

Numerics

802.1p bits, 156

A

acceptance testing, 297–298

access

as server provider selection criteria, 28

access technologies

ATM, 57

QoS characteristics, 57

ATM PVC from CE to PE, 59

dedicated circuit from CE to PE, 58

Frame Relay, 57

Frame Relay PVC from CE to PE, 60

metro Ethernet, 60–61

ACLs

boundary ACLs, 215

configuring, 216–217

effectiveness against attacks, 247

infrastructure ACLs, 248–250

receive ACLs, 247

Acme

backbone WAN, 12

global span, 10

IT applications base, 10

IT communications infrastructure, 11

management's business needs, 10

new technology considerations, 13

Layer 2 IP/MPLS VPN services, 18, 20–21

Layer 3 IP/MPLS VPN services, 13, 16–18

regional WANs, 12

Acme, Inc. case studies

remote user access, 369

Acme, Inc. case study

analysing service requirements, 75–77, 79

congestion, 80, 82–83

delay, 79–80

evaluation tools, 83–84

load testing, 80, 82–83

post-transition results, 86–87

routing convergence, 79

TCCP, 84

transition issues, 86

vendor knowledge, 83

QoS for low-speed links, 179, 181

activating

QoS on switch devices, 171–173

address resolution

NHRP, configuring, 357

addressing, 113

addressing schemes for multicast

administratively scoped addresses, 197

well-known group address ranges, 197

administratively scoped multicast addresses, 197

anatomy of DDoS attacks, 264, 266

anycast address, 198

anycast sinkholes, 259

application trust, 155

applying

multicast boundaries to router interface,

216–217

QoS to backup WAN circuits, 156

architecture of botnets, 266

areas, 96

ASICs (application-specific integrated circuits),
201

ASM (Any Source Multicast), 402

ASM (Any-Source Multicast), 203

assigning

metrics, 98

async default ip address command, 338

ATM, 57

QoS characteristics, 57

ATM PVC from CE to PE, 59

attacks

automating with botnets, 266–267

DDoS

anatomy of, 264, 266

identifying, 246

mitigating, 250

mitigation techniques

backscatter traceback, 259, 261

Cisco Guard, 262

*loose uRPF for source-based filtering,
255–256*

*remote-triggered black-hole filtering,
253–255*

- sinkholes*, 258–259
 - strict uRPF*, 256, 258
- preparing for, 245–246
- via worms
 - mitigating*, 268, 270
- authentication**
 - MD5, 120, 236
 - MD5 authentication, 102
 - plaintext password authentication, 102
- automated CE provisioning, 300–302**
- automated PE provisioning, 302**
- automating attacks with botnets, 266–267**
- Auto-RP, 198–199**
- availability, 385**
 - five-nines, 63

B

- backdoor links, 109**
- backhoe fade, 52**
- backscatter traceback, 259, 261**
- backup connections**
 - QoS implementations, 156–157
- bandwidth**
 - of CE-to-PE links, 69
 - QoS service requirement, 62
- bandwidth consumption, 364**
- bandwidth provisioning for LLQ, 151**
- bandwidth requirements for services, 46–47**
 - conversational/realtime services, 49
 - interactive services, 47
 - noninteractive services, 47
 - streaming services, 48
 - triple-play service bundles, 50–51
- baselines**
 - creating, 68
- best-effort data traffic, 171**
- best-effort service, 64, 141**
- best-effort service model, 143**
- BGP**
 - CE-to-PE routing configuration, 119–120
 - convergence
 - tuning*, 121–122
 - deploying in Site Type A sites, 131–134
 - high availability issues*, 134

- deploying in Site Type B sites, 128–130
- deploying in Site Type C sites, 124, 126–127
- deploying in Site Type D sites, 122–123

Bidir-PIM, 193–194

black-hole filtering

- enterprise network susceptibility to, 229

bogons, 249

Bollapragada, Vijay, 359

botnets

- architecture of, 266
- attacks, automating, 266–267
- identification tools, 268

boundary ACLs, 215

bulk background traffic, 68

bulk data, 171

C

cable access

- remote access architecture, 347

cable remote access, 347

calculating

- rate-limiting requirements, 218

call procedure for L2TP, 340

capturing

- network events, 284

case studies

- Acme, Inc.

