client connectivity models, scalability, 155–156
Client Mode (EzVPN), 96
Client Mode (EzVPN)
hardware client configuration, 96
server configuration, 98–99
clustering for peer redundancy, 210–212
commands, crypto ca trustpoint, 104
configuring
DPD, 44–47
hub sites, 115–118
idle timeout, 47–50
look ahead fragmentation, 69
multicast on full-mesh point-to-point GRE/IPSec tunnels, 282–284
multicast over IPSec-protected GRE, 280–282
PAT for ESP pass-through, 84–87
RRI, 50–53
spoke sites, 118–120
stateful failover
with SSO, 63
with SSP, 57–63
TED, 217–221
crypto map state, 222–223
fault tolerance, 225
IPSec proxy establishment, 224
redundant peer recovery, 225–227
connection models, 109
GRE model, 73, 111
full-mesh architecture, 165–169
hub-and-spoke architecture, 128–144
keepalives, 73–75
IPSec model, 110
disadvantages of, 110
hub and spoke architecture, 114–120
remote access client model, 112, 144–155
CRL (Certificate Revocation List), 105
crypto ca trustpoint command, 104
crypto keyrings, enabling network-based VPNs, 297
crypto map files, designing for spoke-to-spoke connectivity, 122–124
cryptographic algorithms, 12
asymmetric, 13–14
symmetric, 12

D

databases
SADB, 33
SPD, 32
decoupled VoIP and data architectures, 272–274
decryption, 12
delay, VoIP application requirements for IPSec VPN networks, 267–269
deploying network-based VPNs, 324
FVRF, 300
IPSec to L2 VPNs, 330–334
IPSec to MPLS VPN over GRE, 324–330
PE-PE encryption, 334–339
single IP address on PE, 300–304
designing fault tolerant IPSec VPNs
access links, 175–176
of access links
multiple IKE identities, 176–182
single IKE identity, 183–187
single IKE identity with MLPPP, 188–189
of backbone network, 174
dial backup
with multiple IKE identities, 182
with single IKE identity, 183–187
Diffie-Hellman key exchange, 21–22
digital certificates, 103
  CA enrollment, 104
  revocation, 105–106
digital signature
digital signatures, 14–15
  authentication (IKE), 29–30
  message digests, 14
DMVPN (Dynamic Multipointing VPN), 228, 285–286
  architectures
    dual hub-and-spoke, 250–254
    VoIP, 278–279
  bearer path optimization, 279
  bearer path synchronization, 279
dynamic IPSec proxy instantiation, 236–237
  establishing, 237–247
  functional components of, 229
  mGRE, 229–231
  NHRP, 232–235
DPD (dead peer detection), 43–47
dual hub-and-spoke DMVPN architecture, 250–254
dynamic IPSec proxy instantiation, 236–237
ESP (Encapsulating Security Protocol), 18
  and NAT, 76
  padding, 19
  passing through PAT, 83–87
  SPI, 19
  establishing DMVPN, 237–247
EzVPN, 95
  Client Mode, 96
    hardware client configuration, 96
  on remote access client connection model, 145–151
  server configuration, 98–99
Network Extension Mode, 99
  client configuration, 99
  on remote access client connection model, 151–155
  pushing attributes, 99–101

---

E

EIGRP route blocking, configuring with GRE connection model, 139–140
encryption, 11
  cryptographic algorithms, 12
    asymmetric, 13–14
    symmetric, 12
digital signatures, 14–15

F

fault tolerance
  of access links, 175–176
  multiple IKE identities, 176–182
  single IKE identity, 183–187
  single IKE identity with MLPPP, 188–189
  of backbone network, 174
  peer redundancy
    Cisco VPN 3000 clustering, 210–212
    IPSec stateful failover, 196–200
    simple peer redundancy model, 189–194
    with GRE, 200–204
    with HSRP, 194–196
    with SLB, 204–210
  of TED, 225–227
fragmentation, 65–66
look ahead fragmentation, configuring, 69
full-mesh architectures, 156
GRE model, 165
spoke configuration, 168–169
native IPSec connectivity model, 156
Internet access, 161
spoke configuration, 156–159, 163–164
full-mesh point-to-point GRE/IPSec tunnels
multicast configuration, 282–284
functional components of DMVPN, 229
dynamic IPSec proxy instantiation,
236–237
mGRE, 229–231
NHRP, 232–235
FVRF (front-door VRF), deploying PE-based
VPNs, 300

