
- route flaps, BGP, 340
- route leaking, 203
- route maps
 - BGP filtering, 430
 - EIGRP, 104–108
 - selecting routes to advertise, 109
 - selective filtering, 109
 - setting tags on redistributed routes, 110
 - IS-IS, 205
 - preventing redistribution routing loops, 130–131
- route reflectors, BGP, 242–245
- route servers, 245–247
- route summarization, BGP, 432
- route tags
 - IS-IS, 205
 - prefix-driven route table installation, 217
- router IDs, 399
- router isis configuration mode, 201, 204, 210, 213
- routers, 310
 - control versus forwarding planes, 265
 - intermediate systems (IS-IS), 190
- routing
 - access layer, 83
 - best next hop, 86–87
 - dual-homed remotes, 85–86
 - single-homed sites, 84
 - calculating routes, 296
 - IS-IS, 413–414
 - OSPF filtering, 164
 - SIA routes, 391–393
- routing areas, IS-IS, 198–202
 - aggregating routes, 204
 - leaking routes into L1 routing domain, 203–204
- routing attacks, 317
 - disrupting peering, 318
 - flooding, 318

- protocol-level attacks, 318
 - transport-level attacks, 318
 - disrupting routing domain stability, 324–325
 - DoS attacks, 334–335
 - preventing via edge filters, 335
 - preventing via GTSM, 335–337
 - falsifying routing information, 323–324
 - transiting authorization, 314–316
 - routing domains, 190, 326
 - illegitimate devices, thwarting, 330
 - IPSec, 333–334
 - MD5 authentication, 331–333
 - IS-IS, 190
 - L1 versus L2, 198
 - L2 in the core, 194
 - overlapping L1/L2, 195
 - splitting single into multiple, 190
 - router compromise, avoiding, 326
 - filtering access, 328–330
 - using passwords, 326–328
 - routing loops, 129, 310
 - IS-IS, 205
 - preventing, 130–134
 - routing policies, 310
 - routing protocols, 309
 - comparing OSPF and EIGRP, 457
 - convergence time, 459–462
 - ease of troubleshooting, 458–459
 - suitability of network designs, 462–468
 - GR operation, 266
 - security, 343
 - 802.1x, 343–344
 - soBGP, 344–348
 - routing tables
 - BGP load sharing, 249
 - IS-IS, 216–217
- S**
-
- scalability, 20
 - and redundancy, 26–27
 - BGP, 236–237
 - secure origin BGP. *See* soBGP
 - security
 - attacks
 - BGP, 321
 - IS-IS, 318–320
 - OSPF, 318–320
 - protocol-layer attacks, 322
 - authentication, 311
 - transiting, 311
 - transiting trust, 311–313
 - authorization, 311
 - transiting trust, 311–313
 - brittleness, 316
 - extranets, 337–338
 - BGP, 339
 - dampening prefixes, 340
 - filtering routes, 339–340
 - limiting route count, 341
 - using EGP, 339
 - Internet connections, 341
 - protecting against transit, 342–343
 - route dampening, 343
 - router filtering, 341
 - IPSec, 333
 - protecting information, 337
 - protocol-layer attacks, 322
 - RADIUS servers, 328
 - routing attacks
 - disrupting peering, 318
 - disrupting routing domain stability, 324–325
 - DoS attacks, 334–335
 - falsifying routing information, 323–324
 - routing protocols, 343
 - 802.1x, 343–344
 - soBGP, 344–348
 - routing systems, 316
 - social engineering, 316
 - TACACS servers, 328
 - TCP, 322
 - trust, 311–313
 - selecting appropriate hierarchical networks, 45
 - selector bits, 216
 - separating network functionality, 32
 - set metric-type internal command, 233
 - shortest path first (SPF) algorithm. *See* SPF
 - show cdp neighbor detail command, 219
 - show clns neighbor command, 218
 - show ip bgp neighbor command, 227–228
 - show ip bgp neighbors command, 279
 - show ip eigrp neighbor command, 128
 - show ip eigrp neighbors command, 121–122
 - show ip eigrp topo command, 296–298