- implementing multicast over MPLS*, 210–212, 214–216, 218–221, 223–226
- remote user access*, 369

- QoS for low-speed links, 179, 181

case study

- Acme, Inc. service requirements, 75–77, 79

- congestion*, 80, 82–83
- delay*, 79–80
- evaluation tools*, 83–84
- load testing*, 80, 82–83
- post-transition results*, 86–87
- routing convergence*, 79
- TCCP*, 84
- transition issues*, 86
- vendor knowledge*, 83

Catalyst switches

QoS

*activating, 171–173***CBWFQ (class-based weighted fair queuing), 147****CE provisioning, 291****CE-CE monitoring, 287****CE-to-CE IPsec**

mGRE, 356–357

routing protocol concerns, 358–359

CE-to-CE IPsec

DMVPN, 355–356

CE-to-PE link access, 58

ATM PVC from CE to PE, 59

dedicated circuit from CE to PE, 58

Frame Relay PVC from CE to PE, 60

CE-to-PE link bandwidth, 69**CE-to-PE routing**

with EIGRP, 118–119

CGMP (Cisco Group Management Protocol), 201**channel botnets, 266****CHAP (Challenge Handshake Authentication Protocol), 337****circuit protection**

service requirements, 51–52

Cisco Guard

attack mitigation, 262

Cisco IOS tunnel interfaces

and IPsec tunnels, 349

classification

real-time traffic flows, identifying, 165

classification of packets, 66–67**classifying**

data traffic on WAN edge, 176

video traffic on WAN edge, 175

voice bearer traffic, 156

voice traffic on WAN edge, 174–175

commands

async default ip address, 338

crypto isakmp key, 360

crypto isakmp policy 10, 360

ip multicast auto-rp, 200

ip multicast boundary, 199

ip nhrp authentication test, 357

ip ospf broadcast, 358

ip pim spt-threshold infinity, 193

no ip route-cache, 339

comparing

MPLS and IP network operation, 231

source trees and shared trees, 191–192

two-label MPLS imposition to Frame Relay security, 234, 236

components

of L2TP, 340

components of remote-access architecture, 342–343**configuring**

BGP between CE and PE, 119–120

boundary ACLs, 216–217

EIGRP for CE-to-PE routing, 118–119

GRE resiliency, 353

IPsec VPNs, 359

management VRF, 295–296

NHRP, 357

RAS, 338

rate limiting, 219

congestion

of multicast traffic on WAN links, controlling, 189

congestion avoidance, 67**congestion management, 67****congestion-avoidance techniques, 147****connection options**

for Site Type A attached sites, 108–110

for Site Type B dual-attached sites, 110

for Site Type D single-attached sites, 111

content-delivery services, 47**convergence, 99**as server provider selection criteria, 30
BGP*parameters, tuning, 121–122*

service provider mechanisms, 112–113

convergence services

deploying in L3 IP/VPNs

*Internet access, 22**mobile access, 22**voice services, 22***conversational services**

performance targets, 49

cooperation

as server provider selection criteria, 38–39

CoS

requirements for SP networks, 163

ToS, 145

course outlines for system administrator training, 385–387**coverage**

as server provider selection criteria, 28

CPE-to-CPE VPNs

IPsec DMVPN solution, 359, 361

CPN (Cisco Powered Network) IP Multiservice SLA, 382**CPU usage of routing protocols, 100****creating**

design document

table of contents, 379–381

QoS baselines, 68

crypto isakmp key command, 360**crypto isakmp policy 10 command, 360****crypto maps, 349****customer edge router management**

as server provider selection criteria, 40–41

pre-migration considerations, 398–399

customer reports

as server provider selection criteria, 41–42

customer traffic monitoring, 284–285

D**data MDTs, 209****data rates**

for interactive services, 47

data traffic

classifying on WAN edge, 176

QoS requirements, 170–171

DDoS attacks

anatomy of, 264, 266

dedicated circuit from CE to PE, 58**default PIM interface configuration mode, 200****delay variation, 64****delay-sensitive business traffic, 68****deploying**

EIGRP/BGP

in Site Type A sites, 131–134

high-availability issues, 134

in Site Type B sites, 128–130

in Site Type C sites, 124, 126–127

in Site Type D sites, 122–123

Internet access in L3 IP/VPNs, 22

IP multicast service, 198, 200

mobile access in L3 IP/VPNs, 22

design document

creating, 379–381

developing

subscriber network design, 68, 70

device trust, 155**dial access**

RAS, 336

via L2TP, 339

call procedure, 340

dial access users

remote access architecture, 344–345

dialup

VPDN, 340

dial-up access, 336**DiffServ**

tunneling modes, 162

Pipe tunneling mode, 163

Short-Pipe tunneling mode, 163

Uniform tunneling mode, 162

DiffServ (Differentiated Services) service model, 143**distance-vector routing protocols**

