INDEX

Numerics

12tp authentication password command, 789
12tp security crypto-profile command, 734
3DES (Triple DES)
defined, 418
IKE, 462
6VPE
configuring, 395-401
overview, 392-393
packet forwarding, 394-395
route exchange, 393-394
verifying 6VPE, 401-403
802.1Q Ethernet, 8, 163-170
AToM pseudowire transport, 157-165
L2TPv3 pseudowire transport, 50-52

A

AAA (authentication, authorization, administration)
RADIUS servers, 736
remote AAA, configuring
SSL VPNs on Cisco ASA 5500 Series devices, 972-973
SSL VPNs on Cisco IOS devices, 964-965
aaa authentication command, 871
aaa authentication login command, 825, 872
aaa authentication ppp default group radius command, 791
aaa authorization command, 871
aaa authorization network command, 825, 873
aaa authorization network default group radius command, 791
aaa new-model command, 791, 825
aaa-server command, 830, 973
AAL (ATM Adaption Layer), 70
AAL0 encapsulation, 215
AAL5 encapsulation, 214
AAL5 PDU, 70
AAL5 SDU
OAM cells, transparent forwarding, 73
overview, 70
transporting ATM traffic over L2TPv3 pseudowires, 89-92
About tab (Cisco SSL VPN Client), 952
accept-dial command, 795
accept-dialin command, 734
access-list command, 878
acl command, 826
Address field
Cisco HDLC frame, 53
Frame Relay frame, 61-62
PPP frame, 56
Address messages, 142
address negotiation, 814-816
address pools, 725, 817
Address Withdraw messages, 142
address-family ip4 vrf vrf-name command, 247
address-family ipv4 mdt command, 367
address-family ipv4 vrf vrf-name command, 245-248
address-family vpnv4 command, 242
address-pool command, 831
AES (Advanced Encryption Standard)
IKE, 462
IPsec, 418
aggressive mode negotiation (IKE phase 1), 435-436
AH (Authentication Header)
ESP, configuring together, 430-431
headers, 423
IPsec, 422-426
NAT/PAT, 503, 507-508, 518
packet capture, 425
transform sets, 471
transport mode, 423
tunnel mode, 424
alert protocol, SSL, 908-910
Any Transport over MPLS. ***See*** **AToM**
AppleTalk, L2TP remote access VPNs, 711
application data protocol, 908-910
Application Layer VPNs, 18
ARP mediation, 102
ASA 5500 Series appliances
SSL remote access VPNs, deploying
cryptographic algorithms, configuring, 978
e-mail proxy, configuring, 976-977

file access/entry/browsing, configuring, 974
HTTP server, configuring, 971
login/home pages, customizing, 978-979
operation of, verifying, 979-980
overview, 970
port forwarding, configuring, 975
SSL trustpoint, specifying, 977
SSL versions, restricting, 977-978
URL lists, specifying, 973-974
user authentication, configuring, 972-973
user group policy, configuring, 971-972
WebVPN, enabling on outside interface, 971

ASBRs (Autonomous System Boundary Routers), 316
MPLS Layer 3 VPNs
advertisement of labeled VPN-IPv4 routes, 325-333
VRF-to-VRF connectivity, 316-324

async mode interactive command, 790
async-bootp dns-server command, 795
ATM
cell format, 68-69
NNI header, 69
OAM cells, 71-73
UNI header, 69
header format, 68
overview, 67-70
reference model, 67-68

ATM AAL5 PDU mode, 177
ATM AAL5 SDU mode, 177
ATM cell relay
ATM n-to-one mode, 176
transporting ATM traffic over AToM
cell packing, 180-184
n-to-one mode, 180-187
port mode, 178-180
single cell relay, 180
VCC cell relay, 176, 180-185
VPC cell relay, 176, 180-187
transporting ATM traffic over L2TPv3
AAL5 SDU mode, 89-92
advantages/disadvantages, 77
cell packing, 77-78
encapsulation, 73
OAM cells, 71-73
overview, 66-70
port mode cell relay, 84-85
VCC cell relay, 79-88

ATM layer (ATM reference model), 68
atm mcpt-timers command, 87, 184, 187
atm pvp vpi 12transport command, 186
AToM (Any Transport over MPLS), 137
advanced features
data channel packet drop, resolving, 217-222
interworking, 188, 207-211
local switching, 188, 211-217
pseudowire switching, 202-207
QoS, 188-194
tunnel selection, 188, 195-202
tunnel switching, 188
channels, 139
Draft Martini, 139
GRE, 138
LDP discovery, 143
pseudowires
data channel packet forwarding, 154-156
deploying, 156-187
overview, 137
types, 147
setup, 142-150
FEC TLV, 145-146
Generic Label TLV, 146
signaling, 150-153

AToM-based L2VPNs
advantages/disadvantages, 138-139
control channel messages, 139
header fields, 140
LDP, 141-142
data channel messages, 139
data channel packet drops, 217-222
interworking, 188, 207-211
IPX, 138
local switching, 188, 211-212
circuits on same interface, 216-217
different types of physical interfaces, 215-216
same types of physical interfaces, 213-215
pseudowire switching, 202-207
QoS, 188-194
setup, 142-150
FEC TLV, 145-146
Generic Label TLV, 146
signaling, 150-153

tunnel selection, 188, 195-202
tunnel switching, 188
AToM-based pseudowires
ATM traffic, transporting
overview, 176-178
ATM cell relay, 178-187
Ethernet mode interworking, 207
Ethernet traffic, transporting
overview, 156-157
port transport, 157-163
VLAN transport, 163-165
Frame Relay traffic, transporting, 171-176
HDLC traffic, transporting, 165-170
IP mode interworking, 207-211
PPP traffic, transporting, 165-170
attachment circuit status, 151-153
authentication
certificates, 847
data origin, 410
digital signatures, 448-451, 724, 743-756, 833-834
authenticating CAs, 454-456
auto-enrolling with CAs, 459-460
automating re-enrollment with CAs, 460-461
Cisco ASA 5500, 842-844
Cisco IOS routers, 842
Cisco VPN 3000 concentrators, 834-842
clients, 844-847
declaring CAs, 452-454
enrolling with CAs, 456-459
generating RSA keys, 451-452
groups, 756-759
host/domain name configuration, 451
Windows, 759-765
encrypted nonces, 444-448
Hybrid Authentication
Cisco VPN 3000 concentrators, 848-849
Cisco VPN Clients, 849-850
overview, 847
IKE, 434, 441, 464, 725
digital signatures, 448-461, 555-556
encrypted nonces, 444-448, 553-554
preshared keys, 441-444, 550-552
IKEv1, 810
address negotiation, 814-816
CRACK, 813-814
Hybrid Authentication, 812-813
Xauth, 810-811
IPsec, 410, 725
hash, 410-413
HMAC, 413-414
MAC, 413-414
L2TP/IPsec, 713
no12tp tunnel authentication command, 734
NTP, 450
PPP, 780
preshared key, 724, 816
Cisco ASA 5500, 827-831
Cisco IOS routers, 824-827
Cisco VPN Client, 832-833
configuring, 817-824
PSK on Cisco routers, 732-736
RADIUS servers, 830
RASCHAP.log file, 773
remote AAA, 964-965, 972-973
SSL remote access VPNs
RSA handshake with client, 920-922
RSA handshake with VPN gateway only, 910-920
Windows PSK authentication, 736-742
authentication command, 825
IKE, 464
options, 465
Authentication Header. *See* AH
authentication-only flag, ISAKMP, 809
authentication-server-group command, 830
auto-enroll command, 460
auto-initiation, wireless VPNs, 896
Autonomous System Boundary Routers. *See* ASBRs
autonomous-system autonomous-system-number command, 246
autoselect PPP command, 790
availability. *See* high availability
AVPs (attribute-value pairs), 31-32

B

backbone network IGP, configuring in MPLS Layer 3 VPNs
IS-IS as, 240-241
OSPF as, 239-240

backup-gateway command, 826
banner command, 829
base groups, configuring, 727-731
BGP/MPLS VPNs. *See* MPLS Layer 3 VPNs
block ciphers
AES, 418
DES, 418
IPsec, 416-418
brute-force attacks, 418
BVI (Bridge Virtual Interface), 100

C

C (Customer) devices, 5
Cache Cleaner module (Cisco Secure Desktop)
Mac/Linux users, 961-962
Windows users, 957-958
Call-Disconnect-Notify (CDN) message, 716
carrier of carriers, 11
carrier_s carrier VPN service, 11
carriers' carrier architecture. *See* CSC
CAs (certificate authorities)
defined, 434
digital signature authentication, 743-756
IOS routers, enrolling, 965
IPsec VPN gateways, 452-461
L2TP/IPsec, 759-760, 763-765
Microsoft, 752
re-enrollment, 460
SCEP, 837, 839
CDP (CRL Distribution Point), 572
CE (Customer Edge) devices, 5
configuring for MPLS Layer 3 VPNs, 236
IP reachability in MPLS Layer 3 VPNs, 227-229
size sweeps, 219
CEF (Cisco Express Forwarding), 43
L2TPv3 dynamic session setup, 43
L2TPv3 static session setup, 93
Cell Loss Priority (CLP) field (UNI ATM cell header), 69
cell packing transport
over AToM, 184-185, 214
over L2TPv3, 77-78, 85-88
cell-packing command, 87, 184, 187
cells (ATM), 68-69
NNI header, 69
OAM cells, 71-73
UNI header, 69
CE-r (Customer Edge routers), 5
certificate authorities. *See* CAs
certificate ca command, 456
certificate repository, 572
certificate requests, 748
Certificate Revocation Lists, 435, 563-567, 572
certificate servers, configuring for PKI deployments, 580-590
Certificate SSL/TLS handshake protocol message, 910-916, 922
CertificateRequest SSL/TLS handshake protocol message, 910, 922
certificates
authentication, 847
L2TP/IPsec, 759-760, 763-765
PKI
approving/rejecting, 590-592
requesting manually, 593
revoking, 563-568, 592-593
X.509 certificates, 558-562
CertificateVerify SSL/TLS handshake protocol message, 910, 922
CE-s (Customer Edge switches), 5
Challenge/Response Authentication of Cryptographic Keys, 810, 813-814
change cipher spec protocol, 908-910
CHAP voluntary tunnel mode, 712
Cipher Feedback (CFB) mode, 416
Cipher-Block Chaining (CBC) mode, 416
ciphertext
defined, 415
public key algorithms, 419
Cisco ASA 5500 Series appliances, deploying SSL remote access VPNs
cryptographic algorithms,configuring, 978
e-mail proxy, configuring, 976-977
file access/entry/browsing, configuring, 974
HTTP server, configuring, 971
login/home pages, customizing, 978-979
operation of, verifying, 979-980
overview, 970
port forwarding, configuring, 975
SSL trustpoint, specifying, 977

