Index

3DES (triple DES), 6, 65, 87, 171, 178, 210, 347, 366
  definition of, 65

Aboba, B., 162, 407, 409, 415
`accept` function, 424
access concentrator, definition of, 99
ACCM (asynchronous control character map)
  attribute value field, 134
  definition of, 133
ACK flag, definition of, 27
Adams, R., 343
address
  broadcast, 19
  IPv6, 44–45
  limited broadcast, 19
  network-directed broadcast, 19
  private, 35–40, 54, 93, 104, 350
Address Resolution Protocol, *see* ARP
addressing
  classful, 13–19
  IP, 13–19
Adleman, L.M., 70, 81, 84
Advanced Encryption Standard, *see* AES
AES (Rijndael), 6, 65–67, 72, 87, 271, 282, 291, 365–366
Agarwal, P., 137
aggressive mode, definition of, 376
AH (Authentication Header protocol), 46, 168, 308–339, 341–342, 355, 358, 365–366, 373, 376, 389, 393, 395, 397–398, 400–403, 410, 416
  definition of, 309, 325
  header, 326–328
  header, definition of, 327
  input processing, 331
  IPsec protocol, 7–8
  IPv6, 336–337
  output processing, 330–331
  processing, 330–331
  transport mode, 331–333
  tunnel mode, 333–336
Akyol, B., 137
Albaugh, T., xv
alert
  message types, SSL, 181
  SSL, 180
algorithm
  Bellman-Ford, 50
  Dijkstra's, 50
  extended Euclidean, 71
alleged RC4, 59
Allen, C., 166
Alvestrand, H.T., 237
Anderson, R., 76

Andersson, L., 138
AppleTalk, 42, 55
application layer, 11–12, 20, 157
  definition of, 10
arithmetic, ones-compliment, 55
Arkko, J., 399
ARP (Address Resolution Protocol), definition of, 15
assigned
  session ID, definition of, 126
  tunnel AVP, definition of, 119
asymmetric cipher, 6, 57, 69–75, 87
asynchronous control character map, *see* ACCM
Atkinson, R., 311, 325, 341, 350, 398, 401, 403
attack
  DOS, 37
  Smurf, 19
attribute value pair, *see* AVP
attribute value pair, 113–115
authentication, 3–8, 42, 57, 155–162, 168, 171, 204, 207, 220, 271, 292–295, 308–313, 315–318, 321, 323, 325–326, 331–333, 336, 339, 341–345, 347, 350, 354–355, 357–358, 361, 365, 379, 403, 406
Authentication Header protocol, *see* AH
authentication, VTun, 269–271
`auth-up` file, 431
autonomous system, *see* AS
autonomous system, 49, 51–55, 135, 139–140, 151
avalanche effect, definition of, 76
AVP (attribute value pair)
  definition of, 111
  HELLO, 125
  L2TP message type, 116
  Result code, 121
AVPs
  CDN, 132
  ICCN, 128
  ICRP, 127
  ICRQ, 126
  OCCN, 132
  OCRP, 131
  OCRQ, 131
  SCCCN, 120
  SCCRP, 120
  SCCRQ, 119
  SLI, 133
  SopCCN, 121
  WEN, 133

Barrett, D.J., 214, 221, 228
`bash` program, 207
Baugher, M., 363
Baze, M., 307
`bc` program, 71–72, 422
bearer
  capabilities, definition of, 119
  type, definition of, 126
Begley, L., xv
Bellare, M., 80, 171, 242, 259–260, 292, 343
Bellman-Ford algorithm, 50
Bellovin, S.M., 341, 355–356
Bentley, J., xiv
BGP (Border Gateway Protocol), 51–55, 138–141, 144
birthday paradox, 75–76, 83
bit-flipping, definition of, 157
BITS (bump-in-the-stack), definition of, 311
BITW (bump-in-the-wire), definition of, 312
Bleichenbacher, D., 72, 230–231
block cipher, 57, 60–69, 87–88, 159, 166, 210, 233, 259–260, 282, 285, 342–343, 345, 355–356
Blowfish, 67–69, 87, 210, 271, 274, 281, 286, 291, 366
Blunk, L.J., 407
Boneh, D., 291
Booth, S., 162
BOOTP, 19
Border Gateway Protocol, *see* BGP
border router, definition of, 49
Borman, D., 22
Braden, R.T., 22
broadcast address, 19
Brumley, D., 291
BSD r-commands, 7, 207–208, 227, 266
`bsd` work station, 5, 34–35
bump-in-the-stack, *see* BITS
bump-in-the-wire, *see* BITW

CA (certificate authority), 84–87, 175, 188, 198, 293–294, 370
  definition of, 84
call serial number, definition of, 126

called number, definition of, 127
calling number, definition of, 127
Callon, R., 138
Canetti, R., 80, 171, 292, 343
Canvel, B., 204
Carlson, J., 43, 100, 125, 407, 432
Carrel, D., 96, 357
`cat` program, 425
CBC mode, definition of, 60
CCP (Compression Control Protocol), definition of, 42
CDN AVPs, 132
certificate authority, *see* CA
certificate, 6, 57, 83–88, 168, 217, 246, 293–294, 299, 369, 382–384, 401, 406
  chain, 86–87
  revocation, 87
  SSL, 175–176, 178, 180, 185–186, 188–189, 193, 195–198, 205
  types, IKE, 371
  X.509, 84–86
CFB (cipher feedback mode), definition of, 295
challenge, definition of, 119
Challenge-Handshake Authentication Protocol, *see* CHAP
Chandra, P., 192
change cipher spec, SSL, 177–178
channel messages, SSHv2, 250
CHAP (Challenge-Handshake Authentication Protocol), definition of, 42
Cheval, P., 137
CIDR (classless interdomain routing), 16–19, 43, 54
CIPE, 7, 162–163, 267, 272–283, 302
  binary packet, 273–274
  binary packet, definition of, 274
  configuration data, definition of, 281
  control message types, 281
  control messages, 281–282
  key exchange packet, definition of, 275
  key exchange types, 275
  key negotiation, 274–277
  P byte, definition of, 274
  security, 282–283
`ciped` program, 273, 280–281
cipher block chaining mode, *see* CBC
cipher feedback mode, *see* CFB
cipher
  asymmetric, 6, 57, 69–75, 87
  block, 57, 60–69, 87–88, 159, 166, 210, 233, 259–260, 282, 285, 342–343, 345, 355–356
  Feistel, 62, 66–67
  stream, 57–60, 87, 157, 163, 166, 171, 241, 324, 343, 345
  suite, SSL, 166–167
  symmetric, 6, 57–69, 72–73, 80
Clark, J., xiv
classful
  address ranges, 14
  addressing, 13–19
classless interdomain routing, *see* CIDR
client
  authentication, SSL, 185–188
  hello, SSL, 173–174
  key exchange, SSL, 176–177
closure notification, SSL, 180
Cobb, S., 157
combined
  mode cryptographic algorithms, 403
  security associations, 318–320
Comer, D.E., 9, 47
Compression Control Protocol, *see* CCP
computationally infeasible, definition of, 83
connection
  set up, 28–30
  shutdown, 30–31
connection-based, 9, 24–25
connectionless, 9, 22, 25
  definition of, 20
conservative label retention mode, definition of, 138
Conta, A., 137
control messages
  L2TP, 116
  PPTP, 107
counter mode, *see* CTR
CRC (cyclic redundancy check), 41–42, 91, 109, 203, 210, 216, 231, 233, 259, 266, 273, 276–277, 282
CRC-32 compensation attack detector, 231
Crocker, S.D., 177
cryptographic, 4
  hash function, 75–87
  implementations, 419–423