CPU usage, 100

distribution trees, 191**diversity, 108****DMVPN, 355–356**

summary of operation, 361–362

DMVPN (Dynamic Multipoint VPN), 355**DOCSIS 1.0**

cable remote access, 347

DoS attacks, 243

history of, 244

DSL, 345, 347**DSL access**

remote access architecture, 345, 347

dynamic diversion architecture, 262

E**ECN (Explicit Congestion Notification), 164****ECT (ECN-capable Transport) bit, 164****Eggdrop Bot, 266**

Eight-Class Model, 176

- implementing, 178

EIGRP

- CE-to-PE routing, 118–119

- CPU usage, 101

- deploying in Site Type A sites, 131–134

- high-availability issues, 134*

- deploying in Site Type B sites, 128–130

- deploying in Site Type C sites, 124, 126–127

- deploying in Site Type D sites, 122–123

- PE-to-CE routing, 114

- metric propagation, 117*

- multiple VRF support, 117*

- redistribution into BGP, 115

EMSS (Ethernet multipoint services), 61**enabling**

- SSM, 206

end-to-end delay, 65**end-to-end remote-access architecture, 345****enforcement of QoS classes on SP IP network, 160****enhanced SLAs**

- as server provider selection criteria, 39

enterprise networks

- connecting at Layer 3 to provider networks, 244–247, 249–252

enterprise networks, 5

- hub-and-spoke topology, 5

- optimizing, 7, 9

- resiliency, 7

- sample network

- backbone WAN, 12*

- global span of, 10*

- IT applications base, 10*

- IT communications infrastructure, 11*

- management's business desires, 10*

- new technology considerations, 13, 16–18, 20–21*

- regional WANs, 12*

- susceptibility to black-hole filtering, 229

enterprise VPN management, 290

- acceptance testing, 297–298

- CE management access, 293, 295–297

- CE provisioning, 291

- monitoring, 298

- optimization, 299

- ordering, 291

- planning, 290

establishing

- hierarchical topologies, 95

- trust boundaries, 153

events

- capturing, 284

examples

- of interactive services, 46

exceeding SPD punt limits, 225**extranets, 74–75****F****fault management**

- alarms, 284

- handling reported faults, 281–282

- passive

- customer traffic monitoring, 284–285*

- network events, capturing, 282–284*

- proactive monitoring, 285, 287–288, 306–307,

- 311–315, 317

- of PE-PE LSPs, 317, 319*

fault monitoring

- MPLS-related MIBs, 302

- BGPv4-MIB, 304*

- MPLS-VPN-MIB, 303*

- resource monitoring, 304–305

financial strength of service provider

- as server provider selection criteria, 29–30

five-nines, 63**flexibility, 104****flow-based load balancing, 52****fragmentation**

- serialization delay, 151

- SPD (Selective Packet Discard) punt limit, exceeding, 225

fragments

- LFI fragment sizing, 159

- queuing, 159

Frame Relay, 57
security of, comparing to MPLS VPN security,
234, 236
Frame Relay PVC from CE to PE, 60
FRTS (Frame Relay traffic shaping), 148
fully managed services, 17

G

generic MIBs
including in fault management strategy, 283
GLBP (Gateway Load Balancing Protocol), 52
governance checkpoints, 171
GRE
resiliency
configuring, 353
GRE tunnels
resiliency, 352
GRIP (Globally Resilient IP), 52
GTS (generic traffic shaping), 148
guaranteed service model, 143

H

hardware queuing, 146
hardware-based forwarding, 232
hat, 409
HG (home gateway), 342
hierarchical campus networks, 54
hierarchical topologies
establishing, 95
scalability, 99
history of IP network attacks, 244
hosting capability
premigration considerations, 407
host-signaling methods, SSM, 205
hub/leaf botnet architecture, 266
hub-and-spoke topology
enterprise network implementation, 5

I

ICMP backscatter traceback, 261

identifying
attacks, 246
real-time traffic flows, 165
worms with NetFlow, 269
identifying botnets, 268
IETF drafts
security-related, 243
IGMP
supported OSs, 206
IGMP (Internet Group Management Protocol), 200
IGMP v3, 205
IGMP v3lite, 205
implementation planning
phase 1 documentation, 388
phase 2 documentation, 389
phase 3 documentation, 389
phase 4 documentation, 390
implementing
Eight-Class Model, 178
multicast over MPLS
case study, 210–212, 214–216, 218–221, 223–226
QoS in IP networks, 67
route limiting on PE routers, 237
routing protocols, 95
WRED, 163
improving BGP convergence, 121–122
incorporating performance characteristics into SLAs, 384
infrastructure ACLs, 248–250
interactive services
examples of, 46
performance targets, 47
interactive video traffic
marking, 177
interdomain multicast protocols, 194
MBGP, 194
MSDP, 195
Internet access
deploying in Layer 3 IP/VPNs, 22
in VPNs, 366–368
pre-migration considerations, 410
inter-provider IP/VPN implementation
premigration considerations, 406
IntServ (Integrated Services) service model, 143
IP addressing, 113