SSL versions, restricting, 977-978
URL lists, specifying, 973-974
user authentication, configuring, 972-973
user group policy, configuring, 971-972
WebVPN, enabling on outside interface, 971
Cisco Express Forwarding. *See* CEF
Cisco HDLC frame, 53
Cisco IOS devices, enabling SSL VPNs
basic SSL parameters, configuring, 966-967
domain name address, configuring, 964
IOS router, enrolling with a CA, 965
login/home pages, customizing, 967-969
name server address, configuring, 964
overview, 963
port forwarding, configuring, 969-970
remote AAA, configuring, 964-965
URLs, specifying, 969
webvpn enable command, 966
Cisco Secure ACS
compulsory tunnel mode, 796
IETF tunnel attributes, 792-793
Cisco Secure Desktop
configuring for Windows clients
Cache Cleaner module, 957-958
location settings, 954-956
Secure Desktop module, 959-961
VPN Feature Policy module, 958-959
enabling, 962-963
installing, 954
Mac and Linux Cache Cleaner options, 961-962
overview, 952-953
Cisco SSL VPN Client
advantages/disadvantages, 948
enabling, 949
installing, 948
overview, 905, 948
remote access connectivity, 950-952
Cisco VPN 3000 concentrators
clientless SSL remote access VPNs, enabling
configuration tasks, 925-930
e-mail proxy, 943-948
file server access, 930-935
overview, 924-925
TCP-based application access, 937-942
web server access, 936-937
digital signature authentication, 834-842
L2TP/IPsec digital signature authentication, 743-759
L2TP/IPsec VPN gateway, 725-732
NAT-T, 775
preshared key authentication, 817-824
Cisco VPN Client
logs, 861
overview, 807
preshared key authentication, 832-833
class class-default command
AToM QoS, 194
L2TPv3 tunnel marking, 125
class maps, configuring for L2TPv3 tunnel marking, 123-124
class-map command, 190
cleartext, 415
client authentication command, 872
client configuration address command, 873
client software, 711
client user accounts
L2TP/IPsec, 769-773
PSK authentication, 731
ClientHello SSL/TLS handshake protocol message, 909-914, 920
client-initiated remote access VPNs, 16
client-initiated tunnel mode. *See* voluntary/client-initiated tunnel mode
ClientKeyExchange SSL/TLS handshake protocol message, 910-912, 916-917
clientless SSL remote access VPNs
advantages, 9
e-mail proxy, 943-948
file server access, 930-935
overview, 924
TCP-based application access, 937-942
web server access, 936-937
clock set command, 843
clock timezone command, 843
cloning LNS, 797-798
close_notify Alert message, 924
CLP (Cell Loss Priority) field (UNI ATM cell header), 69
cluster encryption command, 886
cluster ip address command, 886
cluster key command, 886
cluster port command, 887
commit flag, ISAKMP, 809

Common Part Convergence Sublayer (CPCS), 70
Common Part Indicator (CPI) field (AAL5 CPCS PDU), 70
compression transform sets, 471
compulsory tunnel mode
12tp authentication password command, 789
accept-dialin command, 795
async mode interactive command, 790
async-bootp dns-server command, 795
autoselect PPP command, 790
debug vtemplate command, 797
domain command, 789
encapsulation ppp command, 790
group-range command, 790
initiate-to ip command, 789
ip local pool command, 795
ip unnumbered command, 795
ip unnumbered loopback 100 command, 797
isdn incoming-voice modem command, 790
isdn switch-type command, 790
L2TP remote access VPNs, 782-783
LACs, 784-785, 788-790
LNSs, 786-788, 794-798
modem autoconfigure type mica command, 790
modem InOut command, 790
no peer default ip address command, 790
peer default ip address pool command, 795
peer default ip address pool vpn1_pool command, 797
ppp authentication chap command, 790, 795
pri-groups timeslots command, 789
protocol 12tp command, 789
request-dialin command, 789
terminate-from hostname command, 795
virtual-template command, 795
vpdn enable command, 789
vpdn search-order domain command, 789
vpdn-group command, 789
compulsory tunnel mode remote access VPNs, 15-16
compulsory/NAS-initiated tunnel mode, 710
confidentiality, 410, 426
Configuration Method, ISAKMP, 814
connect command, 175, 212-213, 867
connection statistics, VPNs, 860
connectionless integrity
AH, 422-426
ESP, 426-427
IPsec, 409
connectionless VPNs, 17
connection-oriented VPNs, 17
Control (CTRL) field
Cisco HDLC frame, 53
PPP frame, 56
control channel messages
AToM-based L2VPNs, 139-140
L2TPv3-based L2VPNs, 31-34
LDP, 141-142
control connection (L2TPv3)
setup, 34-36
teardown, 36-37
Control Connection ID field (L2TPv3 control channel messages), 32
Control field (SNAP header), 47
control words
802.1Q transport, 163
ATM transport, 177
data channel packet forwarding, 154
DLCI-to-DLCI switching, 172
Ethernet port transport, 157
Ethernet pseudowires, 157
Ethernet VLAN transport, 163
HDLC, 155
HDLC/PPP, 165
Convergence Sublayer (CS), 70
Cookie field (L2TPv3 data channel messages), 33
cookies
IKE, 506
ISAKMP, 809
copy running-config startup-config command, 459
CPCS (Common Part Convergence Sublayer), 70
CPCS Payload field (AAL5 CPCS PDU), 70
CPCS UU field (AAL5 CPCS PDU), 70
CPI (Common Part Indicator) field (AAL5 CPCS PDU), 70
CRACK (Challenge/Response Authentication of Cryptographic Keys), 810, 813-814
CRC field (AAL5 CPCS PDU), 70
CRL Distribution Point, 572
crl optional command, 843
crl required command, 843
CRLs (Certificate Revocation Lists), 435, 563-567, 572

cRTP (compressed RTP), 672
crypto access lists
configuring, 475-479
mirroring, 479
crypto ca authenticate command, 843
crypto ca certificate map command, 844
crypto ca enroll command, 843
crypto ca trustpoint command, 843
crypto dynamic-map command, 531, 826, 830
crypto generate rsa command, 843
crypto ipsec client ezvpn command, 867-868
crypto ipsec client ezvpn connect command, 867
crypto ipsec client ezvpn xauth command, 869
crypto ipsec profile command, 537
crypto ipsec security-association replay disable command, 669
crypto ipsec security-association replay window size command, 669
crypto ipsec transform-set command, 436, 471, 830, 873
crypto isakmp client configuration group command, 826, 872
crypto isakmp key command, 441, 531
crypto isakmp policy command, 433, 461, 825
crypto isakmp profile command, 872
crypto key generate rsa command, 451
crypto keyring command, 877
crypto map command, 826, 830, 872-873
crypto map local-address command, 457
crypto maps
applying to (outside) interface, 481
configuring, 479-480
IPsec VPNs, 531
PFS, 480
crypto pki authenticate command, 455
crypto pki certificate chain command, 456
crypto pki enroll command, 456
crypto pki trustpoint command, 453, 456
cryptographic algorithms
IKE, 461
authentication methods, 464
Diffie-Hellman algorithms, 462-463
encryption algorithms, 462
hash algorithms, 463-464
IKE SA lifetime, 465
multiple policies, 466-467
sample policy, 466
IPsec, 410
authentication, 410-414
encryption, 415-419
public key, 419-422
CS (Convergence Sublayer), 70
CSC (carrier's carrier) architecture
overview, 293-294
when MPLS is enabled, 307-314
hierarchical VPNs, enabling, 310-314
packet forwarding, 309-310
route advertisement, 307-309
when MPLS is not enabled, 294-305
packet forwarding, 304-307
route advertisement, 295-304
cs-label.ser file, 586
CTRL (Control) field, 56
Customer devices. *See* C (Customer) devices
Customer Edge devices. *See* CE (Customer Edge) devices
Customer Edge routers, 5
Customer Edge switches, 5
customer provisioned VPNs
overview, 10-11
remove access, 15-16
route distribution, provisioning in MPLS Layer 3 VPNs
controlling with RTs, 233-235
extranet topology, 259-269
full-mesh topology, 251-252
hub-and-spoke topology, 252-258
overview, 250-251
site-to-site, 15
VRF protocols, configuring in MPLS Layer 3 VPNs, 244-248
cut-and-paste attacks, 474

D

Data (Information) field, Cisco HDLC frame, 53
data channel messages
AToM packet drop, resolving, 217-222
AToM-based L2VPNs, 139
L2TPv3-based L2VPN, 31-33
packet forwarding, 154-156
data confidentiality
ESP, 426
IPsec, 410

Data Encryption Standard. *See* DES
data origin authentication
AH, 422-426
ESP, 426-427
IPsec, 410
database level complete command, 587
database level minimal command, 586
database level names command, 586
debug crypto ipsec command, 860
debug crypto ipsec ezvpn client command, 869
debug crypto isakmp command, 603-604, 860
debug crypto isakmp sa command, 852
debug ip bgp neighbor-ip-address updates command, 274
debug ip eigrp vrf vrf-name command, 276-277
debug mpls 12transport signaling message command, 150-151
debug ppp negotiation command, 169
debug vtemplate command, 797
decryption, 415
default-information originate command, 281
denial-of-service attacks, 506
DES (Data Encryption Standard)
brute-force attacks, 418
IKE, 462
IPsec, 418
DHCP relay, 897
Diffie-Hellman algorithm, 419
IKE, 433, 462-463
key exchange, 421-422
Diffserv tunneling models, 377-380
IPsec VPNs, 656-658
digest check command, 45
digital certificates. *See* certificates
digital signature authentication
CAs, 743-756
Cisco ASA 5500, 842-844
Cisco IOS routers, 842
Cisco VPN 3000 concentrators, 743, 834, 837-842
CA certificates, 743-756
groups, 756-759
clients, 844-847
groups, 756-759
IKE, 434, 448-451
authenticating CAs, 454-456
auto-enrolling with CAs, 459-460
automating re-enrollment with CAs, 460-461
configuring host/domain names, 451
declaring CAs, 452-454
enrolling with CAs, 456-459
generating RSA keys, 451-452
L2TP, 724
overview, 555-556, 743-756, 833-834
PKI
approving/rejecting certificates, 590-592
components, 568-572
deployment considerations, 579
IOS certificate server, configuring, 580-590
requesting certificates manually, 593
revoking certificates, 563-568, 592-593
trust models, 572-578
X.509 certificates, 558-562
public key algorithms, 419-421
Windows, 759-765
discovery
AToM, 143
LDP, 142
DLCI-to-DLCI switching, 172-176
Frame Relay transport
over L2TPv3, 62, 64-66
DMVPN (Dynamic Multipoint VPN), 532
advantages, 532
hub site gateways, configuring
crypto profile, 537
mGRE tunnel interface parameters, 538-539
overview, 537
routing protocol for site-to-site reachability, 539-541
sample configuration, 542-543
IPsec VPN high availability
gateway connections over one DMVPN, 642-648
gateway connections over two DMVPNs, 649-655
overview, 642
operation, 532-536
overview, 532
sample topology, 533-534
spoke site gateways, configuring
dynamically assigned IP addresses, 547-550

GRE tunnel interface parameters, 543-545
overview, 543
routing protocol for site-to-site reachability, 545
sample configuration, 546-547
DNS server addresses, 814-816
domain command, 789, 826
Draft Martini, 8, 139
DSL Access Multiplexor (DSLAM), 782
frame-relay interface-type, 175
DWORD values, 770, 774
dynamic crypto maps, 531
Dynamic Multipoint VPN. *See* DMVPN
dynamic routing, IPsec, 408
dynamic session setup (L2TPv3-based L2VPNs)
advantages/disadvantages, 41-42
ATM traffic, transporting, 66-92
AAL5 SDU mode, 89-92
ATM cell relay, 75-88
encapsulation, 73
OAM cells, 71-73
CEF, configuring, 43
Ethernet traffic, transporting, 46-52
Frame Relay traffic, transporting, 60-66
HDLC traffic, transporting, 53-56
L2TPv3 classes, configuring, 43-45
loopback interfaces, configuring as pseudowire endpoints, 43
PPP traffic, transporting, 56-58
pseudowire classes, configuring, 45
X.25 traffic, transporting, 59-60

