



Symbols

| (vertical bar), string searches, 19–20

A

AAA (Authorization, Authentication, and Accounting)

- command auditing, 156–158
- controlling router access, 154–155

access, out-of-band management

- console servers, 310–311
- modems, 310
- out-of-band circuits, 312
- out-of-band ISDN, 312

access layer, PoP topologies, 228–229

access lists

- route flap-dampening, 373–374
- templates, 333
- types of, 323–324

access network prefixes, 75

access servers, sample configuration, 361–365

ACE depth limit, ASIC-based ACLs, 184

ACLs, 179

- ASIC-based, 183–184
- black-hole routing, 189, 191
- effect on CPU utilization, 179–180
- egress packet filtering, 185
- ingress packet filtering, 187–189
- ISP migration strategies, 391–392
 - antispoofing filters, 393–396
- on VTY ports, 149–150
- PSA, 185
- Turbo ACLs, 181–183

activate command, 128

active configurations, storing on NVRAM, 15–17

active NTP modes, 26–27

adding prefixes

- to IGPs, 70–72
- to OSPF, 77

address families, 125

- activate style commands, 128
- network style commands, 129

address space

- applying for, 256
- assigning to customers, 254–255

addressing, sample configuration, 339

adjacency change logging, IGPs, 72–73

advertisements, route filtering, 170–173

- CIDR, 174–178

aggregates, 62

- comparing old and address family style, 133

aggregation routers

- configuring BGP next-hop-self, 95
- packet filtering, 305
- sample configuration, 349–353

analyzing syslog data, 23–24

anti-spoofing filters, peer configuration, 393–396

applications

- BigBrother, 383
- CAIDA, 380
- cflowd, 380
- Gnuplot, 384
- looking glasses, 383–384
- MIBs, 385
- MRTG, 381
- NeTraMet, 380
- NetSaint, 382
- RAToolSet, 385
- RRDTool, 381
- RTRMon, 384
- Scion/NetScarf, 380
- Scotty, 382
- syslog daemons, 385–386
- SysMon, 382
- traceroute, 383
- Treno, 382
- updating, 242
- Vulture, 381
- whois, 384

applying for address space, 256

architecture, NTP, 25

- client/server models, 26–27

AS number, 262

AS path, length restrictions, 105

ASIC-based ACLs, 183–184

assigning address space to customers, 254–255

association modes, NTP, 26–27

attributes (BGP)

- community, 87, 298
 - RFC 1998, 298–300
 - service provider usage, 301–303

MED

- deterministic, 101
- forcing value to zero, 101

auditing commands, 156–158

authentication

- controlling router access, 153–154
- MD5, 164, 167–169
- one-time passwords, 158–160
- plain-text, 166
- routing updates, 164–166

autonomous systems

- communities, 298
 - RFC 1998, 298–300
 - service provider usage, 301–303
- multihoming, 265–268
 - eBGP multihop, 270, 272
 - general configuration, 272–273
 - stub networks, 268–270
 - to different ISP, 280–285
 - to same ISP, 273–277, 280

autosummarization

- BGP-4, 86–87
- EIGRP, 81

B

backbone networks, 232–234

- BGP model, 258–259
- IP addressing, 243
 - deployment strategy, 251–254

backing up

- images in Flash memory, 8
- running configuration off-router backup, 15–16

bandwidth command, 45

Bates, Tony, 174

BCP 38

- implementing, 191
- uRPF, 191–194
 - configuring, 195–199
 - routing table requirements, 199–200
 - Strict mode, 200–206

best-path algorithm (BGP-4), 82–84

best-path forwarding, 202

BGP. *See also* BGP-4

- address families, 125
- AS path, length restrictions, 105
- communities, 298
 - RFC 1998, 298–300
 - service provider usage, 301–303
- deterministic MED, 101
- eBGP
 - flap dampening, 265
 - flap damping, 264
 - route refresh, 262–264
- fast-external-failover, 106
- filters, processing order, 117–118
- iBGP, scalability, 259–261
- local-as neighbor option, 103
- MED attribute, forcing value to zero, 101
- multihoming, 262, 265–268
 - basic configuration, 272–273
 - eBGP multihop, 270–272
 - stub networks, 268–270
 - to different ISP, 280–285
 - to same ISP, 273–277, 280
- multipath features, 109
 - eBGP Multihop, 109–111
 - eBGP Multipath, 109
 - iBGP Multipath, 111