IP multicast

premigration considerations, 402–403

ip multicast auto-rp command, 200**ip multicast boundary command, 199****IP network operation**

comparing to MPLS network operation, 231

IP networks

QoS, implementing, 67

ip nhrp authentication test command, 357**ip ospf network broadcast command, 358****ip pim spt-threshold infinity command, 193****IP telephony call agent**

premigration considerations, 408–409

IP telephony PSTN integration

premigration considerations, 408

IPSec

CPE-to-CPE VPNs

DMVPN solution, 359, 361

multiservice traffic transport, effect of, 362, 364–365

split tunneling, 365

tunnels

and Cisco IOS tunnel interfaces, 349

IPSec VPNs

configuring, 359

prefragmentation, 362

IPSec-to-MPLS access architecture, 349**IPv6**

as server provider selection criteria, 35–36, 38

pre-migration considerations, 406

IPXCP (IPX Control Protocol), 337**ISAKMP (Internet Security Association and Key Management Protocol), 349****J****jitter, 64**

incorporating into SLAs, 384

QoS service requirement, 63

K**Khalid, Mohamed, 359****L****L2 queuing, 146****L2TP, 339**

call procedure, 340

components of, 340

L3 IP/VPNs

Internet access

deploying, 22

mobile access

deploying, 22

voice services

deploying, 22

LAC (L2TP Access Concentrator), 340**Layer 2 QoS service requirements, 65–67****LDP (Label Distribution Protocol) MIB, 282****leased lines**

recommended QoS design, 181

LFI

fragment sizing, 159

LFI (Link Fragmentation and Interleaving), 150**link-state routing protocols**

CPU usage, 101

live events

multicasting

scalability of, 187

LLQ

bandwidth provisioning, 151

LLQ (low-latency queuing), 147**LNS (L2TP Network Server), 340****load balancing, 98**