cryptographically secure random number, 177
cryptography, 4–8, 57–88
  elliptic curve, 75
`csh` program, 207
CTR mode, definition of, 61
cyclic redundancy check, *see* CRC

Dai, W., 259
Data Encryption Standard, *see* DES
Datagram Transport Layer Security, *see* DTLS
datalink layer, definition of, 10
Davari, S., 137
Davie, B., 137
Davis, C.R., 75
Dawson, E., 58
`dc1` device, 98–99
de Groot, J.G., 35
de Wegner, B., 83
decorrelation, definition of, 399
Deep Crack, 65
Deering, S., 21
Deering, S.E., 45–46, 327
denial of service, *see* DOS
DES (Data Encryption Standard), 6, 61–67, 72, 87, 210
`/dev/urandom` device, 275
DHCP (Dynamic Host Configuration Protocol), 19, 381
DiBurro, L., 397, 410
Dierks, T., 166
Diffie, W., 70, 74, 84
Diffie-Hellman key
  exchange, 57, 74–75, 192
  exchange, SSL, 188–191
digital signature, 6, 80–83, 85, 87, 371, 376, 393–395, 401
Digital Signature Algorithm, *see* DSA
Digital Signature Standard, *see* DSS
Digital Subscriber Line, *see* DSL
Dijkstra, E.W., 50
Dijkstra's algorithm, 50
discrete logarithm, 73–75, 240
`DISPLAY` variable, 220–221
distance vector protocol, 50–51, 55
Dixon, W., 162, 409, 415
DNS (Domain Name System), 42, 158, 162, 212, 320–321
DOI (Domain of Interpretation), definition of, 362
Domain Name System, *see* DNS
Domain of Interpretation, *see* DOI
Dommety, G., 101
Doolan, P., 138
Doraswamy, N., 75, 343
DOS (denial of service), 344, 358, 377
  attack, 37
downstream on demand mode, definition of, 138
Dreyfus, S., 143
DSA (Digital Signature Algorithm), 81–83, 407
DSL (Digital Subscriber Line), 95–100
  definition of, 95
DSS (Digital Signature Standard), 78, 81–83, 244, 381
  definition of, 81
DTLS (Datagram Transport Layer Security), definition of, 168
Dynamic Host Configuration Protocol, *see* DHCP

EAP (Extensible Authenication Protocol), definition of, 42
Eastlake, D.E., 3rd, 177
EBC mode, definition of, 60
`echo`
  function, 194
  program, 28–30
`echoit` program, 197–199, 226–227
ECP, definition of, 42
EDE mode, definition of, 65
Effective TCP/IP Programming, *see* ETCP
Egevang, K.B., 40
EGP (Exterior Gateway Protocol), 51–55
  definition of, 49
egress router, definition of, 138
EIGRP (Enhanced Interior Gateway Routing Protocol), 51
electronic code book mode, *see* ECB
Electronic Frontier Foundation, 65
ElGamal, 6, 70, 73–75, 82, 87
ElGamal, T., 73
elliptic curve cryptography, 75
Encapsulating Security Payload, *see* ESP
encapsulation, 6–7, 11–13, 32, 54, 89–90, 92,

99, 102–104, 110, 145, 151, 160, 172, 271, 284, 288, 290, 294, 302, 307–308, 312–315, 318–320, 330, 332–333, 335–337, 339, 344, 348, 353, 410, 415, 431
encrypt-decrypt-encrypt mode, *see* EDE
encryption, 3–8, 42, 57–88, 113–114, 155–162, 167–168, 176, 204, 207, 209–210, 232–235, 237–238, 260, 267–268, 270–272, 285, 292–293, 295, 308–311, 315, 318, 323, 325, 336, 338, 342, 344–345, 354, 361, 365–366, 406
  symmetric, 383–385
endpoint authentication, definition of, 158
Enhanced Interior Gateway Routing Protocol, *see* EIGRP
`errno` variable, 423
error codes, L2TP, 122
`error` function, 147, 193, 423
`ERROR` macro, 193
ESN (extended sequence number), definition of, 401
ESP (Encapsulating Security Payload), 40, 46, 157, 160, 163, 168, 296, 308–310, 312–315, 317–319, 321–326, 336, 338, 341–356, 358, 364–366, 373, 376, 393, 397–405, 410, 412–417
  definition of, 309, 341
  header, 342–343
  header/trailer, definition of, 342
  input processing, 345
  IPsec protocol, 7–8
  IPv6, 353–354
  output processing, 344–345
  processing, 344–345
  transport mode, 345–348
  tunnel mode, 348–353
ESPv3, 403–404
  header, definition of, 404
ETCP ({Effective TCP/IP Programming}), 5, 24, 31, 180, 193, 204, 294, 419, 423, 429
`/etc/ppp/auth-down` file, 431
`/etc/ppp/auth-up` file, 431
`/etc/ppp/ip-down` file, 432
`/etc/ppp/ip-up` file, 432
`/etc/ppp/ppp.conf` file, 433
`/etc/ppp/ppp.linkdown` file, 434
`/etc/ppp/ppp.linkup` file, 434
`eth1` device, 99
`ethereal` program, 429
`etherpeek` program, 429
Etienne, J., 272
Evarts, J., 96
exchange types, IKE, 361
`exec` function, 228
`execl` function, 263
explicit congestion notification, *see* ECN
extended sequence number, *see* ESN
extended
  Euclidean algorithm, 71, 421–423
  sequence numbers, 401–403
Extensible Authenication Protocol, *see* EAP
extension headers, IPv6, 46–47, 55
Exterior Gateway Protocol, *see* EGP
Exterior Gateway Protocol, *see* EGP