neighbors

- authentication, 100
- changes, logging, 104
- prefixes, restricting, 104–105

network statement, 102

next-hop-self

- aggregation routers, 95
- external connections, 93–94

ORF, configuring, 120–122

peer groups, 106–108

policy accounting, 123

- configuring, 123
- displaying status, 124

prefix lists, 112

- configuring, 112–113
- incremental configuration, 114–116

prefixes, 118–120

private autonomous systems, configuring, 102

- route damping, 95–98
 - clearing statistics, 100
 - parameters, 98
 - statistics, 99–100
 - route filtering, 170–172
 - route reflectors, 90–92
 - router IDs, comparing, 102
 - weight, 206
- BGP-4**
- autosummarization, 86–87
 - best-path algorithm, 82–84
 - communities, 87
 - neighbor shutdown, 88
 - prefixes, inserting, 73–74
 - route refresh, 89–90
 - soft reconfiguration, 88–89
 - stable iBGP configuration, 85–86
 - synchronization, 87
- BigBrother**, 383
- black-holes**
- filtering, 178
 - routing, 189–191
- black-list filtering**, 190
- booting images from router**, 14–15
- bootp service**, as security risk, 142
- border routers**, sample configuration, 340–345
- border security**, packet filters, 304–305
- breaches in security**, reacting to, 217–218
- broadcast/multicast mode (NTP)**, 26
- building IP devices on ISP backbone**, 161–164
- Bush, Randy**, 386

C

- clearing route damping statistics, 100
- CLI (command-line interface), 18
 - Cisco IOS Software Release 12.0ST
 - BGP configuration CLI, 125–126, 128
 - old/new command style comparison, 128–133
 - editing keys, 18
 - string search, 19–20
 - upgrading, 133–135
- CDP (Cisco Discovery Protocol), as security risk, 143–144
- CEF (Cisco Express Forwarding), 50–51
- cflowd command, 380
- change management, 318–319
- choosing Cisco IOS Software, 3–5
- CIDR (Classless Inter-Domain Routing), 61, 174–175
- Cisco IOS
 - CLI, 18
 - BGP configuration, upgrading, 133–135
 - editing keys, 18
 - string search, 19–20
 - core dumps, 34–35
 - Flash memory, copying images to, 11–13
 - HSRP, 65–67
 - logging configuration, 20–22
 - analyzing syslog data, 23–24
 - syslog topologies, 23
 - regular expressions, 324–325
 - selecting, 3–5
 - software management
 - Flash memory, 7, 9
 - system memory, 9
 - upgrading software, 9–11
 - supported access list types, 323–324
- Cisco IOS 12.0S
 - obtaining information, 5
 - release notes, 5
- Cisco IOS 12.0ST, 5
 - BGP configuration CLI, 125–126
 - command group organization, 126–128
 - old/new command style comparison, 128–130, 132–133
- Cisco IOS 12.2T, 5
- classful networks
 - autosummarization, 86–87
 - synchronization, 87
- clearing route damping statistics, 100
- CLI (command-line interface), 18
 - Cisco IOS Software Release 12.0ST
 - BGP configuration CLI, 125–126, 128
 - old/new command style comparison, 128–133
 - editing keys, 18
 - string search, 19–20
 - upgrading, 133–135
- CAIDA (Cooperative Association for Internet Data Analysis), 380
- CAR (Committed Access Rate), 179
 - preventing smurf attacks, 211–213
 - rate-limiting, 214–216
- carrier hotels, 223
- case studies, load sharing on outbound traffic, 292–297
- caching DNS, 237–238

- client mode (NTP), 26
- client/server models, NTP, 26–27
- cluster ID, 90–92
- clusters, overlapping, 92
- collecting logging information, 21–22
- commands, 126–128
 - activate, 128
 - bandwidth, 45
 - description, 45
 - enable secret password, built-in security features, 145
 - ident, 146
 - ip classless, classless routing, 62–63
 - ip subnet-zero, classless routing, 63
 - ip unnumbered, 45, 47–48
 - more, 19–20
 - network, 129
 - next-hop-self, 93–95
 - no logging console, 22
 - passive-interface default, 77
 - redistribute connected, 71–73
 - redistribute static, 71, 74
 - reload, 14–15
 - show IDB, 50
 - show interface stats, 49
 - show interface switching, 48–49
 - write net, 16
- communities, 298
 - BGP-4, 87
 - RFC 1998, 298–300
 - service provider usage, 301–303
- comparing
 - old and new BGP configuration commands, 128–133
 - router IDs, 102
- conditional advertisements, 118–120
- configuration templates, 327–328
 - general eBGP, 332
 - general iBGP, 331
 - general interface, 329
 - general security, 330
- configuring
 - BGP
 - cluster ID, 90, 92
 - conditional advertisements, 118–120
 - deterministic MED, 101
 - fast-external-failover, 106
 - iBGP, 85–86
 - local-as neighbor option, 103
 - neighbor authentication, 100
 - network statement, 102
 - next-hop-self, 93–95
 - ORF, 120–122
 - peer groups, 106–108
 - policy accounting, 123–124
 - prefix lists, 112–114, 116
 - private autonomous systems, 102
 - restricting neighbor prefixes, 104–105
 - route damping, 95–98
 - EIGRP, 80–81
 - IGPs
 - network design, 75
 - prefixes, 75–76
 - interfaces
 - bandwidth command, 45
 - description command, 45
 - ip unnumbered command, 45–48
 - ipchains, 307–308
 - IS-IS, 78–79
 - load sharing, outbound traffic, 285–292
 - logging, 20–22
 - syslog topologies, 23–24
 - multihoming
 - to different ISP, 280–285
 - to same ISP, 273–280
 - OSPF, 77–78
 - route flap-dampening, 373–376
 - SPD, 64–65
 - Turbo ACLs, 183
 - uRPF, 195–196
 - ACL option, 196, 198
 - debug option, 198–199
 - routing table requirements, 199–200
- congestion, Nagle algorithm, 55–56
- console servers, out-of-band management, 310–311
- controlling
 - router access, 148
 - AAA, 154–155
 - access lists, 149–150
 - building new devices, 161–164
 - command auditing, 156–158
 - ICMP unreachable messages, 160–161