flow-based, 52

GLBP, 52

loose uRPF for source-based filtering, 255–256**loss**

incorporating into SLAs, 384

low-speed links

QoS case study, 179, 181

LSR-MIB, 282**M****managed services**

zero-touch deployment, 300–302

management VRF

configuring, 295–296

mapping VLANs to VPNs, 55–56

marking

interactive video traffic, 177

MBGP (Multicast Border Gateway Protocol), 194

MCMP (Multiclass Multilink PPP), 52

MD5, 236

neighbor authentication, 120

MD5 (Message Digest 5), 337

MD5 authentication, 102

MDs (multicast domains), 209

MDTs (Multicast Distribution Trees), 209

memory usage of routing protocols, 100

metrics

assigning, 98

route selection, 98

metro Ethernet, 60–61

mGRE, 356–357

mGRE (multipoint GRE), 356

MIBs

LDP-MIB, 282

LSR-MIB, 282

MPLS-related, 302

BGPv4, 304

MPLS-VPN-MIB, 303

MPLS-VPN-MIB, 283

migrating to MVPN, 219

mitigating attacks, 250

Cisco Guard, 262

through backscatter traceback, 259, 261

through loose uRPF for source-based filtering,
255–256

through remote-triggered black-hole filtering,
253–255

through sinkholes, 258–259

through strict uRPF, 256, 258

MLP (multilink PPP), 51

mobile access

deploying in Layer 3 IP/VPNs, 22

modularity, 54

monitoring

customer traffic, 284–285

MPLS-related MIBs, 302

BGPv4-MIB, 304

MPLS-VPN-MIB, 303

**M-RIB (Multicast Routing Information Base),
194**

MSBs (most-significant bits), 145

**MSDP (Multicast Source Discovery Protocol),
195**

MTTR, 385

MTU

premigration considerations, 407

multicast, 187

addressing

administratively scoped addresses, 197

well-known group address ranges, 197

Auto-RP, 198–199

Bidir-PIM, 193–194

deployment models

ASM, 203

SSM, 204–206

host signaling, 200

IGMP, 200

implementing over MPLS, case study, 220–
221, 223–226

boundary ACL, 216

boundary ACLs, 214–215

multicast address management, 212

multicast addressing, 210–211

multicast boundaries, 215

MVPN deployment strategies, 219

predeployment considerations, 212

rate limiting, 218–219

interdomain multicast protocols, 194

MBGP, 194

MSDP, 195

IP addressing scheme, 196

multimedia content

scalability, 187

MVPN, 207

MDTs, 209

MPLS VPN support, 207–208

over MPLS

*preproduction user test sequence, 220,
222–224*

PIM

default interface configuration mode, 200

PIM-DM, 192

PIM-SM, 192

RP, 193

premigration considerations, 402–403

source trees

versus shared trees, 191–192

- sourcing, 202
- SSM, 195–196
- WAN link congestion, controlling, 189
- multicast boundaries, 214**
 - applying to router interface, 216–217
 - positioning, 215
- multicast forwarding, 190**
 - RPF, 190
 - distribution trees, 191*
 - RPF check procedure, 191*
- multicast routing, 190**
- multicasting**
 - on-demand content, 189
 - PIM-SM, 190
- multipoint technologies, 61**
- multipoint-to-point technologies**
 - mGRE, 356–357
- multiservice traffic**
 - transporting over IPsec, effect of, 362, 364–365
- multi-VRF CE, 241**
- MVPN**
 - lack of support for, 224–225
 - MDTs, 209
 - migration strategies, 219
- MVPN (multicast VPN)**
 - MPLS VPN support, 207–208
 - multicast support, 207
- MVRF (multicast VRF), 208**
- MVRFs**
 - MDs, 209

N

- neighbor authentication**
 - using MD5, 120
- NetFlow, 166**
 - identifying worms, 269
- network events**
 - capturing, 284
- network management**
 - enterprise VPN management, 290
 - acceptance testing, 297–298*
 - CE management access, 293, 295–297*
 - CE provisioning, 291*
 - monitoring, 298*
 - optimization, 299*

- ordering, 291*
- planning, 290*
- service provider network management
 - fault management, 281–285, 287–288*
 - proactive fault management, 320, 322, 324, 326*
 - proactive monitoring, 306–307, 311–315, 317, 319*
 - provisioning, 279–280*
 - reactive fault management, 326*
 - reporting, 289, 331*
 - root cause analysis, 289*
 - SLA monitoring, 280–281, 327, 329–331*

network traffic

- types of, 68

NHRP

- configuring, 357

NHRP (Next-Hop Resolution Protocol), 356

no ip route-cache command, 339

non-delay-sensitive business traffic, 68

noninteractive services, 47

O

off-box reachability testing, 309

off-net access to VPNs, 335

on-box reachability testing, 309

on-demand content

- multicasting, 189

operating systems supporting IGMP, 206

optimizing

- enterprise networks, 7, 9

out-of-sequence packet reordering, 33

overhead, 362

P

packet classification, 66–67, 147

packet delay

- QoS service requirement, 63

packet loss

- causes of, 65

- QoS service requirement, 63

packets

- out-of-sequence reordering, 33
- with spoofed bogon addresses
 - tracking*, 251–252

PAP (Password Authentication Protocol), 337**passive fault management**

- customer traffic monitoring, 284–285
- network events, capturing, 282–284

password management, 245**PE**

- automated configuration, 302

PE routers

- route limiting, 237

PE-CE links

- monitoring, 286

PE-PE links

- monitoring, 287

per-customer firewalls within provider network, 242**per-destination load balancing, 98****performance characteristics**

- incorporating into SLAs, 384

performance issues

- troubleshooting, 319–320

performance targets

- for conversational/realtime services, 49
- for interactive services, 47
- for streaming services, 48

performance-reporting portals, 289**performing site surveys**

- required tasks, 390–391

per-packet load balancing, 98**PE-to-CE routing**

- with EIGRP, 114
 - metric propagation*, 117
 - multiple VRF support*, 117

PIM

- Bidir-PIM, 193–194
- default interface configuration mode, 200
- SSM, 195–196

PIM-DM, 192**PIM-SM, 190, 192**

- RP, 193

Pipe mode MPLS tunneling, 35**Pipe tunneling mode, 163****plaintext password authentication, 102****point-to-point technologies, 61****policing, 67****policing traffic, 157–158****policy-based routing, 240****positioning**

- multicast boundaries, 215

PPP (Point-to-Point Protocol), 336**PPPoA (Point-to-Point Protocol over Ethernet), 343****PPPoE (Point-to-Point Protocol over Ethernet), 343****prefragmentation, 362****premigration considerations**