Farinacci, D., 101, 137
FCS (frame check sequence), 41, 100
FEC to NHLFE map, *see* FTN
FEC (forwarding equivalence class), definition of, 136
Fedorkow, G., 137
Feistel network, *see* Feistel cipher
Feistel cipher (Feistel network), 62, 66–67
  definition of, 62
Feldman, N., 138
Feng, D., 83
Ferguson, N., 57, 61, 65, 70, 73, 81, 84, 87, 309, 313, 316–317, 324–325, 341, 344, 355
Fermat's little theorem, 71
FIN flag, definition of, 27
finished message, SSL, 178–180
flooding, definition of, 50
Fluhrer, S., 60, 324
Ford, L.R., 50
Ford, W., 85
`fork` function, 228, 263
forwarding equivalence class, *see* FEC
four-way handshake, 29
frame check sequence, *see* FCS
frame formats, PPP, 43
framing
  capabilities, definition of, 119
  type, definition of, 127
Francis, P., 40
Franz, M., xv
Fredette, A., 138
Freier, A.O., 166

Friedman, A.A., 231
FTN (FEC to NHLFE map), definition of, 137
FTP, definition of, 40
`ftp` program, 7, 39–40, 136, 207, 266
Fulkerson, D.R., 50
Fuller, V., 19
function, cryptographic hash, 75–87
Futoransky, A., 231, 282

Garman, J., 214
GCHQ (Government Communications Headquarters), 70
general authentication messages, SSH, 243
Generic Routing Encapsulation, *see* GRE
`geqn` program, xiv
`gethostbyname` function, 149
`gif` device, 92, 101
Glenn, R., 327, 343
Goldberg, I., 165
Government Communications Headquarters, *see* GCHQ
`gpic` program, xiv
GRE (Generic Routing Encapsulation), 100–104, 106–107, 110, 151–152, 161
  definition of, 100
`gre` device, 101
GRE header, definition of, 101
`gretun` device, 102–103
Gross, P., 49
group generator, definition of, 73
`gtbl` program, xiv
`gtunnel`, 145–151
  program, 6–7, 145, 147–148, 151–152, 201, 205, 261–262, 266, 311, 339, 432
`gtunnel.c` file, 145, 148
Guichard, J., 144
Gutmann, P., 3, 84, 87, 242, 272, 283, 292

half close, 31
Haller, N.M., 215
Hamzeh, K., 109
handshake
  four-way, 29
  messages, SSL, 171–172
  three-way, 28–29
  types, SSL, 172
Hanks, S., 101
Hanson, D., xiv
Harding, T., xiv
Hardjono, T., 363
Harkins, D., 75, 343, 357
Harney, H., 363
hash function, cryptographic, 75–87
Hatch, B., 261
HDLC (High-Level Data Link Control Protocol), 40–42, 55, 100
  definition of, 41
header
  AH, 326–328
  IP, 20–22
  IPv6, 45–46
  TCP, 25–28
  UDP, 23
Hedrick, C., 50
Heinanen, J., 137
Hellman, M., 70, 74, 84
HELLO
  AVP, 125
  definition of, 125
hello done, SSL, 176
Henry-Stocker, S., xiv
Herzog, J., 240
Hickman, K.E.B., 165
hidden AVP, definition of, 114
High-Level Data Link Control Protocol, *see* HDLC
Hiltgen, A., 204
Hinden, R.M., 19, 45–46, 327
HMAC, 6, 80–83, 134, 158, 166, 170–172, 178, 233, 284–286, 292–293, 295, 298, 300–301, 303, 327–328, 336, 343, 347–348, 353, 370, 379, 388, 394
Holdrege, M., 40
Hollenbeck, S., 174
host ID, definition of, 14
Housley, R., 85
Huitema, C., 16, 47
Huttunen, A., 397, 410–411

IANA (Internet Assigned Numbers Authority), definition of, 102
ICCN AVPs, 128
ICMP (Internet Control Message Protocol), 10, 21–22, 25, 45, 54, 91, 93, 95, 103–104, 203–204, 297, 314, 323, 333, 336, 345,

348, 372, 399–400, 404, 416, 427
definition of, 32
echo reply, 32–33
echo request, 32–33
error messages, 34–35
message types, 33
protocol, 31–35
ICRP AVPs, 127
ICRQ AVPs, 126
identification
payload, IPsec, 369
types, IPsec, 369
IETF (Internet Engineering Task Force), 7, 47, 54, 84, 96, 109, 113, 134, 162, 166, 208, 232, 238, 259, 307, 365, 373
`ifconfig` program, 92, 102–103, 150
IGMP (Internet Group Management Protocol), 10
IGP (Interior Gateway Protocol), 49–51, 54–55
definition of, 49
IKE (Internet Key Exchange), 308–310, 312, 317, 321–323, 330, 357–395, 397, 400–401, 404–414, 416–417
authentication with signatures, 381–383
certificate types, 371
definition of, 7, 309, 357
exchange types, 361
IPsec protocol, 7–8
key generation, 378–379
new group exchange, 386–387
notification message types, 374
payload types, 360
phase 1, 376–378
phase 1 attributes, 367
phase 2 attributes, 367
phase 2 quick mode, 387–388
public key authentication, 383
revised public key authentication, 383–386
shared secret authentication, 379–381
IKEv2, 401, 404–409, 416–417
exchanges, 405–409
messages, 405
ILM (incoming label map), definition of, 137
`inbound` function, 145, 147, 149
incoming label map, *see* ILM
`inet_aton` function, 149
`inetd` program, 258–259
`inetd.` program, 259
ingress router, definition of, 136
`INIT` macro, 147, 193
initial received LCP CONFREQ, definition of, 127
initialization vector, *see* IV
Integrated Services Digital Network, *see* ISDN
integrity check value, *see* ICV
interface layer, 12, 40, 92, 134–135, 202
definition of, 10
Interior Gateway Protocol, *see* IGP
Intermediate System to Intermediate System Protocol, *see* IS-IS
International Telecommunication Union, 84
Internet Assigned Numbers Authority, *see* IANA
Internet Control Message Protocol, *see* ICMP
Internet Engineering Task Force, *see* IETF
Internet Group Management Protocol, *see* IGMP
Internet Key Exchange, *see* IKE
Internet Protocol, *see* IP
Internet layer, definition of, 10
internet protocol numbers, 22
Internet Security Association and Key Management Protocol, *see* ISAKMP
internet service provider, *see* ISP
Ioannidis, J., 307
IP (Internet Protocol)
addressing, 13–19
header, 20–22
layer, 283
`ip` program, 102
IP security, *see* IPsec
IP protocol, 20–22
`ip` variable, 150
`ip_len` member, 150
`ip_p` member, 103
IP-in-IP tunnel, 92–95, 100–101, 141, 147–152, 262, 311, 315, 324, 336
`ipip` program, 150, 152
`ipip.c` file, 148
`IPPROTO_IPIP` socket option, 149
IPsec (IP security), 6–8, 40, 46, 55, 74, 80, 157, 160–163, 168, 224, 267, 283, 296, 301–302, 307–318, 320–325, 328, 330, 333, 338, 341–345, 347, 350, 354, 357–358, 362–365, 368–369, 372–373,