- one-time passwords, 158–160
 - SSH, 151–153
 - user authentication, 153–154
- copying images to Flash memory
 - with FTP, 13
 - with TFTP, 11–12
- core, PoP topologies, 224–225
- core dumps, 34–35
- core routers, sample configuration, 345–349
- creating net police filters, 177–178
- customer networks, IP addressing, 253–255
- customer routers, packet filtering, 306–307
- customer support versus network operations, 317–318
- cut-and-past templates, 327–328

D

- dampening flapping routes, 264–265, 373–376
- debug option, uRPF configuration, 198–199
- default gateways, HSRP, 65–67
- denying unauthorized access, 396–397
- deploying
 - caching DNS, 238
 - IP addressing plan, backbone networks, 251–254
 - IP devices on ISP backbone, 161–164
 - NTP, 27
 - example, 28
 - on a PoP, 28–30
- description command, 45
- designing
 - backbone networks, 232–234
 - BGP model, 258–259
 - IP address space, 244–251
 - flap damping parameters, 98
 - IGP networks, 75
 - PoP topologies, 231
 - access layer, 228–229
 - core, 224–225
 - distribution layer, 225–228
 - Web hosting, 230
 - test laboratories, 315
- Destination Unreachable messages, managing router access, 160–161
- deterministic MED (BGP), 101

- devices
 - routers
 - building new devices, 161–164
 - controlling access, 148–161
 - securing, 141–143
 - testing, 313–314
 - unauthorized access, denying, 396–397
- disabling ICMP unreachable, 161
- displaying route flap statistics, 99–100
- distribution layer, PoP topologies, 225–228
- DNS, 235
 - caching DNS, 237–238
 - mapping IP addresses to names, 56–57
 - name resolution, 58
 - primary DNS, 235
 - secondary DNS, 236–237
- Doran, Sean, 175
- DoS attacks, smurf attacks, 211–213
- dropped packets, SPD, 64–65
- Dynamic Packet Transport, 227

E

- eBGP, peering
 - flap dampening, 264–265
 - route refresh, 262–264
- eBGP Multihop, 109–111
 - multihoming, 270–272
- eBGP Multipath, 109
- editing keys (CLI), 18
- EGPs, BGP-4, 69. *See also* BGP-4
- egress filtering, 170
- EIGRP (Enhanced IGRP), configuring, 80–81
- enable secret password command, built-in security features, 145
- encryption, user passwords, 145–146
- engineering, operational practices, 318
- example configurations
 - aggregation routers, 349–353
 - border routers, 340–345
 - core routers, 345–349
 - ISP addressing plan, 339
 - NTP deployment, 28

expansion

- backbone networks, planning IP address space, 254
 - after six months, 248–249
 - end of first year, 249–251
 - initial needs, 246–248
- Flash memory, 8
- exporting NetFlow data, 54–55
- extended ACLs
 - ASIC-based ACLs, 183–184
 - PSA ACLs, 185
 - Turbo ACLs, 182–183
- exterior routing, AS number, 262
- external prefixes, 76

F

fast-external-failover, 106

feature acceleration, NetFlow, 52

filtering. *See also* ACLs

- ingress/egress traffic, 170
- packets, 178–179
 - access lists, 323–324, 333
 - anti-spoofing filters, 393–396
 - BCP 38, 191, 201–206
 - BGP, processing order, 117–118
 - black-hole routing, 189–191
 - border security, 304–305
 - egress traffic, 185
 - ingress traffic, 187–189
 - net police filters, 176–178
 - on aggregation routes, 305
 - on customer routes, 306–307
 - uRPF, 191–200
- prefixes, BGP prefix lists, 112–116
- routes, 170–173
 - CIDR, 174–178

firewalls, 308

flapping routes

- clearing statistics, 100
- dampening, 265, 373–376
- damping, 95–98, 264
- statistics, 99–100

Flash memory

- Cisco IOS Software management, 7–9
- images
 - copying with FTP, 13
 - copying with TFTP, 11–12
 - reloading, 14–15
- forcing MED value to zero, 101
- forward zones, 236
- forwarding CEF, 50–51
- FTP (File Transfer Protocol), copying images to Flash memory, 13