G
GDOI (Group Domain of Interpretation), 287
GRE (Generic Routing Encapsulation), 6
keepalives, 73–75
multicast configuration, 280–282
peer redundancy, 200–204
GRE connection model, 73, 111
full-mesh architecture, 165
spoke configuration, 168–169
hub-and-spoke architecture, 128
EIGRP route blocking, configuring,
139–140
establishing tunnel connectivity,
135–136
hub configuration, 130–133
hub configuration with dynamic
routing, 136–138
scalability, 143–144
spoke configuration, 134–135
spoke configuration with dynamic
routing, 138–139
transit site-to-site connectivity,
140–141
transit site-to-site connectivity with
Internet access, 141–143
group security association, 289
group security key management, 287

H
hardware client (EzVPN), configuring, 96
HSRP (Hot Standby Routing Protocol)
and RRI, 53–56
peer redundancy, 194–196
hub configuration
for GRE model, 130–138
for spoke-to-spoke connectivity, 124
hub-and-spoke architecture
and IPSec connection model, 114
hub site configuration, 115–118
spoke site configuration, 118–120
DMVPN configuration, 237–250
GRE model, 128
establishing tunnel connectivity,
135–136
hub configuration, 130–133
hub configuration with dynamic
routing, 136–138
scalability, 143–144
spoke configuration, 134–135
transit site-to-site connectivity, 140–141
transit site-to-site connectivity with Internet access, 141–143
GRE with dynamic routing
EIGRP route blocking, configuring, 139–140
spoke configuration, 138–139
Internet connectivity, 126–127
IPSec connection model, scalability, 127–128
NHRP route resolution process, 234–235
remote access client model, 144
EzVPN client mode, 145–151
EzVPN Network Extension mode, 151–155
transit spoke-to-spoke connectivity, 120
crypto map files, designing, 122–124
hub configuration, 124
spoke configuration, 125–126
VoIP, 277
digital signature authentication, 29–30
main mode, 26–27
pre-shared key authentication, 28
phase 2 operation, 30
Quick Mode, 30–32
SAs, 23–25
internal redundancy
stateful IPSec redundancy, 213–214
stateless IPSec redundancy, 213
Internet connectivity, 126
crypto map profiles, 127
for native IPSec connectivity model, 161
IP QoS mechanisms, packet classification, 258
applying to IPSec transport mode, 260
applying to IPSec tunnel mode, 261
attribute preservation of GRE tunnels, 262–264
internal attribute preservation, 264
transitive QoS applied to IPSec, 264
IPSec connection models, 109
GRE model, 111
hub-and-spoke architecture, scalability, 127–128
IPSec model
disadvantages of, 110
hub and spoke architecture, 114–120
remote access client model, 112
IPSec SAs, 23–24
IPSec transport mode, 16–17, 21
IPSec tunnel mode, 17
ISAKMP
profiles, enabling network-based VPNs, 297–299
versus IKE SAs, 24
idle timeout, configuring, 47–50
IGPs (Interior Gateway Protocols), IPSec connection model, 110
IKE
and NAT, 77
Diffie-Hellman key exchange, 21–22
keepalives, 41–42
messages, 24
passing through PAT, 83
phase 1 operation, 25
Aggressive mode, 27–28
authentication methods, 28
IVRF (Inside VRF), deploying PE-based VPNs, 300

J-K

jitter
VoIP application requirements for IPSec VPN networks, 269

keepalives
GRE, 73–75
IKE, 41–42
key management, 21
Diffie-Hellman, 21–22

L

L2TP (Layer 2 Transport Protocol), 8
LACs (local access concentrators), 8
Layer 2 VPNs, 6
Layer 3 VPNs, 6
GRE, 6
IPSec VPNs, 7
MPLS VPNs, 6–7
leased lines, 3
limitations
of PE-based VPNs, 294–296
of TED, 220–221
load balancing, SLB, 205
IPSec peer redundancy, 205–210
look ahead fragmentation, configuring, 69
loss, VoIP application requirements for IPSec VPN networks, 270