376, 378, 387–389, 393–394, 397–401, 404, 406, 409–410, 412–413, 415–416
and multicast, 400
architecture, 311–324, 398–401
definition of, 307
futures, 397–417
ICMP processing, 323
identification payload, 369
identification types, 369
inbound processing, 322–323
modes, 313–316
outbound processing, 322
overview, 308
policies, 320–321
policy, definition of, 320
processing, 321–323
protocol, AH, 7–8
protocol, ESP, 7–8
protocol IDs, 364
protocol, IKE, 7–8
protocols, 312–313
selectors, definition of, 321
sequence numbers, 328–330
transform IDs, 366
`iptrace` program, 429
`ip-up` file, 201
IPv4, definition of, 21
IPv6, 43–47, 54–55, 327, 330, 338, 359, 398–399, 416
address, 44–45
AH, 336–337
anycast address, definition of, 44
definition of, 45
ESP, 353–354
extension headers, 46–47, 55
header, 45–46
muticast address, definition of, 44
pseudoheader, definition of, 46
unicast address, definition of, 44
IPX, 42, 55, 89–90
ISAKMP (Internet Security Association and Key Management Protocol), 357–376, 378–380, 386–388, 392–394
attribute, definition of, 362
certificate payload, 369–370
certificate payload, definition of, 370
certificate request, definition of, 370
cookies, 358–359
delete payload, 373
delete payload, definition of, 375
generic header, definition of, 362
hash payload, 370
hash payload, definition of, 371
header, 359–361
header, definition of, 360
identification payload, 368–369
key exchange payload, 367–368
key exchange payload, definition of, 368
message processing, 373–375
nonce payload, 372
nonce payload, definition of, 372
notification payload, 372–373
notification payload, definition of, 372
payloads, 361–362
proposal payload, definition of, 364, 368
SA payload, definition of, 363
signature payload, 370–371
signature payload, definition of, 371
transform payload, definition of, 365
vendor ID payload, definition of, 375
vendor payload, 373
ISDN (Integrated Services Digital Network), definition of, 132
IS-IS (Intermediate System to Intermediate System Protocol), 51
iterated tunneling, definition of, 319
IV (initialization vector), definition of, 60

Jacobson, V., 41
Johnson, D.B., 399

Kalisky, B., 72, 231
Kargieman, E., 231, 282
Karlton, P., 166
Karrenberg, D., 35
Kaufman, C., 134
Kent, S., 309, 311, 325, 341, 350, 398, 401, 403
`kermit` program, 259
Kernighan, B., xiv
key management, 7
Kivinen, T., 397, 411
Klima, V., 83
Knuth, D.E., 71, 422
Kocker, P.C., 166
Kohno, T., 242, 259–260
Kolesnikov, O., 261

Krawczyk, H., 80, 171, 292, 343, 345, 358
Krishnan, R., 137

L2F (Layer Two Forwarding), definition of, 109
L2TP Access Concentrator, *see* LAC
L2TP Network Server, *see* LNS
L2TP (Layer Two Tunneling Protocol), 109–134, 151–152, 158–163, 222, 224, 409
  attribute value pair, definition of, 113
  AVP, definition of, 113
  common header, definition of, 111
  control messages, 116
  definition of, 109
  error codes, 122
  message type AVP, 116
  proxy authentication types, 128
L2TPv3, 134
label distribution protocol, *see* LDP
label switched path, *see* LSP
label switching router, *see* LSR
label
  distribution protocol, 138–139
  MPLS, 137
LAC (L2TP Access Concentrator), definition of, 109
Lai, X., 83
`LANalyzer` program, 429
`laptop` work station, 5, 28–29, 34–35
last
  received LCP CONFREQ, definition of, 127
  sent LCP CONFREQ, definition of, 127
Layer Two Forwarding, *see* L2F
Layer Two Tunneling Protocol, *see* L2TP
layering, 9–11, 39, 54
LCP (Link Control Protocol), definition of, 42
LDP (label distribution protocol), definition of, 138
Le Faucheur, F., 137
Lear, E., 35
leased line, 2–3, 141, 143, 155–156, 163, 311
Lemberg, W., xiv
Lenstra, A., 83
Levkowetz, H., 407
Li, T., 19, 51, 101, 137
liberal retention mode, definition of, 138
Lidl, K., 96
lightweight VPN, 162–163, 267–303, 307, 309
limited broadcast address, 19
Link Control Protocol, *see* LCP
link layer, 109, 134, 283
  definition of, 10
link-state protocol, 50–51, 55
`linux` work station, 5, 30, 33, 35
`linuxlt` work station, 5
Little, W.A., 109
LNS (L2TP Network Server), definition of, 109
logarithm, discrete, 73–75, 240
`loom` program, xiv
LSP (label switched path), definition of, 136
LSR (label switching router), definition of, 136