G

general eBGP templates, 332

general iBGP templates, 331

general interface templates, 329

general security templates, 330

general system templates, 327–328

Gnuplot, 384

H

hardware, testing, 313–314

hash, 167

HSRP (Hot Standby Routing Protocol), 65–67

HTTP servers, 34

hybrid routing protocols, EIGRP, 80–81

I

iBGP (internal BGP), scalability, 259

- peer groups, 260–261
- route reflectors, 260

iBGP Multipath, 111

ICMP (Internet Control Message Protocol), unreachable messages, 160–161

ident command, 146

IGPs (Interior Gateway Protocols), 69

- adjacency change logging, 72–73
- network design, 75
- OSPF, inserting prefixes, 77

- prefixes, 75
 - access network prefixes, 75
 - external prefixes, 76
 - infrastructure prefixes, 76
 - inserting, 70–72
 - selecting, 70
- RID (router ID), 69
- summarization, 72
- images
 - backing up, 8
 - copying to Flash memory
 - with FTP, 13
 - with TFTP, 11–12
 - reloading, 14–15
 - service provider feature set, 4
 - storing on NVRAM, 15–17
- implementing
 - BCP 38, 191–200
 - uRPF strict mode, 200–206
 - NTP on routers, 27
 - example, 28
 - PoP deployment, 28–30
- inbound traffic, 275
 - multihoming, 265–268
 - basic configuration, 272–273
 - eBGP multihop, 270–272
 - stub networks, 268–270
 - to different ISP, 280–285
 - to same ISP, 273–277, 280
- infrastructure prefixes, 76
- ingress filtering, 170
- inserting prefixes
 - into BGP-4, 73–74
 - into IGP, 70–72
 - into OSPF, 77
- interfaces
 - configuring
 - bandwidth command, 45
 - description command, 45
 - ip unnumbered command, 45–48
 - status checking
 - show IDB command, 50
 - show interface stats command, 49
 - show interface switching command, 48–49
 - unnneeded, removing, 142–143
- interior routing protocols, 257
 - scalability, 259
 - peer groups, 260–261
 - route reflectors, 260
- Internet Routing Table, CIDR, 175
- IP addresses
 - applying for address space, 256
 - assigning address space to customers, 254–255
 - backbone networks, 243
 - deployment strategies, 251–254
 - CIDR, 61
 - classless routing
 - ip classless command, 62–63
 - ip subnet-zero command, 63
 - DNS name resolution, 58
 - mapping to names, 56–57
 - prefix lists, route flap-dampening, 375–376
- ip classless command, classless routing, 62–63
- IP source routing, 68
- ip subnet-zero command, classless routing, 63
- ip unnumbered command, 45–48
- ipchains, configuring, 307–308
- IS-IS (Intermediate System-to-Intermediate System), configuring, 78–79
- ISPs
 - BGP
 - AS path length, limiting, 105
 - autosummarization, 86–87
 - comparing router IDs, 102
 - conditional advertisements, 118–120
 - deterministic MED, 101
 - fast-external-failover, 106
 - filter processing order, 117–118
 - local-as neighbor option, 103
 - logging neighbor changes, 104
 - multipath features, 109–111
 - neighbor authentication, 100
 - neighbor shutdown, 88
 - network statement, 102
 - next-hop-self, 93–95
 - ORF, configuring, 120–122
 - peer groups, 106–108
 - policy accounting, 123–124
 - prefix lists, 112–114, 116
 - private autonomous systems, 102
 - route damping, 95–96, 98
 - route reflectors, 90–92

- route refresh, 89–90
- soft reconfiguration, 88–89
- synchronization, 87

IGPs

- EIGRP, 80–81
- IS-IS, 78–79
- network design, 75
- OSPF, 77–78
- prefix types, 75–76

services

- caching DNS, 237–238
- primary DNS, 235
- secondary DNS, 236–237
- mail, 238–239
- news, 240

- source routing, 68

- isp-geeks software, 4

- IXPs (Internet eXchange Medium), route filtering, 172

K

- Kaspia, 388

- keyboard shortcuts, editing, 18

- keys (authentication)