- relating to coverage and topology, 398
- relating to customer edge route management, 398–399
- relating to hosting capability, 407
- relating to Internet access, 410
- relating to inter-provider IP/VPN implementation, 406
- relating to IP telephony call agent, 408–409
- relating to IP telephony PSTN integration, 408
- relating to IPv6, 406
- relating to MTU, 407
- relating to multicast capability, 402–403
- relating to network access, 399–400
- relating to QoS capability, 400, 402
- relating to remote access, 409
- relating to routign protocol capability, 403
- relating to routing protocol capability
 - SLAs*, 404–405
- relating to security, 405–406
- relating to software deployment process, 406

preparing for attacks, 245–246**proactive fault management**

- on service provider network, 320, 322
 - case study*, 324, 326

proactive monitoring, 285, 287–288, 306–307, 311–315, 317

- of PE-PE LSPs, 317, 319

project management methods, 381**propagation delay, 63****protecting against Internet worms, 268, 270****provider WAN infrastructure**

- susceptibility to attacks, 230

provisioning, 141–142

- CE provisioning, 291
- PE configuration, 302
- zero-touch deployment, 300–302

provisioning VoIP bandwidth, 168**provisionless VPWS-based services, 19****public Frame Relay networks**

- bandwidth sharing, 101

pull model, 192**push model, 192****Q****QoS**

- application trust, 155
- at Layer 2
 - service requirements, 65–67*
- classes of service in SP IP core, 160
- configuring on switch devices, 171–173
- CoS
 - ToS, 145*
- data traffic requirements, 170–171
- device trust, 155
- DiffServ
 - Pipe tunneling mode, 163*
 - Short-Pipe tunneling mode, 163*
 - tunneling modes, 162*
 - Uniform tunneling mode, 162*
- implementing, 143
- LLQ
 - bandwidth provisioning, 151*
- marking schemes
 - as service provider selection criteria, 31, 34*
- on backup connections, 156–157
- on SP networks
 - CoS requirements, 163*
 - transparency requirements, 161–162*
- packet classification, 66–67, 147
- policing, 157–158
- premigration considerations, 400, 402
- sample policy template, 179
- service models, 142
- service requirements
 - bandwidth, 62*
 - jitter, 63*

- packet delay, 63*
- packet loss, 63*
- subscriber network design
 - baselines, creating, 68*
 - developing, 68, 70*
- traffic shaping, 157–158
 - FRTS, 148*
- trust boundaries, 152–154
- trusted edge, 154
- video traffic requirements, 169
- voice traffic requirements, 167–168
- VoIP bandwidth provisioning, 168

QoS policies, 69**QoS reporting, 181–182****QoS signaling, 67****quadruple-play service bundles, 51****queuing**

- TX ring buffer, 158

queuing algorithms, 147

- WRED, 148

R**RAS**

- configuring, 338

RAS (remote-access server), 336**rate limiting**

- applying, 218–219
- configuring, 219

RBE (Routed Bridge Encapsulation), 343**reachability testing, 307**

- off-box, 309
- on-box, 309

reactive fault management

- on service provider network, 326

real-time services

- performance targets, 49

real-time traffic, 68**real-time traffic flows**

- identifying, 165

receive ACLs, 247**redistribution**

- EIGRP into BGP, 115

re-marking excess data traffic, 33–34

remote access

- Acme, Inc. case study, 369
- premigration considerations, 399–400, 409
- RAS, 336
 - configuring*, 338
- via cable, 347
- via DSL, 345, 347
- via L2TP, 339
 - call procedure*, 340

remote-access

- dial-up, 336

remote-access architecture

- cable access, 347
- components, 342–343
- dial access, 344–345
- DSL access, 345, 347
- end-to-end, 345

remote-triggered black-hole filtering, 253–255**resiliency**

- in enterprise networks, 7
- of GRE tunnels, 352
- service requirements, 51–52

resource monitoring, 304–305**RFP (Request for Proposal), 375****RFPs**

- writing, 375–378

root cause analysis, 289**route limiting**

- implementing on PE routers, 237

route summarization, 96–97

- effects of, 97

route tagging, 116**routes**

- selecting, 98

routing

- multicast routing, 190
- selecting appropriate protocol, 93–94

routing protocols

- authentication mechanisms, 102
 - MD5 authentication*, 102
 - plaintext password authentication*, 102
- CPU usage, 100
- EIGRP
 - CE-to-PE routing*, 118–119
 - PE-to-CE routing*, 114, 117
- hierarchical topologies, establishing, 95
- implementing, 95

- memory usage, 100

metrics

- assigning*, 98
- premigration considerations, 403
- scalability, 99
- selecting, 93–94
- SLAs
 - premigration considerations*, 404–405

RP

- Auto-RP, 198–199

RP (rendezvous point), 191**RPF, 190**

- distribution trees, 191
- RPF check procedure, 191

RPF (Reverse Path Forwarding), 190**RPMS (Resource Pool Manager Server), 342–343**

S

sample QoS policy template, 179**sample RFP table of contents, 376–378****scalability**