MAC (message authentication code), 57, 79–83, 87–88, 159, 205, 210, 216, 231, 233, 238, 242, 259, 266, 272, 282, 292, 312, 325, 327, 401
  address, 16
  address, definition of, 15
  definition of, 79
Madson, C., 327, 343
Main mode, definition of, 376
Malkin, G.S., 50
Mamakos, L., 96
mandatory mode, definition of, 107
Mantin, I., 60, 324
manual keying, definition of, 317
Maughan, D., 357
maximum receive unit, *see* MRU
maximum transmission unit, *see* MTU
maximum bps, definition of, 131
McLaughlin, R., xiv
MD5, 76–83, 88, 115, 134, 213, 217–218, 231, 233, 271, 295, 301, 327, 343, 347–348, 366, 411
`md5` program, 76
Menezes, A.J., 57, 70–71, 295
Merkle, R., 70
message authentication code, *see* MAC
message integrity code, *see* MIC
message
  authentication, definition of, 158
  types, SSHv1, 211
Messier, M., 192

Messmer, E., 162
Meyer, D., 101
MH (mobility header), definition of, 399
MIC (message integrity code), definition of, 159
Microsoft Challenge Handshake Authentication Protocol, *see* MS-CHAP
Microsoft Point-to-Point Encryption, *see* MPPE
minimum bps, definition of, 131
Mister, S., 60
mobility header, *see* MH
Modadugu, N., 168
mode
  transport, 314–315
  tunnel, 315–316
modes, IPsec, 313–316
Mogul, J., 16, 21
Moskowitz, R.G., 35
Moy, J., 51
MPLS (Multiprotocol Label Switching), 135–144, 151–152, 156
  definition of, 135
  label, 137
  tunnel, 139–144
  VPN, 141–144, 155–156
MPPE (Microsoft Point-to-Point Encryption), 157–159
MRU (maximum receive unit), 42
`ms` macro, xiv
MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), 157–158, 162
MTU (maximum transmission unit), 21, 29, 55, 94–95, 151, 203, 288, 323
Mudge, 158
multicast, 13
Multiprotocol Label Switching, *see* MPLS
mutable
  but predictable, 326
  IP header fields (AH), definition of, 326
  IPv6 header fields (AH), definition of, 337

Nadeau, T.D., xiv
Namprempre, C., 242, 259–260
NAP (network access point), 52
  definition of, 49
Narten, T., 313
NAT transversal, *see* NAT-T
NAT (network address translation), 6, 8, 35–40, 43, 54, 93, 110, 134, 141, 161–162, 201, 271, 273, 309, 333, 336, 339, 350, 397, 409–417, 433
  keep-alives, 410
NAT-D payload, definition of, 412
National Security Agency, *see* NSA
NAT-OA payload, definition of, 414
NAT-T (NAT transversal), 8, 40, 134, 162, 309, 397, 409–417
  definition of, 162, 397
`nc` program, 28, 425
NCP (Network Control Protocol), definition of, 42
netcat, 28, 34, 196–199, 212, 425–426
  command line options, 426
`nettl` program, 429
network access point, *see* NAP
network address translation, *see* NAT
Network Control Protocol, *see* NCP
network
  ID, definition of, 14
  layer, 10–13, 22, 32–33, 39, 42, 45–47, 89–90, 92, 95, 106, 135, 137–138, 152, 157, 268, 272, 307, 328
  layer, definition of, 10
Network Layer Security Protocol, *see* NLSP
network traces, 3
network-directed broadcast address, 19
new IPsec processing model, 398
`newmail` function, 230
next hop label forwarding entry, *see* NHLFE
NHLFE (next hop label forwarding entry), definition of, 137
Nielsen, L., 58
NIST, 61–62, 65–67, 78, 81–83
NLSP (Network Layer Security Protocol), definition of, 307
Nolan, C., xv
nonce, definition of, 134
Nordmark, E., 313
notification
  message types, IKE, 374
  payload, ISAKMP, 372–373
`notify` function, 229–230
NSA (National Security Agency), 70, 78

Oakley Key Determination Protocol, *see* OAKLEY

OCCN AVPs, 132
OCRP AVPs, 131
OCRQ AVPs, 131
OFB (output feedback mode), definition of, 295
one time pad, 58
ones-compliment arithmetic, 55
open failure reason codes, SSHv2, 253
Open Shortest Path First Protocol, *see* OSPF
Open Systems Interconnection, *see* OSI
OpenSSH, 208–210, 212, 215–216, 228, 231, 237–238, 244
OpenSSL, 174, 179, 191–196, 205, 271, 277, 286, 291–292, 302, 429
`openssl` program, 205
OpenVPN, 7, 163, 267, 283, 292–303
  control channel, 297–301
  control channel packet, definition of, 298
  data channel, 294–296
  data packet, definition of, 296
  key exchange message-1, definition of, 299
  key exchange message-2, definition of, 300
  OCC message, definition of, 297
  OCC op codes, 297
  op codes, 295
  packet header, definition of, 295
  ping and OCC protocols, 296–297
  security, 301–302
  security models, 293–294
optional ESP padding, 403–404
orderly release, 31
Orman, H.K., 358
OSI reference model, 11
OSPF (Open Shortest Path First Protocol), 51–52, 140, 283
`outbound` function, 145, 147, 149
output feedback mode, *see* OFB

PAC (PPTP Access Concentrator), definition of, 105
Pacetti, A.M., 231, 282
packet
  PPP, 42
  sniffers, 426–429
  types, PPPoE, 98
PAD (peer authentication database), 400–401
  definition of, 400
PADI (PPPoE Active Discovery Initiation), 95–100
  definition of, 96
PADO (PPPoE Active Discovery Offer), 95–100
  definition of, 96
PADR (PPPoE Active Discovery Request), 95–100
  definition of, 96
PADS (PPPoE Active Discovery Session-confirmation), 95–100
  definition of, 96
PADT (PPPoE Active Discovery Terminate), 95–100
  definition of, 96
Pall, G.S., 109, 113, 134, 157
Palter, B., 113, 134
PAP (Password Authentication Protocol), definition of, 42
Partridge, C., 22
Password Authentication Protocol, *see* PAP
Patel, B.V., 162
path MTU, *see* PMTU
path-vector protocol, 53
payload types, IKE, 360
PCT (Private Communications Technology), definition of, 166
peer authentication database, *see* PAD
penultimate hop popping, definition of, 138
Pepelnjak, I., 144
Pereira, R., 343
perfect forward secrecy, *see* PFS
Perkins, C., 94, 323
Perkins, C.E., 399
Perlman, R., 3, 47, 51, 134
PFP (populate from packet flags), definition of, 400
PFS (perfect forward secrecy), definition of, 159
phase
  1 attributes, IKE, 367
  2 attributes, IKE, 367
physical channel ID, definition of, 127
`pid` variable, 32
`ping` program, 31–34, 91, 93, 99–100, 103–104, 129, 150–151, 202–204, 264–265, 332, 334, 336, 347, 389–390, 393, 395, 426–427
Piper, D., 362–363