- guarding, 166

- message digest, 167

L**LANs**

- default gateways, HSRP, 65–67

- IP addressing, 253

limiting

- AS path length, 105

- BGP neighbor prefixes, 104–105

link-state routing protocols

- IS-IS, configuring, 78–79

OSPF

- configuring, 77–78

- inserting prefixes, 77

- load sharing, outbound traffic, 285–292

- case study, 292–297

- multiple upstream ISPs, 291–292

- one upstream ISP/one local peer, 286–287

- two upstream ISPs/one local peer, 287–290

- local-as neighbor option, BGP configuration, 103

- logging, 20–22

- BGP neighbor changes, 104

- commands used by employees, 156–158

- IGPs, adjacency changes, 72–73

- syslog

- analyzing data, 23–24

- topologies, 23

- logging in

- banners, as security risk, 144–145

- password encryption, 145–146

- looking glasses, 383–384

- loopback interfaces, 39–40

- FTP exception dumps, 41

- IP addressing, 252

- Netflow flow export, 42–43

- NTP source interface, 43

- RCMD, 44

- router ID, 40

- server access, 41–42

- SNMP traps, 148

- syslog source interface, 43

- telnetting to router, 44

M

- mail services, 238–239

- maintenance, 316–317

- mapping IP addresses to names, 56–57

- martian networks, access lists, 333–334

- MD5 authentication, 164, 167, 169

- MED (multi-exit discriminator) value, forcing to zero, 101

memory

- Flash memory

- Cisco IOS Software management, 7, 9

- copying images to, 11–13

- NVRAM, storing active configurations, 15–17

- system memory, Cisco IOS Software

- management, 9

messages

- ICMP unreachable, 160–161

- syslog

- collecting, 21–22

- time-stamping, 21–22

MIBs, 385
 migration strategies, access security, 391–392
 anti-spoofing filters, 393–396
 denying unauthorized access, 396–397
 modems, out-of-band management, 310
 Modular Syslog, 386
 monitoring
 flapping routes, 99–100
 traffic
 NetFlow, 51–55
 viewing statistics, 53–54
 more command, 19–20
 MRTG (Multi Router Traffic Grapher), 381
 MTRIEs, 179
 multihoming, 262–268
 basic configuration, 272–273
 eBGP multihop, 270, 272
 leased-line customers
 example configuration, 206–210
 uRPF Strict mode, 201–206
 load balancing, 267
 stub networks, 268–270
 to different ISP, 280–285
 load sharing, 282–285
 primary/backup paths, 281
 to same ISP, 273–277, 280
 dual-homed customers, 278–280
 end sites, 273
 load sharing, 276–277
 primary/backup paths, 274–276
 multipath features of BGP, 109
 eBGP Multihop, 109–111
 eBGP Multipath, 109
 iBGP Multipath, 111

N

Nagle congestion-control algorithm, 55–56
 neighbors
 authentication, 164–166
 MD5, 167–169
 plain-text, 166
 BGP
 logging changes, 104
 shutting down, 88
 IGP, logging changes, 72–73

net police filters, 176
 creating, 177–178
 NetFlow, 51
 exporting data, 54–55
 feature acceleration, 52
 viewing statistics, 53–54
 NeTraMet, 380
 NetSaint, 382
 NetStat, 386
 network command, 129
 network design
 aggregation routers, packet filters, 305
 backbone network 232–234
 BGP model, 258–259
 IP address space, 244–254
 border security, packet filters, 304–305
 customer routers, packet filters, 306–307
 IGPs, 75
 news-delivery services, 240
 out-of-band management
 console servers, 310–311
 modems, 310
 out-of-band circuits, 312
 out-of-band ISDN, 312
 PoP topologies, 231
 access layer, 228–229
 core layer, 224–225
 distribution layer, 225–228
 network diagram, 337
 Web hosting, 230
 security
 firewalls, 308
 ingress/egress filtering, 170
 packet filtering, 178–179
 remote access, 309
 route filtering, 170–178
 network management
 best practices, 387–389
 SNMP, 31
 operability with commercial software, 33
 read-only mode, 31–32
 read-write mode, 33
 security, 147
 traps, 148
 tools
 Gnuplot, 384
 looking glasses, 383–384

- MIBs, 385
- RAToolSet, 385
- RTRMon, 384
- syslog daemons, 385–386
- traceroute, 383
- whois, 384

network operations versus customer support, 317–318

news services, 240

- network design, 240

next-hop-self command, 93–95

no ip finger, as security risk, 142

no logging console command, 22

NOC routers, sample configuration, 358–361

NTP (Network Time Protocol), 24–25

- architecture, 25
- client/server models, 26–27
- implementing, 27–28
- PoP deployment, 28–30

NVRAM (non-volatile RAM), storing active configurations, 15–17

O

obtaining information on Cisco IOS 12.0S, 5

off-router backup of running configuration, 15–16

old style BGP commands

- activate, 128
- network, 129

one-time passwords, 158–160

operational practices

- change management, 318–319
- engineering, 318
- maintenance, 316–317
- network operations versus customer support, 317–318

ordering procedures for Cisco IOS Software, Web site, 5

OSPF (Open Shortest Path First)