E

Easy VPN, 865-869
EBGP, configuring for customer VPN sites, 247-248
EFCI (Explicit Forward Congestion Indication), 69
EIGRP, configuring
for customer VPN sites, 245-246
on DMVPN hub site gateways, 540-541
Electronic Codebook (ECB) mode, 416
ElGamal algorithm, 419
E-LSPs (EXP-Inferred Per-Hop-Behavior Scheduling Class), 189
e-mail proxy, configuring for SSL remote access VPNs
on Cisco ASA 5500 Series appliances, 976-977
on Cisco VPN 3000 concentrators, 943-948
Encapsulating Security Payload. *See* ESP
encapsulation
AAL5 SDUs, 89-91
encapsulation aal5 command, 91
encapsulation aa10 command, 183
encapsulation dot1Q vlan-id command, 51-52
encapsulation dot1q vlan-id command, 164
encapsulation frame-relay command, 175
encapsulation hdlc command, 167
encapsulation mpls command, 179, 198
encapsulation ppp command, 169, 790
L2TPv3 encapsulation for ATM cell relay, 78
encrypted nonces
IKE, 434, 444-448
IPsec VPNs, 553-554
encryption
defined, 415
IKE, 462
IPsec, 415-416
block ciphers, 416-418
stream ciphers, 418-419
preshared keys, 444
public key algorithms, 419
voluntary tunnel mode, 712
encryption command, 462
encryption flag, ISAKMP, 809
end entities (PKI), 570
enrollment mode ra command, 453
enrollment url command, 453
enterprises
AToM-based L2VPNs, 138
L2TPv3-based L2VPNs, 29
ephemeral RSA handshake, 920
error messages, LDP, 142
ESP (Encapsulating Security Payload)
AH, configuring together, 430-431
headers, 427-430
IPsec, 426-430
NAT/PAT, 503
NAT/PAT devices, 510
packet capture, 429
PAT devices, 508
transform sets, 471

transport mode, 428
tunnel mode, 428
Ether Type field (SNAP header), 47
Ethernet mode interworking
AToM, 207
L2TPv3, 99-102
Ethernet traffic
802.1 transport, 163-165
transporting over AToM pseudowires
overview, 156-157
port transport, 157-163
VLAN transport, 163-165
transporting over L2TPv3 pseudowires
overview, 46
port transport, 46-50
VLAN transport, 50-52
Ethertype field, Cisco HDLC frame, 53
EXP-Inferred Per-Hop-Behavior Scheduling Class LSPs (E-LSPs), 189
Explicit Forward Congestion Indication (EFCI), 69
| export | both route-target-ext-community command, 243
Extended Authentication within IKE. *See* Xauth
external routes, advertising, 296-298, 307-309
extranet VPNs. *See also* site-to-site VPNs
overview, 11
provisioning MPLS VPNs, 258-269
EZVPN (Easy VPN), 865-869

F

F4 OAM cells (ATM), 71-72
F5 OAM cells (ATM), 71-72
failover, IPsec remote access connections, 887-889
FAILURE messages (CA), 571
fast-reroute, 138, 201
FCS (Frame Check Sequence) field
Cisco HDLC frame, 53
Frame Relay frame, 61
PPP frame, 56
FEC (Forwarding Equivalence Class)
Overview, 142
PW ID FEC element, 147-149
FEC TLV, 145-146
FIFO (first-in, first-out) queue, 672
file servers, enabling access with SSL remote access VPNs, 930-935
Finished SSL/TLS handshake protocol message, 910-912, 916-918, 922-923
firewall are-u-there command, 826
firewalls, IPsec traffic, 519-520, 892-894
Flag field
Cisco HDLC frame, 53
Frame Relay frame, 61
PPP frame, 56
flags, ISAKMP, 809
Flags field, Cisco HDLC frame, 53
Forwarding Equivalence Class. *See* FEC
fragmentation
avoiding with L2TPv3 pseudowires, 128-133
IPsec packets
GRE/IPsec packets, 685-686
IPsec and GRE/IPsec packets, 678-679
overview, 677-678
plain IPsec packets, 679-685
PMTUD, 686-695
solutions, 695-703
Frame Check Sequence (FCS) field, Cisco HDLC frame, 53
Frame Relay traffic
IP mode L2VPN interworking
Ethernet circuits, 104-108
PPP circuits, 108-111
transporting over AToM pseudowires
DLCI-to-DLCI switching, 172-176
Overview, 171
port transport, 171-172
transporting over L2TPv3 psuedowires
DLCI-to-DLCI switching, 62-66
frame formats, 61-62
Frame Relay trunks, 66
overview, 60
QoS, 118-119
frame-relay interface-dlci command, 213
frame-relay switching command, 175, 213
full-mesh MPLS VPNs, 251-252, 408
functions port-forward command, 975

G

gateways
authenticating CAs, 454-456
backup VPN gateways, 889-892
Cisco routers, 732-736
Cisco VPN 3000 concentrators, configuring
address pools, 725-727
base groups, 727-731
client user accounts, 731
optional parameters, 732
declaring CAs, 452-454
defined, 409
digital signature authentication
described, 743-756
groups, 756-759
Windows, 759-765
enrolling with CAs
auto-enrolling, 459-460
automating re-enrollment, 460-461
described, 459-460
firewalls, 892-894
head end, 779
host/domain names, configuring, 451
IPsec VPNs
described, 824-831
DMVPN hub site gateways, configuring, 537-543
DMVPN spoke site gateways, configuring, 543-545
example configuration, 481, 485
remote access, 892-894
L2TP LNSs, 710
L2TP/IPsec VPNs
Cisco routers, 776-782
NAT devices, 773-776
verifying, 765-773
PSK authentication, 736-742
RSA keys, generating, 451-452
setting time, 449-451
Generic Flow Control (GFC) field (UNI ATM cell header), 69
Generic Label TLV, 146
Generic Routing Encapsulation. *See* GRE
GFC (Generic Flow Control) field (UNI ATM cell header), 69
GRE (Generic Routing Encapsulation)
AToM, 138
overview, 8
tunnels, 485-486
crypto access lists, configuring, 489
crypto maps, configuring/applying, 490
example configuration, 490-495
high availability, 628
high availability, with DMVPN, 642-655
high availability, with point-to-point tunnels, 628-639, 641-642
IKE policies, configuring, 489
interfaces, configuring, 486-487
ip mtu command, configuring, 696-697
ip tcp adjust-mss command, configuring, 697-699
MPLS Layer 3 VPN multicast transport, 349-351
routing protocol/static routes, configuring, 487-489
spoke site gateway parameters, configuring, 543-545
transform sets, configuring, 489
group command, 826, 867, 874
group-policy command, 829, 972
group-range command, 790
groups
Diffie-Hellman, 463
digital signature authentication, 756-758
IPsec remote access, 819-820

H

handshake protocol, 908-910
hardware clients, 806
hash algorithms
IKE, 463-464
IPsec, 410-413
MD5, 410
shared keys, 413
hash command, 464, 825
Hashed Message Authentication Code (HMAC) algorithm, 413-414
HDLC traffic
802.1 transport, 165-170
described, 171

transporting over AToM pseudowires, 165-170
transporting over L2TPv3 pseudowires, 53-56
head-end VPN gateways, 779
header checksum verification, 503, 511
Header Error Control (HEC) field (UNI ATM cell header), 69, 77
headers
AH
ESP, configuring together, 430-431
IPsec, 422-426
NAT/PAT devices, 503, 507-508, 518
packet capture, 425
transform sets, 471
transport mode, 423
tunnel mode, 424
ATM
cell format, 68-73
header format, 68
overview, 67-70
AToM control channel messages, 140
ESP, 426-430
AH, configuring together, 430-431
IPsec, 426-430
NAT/PAT devices, 503, 508-510
packet capture, 429
transform sets, 471
transport mode, 428
tunnel mode, 428
ISAKMP, 808-809
L2TPv2, 713-716
L2TPv3
control connection messages, 32
data channel messages, 32-33
LDP, 140
HEC (Header Error Control) field (UNI ATM cell header), 69, 77
Hello messages
L2TPv2, 716
L2TPv3, 40
LDP, 141
HelloRequest SSL/TLS handshake protocol message, 909
hierarchical hub-and-spoke architecture, IPsec, 526-527
hierarchical VPNs, enabling in CSC MPLS architecture, 310-314
high availability, IPsec VPNs
with GRE tunnels
DMVPN, 642-655
overview, 628
point-to-point tunnels, 628-642
with HSRP
overview, 594
stateful, 611-627
stateless, 595-596
stateless, with HSRP on inside interface, 606-611
stateless, with RRI, 596-606
overview, 593
remote access, 880
backup VPN gateways, 889-892
failover, 887-889
load balancing, 881-887
VRRP, 887-889
HMAC (Hashed Message Authentication Code) algorithm, 413-414
home pages, customizing for SSL VPNs
Cisco ASA 5500 Series devices, 978-979
Cisco IOS devices, 967-969
hostname command, 843
HSRP (Hot Standby Routing Protocol)
IPsec high availability
overview, 594
stateful, 611-627
stateless, 595-606
hub site gateways, configuring
crypto profile, 537
DMVPN, 538-543
mGRE tunnel interface parameters, 538-539
overview, 537
routing protocol for site-to-site reachability, 539-541
hub-and-spoke architecture
described, 408
IPsec VPNs, 525-527
MPLS VPNs, 252-258
Hybrid Authentication, 810-813, 847
Cisco VPN 3000 concentrators, 848-849
Cisco VPN Clients, 849-850
L2TP, 711

I

identity certificates, 846
IEEE 802.1Q tunneling, 8, 163-170
AToM pseudowire transport, 157-165
L2TPv3 pseudowire transport, 50-52
IETF
L2TP remote access VPNs, 711
tunnel attributes
Cisco Secure ACS, 792-793
LACs, 791
Merit RADIUS server, 793
IGP backbone networks, configuring in MPLS Layer 3 VPNs, 239-241
IKE authentication, 432, 725
automated SA/key management
authentication, 441-461
cryptographic parameters, 461-467
CRLs, 435
cryptographic parameters, 461
authentication methods, 464
Diffie-Hellman algorithms, 462-463
encryption algorithms, 462
hash algorithms, 463-464
IKE SA lifetime, 465
multiple policies, 466-467
sample policy, 466
Diffie-Hellman algorithms, 462-463
digital signature authentication, 434, 840-842
encrypted nonces, 434
encryption algorithms, 462
exchange types, 809
GRE, 489
hash algorithms, 463-464
IKE SA lifetime, 465
IPsec
address negotiation, 814-816
authentication, 810
CRACK, 813-814
digital signatures, 555-556
encrypted nonces, 553-554
Hybrid Authentication, 812-813
ISAKMP header fields, 809
overview, 807-809
TED (Tunnel Endpoint Discovery), 528-531
unique preshared keys, 550-552
Xauth, 810-811
L2TP, 724
digital signature authentication, 724
preshared key authentication, 724
PSK authentication, 725-732
L2TP/IPsec remote access VPNs, 717-718
message format, 808
methods, 464
oakley.log, 732
parameters, 822
Phase 2, 856
PKI
approving/rejecting certificates, 590-592
requesting certificates manually, 593
revoking certificates, 563-568, 592-593
X.509 certificates, 558-562
preshared keys, 434
proposals, 822
SA lifetime, 465
version 1
authentication during negotiation, 434
overview, 432
phase 1 aggressive mode negotiation, 435-436
phase 1 main mode negotiation, 433-435
phase 2 quick mode negotiation, 436-437
version 2
negotiation, 437-438
overview, 437
Xauth, 854
import RTs (Route Targets), 235
inbound processing (IPsec), 439-440
Incoming-Call-Connected (ICCN) message (L2TPv2), 716
Incoming-Call-Reply (ICRP) message (L2TPv2), 716
Incoming-Call-Request (ICRQ) message (L2TPv2), 716
Information field
Frame Relay frame, 61
PPP frame, 56
Initialization messages (LDP), 141
initiate-to ip command, 789
initiator cookie, 809