pkcipe, 277–281
PKCIPE
  message types, 278
  packet, definition of, 277
pkcipe program, 273–274, 277
PKCS #1, 72, 81
PKI (public key infrastructure), 84–87
  definition of, 84
Plummer, D.C., 16
PMTU (path MTU), 21, 47, 288
PNS (PPTP Network Server), definition of, 105
Point to Point Protocol, *see* PPP
Point to Point Tunneling Protocol, *see* PPTP
policies, IPsec, 320–321
Polk, T., 85
pooled mode, definition of, 37
popen function, 229
populate from packet flags, *see* PFP
port address translation, *see* PAT
port
  address translation, definition of, 37
  forwarding, SSH, 223–226
Postel, J.B., 16, 20, 23, 25, 32, 39
PPP over Ethernet, *see* PPPoE
PPP (Point to Point Protocol), 6, 10, 40–43, 54–55, 90–92, 95–96, 98–100, 104–134, 145, 151, 157–162, 199–205, 261, 266, 268–269, 431–434
  frame formats, 43
  packet, 42
ppp program, 201–202, 432–434
ppp.conf file, 98, 433–434
pppd
  command line options, 431
  program, 99, 145, 200, 202, 431–432
ppp.linkup file, 201–202
PPPoE Active Discovery Initiation, *see* PADI
PPPoE Active Discovery Offer, *see* PADO
PPPoE Active Discovery Request, *see* PADR
PPPoE Active Discovery Session-confirmation, *see* PADS
PPPoE Active Discovery Terminate, *see* PADT
PPPoE (PPP over Ethernet), 95–100, 151, 201
PPPoe, definition of, 95
PPPoE (PPP over Ethernet)
  header, definition of, 98
  packet types, 98
pppoe program, 99
PPPoE tag, 97
PPTP Access Concentrator, *see* PAC
PPTP Network Server, *see* PNS
PPTP (Point to Point Tunneling Protocol), 101–102, 104–110, 118, 151–152, 157–159, 161, 163
  control message header, definition of, 106
  control messages, 107
  definition of, 105
  extended GRE header, definition of, 108
Preneel, B., 79
printf function, 423
private address, 35–40, 54, 93, 104, 350
  ranges, 36
Private Communications Technology, *see* PCT
private
  group, definition of, 128
  peering, 52
protocol
  distance vector, 50–51, 55
  ICMP, 31–35
  IDs, IPsec, 364
  IP, 20–22
  label distribution, 138–139
  link-state, 50–51, 55
  path-vector, 53
  TCP, 24–31
  UDP, 22–23
  version, definition of, 119
protocols, IPsec, 312–313
Provan, D., 89
proxy
  ARP, definition of, 15
  authen challenge, definition of, 127
  authen ID, definition of, 127
  authen name, definition of, 127
  authen response, definition of, 128
  authen type, definition of, 127
pseudo-header, 23, 39
pseudo-randomness, definition of, 231
pseudowire, 134
PSH flag, definition of, 27
public key infrastructure, *see* PKI
public key signature data, SSHv2, 245
Pyle, E., xv
python program, 59, 71, 229, 419–420, 422

Quick mode, definition of, 387

rand function, 271, 274
random
  device, definition of, 275
  vector, definition of, 120
random device, 275
random/urandom device, 275
RAS (remote access server), definition of, 104
rbiff program, 229
rbiffd program, 229–230, 259
RC4, 6, 58–60, 62, 87–88, 157–158, 171, 205, 241, 259–260, 279, 324, 420–421
  alleged, 59
rcp program, 207, 227–228
read function, 192, 194
receive window, definition of, 119
record layer
  message types, SSL, 171
  SSL, 170–171
recv_char() program, 40
reference model, OSI, 11
Rekhter, Y., 19, 35, 49, 51, 137–138, 140–141
reliable, 9, 20, 24, 124–125, 204, 208, 232, 283, 292–293, 302, 374, 416
remote access server, *see* RAS
remote variable, 148–149
Rescorla, E., 165, 167–168, 174, 185, 192, 430
Result code AVP, 121
result codes, StopCCN, 121
resumed session, SSL, 180–183
rexec program, 207
Reynold, J.K., 39
Rijndael, *see* AES
RIP, 50–51
Rivest, R., 70, 76, 78, 81, 84
rlogin program, 207
Robshaw, M., 59, 72
Romkey, J.L., 40
Roos, A., 60
rootcert.pem file, 198
Rosen, E.C., 137–138, 140–141
round trip time, *see* RTT
round keys, 62
route program, 103
routing, 4, 6, 9–10, 14, 16–19, 43–44, 46–55, 93, 135–144, 151, 156, 163, 283, 288, 313, 333, 353, 398
RSA, 6, 70–73, 81, 87–88, 176–177, 188, 212, 214, 217, 237, 242, 244–245, 266, 277, 280, 286–287, 291, 381, 383, 407, 421
  Laboratories, 72, 81
rsh program, 207–209, 227
RST flag, definition of, 27
RTT (round trip time), 29
Rubens, A., 113, 134
Rx connect speed, definition of, 127

s_client program, 192, 194–195
s_server program, 192
SA (security association), 309, 316–324, 327, 330–331, 341–342, 344–345, 347, 350, 355, 357–395, 398–401, 404–409, 414–417
  definition of, 309, 316–317
  proposal and transform payloads, 362–367
SAD (security association database), definition of, 317
S-box (substitution box), definition of, 64
SCCCN AVPs, 120
SCCRP AVPs, 120
SCCRQ AVPs, 119
Schertler, M., 357
Schiller, J.I., 177
Schneider, M., 357
Schneier, B., 57–58, 61–62, 65, 70, 72–73, 75, 81–82, 84, 87, 158, 204, 309, 313, 316–317, 324–325, 341, 344, 355–356
SCP (Secure Copy Program), 227–230
scp program, 227–228, 248, 258, 266
Secure Copy Program, *see* SCP
Secure Data Network System, *see* SP3
Secure Hash Algorithm, *see* SHA
Secure Shell, *see* SSH
Secure Sockets Layer, *see* SSL
security association, *see* SA
security association database, *see* SAD
security parameter index, *see* SPI
security policy database, *see* SPD
security association, 7, 309, 316–321, 324, 357, 363, 393
select function, 147, 149
send_char() program, 40
sendto function, 149
SEQ_LT, definition of, 112
SEQ_LT macro, 112
sequencing required, definition of, 128