- configuring, 77–78
- inserting prefixes, 77

outbound traffic, load sharing, 285–292

- case study, 292–297
- multiple upstream ISPs, 291–292
- one upstream ISP/one local peer, 286–287
- two upstream ISPs/one local peer, 287–290

out-of-band management

- access, 148
- circuits, 312
- console servers, 310–311, 366–370
- modems, 310
- out-of-band circuits, 312
- out-of-band ISDN, 312

overlapping route-reflector clusters, 92

P

packet filtering, 178–179

- access list types, 323–324, 333
- anti-spoofing filters, peer configuration, 393–396
- BCP 38, 191
 - uRPF, 191–206
- black-hole routing, 189–191
- border security, 304–305
- egress traffic, ACLs, 185
- ingress traffic, ACLs, 187–189
- on aggregation routers, 305
- on customer routers, 306–307
- SPD, 64–65

passive NTP modes, 26–27

passive-interface default command, 77

passwords

- authentication keys, 166
- encryption, 145–146
- one-time, 158–160

path-selection process, BGP-4, 82–84

peer groups, 106–108, 260–261

- comparing old and address family style, 129
- interaction with route maps, 108

peer mode (NTP), 26

peering

- anti-spoofing filters, configuring, 393–396
- BGP, neighbor authentication, 100
- eBGP
 - flap dampening, 264–265
 - route refresh, 262–264

plain-text authentication, 166

planned software upgrades, reloading images, 14–15

planning backbone IP address space, 245

- after six months, 248
- current needs, 246–248
- end of first year, 249, 251

policy accounting (BGP)

- configuring, 123
- displaying status, 124

policy routing (BGP), prefix lists, 112

- configuring, 112–113
- incremental configuration, 114–116

PoP (Points of Presence), 223, 231

- access layer, 228–229
- core, 224–225
- diagram, 337
- distribution layer, 225–226, 228
- NTP deployment, 28, 30
- Web hosting, 230

prefix lists

- BGP, 112
 - configuring, 112–113
 - incremental configuration, 114–116
- route flap-dampening, 375–376

prefixes (IGPs)

- conditional advertisements, 118–120
- IGPs, 75
 - access network prefixes, 75
 - external prefixes, 76
 - infrastructure prefixes, 76
- inserting
 - into BGP-4, 73–74
 - into IGPs, 70–72
 - into OSPF, 77
- restricting from BGP neighbors, 104–105

preventing sabotage, 156–158

primary DNS, 235

private autonomous systems, 102

processing order, BGP filters, 117–118

Product Bulletin Web site, 5

Proxy ARP, 142

PSA ACLs, 185

Q

QoS, CAR (committed access rate)

- preventing smurf attacks, 211–213
- rate-limiting, 214–216

R

rate-limiting, 214–216

- ICMP Unreachable, 160–161

RAToolSet, 385

reacting to security breaches, 217–218

read-only mode (SNMP), 31–32

read-write mode (SNMP), 33

recommended ISP software, Cisco IOS, 3–5

recommended practices, loopback interfaces, 39–40

- FTP exception dumps, 41
- NetFlow flow export, 42–43
- NTP source interface, 43
- RCMD, 44
- router ID, 40
- server access, 41–42
- syslog source interface, 43
- telnetting to router, 44

redistribute connected command, 71–73

redistribute static command, 71, 74

redistribution, comparing old and address family style, 131

regular expressions, 324–325

- string searches, 19–20

release notes for Cisco IOS 12.0S, 5

reload command, 14–15

remote access, out-of-band management, 309

- console servers, 310–311
- modems, 310
- out-of-band circuits, 312
- out-of-band ISDN, 312

removing

- unnneeded interfaces, 142–143
- unnneeded services, 141–142

resetting BGP sessions, 90

resolving DNS names, 58

- restricting
 - AS path length, 105
 - BGP neighbor prefixes, 104–105
- reverse zones, 236
- RFC 1998, communities, 298–300
- RIDs (router IDs), 69, 102
- RIRs, applying for address space, 256
- route damping, 95–98
 - parameters, 98
 - statistics, clearing, 100
- route filtering, 170–173
 - access lists, 333
 - CIDR, 174–178
- route leaking, 170
- route maps
 - comparing old and address family style, 130
 - interaction with peer groups, 108
- route reflectors, 90–92, 260
 - comparing old and address family style, 132
- route refresh, 262–264
 - BGP-4, 89–90
- router IDs (RIDs), 69, 102
- routers
 - controlling access, 148
 - AAA, 154–155
 - access lists, 149–150
 - building new devices, 161–164
 - command auditing, 156–158
 - ICMP unreachable messages, 160–161
 - one-time passwords, 158–160
 - SSH, 151–153
 - user authentication, 153–154
 - loopback interfaces, 39–40
 - FTP exception dumps, 41
 - NetFlow flow export, 42–43
 - NTP source interface, 43
 - RCMD, 44
 - router ID, 40
 - server access, 41–42
 - syslog source interface, 43
 - telnetting, 44
 - NetFlow
 - enabling, 51
 - exporting data, 54–55
 - feature acceleration, 52
 - viewing statistics, 53–54
 - security, 141
 - removing unneeded interfaces, 142–143
 - removing unneeded services, 141–142
- routes, dampening, 373–376
- routing policies (BGP-4), communities, 87
- routing protocols, 82–84
 - BGP-4
 - autosummarization, 86–87
 - communities, 87
 - neighbor shutdown, 88
 - route damping, 95–98
 - route reflectors, 90–92
 - route refresh, 89–90
 - soft reconfiguration, 88–89
 - stable iBGP configuration, 85–86
 - synchronization, 87
 - classless
 - ip classless command, 62–63
 - ip subnet-zero command, 63
 - EIGRP, configuring, 80–81
 - IGPs, 69
 - access network prefixes, 75
 - adjacency change logging, 72–73
 - external prefixes, 76
 - infrastructure prefixes, 76
 - inserting prefixes, 70, 72
 - network design, 75
 - prefixes, 75
 - RIDs, 69
 - selecting, 70
 - summarization, 72
 - IS-IS, configuring, 78–79
 - OSPF, configuring, 77–78
 - security, 164
 - MD5 authentication, 167–169
 - plain-text authentication, 166
 - updates, authenticating, 164–166
 - SPD, 64–65
- RRDTool, 381
- RTRMon, 384
- running configurations
 - off-router backup, 15–16
 - saving, 16–17