- show ip eigrp topology active command, 126–127
- show ip eigrp topology all command, 118
- show ip eigrp topology command, 118
- show ip interface brief command, 219
- show ip ospf command, 292–293
- show ip ospf neighbor detail command, 273
- show ip ospf stat command, 306
- show ip ospf timers rate-limit command, 292
- show ip protocols command, 269
- show ip route command, 115, 201
- show isis data detail command, 215
- show isis database command, 200
- show isis database detail command, 202
- show is-is nsf command, 276
- show isis spf-log command, 306
- SIA (stuck-in-active), 84, 391, 393
 - routes, troubleshooting, 124–128
 - timers, 135
- signaling, link local, 271–272
- single point of redistribution, 64
- single-homed sites, 84
- Smoothed Round Trip Time (SRRT), EIGRP, 121
- soBGP (secure origin Border Gateway Protocol, 344–345
 - authentication, 345–346
 - authorization, 346–347
 - internetwork topology mapping, 347–348
- social engineering, 316
- sockets, 48
- SONET, 284–285
- SoO attribute (EIGRP), 365–367
- speakers, BGP, 238
- SPF (shortest path first), 264
 - calculation time, 291, 306
 - exponential backoff, setting timers, 306–307
 - flooding, 213
 - incremental, IS-IS, 302
 - IS-IS, 213
 - link-state incremental SPF, 300–302
 - link-state partial SPF, 299–300
 - throttling, 292
- spf-interval command, 293
- SRRT (Smoothed Round Trip Time), EIGRP, 121
- SSH (secure shell), passwords, 326
- standards track RFCs for IS-IS, 411
- stub areas, reducing flooding, 153–155, 160
- stub routing, 87–90, 394–395
- Stuck-in-Active. *See* SIA
- subnetworks, BGP, 238
- suboptimal routing, 59–60
 - summarization, 54, 57, 114, 144–145, 393
 - aggregation layer, 98
 - BGP, 432
 - configuring in IS-IS, 204
 - controlling query propagation, 116–117
 - core layer, 77, 98
 - summarizing into core, 80
 - summarizing to distribution layer, 77–78
 - discard routes, 116
 - distribute lists, 116
 - distribution layer, 80
 - summarizing toward core, 80–83
 - summarizing toward remote sites, 83
 - IP summary addresses, 114–115
 - IS-IS, 190
 - metrics, 61–62
 - multiple topology table entries, 118–119
 - stub routers, 87–90
 - suboptimal routing, 59–60
 - versus aggregation, 192
 - summary command, 204
 - suppress adjacency (SA) bit, 275
 - suppress limit, BGP route dampening, 256–257
 - synchronization, iBGP, 431–432

T

- tables, BGP, 234
 - load sharing, 249
- TCP attacks, 321–322
- Telnet, passwords, 326
- third-party next hop, EIGRP, 99
 - NBMA hub-and-spoke networks, 99–102
 - redistributed next hop, 102–104
- three-layer hierarchies, 44–45
- throttling, 292
- Time To Live (TTL) mechanism, 336
- timers, 324
 - EIGRP, 134
 - hold timers, 134–135
 - hold/SIA timer interaction, 135–136
 - SIA timer, 135
 - IS-IS, 264
 - link-state generation timer, 291
 - link-state update generation, 305
 - OSPF, 264
 - SPF, 291
 - exponential backoff, 306–307
- timers active command, 136

- timers lsa arrival command, 292
- timers nsf route-hold command, 269
- timers throttle lsa all command, 292
- topologies
 - BGP, 226
 - full mesh, 167, 170–171
 - hub-and-spoke, 171–177
- topology maps, soBGP, 347–348
- topology tables, 118–119
 - EIGRP, clearing, 390–391
- totally NSSAs, 159–160
- totally stubby areas, 156
- traffic engineering, IS-IS, 213
- transport mode, IPSec, 333
- transit networks, BGP, 253
- transport-level attacks, 318
 - against BGP, 321
 - against EIGRP, 320
 - against OSPF/IS-IS, 318–320
- troubleshooting
 - EIGRP neighbor relationships, 120
 - mismatching primary addresses, 120–122
 - multicast delivery problems, 122–123
 - OSPF neighbor adjacencies, 184–187
- trust
 - security aspects, 316
 - transitive, 311–313
- TSNRFA (totally stubby not really full area), 160
- TTL (Time To Live) mechanism, 336
- tunnel mode, IPSec, 333
- two-layer hierarchies, 43–44

U-V

- updates, BGP, 239
- virtual links, 408
- virtual terminal passwords, 326
- VPNs
 - MPLS, 353–355
 - BGP/MPLS VPNs, 358, 361–370
 - overlaying routing onto, 356–357
 - peer-to-peer routing over, 357
 - multipoint GRE tunnels, 376–378

W-X-Y-Z

- wait timers, 324
- wide metrics, 415
 - IS-IS, 213
- X.509vs certificate, soBGP, 345