- limiting factors, 99
- of multicasting live events, 187
- of routing protocols, 99

scavenger data traffic, 171**scheduling, 147****SCR (sustainable cell rate), 59****security****ACLs**

- infrastructure ACLs*, 248–250
 - receive ACLs*, 247
- attack mitigation techniques**
- backscatter traceback*, 259, 261
 - Cisco Guard*, 262
 - loose uRPF for source-based filtering*, 255–256
 - remote-triggered black-hole filtering*, 253–255
 - sinkholes*, 258–259
 - strict uRPF*, 256, 258

authentication

- MD5*, 120

authentication mechanisms, 102

- MD5 authentication*, 102
- plaintext password authentication*, 102

- connecting at Layer 3 to provider networks, 244–247, 249–252
- DoS attacks, 243
- IETF drafts, 243
- multi-VRF CE, 241
- of two-label MPLS imposition
 - comparing to Frame Relay operation, 234, 236*
- password management, 245
- per-customer firewalls within provider network, 242
- premigration considerations, 405–406
- spoofed packets, tracking, 251–252
- security requirements**
 - SP-managed VPNs, 72–73
 - topology/design considerations, 71–72
- segmentation requirements, 53–54**
 - mapping VLANs to VPNs, 55–56
- selecting**
 - best route to destination, 98
 - routing protocol, 93–94
 - service providers, 27
- serialization delay, 63, 158**
 - effect on end-to-end latency, 158
- service bundles**
 - quadruple-play, 51
 - triple-play, 50
- service management**
 - as server provider selection criteria, 41
- service models, 142**
- service provider convergence, 112–113**
- service provider network management**
 - fault management, 281–284
 - passive, 284–285*
 - proactive fault management, 320, 322, 324, 326*
 - proactive monitoring, 285, 287–288, 306–307, 311–315, 317, 319*
 - reactive fault management, 326*
 - provisioning, 279–280
 - reporting, 289, 331
 - root cause analysis, 289
 - SLA monitoring, 280–281, 327, 329–331
- service provider selection, considerations**
 - access, 28
 - convergence, 30
 - cooperation, 38–39
 - coverage, 28
 - customer edge router management, 40–41
 - customer reports, 41–42
 - enhanced SLAs, 39
 - financial strength of provider, 29–30
 - IPv6, 35–36, 38
 - service management, 41
 - tiered arrangements, 38–39
 - transparency, 31–33, 35
 - QoS, 31, 34*
- service providers**
 - fault monitoring
 - best practices, 302–305*
 - provisioning
 - best practices, 300–302*
 - selecting, 27
- service requirements**
 - Acme, Inc. case study, 75–77, 79
 - congestion, 80, 82–83*
 - delay, 79–80*
 - evaluation tools, 83–84*
 - load testing, 80, 82–83*
 - post-transition results, 86–87*
 - routing convergence, 79*
 - TCCP, 84*
 - transition issues, 86*
 - vendor knowledge, 83*
 - application/bandwidth requirements, 45–51
 - backup/resiliency requirements, 51–52
 - enterprise segmentation requirements, 53–54
 - mapping VLANs to VPNs, 55–56*
 - extranets, 74–75
 - multiprovider considerations, 74
 - security
 - SP-managed VPNs, 72–73*
 - topological/design considerations, 71–72*
- service requirements for QoS**
 - bandwidth, 62
 - jitter, 63
 - packet delay, 63
 - packet loss, 63
- service requirements for QoS at Layer 2, 65–67**
- sham link, 404**
- shaping**
 - See traffic shaping
- shared trees**
 - RP
 - Auto-RP, 198–199*
 - versus source trees, 191–192

Short-Pipe tunneling mode, 163**SID (Service Identifier), 343****single-label MPLS imposition, 232****sinkholes, 258–259****site surveys**

required tasks, 390–391

Site Type A sites

EIGRP/BGP deployment, 131–134

high-availability issues, 134

Site Type B sites

EIGRP/BGP deployment, 128–130

Site Type C sites

EIGRP/BGP deployment, 124, 126–127

Site Type D sites

EIGRP/BGP deployment, 122–123

site typification

effect on topology, 103–104

Site Type A

connection options, 108–110

topology, 104–105

Site Type B

connection options, 110

topology, 105

Site Type C

topology, 105

Site Type D

connection options, 111

topology, 106–107

SLA monitoring, 327, 329–331**SLAs, 66, 382**

CPN (Cisco Powered Network) IP Multiservice

SLA, 382

performance characteristics, incorporating, 384

premigration considerations, 404–405

table of contents, 382–383

slow-speed leased lines

recommended QoS design, 181

SNMP

MIBs, 283

software deployment process

pre-migration considerations, 406

software queuing, 146**SoO (Site of Origin) extended community, 109****source trees, 191**