S

- sabotage, preventing, 156–158
- Salsa ACLs, 184
- sample configurations
 - access servers, 361–365
 - aggregation routers, 349–353
 - border routers, 340–345
 - core routers, 345–349
 - ISP addressing plan, 339
 - NOC routers, 358–361
 - out-of-band console servers, 366–370
 - service routers, 353–358
- saving running configurations, 16–17
- scalability of interior routing protocols, 259
 - peer groups, 260–261
 - route reflectors, 90–92, 260
- Scion/NetScarf, 380
- secondary DNS, 236–237
- security
 - ACLs, 179
 - ASIC-based ACLs, 183–184
 - black-hole routing, 189–191
 - CPU utilization, 179–180
 - egress packet filtering, 185
 - ingress packet filtering, 187–189
 - migration strategies, 391–397
 - PSA ACLs, 185
 - Turbo ACLs, 181–183
 - aggregation route filters, 305
 - BGP, neighbor authentication, 100
 - breaches, reacting to, 217–218
 - CAR
 - preventing smurf attacks, 211–213
 - rate-limiting, 214–216
 - CDP, 143–144
 - customer route filters, 306–307
 - enable secret password command, 145
 - encryption, user passwords, 145–146
 - firewalls, 308
 - general security templates, 330
 - ident command, 146
 - ipchains, configuring, 307–308
 - login banners, removing, 144–145
 - networks, 169
 - ingress/egress filtering, 170
 - packet filtering, 178–179
 - route filtering, 170–178
 - packet filters on ISP border, 304–305
 - remote access, 309
 - routers, 141
 - building new devices, 161–164
 - command auditing, 156–158
 - controlling access, 148–155
 - ICMP unreachable messages, 160–161
 - one-time passwords, 158–160
 - removing unneeded interfaces, 142–143
 - removing unneeded services, 141–142
 - routing protocols, 164
 - MD5 authentication, 167, 169
 - plain-text authentication, 166
 - updates, authenticating, 164–166
 - SNMP
 - inherent risks, 147
 - traps, 148
- selecting
 - Cisco IOS Software, 3–5
 - IGPs, 70
- selection process, BGP-4 best-path, 82–84
- server mode (NTP), 26
- servers
 - HTTP, 34
 - ipchains, configuring, 307–308
- service pad as security risk, 142
- service routers, sample configuration, 353–358
- services
 - mail, 238–239
 - news, 240
- shortcuts
 - editing commands, 18
 - string searches, 19–20
- show IDB command, 50
- show interface stats command, 49
- show interface switching command, 48–49
- shutting down BGP-4 neighbors, 88
- single-homed leased line customers, uRPF Strict mode, 200–201
- smurf attacks, 211–213

SNMP (Simple Network Management Protocol), 31

- operability with commercial software, 33
- read-only mode, 31–32
- read-write mode, 33
- security
 - inherent risks, 147
 - traps, 148
- soft reconfiguration, BGP-4, 88–89
- software
 - Cisco IOS
 - CLI, 18–20
 - core dumps, 34–35
 - logging configuration, 20–24
 - selecting, 3–5
 - upgrading, 9–11
 - Cisco IOS 12.0S
 - obtaining information, 5
 - release notes, 5
 - testing, 313–314
 - upgrading, 242
- software management (Cisco IOS)
 - Flash memory, 7–9
 - copying images to, 11–13
 - system memory, 9
- source routing, 68
- SPD (Selective Packet Discard), 64
 - configuring, 64–65
- split advertisement, 205
- SRP (Spatial Reuse Protocol), 227
- SSH on VTY ports, 151–153
- standard ACLs
 - ASIC-based ACLs, 183–184
 - black-hole routing, 189–191
 - CPU utilization, 179–180
 - egress packet filtering, 185
 - ingress packet filtering, 187–189
 - PSA ACLs, 185
 - Turbo ACLs, 182–183
- star topologies, 232
- storing active configuration on NVRAM, 15–17
- stratum number (NTP), 25
- string searches (CLI), 19–20
- stub networks, multihoming, 268–270
- subnets, 62
- subprefixes, 62
- summarization, IGP, 72
- supernets, 62