M

MAC (message authentication code), 15
main mode (IKE), 26–27
message digests, 14
messages
IKE, 24
IKE keepalives, 41–42
XAUTH, 91
mGRE interfaces, 229–231
MLPPP (multi-link PPP), fault tolerance on access links, 188–189
MODECFG (mode-configuration), 94–95
MPLS VPNs, 6–7
multicast over IPSec VPNs, 280
DMVPN, configuring, 285–286
full-mesh IP tunnels, configuring, 282–284
group security association, 289
group security key management, 287
IPSec-protected GRE, configuring, 280–282
multipoint VPNs, establishing, 237–247, 250–254

N

NAT (Network Address Translation), 76
effect on AH, 76
effect on ESP, 76
effect on IKE, 77
IPSec pass-through, 83
NAT-T, 77–82
native IPSec connectivity model, 156
Internet access, 161
spoke configuration, 156–159, 163–164
Network Extension Mode (EzVPN), 99
  client configuration, 99
  pushing attributes, 99–101
network-based VPNs, 293–294
  deployment models, 324
    FVRF, 300
    IPSec to L2 VPNs, 330–334
    IPSec to MPLS VPN over GRE, 324–330
    IVRF, 300
    PE-PE encryption, 334–339
    single IP address on PE, 300–304
  enabling with Cisco IOS features, 296
    crypto keyrings, 297
    ISAKMP profiles, 297–299
IPSec termination on unique IP address per VRF, 321, 324
  limitations of, 294–296
  mapping IPSec tunnels from telecommuter into IVRF, 315–321
  mapping IPSec tunnel into IVRF, 306–315
  MPLS VPN configuration on PE, 305–306
NHRP, 232
  on hub-and-spoke topologies, 234–235
  non-repudiation, 14

packet classification, 258
  applying
    to IPSec transport mode, 260
    to IPSec tunnel mode, 261
  attribute preservation of GRE tunnels, 262–264
  internal attribute preservation, 264
  transitive QoS applied to IPSec, 264
  packet flow for single IP address on PE
    network-based VPN deployment model, 301–304
  packet size distribution
    effect on queue bandwidth
      assignments, 266
    effect on queue structures, 266
  packets
    fragmentation, 65–66, 69
    GRE keepalives, 75
    IPSec processing, 32
      on Cisco routers, 34–39
      SADB, 33
      SPD, 32
    padding, 19
    PAT (Port Address Translation), 83–84
      configuring to allow ESP, 84–87
    payload data field, 19
PE-based VPNs, 294
  deployment models, 324
    FVRF, 300
    IPSec to L2 VPNs, 330–334
    IPSec to MPLS VPN over GRE, 324–330
    IVRF, 300
    PE-PE encryption, 334–339
    single IP address on PE, 300–304
  enabling with Cisco IOS features, 296
    crypto keyrings, 297
    ISAKMP profiles, 297–299
IPSec termination on unique IP address per VRF, 321, 324
  limitations of, 294–296
  mapping IPSec tunnel from telecommuter into IVRF, 315–321
  mapping IPSec tunnel into IVRF, 306–315
  MPLS VPN configuration on PE, 305–306
peer redundancy

IPSec stateful failover, 196–200
simple peer redundancy model, 189–192
asymmetric routing problem, 192–194
with Cisco VPN 3000 clustering, 210–212
with GRE, 200–204
with HSRP, 194–196
with SLB, 204–210
PKI (Public Key Infrastructure), 30
PMTUD, 66–69
pre-shared key authentication (IKE), 28
private networks, NAT, 76
effect on AH, 76
IPSec pass-through, 83
NAT-T, 77–82
processing packets, 32
on Cisco routers, 34–39
SADB, 33
SPD, 32
public key algorithms, 13
public key encryption, digital signatures, 14–15
public networks, 4
PVCs (permanent virtual circuits), 6

packet size distribution
effect on queue bandwidth assignments, 266
effect on queue structures, 266
Quick Mode (IKE phase 2), 30–32