Serial Line Protocol, *see* SLIP
server
  hello, SSL, 174–175
  key, SSH, 212
session
  key, definition of, 72
  key generation, SSHv2, 241
set link info message, *see* SLI
`setkey` program, 347, 389
`sftp` program, 258
`sh` program, 207
SHA (Secure Hash Algorithm), 76–83, 88, 134, 171, 231, 233, 235, 240–241, 278, 285–286, 291, 295, 301, 327, 336, 343, 353, 365, 370, 379, 381
Shamir, A., 60, 70, 81, 84, 324
Shea, R., 134, 162
`SHELL` variable, 227
shortest path, definition of, 51
signature, digital, 6, 80–83, 85, 87, 371, 376, 393–395, 401
Silverman, R.E., 214
Simone, D., 96
Simpson, W.A., 119, 313
Siverman, R.E., 221, 228
`sleep` function, 229
SLI (set link info message)
  AVPs, 133
  definition of, 132
SLIP (Serial Line Protocol), 40–41, 55
Smurf attack, 19
Snader, J.C., 5
Snader, M, xiv
Snader, R., xiv
`snoop` program, 429
`SOCK_RAW` socket option, 149
`SOCKADDR` macro, 148
`sockaddr` structure, 148
`sockaddr_in` structure, 148
soft state, 95, 323
`solaris` work station, 5, 28–30, 35
Solo, D., 85
Song, D.X., 260
SopCCN AVPs, 121
SP3 (Secure Data Network System), definition of, 307
Spam, 37
SPD (security policy database), 398–399
  definition of, 321
Speciner, M., 134
SPI (security parameter index), definition of, 317
Srisuresh, P., 40
SSH (Secure Shell), 7, 152, 162–163, 207–266, 268, 273, 286, 293, 297, 324, 328
  general authentication messages, 243
  port forwarding, 223–226
`ssh` program, 136, 207–210, 220, 224, 228, 230, 258, 262–263
SSH (Secure Shell)
  server key, 212
  VPN, 260–267
SSH_CMSG_PORT_FORWARD_REQUEST, definition of, 227
SSH_CMSG_REQUEST_PTY, definition of, 219
SSH_CMSG_SESSION_KEY, definition of, 214
SSH_CMSG_X11_REQUEST_FORWARDING, definition of, 221
SSH_MSG_CHANNEL_DATA, definition of, 222
SSH_MSG_CHANNEL_EXTENDED_DATA, definition of, 254
SSH_MSG_CHANNEL_OPEN, definition of, 251
SSH_MSG_CHANNEL_OPEN_CONFIRMATION, definition of, 222, 252
SSH_MSG_CHANNEL_OPEN_FAILURE, definition of, 253
SSH_MSG_CHANNEL_REQUEST, definition of, 254
SSH_MSG_GLOBAL_REQUEST, definition of, 251
SSH_MSG_KEXDH_GEX_REPLY, definition of, 239
SSH_MSG_KEXDH_REQUEST, definition of, 239
SSH_MSG_KEXINIT, definition of, 236
SSH_MSG_PORT_OPEN, definition of, 226
SSH_MSG_USERAUTH_FAILURE, definition of, 244
SSH_MSG_USERAUTH_INFO_REQUEST, definition of, 249
SSH_MSG_USERAUTH_INFO_RESPONSE, definition of, 250
SSH_MSG_USERAUTH_PASSWD_CHANGEREQ, definition of, 247

SSH_SMSG_PUBLIC_KEY, definition of, 213
sshd program, 207, 209, 212, 228, 259, 262–264
SSHv1, 208–231
  authentication, 210–220
  binary packet, definition of, 210
  message types, 211
  remote commands, 226–227
  security, 230–231
  user authentication, 214–220
SSHv2, 232–260
  authentication, 242–248
  binary packet, definition of, 234
  channel messages, 250
  connection protocol, 248–252
  data transfer, 252–253
  Diffie-Hellman key exchange, 238–240
  exchange hash, 240–241
  key generation, 241–242
  keyboard interactive authentication, 247–248
  none authentication, 244
  open failure reason codes, 253
  parameter negotiation, 234–238
  password authentication, 246–247
  port forwarding, 257–258
  public key authentication, 244–246
  public key signature data, 245
  remote commands, 253–256
  security, 259–260
  services, 242
  session key generation, 241
  subsystems, 258–259
  transport message types, 234
  transport protocol, 232–233
  user authentication request, definition of, 243
sshvpn, 262–265
  program, 261–264
SSL (Secure Sockets Layer), 7, 58, 80, 86–87, 156, 162–163, 165–205, 208–209, 212, 260–261, 271, 273, 277, 286, 291–294, 297–302, 324, 429–430, 433
  alert, 180
  alert message, definition of, 180
  alert message types, 181
  certificate, 175–176, 178, 180, 185–186, 188–189, 193, 195–198, 205
  certificate message, definition of, 176
  change cipher spec, 177–178
  cipher suite, 166–167
  cipher suite, definition of, 166
  cipher suites, 167
  client authentication, 185–188
  client cert. request, definition of, 188
  client hello, 173–174
  client hello, definition of, 173
  client key exchange, 176–177
  client key exchange message, definition of, 177
  closure notification, 180
  definition of, 165
  Diffie-Hellman key exchange, 188–191
  finished message, 178–180
  finished message, definition of, 178
  handshake header, definition of, 172
  handshake messages, 171–172
  handshake types, 172
  hello done, 176
  MasterSecret, definition of, 176
  PreMasterSecret, definition of, 176
  protocol, 167–171
  record format, definition of, 170
  record layer, 170–171
  record layer message types, 171
  resumed session, 180–183
  security, 204–205
  server hello, 174–175
  server hello, definition of, 175
  server hello done, definition of, 176
  server key exchange message, definition of, 190
  v2 client hello, 183–185
  v2 record-client hello, definition of, 184
  VPN, 265–266
SSL_accept function, 194
SSL_read function, 192, 194
SSL_set_bio function, 194
SSL_write function, 194
ssldump, 429–430
ssldump program, 165, 174–178, 187, 189, 199, 202, 428–430
sslecho program, 194–195, 198–199, 206
sslecho.pem file, 193
stack
  definition of, 10
  TCP/IP, 10
Staddon, J., 72, 231