input QoS policies
AToM pseudowires, 190-194
L2TPv3 pseudowires, 121-125
installing
Cisco Secure Desktop, 954
Cisco SSL VPN Client, 948
integrity check (AH), 507
inter-AS VPN service, 11
inter-autonomous system MPLS VPN architecture
advertisement of labeled VPN-IPv4 routes between ASBRs
overview, 325
packet forwarding, 331-333
route/label advertisement, 325-331
advertisement of labeled VPN-IPv4 routes between route reflectors
overview, 334-335
packet forwarding, 346-348
route/label advertisement, 335-346
overview, 315-316
VRF-to-VRF connectivity at ASBRs
overview, 316-317
packet forwarding, 322-324
route/label advertisement, 317-322
interface command, 886
internal routes, advertising (CSC MPLS architecture), 298-309
Internet access, provisioning for MPLS Layer 3 VPNs, 277-290
Internet Key Exchange protocol. *See* IKE authentication
Internet Security Association and Key Management Protocol (ISAKMP), 433
Internet VPNs, 18
interprovider MPLS VPN architecture. *See* inter-autonomous system MPLS VPN architecture
interprovider VPN service, 11
interworking
AToM-based L2VPNs, 188
AToM-based pseudowires, 207-211
Ethernet mode L2VPN internetworking, 99-100
IP mode L2VPN internetworking, 102
interworking command, 210
interworking ethernet command, 209
interworking ip command
Ethernet to VLAN, 111-112
Frame Relay to Ethernet, 105
Frame Relay to PPP, 109
intranet VPNs, 11. *See also* site-to-site VPNs
IOS certificate server, configuring for PKI deployments
certificate attributes, configuring, 587-588
CRL lifetime, specifying, 588
database parameters, configuring, 585-587
deployment model, determining, 580-582
enabling server, 589-590
HTTP server, configuring, 585
overview, 580
public/private key pair, generating/exporting, 583-585
time, setting, 583
IOS devices, enabling SSL VPNs
basic SSL parameters, configuring, 966-967
domain name address, configuring, 964
IOS router, enrolling with a CA, 965
login/home pages, customizing, 967-969
name server address, configuring, 964
overview, 963
port forwarding, configuring, 969-970
remote AAA, configuring, 964-965
URLs, specifying, 969
webvpn enable command, 966
IP (Internet Protocol)
address pools, 817
HSRP virtual IP addresses, 594-596
L2TP remote access VPNs, 711
MPLS Layer 3 VPNs, 227-229
overview, 814-816
ip cef command, 43, 159
ip cef distributed command, 159
ip dfbit set command, 132
ip imp sparse-dense mode command, 368
ip local interface interface-name command, 45
ip local pool command
compulsory tunnel mode, 795
MPLS Layer 3 VPNs, 800
overview, 827-829
IP mode L2VPN interworking
AToM pseudowires, 207-211
with L2TPv3, 103-112
advantages/disadvantages, 102
Ethernet to VLAN, 111-112
Frame Relay to Ethernet, 104-108

Frame Relay to PPP, 108-111
Frame Relay to VLAN, 108
Layer 2 address resolution, 103
overview, 102-103
traffic forwarding, 103
ip mtu command, 113, 696-697
ip multicast-routing command, 366-367
ip multicast-routing vrf command, 366
ip nat inside command, 868
ip nat inside source list command, 868
ip nat outside command, 868
ip nhrp authentication command, 538-539
ip nhrp holdtime command, 539
ip nhrp map command, 544
ip nhrp map multicast dynamic command, 538
ip nhrp network-id command, 538-539
ip nhrp nhs command, 544
ip opsf priority command, 545
ip ospf network broadcast command, 540
ip ospf priority command, 540
ip pim autorp listener command, 367
ip pim sparse-dense mode command, 367
ip pim sparse-mode command, 366-368
ip pim ssm range command, 367-368
ip pmtu command, 132
ip route command, 827
ip route vrf command, 878
ip router isis command, 241
ip rsvp bandwidth command, 197
ip tcp adjust-mss command, 697-699
ip tos reflect command, 121-123
ip tos value command, 121-123
ip unnumbered command, 795
ip unnumbered interface command, 197
ip unnumbered loopback 100 command, 797
ip verf forwarding command, 799
ip vrf command, 800
ip vrf forwarding vrf-name command, 243, 300
ip vrf sitemap map-name command, 276
ip vrf vrf-name command, 243
ipconfig /all command, 727, 876
IPLS (IP-only Private LAN Service), 27. ***See also*** **L2VPNs**
IP-only Private LAN Service. ***See*** **IPLS**
IPsec VPNs
access control, 409
advantages/disadvantages, 408-409
AES, 418
asymmetric cryptographic algorithms
Diffie-Hellman key exchange, 421-422
digital signatures, 420-421
encryption, 419
authentication
hash, 410-413
HMAC, 413-414
MAC, 413-414
connectionless integrity, 409
crypto access lists, 475-479
crypto maps, 479-481
cryptographic algorithms
authentication, 410-414
encryption, 415-419
public key, 419-422
data confidentiality, 410
data origin authentication, 410
databases, 432
defined, 409
deployment, 805
DES, 418
digital signature authentication, 840-842
dynamic routing, 408
elements, 409
encryption algorithms
block ciphers, 416-418
overview, 415-416
stream ciphers, 418-419
example configuration, 481-485
firewalls, traversing, 519-520
high availability
with DMVPN, 642-655
with GRE, 628-642
with HSRP, 594-627
overview, 593
IKE, 807-809
address negotiation, 814-816
authentication, 810
CRACK, 813-814
Hybrid Authentication, 812-813
ISAKMP header fields, 809
Xauth, 810-811
keys
IKEv1, 432-437
IKEv2, 437-438
MD5 algorithm, 410

MPLS, 869-880
multicast traffic, 409
multiprotocol traffic, 409
NAT
Cisco ASA 5500, 865
Cisco IOS routers, 864
Cisco VPN 3000 concentrators, 863-864
Cisco VPN Clients, 865
overview, 862-863
NAT/PAT, 502-519
packet drops
PMTUD, 686-695
solutions, 695-703
packet fragmentation
GRE/IPsec packets, 685-686
IPsec and GRE/IPsec packets, 678-679
overview, 677-678
plain IPsec packets, 679-685
solutions, 695-703
packet overhead, 673-677
packet processing
inbound, 439-440
outbound, 438-439
parameters, 822
PAT
Cisco ASA 5500, 865
Cisco IOS routers, 864
Cisco VPN 3000 concentrators, 863-864
Cisco VPN Clients, 865
overview, 862-863
peers, 409
PKI
approving/rejecting certificates, 590-592
components, 568-572
deployment considerations, 579
IOS certificate server, configuring, 580-590
requesting certificates manually, 593
revoking certificates, 563-568, 592-593
trust models, 572-578
X.509 certificates, 558-562
public key algorithms
Diffie-Hellman key exchange, 421-422
digital signatures, 420-421
encryption, 419
QoS
considerations, 671-672
DiffServ model, 656-658
policy configuration, 659-665
replay protection, 665-671
replay protection, 410
SA/key management, manual, 499-502
SAs
IKEv1, 432-437
IKEv2, 437-438
overview, 431-432
scaling
configuration complexity, reducing, 527
DMVPN. See DMVPN
IKE authentication. See IKE authentication
overview, 523-525
TED, 528-531
tunnels required, reducing, 525-527
security
AH, 422-426
AH/ESP together, 430-431
ESP, 426-430
overview, 422, 806
session keys, 433
SHA-1 algorithm, 410
site-to-site VPNs, 8, 407
traffic, 410
flow confidentiality, 410
multicast/multiprotocol, 485-499
selectors, 475
transform sets, 471-474, 830
ipsec-udp enable command, 865
ipsec-users group, 829
IPv4, transporting IPv6 over IPv4 backbones, 114-118
IPv6
protocol demultiplexing, 114-118
traffic transport, MPLS Layer 3 VPNs
configuring 6VPE, 395-401
overview, 392-393
packet forwarding, 394-395
route exchange, 393-394
verifying 6VPE, 401-403
IPX
AToM-based L2VPNs, 138
L2TP remote access VPNs, 711

ISAKMP
Configuration Method, 814
cookies, 506
flags, 809
header format, 808-809
initiator cookie, 809
messages, 808
MjVer/MnVer, 809
NAT/PAT, 503-507
net payload, 809
Request/Reply method, 814
responder cookie, 809
Set/Acknowledgment method, 814
isakmp authorization list command, 873
ISAKMP Configuration Method (Mode Config), 711
isakmp enable command, 831, 887
isakmp ipsec-over-tcp command, 865
isakmp nat-traversal command, 865
isakmp policy command, 831, 843
isdn incoming-voice modem command, 790
isdn switch-type command, 790
IS-IS
configuring
as backbone network IGP, 240-241
for L2VPN interworking, 113
is-type level-2-only command, 240
IWF (interworking function)
AToM-based L2VPNs, 188
AToM-based pseudowires, 207-211
Ethernet mode L2VPN, 99-100
IP mode L2VPN, 102

K

Keepalive messages, 141
key config-key password-encrypt command, 444
keyring command, 878
keys
Diffie-Hellman key exchange, 421-422
IKE configuration, 441
management
IKEv1, 432-438
manual, 499-502
keys command, 826

L

L2F (Layer Two Forwarding) protocol, 7-8
L2F Home Gateway, 7
L2TP Access Concentrators (LACs), 7, 710
l2tp cookie local command, 95
l2tp hello command, 98
l2tp id command, 95
L2TP Network Servers (LNSs)
cloning, 797-798
compulsory tunnel mode
Cisco Secure ACS, 796
Merit RADIUS servers, 797-798
overview, 786-788
RADIUS servers, 795
MPLS Layer 3 VPNs, 799
L2TP over IPsec. *See* L2TP/IPsec
l2tp remote command, 95
L2TP VPNs
advantages/disadvantages, 711-712
client software, 711
compulsory tunnel mode
LACs, 784-785, 788-790
LNSs, 786-788, 794-798
NAS-initiated tunnel mode, 710
overview, 782-783
defined, 9
digital signature authentication, 724
headers, 713-715
Hybrid Authentication Mode for IKE, 711
IETF, 711
IKE authentication
digital signatures, 724
preshared keys, 724-732
IPsec VPNs, 734
L2TP/IPsec VPNs, 713
Mode Config, 711
MPLS Layer 3 VPNs, 798-802
MPPC, 730
multicast traffic, 711
multiprotocol traffic, 711
no 12tp tunnel authentication, 734
PPP, 710-711, 724
preshared key authentication, 724
security, 711
show all vpdn session all command, 767
show caller user command, 768

voluntary tunnel mode
L2TP/IPsec, 713
message formats/types, 713-716
PPP user authentication with IPsec, 713
PPP user authentication without IPsec, 712-713
Xauth, 711
L2TP/IPsec, 713
client workstations, 769-773
digital signatures, 743-756
IKE, 717
NAT devices, transitting, 773-776
PSK authentication
Cisco routers, 732-736
Windows, 736-742
remote access VPNs, setting up, 716-724
SAs, 732
show vpdn session command, 767
voluntary tunnel mode
Cisco routers, 776-782
NAT devices, transitting, 773-776
verifying, 765-773
Windows
clients, 717
digital signature authentication, 759-765
L2TPv3-based L2VPNs
advantages/disadvantages, 28-29
classes, configuring, 45
control channel messages
defined, 31
format, 31-32
functions performed by, 34
header fields, 32
setup, 34-36
teardown, 36-37
data channel messages
defined, 31
format, 31
header fields, 32-33
Layer 2-specific sublayer, 33
deployment models, 30
dynamic session setup, 37-38
advantages/disadvantages, 41-42
ATM traffic, transporting, 66-92
CEF, configuring, 43
Ethernet traffic, transporting, 46-52
Frame Relay traffic, transporting, 60-66
HDLC traffic, transporting, 53-56
L2TPv3 classes, configuring, 43-45
loopback interfaces, configuring as pseudowire endpoints, 43
PPP traffic, transporting, 56-58
pseudowire classes, configuring, 45
X.25 traffic, transporting, 59-60
dynamic session teardown, 38-40
Hello messages, sending, 40
IPv6 protocol demultiplexing, 114-118
L2VPN interworking
Ethernet mode, 99-102
IP mode, 102-112
MTU issues, resolving, 112-113
overview, 98
routing protocol considerations, 113
overview, 8-9, 27
packet drops/fragmentation, 128-133
protocol command, 782
protocols transported by, 30
SLI messages, 41
static session setup
advantages/disadvantages, 41-42
overview, 93
with control connection, 96-98
without control connection, 93-96
L2VPNs (Layer 2 VPNs)
AToM-based
advanced features, 188-222
advantages/disadvantages, 138-139
data channel packet forwarding, 154-156
deploying pseudowires, 156-187
Ethernet traffic, transporting, 156-165
Frame Relay traffic, transporting, 171-176
HDLC traffic, transporting, 165-170
PPP traffic, transporting, 165-170
setup, 143-146
signaling, 150-153
interworking with L2TPv3
Ethernet mode, 99-102
IP mode, 102-112
MTU issues, resolving, 112-113
overview, 98
routing protocol considerations, 113
L2TPv3-based
advantages/disadvantages, 28-29
deployment models, 30
overview, 13