- switching, CEF, 50–51
- synchronization, BGP-4, 87
- synchronized time, NTP, 24–25
 - architecture, 25
 - client/server models, 26–27
 - implementing, 27–28
 - PoP deployment, 28, 30
- syslog
 - analyzing data, 23–24
 - configuring, 20–22
 - topologies, 23
- syslog daemons, 385–386
- system memory, Cisco IOS Software management, 9

T

- TACACS+ (Terminal Access Control Access Control Server plus), router configuration, 155
- TCP (Transmission Control Protocol), identifying ports, 146
- telnet, VTY ports
 - applying ACLs, 149–150
 - SSH, 151–153
- templates
 - general eBGP, 332
 - general iBGP, 331
 - general interface, 329
 - general security, 330
 - general system, 327–328
- test laboratories, 313
 - designing, 315
 - testing hardware, 313–314
- TFTP (Trivial File Transfer Protocol), copying images to Flash memory, 11–12
- threats to security
 - CDP, 143–144
 - login banners, 144–145
 - reacting to, 217–218
 - unnneeded global services, 141–142
 - unnneeded interface services, 142–143
- time synchronization, NTP, 24–25
 - architecture, 25
 - client/server models, 26–27
 - implementing, 27–28
 - PoP deployment, 28–30
- time-stamping syslog messages, 21–22

tools

- network management
 - Cisco MIBs, 385
 - Gnuplot, 384
 - looking glasses, 383–384
 - RAToolSet, 385
 - RTRMon, 384
 - syslog daemons, 385–386
 - traceroute, 383
 - whois, 384
- traffic engineering applications
 - BigBrother, 383
 - CAIDA (Cooperative Association for Internet Data Analysis), 380
 - cflowd, 380
 - MRTG, 381
 - NetSaint, 382
 - NetTraMet, 380
 - RRDTool, 381
 - Scion/NetScarf, 380
 - Scotty, 382
 - SysMon, 382
 - Treno, 382
 - Vulture, 381

topologies

- backbone network
 - BGP model, 258–259
 - IP addressing, 244–254
- PoPs, 223
 - access layer, 228–229
 - core, 224–225
 - distribution layer, 225–228
 - network design, 231
 - Web hosting, 230

traceroute command, 383

traffic

- BGP, policy accounting, 123–124
- congestion, Nagle algorithm, 55–56
- egress filtering, 170
- ingress filtering, 170
- monitoring
 - NetFlow, 51–55
 - viewing statistics, 53–54
- outbound, load sharing, 285–292
- packet filtering, 178–179

traffic engineering tools

- BigBrother, 383
 - CAIDA, 380
 - cflowd, 380
 - MRTG, 381
 - NeTraMet, 380
 - NetSaint, 382
 - RRDTool, 381
 - Scion/NetScarf, 380
 - Scotty, 382
 - Sysmon, 382
 - Treno, 382
 - Vulture, 381
- traps, 148
- Treno, 382
- Turbo ACLs, 181–183

U

- unauthorized access, denying, 396–397
- Unicast RPF, 178
- unnneeded interfaces, removing, 142–143
- unnneeded services, removing, 141–142
- unnumbered point-to-point links, 46
- updates (authentication), 164–166
 - MD5, 167, 169
 - plain-text, 166
- upgrading
 - BGP configuration CLI, 133–135
 - Cisco IOS Software, 9–11
 - software, 242
- upstream ISPs, applying for address space, 256
- uRPF (unicast Reverse Path Forwarding), 191–194
 - configuring, 195–196
 - ACL option, 196–198
 - debug option, 198–199
 - routing table requirements, 199–200
 - strict mode, 200–206
 - example configuration, 206–210
 - multihomed leased-line customers, 201–206
 - single-homed leased-line customers, 200–201
 - with two ISPs, 210
- user authentication, controlling router access, 153–154

V

- versions of Cisco IOS, upgrading, 9–11
- viewing NetFlow statistics, 53–54
- virtual links, 78
- VTY ports
 - applying ACLs, 149–150
 - SSH, 151–153
- Vulture, 381–382

W-Z

- WAN links, IP addressing, 252
- Web hosting, PoP topologies, 230
- Web sites, Product Bulletin, 5
- weight (BGP), 206
- whitepapers, “*Defining Strategies to Protect Against UDP Diagnostic Port Denial-of-Service Attacks*,”
141
- whois command, 384
- write net command, 16