`startup` function, 145, 147–148
static mode, definition of, 37
Stenberg, M., 397, 410
Stevens, W.R., xiv–v, 9, 27, 29, 200, 431
Stevenson, F.A., 60
StopCCN result codes, 121
stream cipher, 57–60, 87, 157, 163, 166, 171, 241, 324, 343, 345
`strerror` function, 423
strong collision resistance, definition of, 75
`stunnel`, 196–204
  program, 192, 196–202, 204–205, 208
`stunnel.` program, 223
`stunnel.client` file, 199
`stunnel.server` file, 198, 200
subaddress, definition of, 127
subnetting, 16
substitution box, *see* S-box
subsystems, SSHv2, 258–259
Swander, B., 397, 410–411
symmetric
  cipher, 6, 57–69, 72–73, 80
  encryption, 383–385
SYN flag, definition of, 27
synchronization segment, *see* SYN
synchronization segment, definition of, 28
synchronous line, 41–42

Taarud, J., 109
tag, PPPoE, 97
Tappan, D., 137
`tar` program, 426
Tavares, S.E., 60
TCP (Transmission Control Protocol)
  data delivery, 25
  definition of, 26
  header, 25–28
  protocol, 24–31
  segment, definition of, 24
`tcp_client` function, 424
`tcp_server` function, 193, 424
`tcpdump` program, 3, 12, 28–30, 33–34, 54, 91, 99, 103, 115–116, 123, 151, 165, 170, 174, 179, 244, 308, 332, 335, 352, 355, 390, 393, 426–430
TCP/IP, 9–55
  stack, 10
`telnet` program, 7, 136, 207, 209, 266, 350–351, 425
testbed, 5–6
TFC (traffic flow confidentiality), definition of, 403
Thomas, B., 138
three-way handshake, 28–29
Tian, X., 260
tie breaker, definition of, 119
time to live, *see* TTL
tinc, 7, 163, 267, 283–292, 296, 302
  binary packet, definition of, 285
  binary protocol, 284–286
  metaprotocol, 286–291
  metaprotocol message types, 287
  security, 291–292
TLS (Transport Layer Security), 165–206, 292–294, 298
  definition of, 166
`tohex` function, 420
Townsley, W.M., 113, 134
traces, network, 3
traffic flow confidentiality, *see* TFC
traffic
  analysis, definition of, 309
  selectors, 399–400
Traina, P., 101
transform IDs, IPsec, 366
Transmission Control Protocol, *see* TCP
transport
  adjacency, definition of, 318
  layer, 10–12, 20, 22, 47, 90, 92, 165, 168, 202, 208, 292, 314, 336
  layer, definition of, 10
Transport Layer Security, *see* TLS
transport
  message types, SSHv2, 234
  mode, 314–315
triple DES, *see* 3DES
TTL (time to live), 21–22, 31, 46, 95, 136–137, 350
`tun` device, 147, 149–150, 267–268, 429, 431, 433
`tun0` device, 261–262, 264
tunnel, 2, 9, 11, 40, 54, 89–152, 155–163, 165, 196–204, 208, 224, 228, 260–262, 264–265, 267–271, 273, 281–283, 286, 296–297, 302, 311, 315–316, 332–333, 346–347, 376, 389, 395, 399, 415, 426, 428, 431, 433
  definition of, 90

IP-in-IP, 92–95, 100–101, 141, 147–152, 262, 311, 315, 324, 336
mode, 315–316
MPLS, 139–144
tunneling, 3–8, 11, 40, 54
definition of, 90
`TUN/TAP` device, 145
`tun/tap` device, 267–268, 283, 429
Turner, J., 357
Tx connect speed, definition of, 127

UDP (User Datagram Protocol)
definition of, 10, 24
header, 23
protocol, 22–23
UNIX, 6, 32, 72, 165, 173, 191, 201, 207, 228, 422, 425, 428–429
unreliable, definition of, 20
unsolicited email, *see* SPAM
unsolicited downstream mode, definition of, 138
urandom device, definition of, 275
`urandom` device, 275
URG flag, definition of, 27
User Datagram Protocol, *see* UDP

Vaananen, P., 137
Valencia, A.J., 113, 134
van Oorschot, P.C., 57, 70–71, 79, 295
Vanstone, S.A., 57, 70–71, 295
Varadhan, K., 19
Varghese, G., 25
Vaudenay, S., 204
Verthein, W., 109
Viega, J., 192
virtual private network, *see* VPN
Viswanathan, A., 138
Vollbrecht, J.R., 407
Volpe, V., 397, 410–411
voluntary mode, definition of, 108
Voydock, V.L., 309
VPN (virtual private network), 3–9, 11, 54, 67, 73, 75, 84, 104, 109–110, 135–136, 141–144, 151, 155–163, 165, 199, 201–205, 208, 225, 260–266, 307–324, 328, 334, 348, 350, 355, 357–358, 383, 400, 406, 409, 415–416, 426, 428
definition of, 3
lightweight, 162–163, 267–303, 307, 309
MPLS, 141–144, 155–156
SSH, 260–267
SSL, 265–266
VTun, 7, 162–163, 267–272, 277, 283, 292, 302
authentication, 269–271
security, 271–272
tunnel parameter options, 270
`vtund` program, 267–269
Vuagnoux, M., 204

Wagner, D., 158, 165, 204, 260
Waissbein, A., 231
WAN error notify message, *see* WEN
Wang, X., 83
Weis, B., 363
WEN (WAN error notify message)
AVPs, 133
definition of, 132
WEP (wired equivalent privacy), definition of, 60
Wheeler, R., 96
Wilson, S., 84
wired equivalent privacy, *see* WEP
Wright, G., xiv
`write` function, 194
Wu, L., 137

X11 forwarding, 220–223, 226, 256–257, 266
X.509, 83
certificate, 84–86
certificate, definition of, 85

Yin, Y.L., 83
Ylönen, T., 227
Yu
Yu, H., 83
Yu, J., 19

zero length body message, *see* ZLB
Zheng, P., 87
ZLB message, definition of, 115
Zorn, G., 109, 113, 134, 157, 162