L3VPNs (Layer 3 VPNs), 13
Label Abort Request messages, 142
Label Mapping messages, 142, 145
Label Release messages, 142
Label Request messages, 142
Label Switch Paths. *See* LSPs
Label Withdraw messages, 142, 151
Label-Only-Inferred Per-Hop-Behavior Scheduling Class LSPS (L-LSPs), 189
labels, exchanging, 150
LACs (L2TP Access Concentrators)
aaa authentication ppp default group radius command, 791
aaa authorization network default group radius command, 791
aaa new-model command, 791
compulsory tunnel mode, 784-790
DSLAMs, 782
L2TP, 710
PSK authentication
Cisco routers, 732-736
Windows, 736-742
radius server host command, 791
service providers, 710
tunnels on RADIUS servers, 791
LAN-to-LAN VPNs. *See* site-to-site VPNs
Layer 1 VPNs, 13
Layer 2 site-to-site VPNs. *See* L2VPNs
Layer 3 site-to-site VPNs, 13
Layer Two Forwarding (L2F) Protocol NAS, 7
Layer Two Forwarding protocol. *See* L2F (Layer Two Forwarding) protocol
Layer Two Tunneling Protocol. *See* L2TP VPNs
Layer Two Tunneling Protocol (L2TP) Access Concentrator (LAC), 7
Layer Two Tunneling Protocol version 3. *See* L2TPv3-based L2VPNs
LDP
AToM discovery, 143
configuring for MPLS Layer 3 VPN PE routers, 237-238
extended discovery, 143-144
FEC TLV, 145-146
Generic Label TLV, 146
header fields, 140-142
messages
Address, 142
Address Withdraw, 142
advertisement, 142
discovery, 142
error, 142
format, 140
Hello, 141
Initialization, 141
Keepalive, 141
Label Abort Request, 142
Label Mapping, 142, 145
Label Release, 142
Label Request, 142
Label Withdraw, 142, 151
Notification, 141, 151-153
session, 142
types, 141-142
PDU, 149
Length field (AAL5 CPCS PDU), 70
Length field (L2TPv3 control channel messages), 32
lifetime command, 465
lifetime crl command, 588
LLQ (Low Latency Queue), IPsec VPNs, 672
L-LSPs (Label-Only-Inferred Per-Hop-Behavior Scheduling Class), 189
LNSs (L2TP Network Servers)
cloning, 797-798
compulsory tunnel mode
Cisco Secure ACS, 796
Merit RADIUS servers, 797-798
overview, 786-788, 794
RADIUS servers, 795
L2TP VPNs, 710
MPLS Layer 3 VPNs, 799
load balancing, IPsec remote access connections
Cisco ASA 5500, 886-887
Cisco VPN 3000 concentrators, 881-886
local switching, AToM-based pseudowires
circuits on same interface, 216-217
overview, 188, 211-212
physical interfaces, 215-216
PVC mode, 215
same types of physical interfaces, 213-215
logging
Oakley, 769
PPP, 769
RASCHAP.log file, 773

login pages, customizing for SSL VPNs
Cisco ASA 5500 Series devices, 978-979
Cisco IOS devices, 967-969
logo command, 969
loopback interfaces, configuring
as L2TPv3 pseudowire endpoint, 43
for MPLS Layer 3 VPN PE routers, 237
Low Latency Queue (LLQ), 672
LSPs (Lable Switch Paths)
E-LSPs, 189
MPLS LSPs, 8
LSR routers, 140

M

M2M (multipoint-to-multipoint) VPNs, 13
MAC (Message Authentication Code) algorithm, 413-414
Mac OS X, L2TP/IPsec client, 711
main mode negotiation (IKE phase 1), 433-435
match address command, 878
match atm clp command, 191
match cos command, 191
match fr-de command, 190
match identity address command, 878
match identity command, 872
match not fr-de command, 123-124
match protocol ipv6 command, 116
MD (multicast domain), MPLS Layer 3 VPNs, 351-353
MD5 (Message Digest 5) algorithm, IPsec, 410
mdt data command, 366
mdt default command, 366
MDTs (multicast distribution trees)
data MDT, 355-359
default MDT
overview, 353-355
signaling, verifying, 370-371
Merit RADIUS servers
compulsory tunnel mode, 797-798
IETF tunnel attributes, 793
MPLS Layer 3 VPNs, 801
Message Authentication Code (MAC) algorithm, 413-414
Message Digest 5 algorithm, 410
metric-style wide command, 197, 241
Microsoft CAs, 752
Microsoft Point-to-Point Compression (MPPC), 730
mirroring crypto access lists, 479
MjVer field, ISAKMP, 809
MnVer field, ISAKMP, 809
mode command, 474, 867
Mode Config, 711, 806, 855
modem autoconfigure type mica command, 790
modem InOut command, 790
MP-BGP
configuring for VPNv4 route exchange, 241-242
redistributing PE-CE routing protocols, 248-250
MPCC (Microsoft Point-to-Point Compression), 730
MP-eBGP, 325
MPLS
enabling, 239
IPsec, 869-880
IS-IS, 160
LSPs, 8
OSPF, 160
QoS, 188
shim header, 189
mpls bgp forwarding command, 328-329
mpls ip command, 160, 163, 239
mpls label protocol ldp command, 159
MPLS Layer 3 VPNs
advantages/disadvantages, 226-227
carrier's carrier architecture
overview, 293-294
when MPLS is enabled, 307-314
when MPLS is not enabled, 294-307
customer VPN route distribution, controlling, 233-235
deploying
CE routers, configuring, 236
extranet connectivity, 259-269
full-mesh connectivity, 250-252
hub-and-spoke connectivity, 252-258
Internet access, provisioning, 277-290
overview, 235-236
P routers, configuring, 250
PE routers, configuring, 236-250
routing loops, preventing, 269-277

inter-autonomous system architecture
advertisement of labeled VPN-IPv4 routes between ASBRs, 325-333
advertisement of labeled VPN-IPv4 routes between route reflectors, 334-348
overview, 315-316
VRF-to-VRF connectivity at ASBRs, 316-324
IP reachability, 227-229
IPv6 traffic transport
configuring 6VPE, 395-401
overview, 392-393
packet forwarding, 394-395
rout exchange, 393-394
verifying 6VPE, 401-403
L2TP remote access, 798-802
Merit RADIUS servers, 801
multicast traffic, forwarding
MVPNs, 451-354
point-to-point GRE tunnels, 349-351
network prefixes, distinguishing between, 232-233
QoS
configuring, 380-392
deployment models, 374-377
DiffServ tunneling models, 377-380
RADIUS servers, 801
user packet forwarding, 229-231

mpls ldp discovery transport-addressinterface command, 301
mpls mtu command, 221
mpls traffic-eng router-id command, 197
mpls traffic-eng tunnels command, 196
MPLS-TE (MPLS traffic engineering), 138
AToM pseudowires, 195-202
fast-reroute, 138, 201
P routers, 199
MTUs (maximum transmission units)
IPSec VPN packets
fragmentation, 677-703
overhead, 673-677
multi-autonomous system MPLS VPN architecture
advertisement of labeled VPN-IPv4 routes between ASBRs
overview, 325
packet forwarding, 331-333
route/label advertisement, 325-331
advertisement of labeled VPN-IPv4 routes between route reflectors
overview, 334-334
packet forwarding, 346-348
route/label advertisement, 335-346
overview, 315-316
VRF-to-VRF connectivity at ASBRs
overview, 316-317
packet forwarding, 322-324
route/label advertisement, 317-322
multicast traffic
IPsec VPNs, 409, 485
GRE tunnels, 485-495
VTIs, 495-499
L2TP VPNs, 711
MPLS Layer 3 VPNs
multicast VPNs. See multicast VPNs
point-to-point GRE tunnels, 349-351
multicast VPNs. *See* MVPNs
multipoint-to-multipoint VPNs, 13
multiprotocol traffic
IPsec, 409
IPsec VPNs, 485
GRE tunnels, 485-495
VTIs, 495-499
remote access L2TP VPNs, 711
multiservice VPNs, 18
MVPNs (multicast VPNs)
advantages, 364
configuring, 364, 366-368
MD (multicast domain), 351-353
MDTs (multicast distribution trees)
data, 355-359
default, 353-355
verifying signaling, 370-371
MVRF (multicast VRF)
MPLS Layer 3 VPNs, 351-353
overview, 351
PIM adjacencies
overview, 359
verifying, 368-370
RPF checks, 360-361
traffic flow, verifying, 372-374
MVRF (multicast VRF), 351-353

N

NAS (Network Access Servers) devices, 7
NAS-initiated remote access VPNs, 16
NASs (Network Access Servers), 710
NAT (Network Address Translation)
AH traffic, dropped, 507-508
embedded IP addresses, 512
ESP packets, 510
IPsec
breaking, 508-510
Cisco ASA 5500, 865
Cisco IOS, 864
Cisco VPN 3000, 863-864
Cisco VPN Clients, 865
IKE negotiation failure, 503-505
overview, 862-863
tunnels, 517-519
ISAKMP traffic, dropped, 506-507
L2TP/IPsec remote access VPNs, 773-776
NAT-T, 773-776
rekeying failure, 506
TCP/UDP header checksum verification failure, 511
timeouts, 510-511
traversal/transparency, 518
user packets, 512-517
verification failure, 506
nat command, 887
NAT/PAT
AH, 518
ESP tunnel mode, 518
negotiation
IKEv1, 435-437
IKEv2, 437-438
NAT/PAT, 503-505
PPP, 713
remote access users, 713
neighbor ip-address activate command, 242, 248
neighbor ip-address as-override command, 272
neighbor ip-address remote-as as-number command, 281
neighbor ip-address remote-as autonomous-system-number command, 241, 247
neighbor ip-address route-map map-name in command, 273, 275
neighbor ip-address send-community extended command, 242
neighbor ip-address update-source interface command, 241
net payload, 809
Network Access Servers, 710
network command, 161
network ip-address command, 245
network ip-address wildcard-mask area area-id command, 160
network network wildcard-mask area area-number command, 246
Network Time Protocol (NTP), 449-450
Network-facing PE (N-PE) devices, 6
Network-to-Network (NNI) ATM cell header, 69
New Connection Wizard, 736, 739
Next Hop Clients (NHC), 534-536
Next Hop Resolution Protocol (NHRP), 532-533
Next Hop Server (NHS), 534-536
Next Received (Nr) field (L2TPv3 control channel messages), 32
Next Sent (Ns) field (L2TPv3 control channel messages), 32
NHC (Next Hop Clients), 534-536
NHRP (Next Hop Resolution Protocol), 532-533
NHS (Next Hop Server), 534-536
NNI (Network-to-Network) ATM cell header, 69
no auto-summary command, 242-248
no bgp default route-target filter command, 328-330
no ip next-hop-self eigrp command, 541, 545
no ip split-horizon command, 541
no ip split-horizon eigrp command, 541, 545
no peer default ip address command, 790
no synchronization command, 241, 248
no12tp tunnel authentication command, 734
Notification messages, LDP, 141, 151-153
N-PE (Network-facing Provider Edge) devices, 6
Nr (Next Received) field (L2TPv3 control channel messages), 32
Ns (Next Sent) field (L2TPv3 control channel messages), 32
NTP (Network Time Protocol), 449-450
ntp server command, 450, 843