versus shared trees, 191–192

sourcing, 202**SP networks**

CoS requirements, 163

QoS transparency requirements, 161–162

SPD (Selective Packet Discard) punt limits

exceeding, 225

"speeds and feeds," 28**split tunneling**

in IPSec, 365

SP-managed VPNs

as service requirement, 72–73

SPTs (shortest-path trees), 191**SRST (Survivable Remote Site Telephony), 52****SSD (Service Selection Dashboard), 343****SSG (Service Selection Gateway), 343****SSM**

enabling, 206

enabling on source server's first hop routers,

213

host-signaling methods, 205

SSM (Source-Specific Multicast), 195–196, 204–205**static routing**

when to use, 94

statistics

QoS reporting, 182

streaming services

performance targets, 48

strict uRPF, 256, 258**subscriber network QoS design**

baselines, creating, 68

developing, 68, 70

summarization, 96–97

effects of, 97

summary of DMVPN operation, 361–362**susceptibility of enterprise networks to black-hole filtering, 229****switches**

QoS

configuring, 171–173

switching delay, 63**system administrators**

training course outlines, 385–387

Sziget, Tim, 178

T

table of contents

- for design document, 379–381
- for SLAs, 382–383

tasks required for performing site surveys, 390–391

TE (traffic engineering), 139

TED (Tunnel Endpoint Discovery), 356

The, 366

tiered arrangements

- as server provider selection criteria, 38–39

TLS, 61

tools

- botnet identification, 268

topologies

- convergence, 99
 - service provider mechanisms, 112–113*
 - tuning BGP parameters, 121–122*

- hierarchical establishing, 95
- premigration considerations, 398
- Site Type A, 104–105
- Site Type B, 105
- Site Type C, 105
- Site Type D, 106–107
- site typification, 103–104

topology

- as service requirement, 71–72
- premigration considerations, 398

ToS (Type of Service), 145

tracking

- spoofed packets, 251–252

traffic conditioning, 148

traffic shaping, 148, 157–158

- FRTS, 148

training system administrators

- course outlines, 385–387

transactional data, 170

transit routers

- enabling for SSM, 206

transparency

- as server provider selection criteria, 31–33, 35
- QoS marking schemes
 - as server provider selection criteria, 31, 34*

transparency requirements on SP networks, 161–162

transport mode (IPSec), 349

transporting

- multiservice traffic over IPSec, effect of, 362, 364–365

triple-play service bundles, 50–51

troubleshooting

- performance issues, 319–320

trust

- application trust, 155
- device trust, 155

trust boundaries, 152–154

trusted edge, 140, 154

tuning

- BGP convergence parameters, 121–122

tunnel mode (IPsec), 349

tunneling modes (DiffServ), 162

two-label MPLS imposition

- comparing to Frame Relay security, 234, 236

TX ring buffer, 158

U

unicast routing, 190

Uniform mode MPLS tunneling, 34

Uniform tunneling mode, 162

unmanaged services, 17

unmanaged VPNs, 72

URD, 205

URD (URL Rendezvous Directory), 205

utilities

- botnet identification, 268

V

Van Jacobsen header compression, 338

vendor-specific MIBs, 283

VHG (Virtual Home Gateway), 343

video traffic

- classifying on WAN edge, 175
- interactive
 - marking, 177*
- QoS requirements, 169

voice bearer traffic classifying, 156

voice services

- deploying in Layer 3 IP/VPNs, 22

voice traffic

- classifying on WAN edge, 174–175
- QoS requirements, 167–168
- VoIP bandwidth provisioning, 168

voice/data integration

- enterprise networks, optimizing, 7, 9

VPDN (Virtual Private Dialup Network), 340

VPLS (Virtual Private LAN Service), 61

VPN life-cycle model, 289

VPNs

- Internet access, 366–368
- off-net access to, 335

VPNv4 addresses, 235

VPWS

- provisionless services, 20

VPWS (Virtual Private Wire Service), 60

VRF, 235

VRFs

- management VRF
 - configuring, 296*

VRFs (virtual routing and forwarding), 54

VSI (virtual switching instance), 61

W

Wainner, Scott, 359

well-known multicast group address ranges, 197

WFQ (weighted fair queuing), 147

Williamson, Beau, 187

worms, 268, 270

WRED, 163

- implementing, 163

WRED (weighted random-early detection), 148

writing

- SLAs

table of contents, 382–383

writing RFPs, 375

- table of contents, 376–378*

Z

zero-touch deployment, 300–302