R

redundancy
stateful, 213–214
stateless, 213
TED peer recovery, 225–227
remote access client connection model, 112
hub-and-spoke architecture, 144
EzVPN client mode, 145–151
EzVPN Network Extension mode, 151–155
remote access VPNs, 8
restricted ESP passing through PAT, 84
revocation of digital certificates, 105–106
RFC 2401, packet processing, 32
RRI (Reverse Route Injection)
and HSRP, 53–56
configuring, 50–53

S

SADB (Security Association Database), 33, 56
SAs
IKE, 23–25
IPSec, 23–24
synchronization, 57
SADB transfer, 57

QoS, 258
packet classification, 258
applying to IPSec transport mode, 260
applying to IPSec tunnel mode, 261
attribute preservation of GRE tunnels, 262–264
internal attribute preservation, 264
transitive QoS applied to IPSec, 264
SAs (security associations)
- idle timeout, configuring, 47–50
- IKE phase 1 operation, 25
  - Aggressive mode, 27–28
  - authentication methods, 28
  - digital signature authentication, 29–30
  - main mode, 26–27
  - pre-shared key authentication, 28
- IKE phase 2 operation, Quick Mode, 30–32
- IPSec, 23–24

scalability
- of client connectivity model, 155–156
- of GRE hub-and-spoke model, 143–144
- of IPSec VPN hub-spoke model, 127–128

security
- authentication
  - digital certificates, 103–106
  - MODECFG, 94–95
  - XAUTH, 89, 92–93
- group security associations, 289
- group security key management, 287
- sequence numbers, 19
- serialization delay, 268
- simple peer redundancy model, 189–192
  - asymmetric routing problem, 192–194
- site-to-site architectures, VoIP over IPSec
- site-to-site VPNs
  - GRE connection model, 111
  - IPSec connection model, 110
  - remote access client connection model, 112
- SLB (Server Load Balancing), peer redundancy, 204–210
- SPD (Security Policy Database), 32

SPI (security parameter index), 19
- split tunneling, 126
- spoke configuration
  - for GRE model, 134–135, 168–169
  - for GRE with spoke default routing, 142–143
  - for native IPSec connectivity model, 156–159, 163–164
  - for spoke-to-spoke connectivity, 125–126
  - GRE model with dynamic routing, 138–139
- spoke sites, configuring, 118–120
- SSO (Stateful Switch Over), configuring, 63
- SSP (State Synchronization Protocol), 57
- standby track command, 196
- stateful failover, 56, 196–200
  - configuring with SSO, 63
  - configuring with SSP, 57–63
- SADB synchronization, 57
- SADB transfer, 57
- stateful IPSec redundancy, 213–214
- stateless IPSec redundancy, 213
- SVCs (switched virtual circuit), 6
- symmetric cryptographic algorithms, 12

TED (Tunnel Endpoint Discovery)
- auto-configuring site-to-site IPSec VPNs, 217–220
- configuring, 221–225
- limitations of, 220–221
- redundant peer recovery, 225–227
- transit site-to-site connectivity on GRE connection model, 140
  - with Internet access, 141–143
transit spoke-to-spoke connectivity, 120
    crypto map files, designing, 122–124
    hub configuration, 124
    spoke configuration, 125–126
transport mode, 16–17
    AH, 21
tunnel mode, 17
two factor authentication, 93

mapping IPSec tunnel from
telecommuter into IVRF,
315–321
mapping IPSec tunnel into IVRF,
306–315
MPLS VPN configuration on PE,
305–306

V

virtual circuits, 6
virtual IPSec peer model, 194–196
VoIP
    application requirements for IPSec VPN networks
        delay, 267–269
        jitter, 269
        loss, 270
decoupled VoIP and data architectures,
272–274
ingeering best practices, 271
hub-and-spoke architectures, 277
over DMVPN architecture, 278–279
over IPSec remote access, 274
over IPSec-protected GRE architectures,
275–276
VPNs
    network-based, 293–294
        deployment models, 300–304,
        324–339
        enabling with Cisco IOS features,
        296–299
        IPSec termination on unique IP address per VRF, 321, 324
        limitations of, 294–296

X-Z

XAUTH (extended authentication), 89, 92–93