O

Oakley Key Determination Protocol, IKEv1, 433
Oakley logging, 732, 769-770
OAM (Operations, Administration, and Management) cells, 71-73
oam-ac emulation-enable command, 73, 177
oam-pvc manage command, 73
OCSP (Online Certificate Status Protocol), 567-568
Organizational Unique Identifier (OUI) field (SNAP header), 47
OSPF
configuring
as backbone network IGP, 239-240
for customer VPN sites, 246-247
on DMVPN hub site gateways, 539-540
for L2VPN interworking, 113
MPLS, 160
OUI (Organizationl Unique Identifier) field (SNAP header), 47
outbound processing (IPsec), 438-439
Outgoing-Call-Connected (OCCN) message (L2TPv2), 716
Outgoing-Call-Reply (OCRP) message (L2TPv2), 716
Outgoing-Call-Request (OCRQ) message (L2TPv2), 716
Output Feedback (OFB) mode (block ciphers), 416
output QoS policies
AToM pseudowires, 190
L2TPv3 pseudowires, 125-128
overlay VPNs, 16-17, 227

P

P routers
configuring
AToM pseudowires, 162-163
MPLS Layer 3 VPNs, 250
MPLS-TE, 199
QoS, 190
packet capture
AH/ESP together, 431
ESP, 429
packet drops (IPsec VPNs)
avoiding with L2Tv3 pseudowires, 128-133
PMTUD
factors, 694-695
overview, 686-687
with GRE/IPsec packets, 692-694
with plain IPsec packets, 687-692
solutions
allowing fragmentation, 702-703
fixing PMTUD, 699
overview, 695
sending smaller packets, 696-699
using prefragmentation for packets, 700-702
packet forwarding
between MPLS Layer 3 VPN sites, 229-231
CSC architecture when MPLS is enabled, 309-310
CSC architecture when MPLS is not enabled, 304-307
hierarchical VPNs, 313-314
inter-autonomous systems, MP-eBGP between ASBRs, 331-333
inter-autonomous systems, MP-eBGP between route reflectors, 346-348
inter-autonomous systems, VRF-to-VRF connectivity, 322-324
IPv6 packets, 394-395
data channel messages, 154-156
packet fragmentation
avoiding with L2TPv3 pseudowires, 128-133
IPsec VPNs
GRE/IPsec packets, 685-686
IPsec and GRE/IPsec packets, 678-679
overview, 677-678
plain IPsec packets, 679-685
PMTUD, 686-695
solutions, 695-703
packet overhead, IPsec VPNs, 673-677
packet processing
IPsec, 438
inbound, 439-440
outbound, 438-439
PAD (Peer Authorization Database), 432
PAD field (AAL5 CPCS PDU), 70
Padding field, PPP frame, 56
PAP voluntary tunnel mode, 712

partial-mesh VPNs, 408
participate command, 887
passive-interface loopback command, 240
password encryption aes command, 444
PAT
AH traffic, dropped, 507-508
embedded IP addresses, 512
ESP packets, 510
IPsec
breaking, 508-510
Cisco ASA 5500, 865
Cisco IOS, 864
Cisco VPN 3000, 863-864
Cisco VPN Clients, 865
IKE negotiation failure, 503-505
overview, 862-863
tunnels, 517-519
ISAKMP traffic, dropped, 506-507
rekeying failure, 506
SPIs, 508
TCP/UCP header checksum verification failure, 511
timeouts, 510-511
user packets, 512-517
verification failure, 506
path MTU, 677
Path MTU Discovery. *See* PMTUD
Payload Type (PT) field (UNI ATM cell header), 69
PE routers
ATM port mode cell relay pseudowire transport, 179
AToM pseudowire, configuring, 158-162
input QoS policies, 191-194
IP reachability in MPLS Layer 3 VPNs, 227-229
LDP extended discovery, 143-144
LDP Identifier field, 140
in MPLS Layer 3 VPNs
configuring, 236-250
customer VPN route distribution, controlling, 233-235
network prefixes, distinguishing between, 232-233
pseudowire status, signaling, 151
PW labels, exchanging, 150
reachability, 160
user packet forwarding between MPLS Layer 3 VPN sites, 229-231
xconnect command, 160
PE-CLE devices, 6
Peer Authorization Database, 432
peer command, 868
peer default ip address pool command, 795
peer default ip address pool vpn1_pool command, 797
peer VPNs, 16-17, 227
peer-id-validate cert command, 843
PENDING messages (CA), 570
PE-POP devices, 6
PE-r (Provider Edge routers), 6
Perfect Forward Secrecy, 436, 480
permit statement
crypto access lists, 476
SAs, 478
PE-rs (Provider Edge routing and switching), 6
PE-s (Provider Edge switches), 6
PFS (Perfect Forward Secrecy)
crypto maps, 480
enabling, 436
PGP (Pretty Good Privacy), 558
physical (PHY) layer (ATM reference model), 67-68
Physical Medium Dependent (PMD) sublayer (ATM reference model), 67
PIM, MVPN adacencies
configuring, 361-362
overview, 359
verifying, 368-370
PIM-SM (PIM sparse mode), 361
PIM-SSM (PIM source-specific multicast), 362
ping, 219
ping mpls, 219
Pipe Model, DiffServ tunneling
implementing, 381-388
overview, 377-379
PKCS#10 certificate requests, 748
PKI (Public Key Infrastructure)
approving/rejecting certificates, 590-592
components, 568-572
IPSec VPN deployments
considerations, 579
IOS certificate server, 580-590
requesting certificates manually, 593

revoking certificates, 563-568, 592-593
trust models, 572-578
X.509 certificates, 558-562
pki keyword, 453
plaintext, defined, 415
PMD (Physical Medium Dependent) sublayer (ATM reference model), 67
PMTUD, IPsec packet drops
factors, 694
fixing, 699
misconfigured firewalls, 694-695
overview, 686-687
with GRE/IPsec packets, 692-694
with plain IPsec packets, 687-692
PNS (PPTP Network Server), 7
point-to-point GRE tunnels
IPsec high availability, 628-642
multicast traffic transport, MPLS Layer 3 VPNs, 349-351
Point-to-Point Tunneling Protocol (PPTP) Access Concentrator (PAC), 7
Point-to-Point Tunneling Protocol, 9
police command
AToM QoS, 194
L2TPv3 tunnel marking, configuring, 125
policy map command. 191
policy maps
applying to L2TPv3 virtual circuits, 124
configuring for L2TPv3 tunnel marking, 124
policy-map command, 124
pool command, 826-827, 874
port forwarding, configuring for SSL remote access VPNs
on Cisco ASA 5500 Series appliances, 975
on Cisco IOS routers, 969-970
port-forward command, 975
PPP (Point-to-Point Protocol)
authentication, 713, 780
autoselect ppp command, 790
encapsulation ppp command, 790
L2TP, 710-711, 724
L2TP/IPsec, 713
logging, 769
negotiation, 713
PPP.log file, 772
RASCHAP.log file, 773
show interface virtual access command, 767
traffic, transporting
over AToM psuedowires, 165-170
over L2TPv3 psuedowires, 56-58
ppp authentication chap command, 790, 795
PPP.log file, 772
PPTP (Point-to-Point Tunneling Protocol), 9
PPTP (Point-to-Point Tunneling Protocol Access Concentrator (PAC), 7
PPTP Network Server (PNS), 7
pre_master_secret key (ClientKeyExchange message), 912
preferred path command, 198
preshared key authentication, 816
Cisco ASA 5500, 827-831
Cisco IOS routers, 824-827
Cisco routers, 732-736
Cisco VPN 3000 concentrators, 725-732, 817-824
Cisco VPN Client, 832-833
encryption, 444
IKE, 434, 441-444
IPsec, 550-552
L2TP, 724
L2TP/IPsec, 725
wildcards, 442, 531
Windows, 736-742
pre-shared key command, 831
pre-shared-key command, 843, 878
Pretty Good Privacy (PGP), 558
pri-groups timeslots command, 789
priority command, 886
protocol 12tp command
compulsory tunnel mode, 789
VPDNs, 734
protocol command, 782
Protocol field, 56
protocols
remote access VPNs, 8-9
site-to-site VPNs, 8
SSL protocols, 908-910
Provider Edge routers, 6
Provider Edge switches, 6
PSK authentication. *See* preshared key authentication
pseudowire-class, 45
PT (Payload Type) field (UNI ATM cell header), 69

public key algorithms
Diffie-Hellman key exchange, 421-422
digital signatures, 420-421
encryption, 419
overview, 419
Public Key Infrastructure. ***See*** **PKI**
Pull method, ISAKMP, 814
Push method, ISAKMP, 814
PVC mode, 215
pvc vpi/vci 12 transport command, 183
PW (pseudowire) ID FEC element, 146

Q

QoS (Quality of Service)
AToM-based L2VPNs, 188-194
E-LSPs, 189
IPsec VPNs
considerations, 671-672
DiffServ model, 656-658
overview, 656
policy configuration, 659-665
replay protection, 665-671
L2TPv3 VPNs
input policy, configuring, 121-125
output policy, configuring, 125-128
overview, 118-121
MPLS Layer 3 VPNs
configuring, 380-392
DiffServ tunneling models, 377-380
overview, 374-377
overview, 656
PE routers, 190
site-to-site VPNs, 21
qos pre-classify command, 659-665
quick mode, 856
quick mode negotiation (IKE phase 2), 436-437

R

RA (registration authority), 572
radius server host command, 791
RADIUS servers
AAA, 736
authentication, 830
Cisco Secure ACS, 792
compulsory tunnel mode, 795
MPLS Layer 3 VPNs, 801
tunnel definitions, 790-793
virtual-profile aaa command, 798
VPDNs, 791
radius-server host command, 825
RASCHAP.log file, 773
ras-sig command, 843
RBE (Route Bridge Encapsulation), 99-100
rd route-distinguisher command, 243
RDs (Route Distinguishers), 232-233
reachability, 160
record protocol, 908-909
redistribute bgp autonomous-system-number subnets command, 246
redistribute connected command, 249, 329
redistribute connected subnets command, 328
redistribute eigrp autonomous-system-number command, 248
redistribute ospf process-id internal external 1 external 2 command, 249
redistribute rip command, 249
redistribute static command, 249
re-enrollment (CAs), 460
regenerate keyword, 461
registration authority (RA), 572
rekeying NAT/PAT, 506
relay, DHCP, 897
remote access, IPsec VPNs
advantages/disadvantages, 806-807
comparing other types, 806-807
deployment, 805
digital signature authentication
Cisco ASA 5500, 842-844
Cisco IOS, 842
Cisco VPN 3000, 834-842
clients, 844-847
overview, 833-834
EZVPN, 865-869
firewalls, 892-894
groups, 819-820
high availability
backup VPN gateways, 889-892
failover, 887-889
load balancing, 881-887
overview, 880
VRRP, 887-889

Hybrid Authentication
Cisco VPN 3000 concentrators, 848-849
Cisco VPN Clients, 849-850
overview, 847
IKE authentication
address negotiation, 814-816
CRACK, 813-814
Hybrid Authentication, 812-813
ISAKMP header fields, 809
overview, 807-809
Xauth, 810-811
NAT transparency
Cisco ASA 5500, 865
Cisco IOS routers, 864
Cisco VPN 3000 concentrators, 863-864
Cisco VPN Clients, 865
overview, 862-863
preshared key authentication
Cisco ASA 5500, 827-831
Cisco IOS, 824-827
Cisco VPN Client, 832-833
configuring, 817-824
overview, 816
split tunneling, 898-901
user accounts, 821
verifying/debugging VPNs
Cisco ASA 5500, 858-860
Cisco IOS, 852-858
Cisco VPN 3000, 850-852
Cisco VPN Clients, 860-862
overview, 850
VPN gateways, 824-831
wireless VPNs, 894-898

remote access, L2TP/IPsec
Cisco routers, 776-782
client workstations, 769-773
IKE authentication, 724
NAT devices, transitting, 773-776
PSK authentication, 725-732
setting up, 716-724

remote access, L2TP VPNs
advantages/disadvantages, 711-712
AppleTalk, 711
client software, 711
compulsory tunnel mode, 782-790, 794-798
IETF, 711
IP, 711
IPX, 711
multicast traffic, 711
multiprotocol traffic, 711
PPP, 711
security, 711
voluntary tunnel mode
L2TP/IPsec, 713
message formats/types, 713-716
overview, 712
PPP user authentication with IPsec, 713
PPP user authentication without IPsec, 712-713

remote access, MPLS Layer 3 VPNs, 798-802

remote access, SSL VPNs
advantages/disadvantages, 906-907
Cisco Secure Desktop
Cache Cleaner settings (Mac/Linux), 961-962
Cache Cleaner settings (Windows), 957-958
enabling, 962-963
installing, 954
location criteria, configuring, 954-956
overview, 952-953
Secure Desktop settings, 959-961
VPN Feature Policy settings, 958-959
clientless
e-mail proxy, 943-948
file server access, 930-935
overview, 924
TCP-based application access, 937-942
web server access, 936-937
closing connections, 923-924
enabling on Cisco ASA 5500 Series appliances
cryptographic algorithms, configuring, 978
e-mail proxy, configuring, 976-977
file access/entry/browsing, configuring, 974
HTTP server, configuring, 971
login/home pages, customizing, 978-979
operation of, verifying, 979-980
overview, 970
port forwarding, configuring, 975
SSL trustpoint, specifying, 977
SSL versions, restricting, 977-978
URL lists, specifying, 973-974

user authentication, configuring, 972-973
user group policy, configuring, 971-972
WebVPN, enabling on outside interface, 971
enabling on Cisco IOS devices
basic SSL parameters, configuring, 966-967
domain name address, configuring, 964
IOS router, enrolling with a CA, 965
login/home pages, customizing, 967-969
name server address, configuring, 964
overview, 963
port forwarding, configuring, 969-970
remote AAA, configuring, 964-965
URLs, specifying, 969
webvpn enable command, 966
overview, 905-906
resuming sessions, 922-923
RSA handshake authentication
with client, 920-922
with VPN gateway only, 910-920
thick-client connectivity, 948
remote circuit id command, 165
remote circuit id remote-vlan-id command, 165
replay protection
AH, 422-426
ESP, 426-427
IPsec, 410, 665-671
Request/Reply method, ISKMP, 814
request-dialin command, 789
responder cookies, 809
reverse-path forwarding (RPF) checks, 360-361
reverse-route command, 873
revocation-check command, 453
revocation-check crl none command, 586
revocation-check crl optional command, 586
RIP, configuring on DMVPN hub site gateways, 541
RIPv2, configuring for customer VPN sites, 244-245
Rivest, Shamir, and Addlemen algorithm. ***See*** **RSA handshake authentication**
route advertisement, CSC architecture
hierarchical VPNs, 310-313
when MPLS is enabled, 307-309
when MPLS is not enabled, 295-304
Route Bridge Encapsulation, 99-100
route command, 829
Route Details tab (Cisco SSL VPN Client), 952
Route Distinguishers (RDs), 232-233
route leaking, MPLS Layer 3 VPNs, 282-286
route reflectors
inter-autonomous system MPLS VPNs, deploying, 334-348
MP-BGP for VPNv4 route exchange, configuring, 241-242
Route Targets, 233-235
router bgp autonomous-system-number command, 247-248
router bgp command, 241
router eigrp autonomous-system-number command, 246
router eigrp command, 541
router isis command, 240
router ospf command, 239, 540
router ospf process-id command, 160
router ospf process-id vrf vrf-name command, 246
router rip command, 245, 541
routing loops, preventing, 269-277
routing protocols
GRE tunnels, 487
L2VPN interworking considerations, 113
spoke site gateway protocols for site-to-site reachability, 545
RPF (reverse-path forwarding) checks, 360-361
RRI, 596-606
RSA handshake authentication
IPsec VPN gateways, 451-452
overview, 419
SSL remote access VPNs
with client, 920-922
with VPN gateway only, 910-920
RSVP, 671
RTs (Route Targets), 233-235

S

SAD (Security Association Database), 432
SAR (Segmentation and Reassembly) sublayer (AAL), 70
SAs (security associations)
defined, 431

IKE, configuring, 441
L2TP/IPsec, 732
management, 432
IKEv1, 432-437
IKEv2, 437-438
manual, 499-502
NAT/PAT timeouts, 510-511
permit statements, 478
scaling IPsec VPNs
authentication
digital signatures, 555-556
encrypted nonces, 553-554
preshared keys, 550-552
configuration complexity, reducing, 527
DMVPN
advantages, 532
hub site gateways, configuring, 537-543
operation of, 532-536
overview, 532
sample topology, 533-534
spoke site gateways, configuring, 543-550
overview, 523-525
TED, 528-531
tunnels required, reducing, 525-527
SCEP (Simple Certificate Enrollment Protocol)
CAs, 837-839
defined, 453
SDU (Service Data Unit), 137
secondary-color command, 969
secret keys (Diffie-Hellman), 421-422
Secure Desktop. *See* Cisco Secure Desktop
Secure Desktop General module (Cisco Secure Desktop), 959-961
Secure Hash Algorithm
IPsec, 410
IKE, 464
Secure Sockets Layer. *See* SSL remote access VPNs
security
AH, 422-426
Cisco Secure Desktop, 952-953
Cache Cleaner Settings (Mac/Linux), 961-962
Cache Cleaner Settings (Windows), 957-958
enabling, 962-963
installing, 954
location criteria, 954-956
Secure Desktop settings, 959-961
VPN Feature Policy settings, 958-959
ESP, 426-427
IPsec, 408, 806
L2TP, 711
split tunneling, 898-901
Security Association Database (SAD), 432
security associations. *See* SAs
security gateway, defined, 409
Security Policy Database (SPD), 432
Segmentation And Reassembly (SAR) sublayer (AAL), 70
ServerHello SSL/TLS handshake protocol message, 910-916, 922, 928, 966
ServerHelloDone SSL/TLS handshake protocol message, 910-916, 922
ServerKeyExchange SSL/TLS handshake protocol message, 910
Service Data Units (SDU), 137
service policy command, 191
service provider provisioned VPNs
overview, 10-11
site-to-site, 13-15
Service Specific Convergence Sublayer, 70
service-policy input command, 124
Session ID field (L2TPv3 data channel messages), 33
session keys
IPsec, 433
manual, 500
session messages, LDP, 142
sessions (L2TPv3)
overview, 27
setup, 37-38
teardown, 38-40
set ip dscp tunnel command, 121, 124
set ip precedence tunnel command, 121, 124
set isakmp-profile command, 873
set mpls experimental imposition value command, 191
set nat demux command, 776
set peer command, 878
set pfs command, 436
set security-association level per-host command, 548
set transform-set command, 537, 826, 873

Set/Acknowledgment method, ISAKMP, 814
Set-Link-Info, 716
set-soo command, 273
SHA-1 (Secure Hash Algorithm)
IKE, 464
IPsec, 410
shared keys, 413
shared service VPNs, 287-290
shim headers. MPLS, 189
Short Pipe Model, DiffServ tunneling
implementing, 388-390
overview, 378-379
show 12tun session command
AAL5 SDU mode L2TPv3 pseudowires, 92
ATM port mode cell relay L2TPv3 pseudowires, 85
ATM VCC cell relay mode L2TPv3 pseudowires, 80-81
ATM VPC cell relay L2TPv3 pseudowires, 83-84
Ethernet port L2TPv3 pseudowires, 49-50
Ethernet VLAN L2TPv3 pseudowires, 52
Frame Relay DLCI-to-DLCI switching L2TPv3 pseudowires, 65-66
HDLC L2TPv3 pseudowires, 55-56
static L2TPv3 pseudowires, 96-98
show atm cell-packing command, 87, 185
show atm pvc command, 215
show atm vc command, 91
show atm vp vpi command, 82-83
show caller user command, 768
show connection name, 213
show connection name command, 215
show crypt isakmp sa command, 857
show crypto accelerator statistics command, 860
show crypto ca certificates command, 860
show crypto ca crls command, 860
show crypto engine connections active command, 514-515
show crypto ipsec ezvpn client command, 869
show crypto ipsec sa command, 475-476, 601-602, 857, 874, 879
show crypto isakmp sa command, 601-602, 869
show crypto isakmp sa detail command, 874, 878
show crypto key mypubkey command, 860
show crypto pki certificate command, 455-457
show frame-relay pvc command, 172, 214
show interface virtual access command, 767
show ip bgp command, 284-285
show ip bgp ipv4 mdt all command, 370-371
show ip bgp neighbor ip-address command, 242
show ip bgp vpnv4 all command, 330-331
show ip bgp vpnv4 vrf vrf-name command, 249
show ip bgp vpnv4 vrf vrf-name network-address command, 273-274
show ip eigrp neighbors command, 498
show ip local pool command, 875
show ip mroute command, 372-373
show ip pim neighbor command, 499
show ip route vrf vrf-name command, 285
show ip router vrf vrf-name command, 249-250
show ip vrf detail vrf-name command, 244
show ipsec sa command, 859
show ipsec stats command, 860
show isakmp sa command, 858
show isakmp stats command, 860
show mpls 12 transport vc command, 201
show mpls 12transport vc detail command, 210
show mpls 12transport vc vcid command, 167-169, 172, 176, 180, 185-187
show mpls forwarding-table command, 305
show mpls interface command, 220
show mpls ldp neighbor neighbor-ip-address detail, 144
show policy-map command, 193
show vpdn session command, 767
show vpdn session all command, 767
show vpdn tunnel command, 780
show vpn-sessiondb command, 979-980
Simple Certificate Enrollment Protocol. ***See*** **SCEP**
Simple Public Key Infrastructure (SPKI), 558
Site of Origin attribute, 270-277
site-to-site VPNs. ***See also*** **IPsec VPNs**
customer provisioned VPNs, 15
deploying, 18-19, 21
devices, 6
overview, 11
protocols, 8
service provider provisioned, 13-15
SKEME (Secure Key Exchange Mechanism), IKEv1, 432
SLI messages, 41
software clients, 805

SoO (Site of Origin) attribute, 270-277
SPD (Security Policy Database), 432
SPKI (Simple Public Key Infrastructure), 558
split tunneling
defined, 741
IPsec, 898-901
spoke site gateways (DMVPN), configuring
dynamically assigned IP addresses, 547-550
GRE tunnel interface, 543-545
overview, 543
routing protocol for site-to-site reachability, 545
sample configuration, 546-547
SSCS (Service Specific Convergence Sublayer), 70
SSL (Secure Sockets Layer)
packet format, 907
protocol overview, 908-910
versions, 907
ssl encryption command, 966
SSL remote access VPNs
advantages/disadvantages, 906-907
Cisco Secure Desktop
Cache Cleaner settings (Mac/Linux), 961-962
Cache Cleaner settings (Windows), 957-958
enabling, 962-963
installing, 954
location criteria, 954-956
overview, 952-953
Secure Desktop settings, 959-961
VPN Feature Policy settings, 958-959
closing connections, 923-924
enabling on Cisco ASA 5500 Series appliances
cryptographic algorithms, configuring, 978
e-mail proxy, configuring, 976-977
file access/entry/browsing, configuring, 974
HTTP server, configuring, 971
login/home pages, customizing, 978-979
operation of, verifying, 979-980
overview, 970
port forwarding, configuring, 975
SSL trustpoint, specifying, 977
SSL versions, restricting, 977-978
URL lists, specifying, 973-974
user authentication, configuring, 972-973
user group policy, configuring, 971-972
WebVPN, enabling on outside interface, 971
enabling on Cisco IOS devices
basic SSL parameters, configuring, 966-967
domain name address, configuring, 964
IOS router, enrolling with a CA, 965
login/home pages, customizing, 967-969
name server address, configuring, 964
overview, 963
port forwarding, configuring, 969-970
remote AAA, configuring, 964-965
URLs, specifying, 969
webvpn enable command, 966
enabling on Cisco VPN 3000 concentrators
e-mail proxy, 943-948
file server access, 930-935
overview, 924
TCP-based application access, 937-942
web server access, 936-937
overview, 905-906
resuming sessions, 922-923
RSA handshake authentication
with client, 920-922
with VPN gateway only, 910-920
thick-client connectivity, 948
ssl trustpoint command, 966
Start-Control-Connection-Connected (SCCCN) message (L2TPv2), 716
Start-Control-Connection-Reply (SCCRP) message (L2TPv2), 716
Start-Control-Connection-Request (SCCRQ) message (L2TPv2), 716
stateful IPsec high availability, 611-627
stateless IPsec high availability
overview, 595-596
with HSRP on inside interface, 606-611
with RRI, 596-606
static routes
configuring for connectivity between customer VPN sites, 248
GRE tunnels, 487
static session setup, L2TPv3-based L2VPNs
advantages/disadvantages, 41-42
overview, 93

with control connection, 96-98
without control connection, 93-96
static VRF routes, redistributing into MP-BGP, 248-250
Statistics tab (Cisco SSL VPN Client), 951
status codes, 152
StopCCN (Stop-Control-Connection-Notification) message, 36-37
Stop-Control-Connection-Notification (StopCCN) message (L2TPv2), 716
stream ciphers, 418-419
SUCCESS messages (CA), 571
switching
ATOM-based pseudowires, 202-207
DLCI-to-DLCI, 172-176
symmetric encryption algorithms, 416
block ciphers, 416-418
IPsec, 415
stream ciphers, 418-419
symmetric key exchange, 419
sysopt connection permit-ipsec command, 831

T

tag-switching ip command, 873
TC (Transmission Convergence) sublayer (ATM reference model), 67-68
TCI field (802.1Q frame), 50
tearing down
L2TPv3 control connection, 36-37
L2TPv3 sessions, 38-40
TED (Tunnel Endpoint Discovery), 528-531
terminate-from hostname command, 795
text-color command, 969
thick clients, SSL remote access connectivity, 948-952
timeouts, NAT/PAT, 510-511
title-color command, 968
TLS (Transport Layer Security), 907
TPID field (802.1Q frame), 50
traceroute command, 304-305, 309-310
traffic flow confidentiality
ESP, 426
IPsec, 410
traffic selectors, IPsec, 475
transform sets
AH, 471
compression, 471
configuring, 471-474
ESP, 471
IPsec, 830
Transmission Convergence (TC) sublayer (ATM reference model), 67-68
transparent command, 245
Transport Layer Security (TLS), 907
Transport Layer VPNs, 18
transport mode
AH, 423
AH/ESP, 430
ESP, 428
Triple DES (3DES)
defined, 418
IKE, 462
trusted VPNs, 17
tunnel definitions, RADIUS servers, 790-793
tunnel destination command, 197
Tunnel Endpoint Discovery (TED), 528-531
tunnel marking, QoS for L2TPv3, 123-125
tunnel mode
AH, 424
AH/ESP together, 430
ESP, 418, 518
tunnel mode gre multipoint command, 539, 545
tunnel mode mpls traffic-eng command, 197
tunnel mpls traffic-eng bandwidth command, 198
tunnel mpls traffic-eng priority command, 198
tunnel protection command, 490
tunnel protection ipsec profile command, 539, 545
tunnel selection
AToM-based L2VPNs, 188, 195
MPLS-TE, 195-202
MPLS-TE, 195-198
P routers, 199
tunnel switching, AToM-based L2VPNs, 188
tunnel-group command, 831, 843
tunnel-group general attributes configuration mode, 831
tunnel-group-map command, 844
tunnels
DiffServ, 377-380, 656-658
GRE
ip mtu command, 696-697

ip tcp adjust-mss command, 697-699
spoke site gateway parameters, 543-545
IETF, 791-793
site-to-site VPNs, 407

U

UNI (User-to-Network Interface) ATM cell header, 69-70
Uniform Model, DiffServ tunneling
implementing, 390-392
overview, 379-380
unique preshared keys, IPsec VPNs, 550-552
U-PE (User-facing Provider Edge) devices, 6
url-list command, 968
user accounts, IPsec remote access, 821
user group policy, configuring for WebVPN, 971-972
user packets
forwarding between MPLS Layer 3 VPN sites, 229-231
NAT/PAT, 512-517
User-facing PE (U-PE) devices, 6
username command, 829
User-to-Network Interface (UNI) ATM cell header, 69-70

V

VCAs (virtual cluster agents), 882
VCC (Virtual Channel Connection) mode cell relay
transporting ATM traffic over L2TPv3 pseudowires
configuring, 79-81
overview, 75
with cell packing, 85-88
VCI (Virtual Channel Identifier) field (UNI ATM cell header), 69, 72
Version (VER) field (L2TPv3 control channel messages), 32
violate-action drop command, 195
Virtual Channel Identifier (VCI) field (UNI ATM cell header), 69, 72
virtual cluster agents (VCAs), 882
Virtual Leased Line Service VPNs, 13
Virtual Path Identifier (VPI) field (UNI ATM cell header), 69, 72, 76
Virtual Private Dialup Networks. *See* VPDNs
Virtual Private LAN Service (VPLS), 27, 138
Virtual Private Wire Service. *See* VPWS
Virtual Private Wire Service (VPWS) VPNs, 13
Virtual Router Redundancy Protocol (VRRP), 887-889
virtual-profile aaa command, 798
virtual-template command, 795
VLAN ID field (802.1Q frame), 50-52
voluntary tunnel mode
CHAP, 712
Cisco routers, 776-782
encryption, 712
L2TP remote access VPNs
L2TP/IPsec, 713
message formats/types, 713-716
PPP user authentication with IPsec, 713
PPP user authentication without IPsec, 712-713
L2TP/IPsec remote access VPNs
digital signature authentication, 724
preshared key authentication, 724
PSK authentication, 725-732
setting up, 716-724
PAP, 712
remote access L2TP VPNs
L2TP/IPsec, 713
message formats/types, 713-716
PPP user authentication with IPsec, 713
PPP user authentication without IPsec, 712-713
remote access L2TP/IPsec VPNs
Cisco routers, 776-782
NAT devices, transitting, 773-776
verifying, 765-773
voluntary tunnel mode remote access VPNs, 16
voluntary/client initiated tunnel mode, 710
VPC (Virtual Path Connection) mode cell relay
transporting ATM traffic over L2TPv3 pseudowires
with cell packing, 85-88
configuring, 81-84
overview, 75

vpdn enable command
compulsory tunnel mode, 789
VPDNs, 734
vpdn search-order domain command, 789
vpdn-group command, 789
VPDNs (Virtual Private Dialup Networks), 16
protocol 12tp command, 734
RADIUS servers, 791
vpdn enable command, 734
VPI (Virtual Path Identifier) field (UNI ATM cell header), 69, 72, 76
VPLS (Virtual Private LAN Service), 27, 138. *See also* L2VPNs
VPN 3000 concentrator. *See* Cisco VPN 3000 concentrators
VPN Feature Policy module (Cisco Secure Desktop), 958-959
vpn load-balancing command, 886
VPN routing and forwarding (VRF) tables, 227-229
vpn-addr-assign command, 831
VPNs. *See also* specific VPN models
accept-dialin, 734
backbone, 5
complementary nature of, 18
devices, 5-7
full mesh, 408
gateways, 409, 824-831
hub and spoke, 408
partial mesh, 408
vpn-tunnel-protocol webvpn command, 972
VPNv4
packet forwarding
between ASBRs, 331-333
between route reflectors, 346-348
route advertisement
between ASBRs, 325-331
between route reflectors, 334-346
route exchange, 241-242
VPWS (Virtual Private Wire Service), 27, 138
VRFs (VPN routing and forwarding) tables, 227-229
VRF-to-VRF connectivity
inter-autonomous system MPLS VPNs
overview, 316-317
packet forwarding, 322-324
route/label advertisement, 317-322
VRRP (Virtual Router Redundancy Protocol), 887-889
VTIs, 495-499

W

WAN-Error-Notify (WEN), 716
web servers, enabling access, 936-937
WebVPN. *See also* SSL remote access VPNs
advantages/disadvantages, 906-907
Cisco Secure Desktop
Cache Cleaner settings (Mac/Linux), 961-962
Cache Cleaner settings (Windows), 957-958
enabling, 962-963
installing, 954
location criteria, 954-956
overview, 952-953
Secure Desktop settings, 959-961
VPN Feature Policy settings, 958-959
clientless VPNs
configuration tasks, 925-930
e-mail proxy, configuring, 943-948
file server access, configuring, 930-935
overview, 924-925
TCP-based application access, enabling, 937-942
web server access, configuring, 936-937
enabling on ASA 5500 Series devices
cryptographic algorithms, configuring, 978
e-mail proxy, configuring, 976-977
file access/entry/browsing, configuring, 974
http server, configuring, 971
login/home pages, customizing, 978-979
on outside interface, 971
operation, verifying, 979-980
overview, 970
port forwarding, configuring, 975
SSL trustpoint, specifying, 977
SSL versions, restricting, 977-978
URL lists, specifying, 973-974
user authentication, configuring, 972-973
user group policy, configuring, 971-972

enabling on Cisco IOS devices
domain name address, configuring, 964
enrolling routers with a CA, 965
login/home pages, customizing, 967-969
name server address, configuring, 964
overview, 963
port forwarding, configuring, 969-970
remote AAA, configuring, 964-965
SSL parameters, configuring, 966-967
URLs, specifying, 969
webvpn enable command, 966
overview, 905-906
RSA handshake authentication
with client, 920-922
with VPN gateway only, 910-920
SSL sessions
closing, 923-924
overview, 907-910
resuming, 922-923
thick-client connectivity, implementing, 948-952
webvpn enable command, 966
wildcard preshared keys
IPsec VPNs, 531
overview, 442
Windows
L2TP/IPsec
multiple clients behind same NAT device, 776
VPN gateways for digitial signature authentication, 759-765
VPN gateways for PSK authentication, 736-742
NAT-T, 773
Oakley logging, 732, 770
Windows 2000, L2TP/IPsec client, 711
Windows XP
ipconfig /all command, 727
L2TP/IPsec client, 711
wins command, 826
WINS server addresses, 814-816
wins-server value command, 829
wireless VPNs, 894-898

X - Z

X.25 traffic, 59-60
X.509 certificates, 558-562
Xauth (Extended Authentication within IKE), 806-811
IKE, 854
L2TP, 711
xconnect command, 45, 160-161, 164-169, 175, 179, 186, 204
xconnect peer-pe-id-address pwid encapsulation mpls command, 160
xconnect peer-pe-ip-address pwid encapsulation mpls command, 167-169

Zero-Length-Body Ack (ZLB Ack) message, 715