

Numerics

- 3 DES (triple Data Encryption Standard), 18
- 4-way handshake, 222
- 802 RM, 61
- 802.11-Security.com, 399

A

- AAA
 - MAC-based authentication, 116
 - servers, 6
 - shared-key authentication, 118
- access
 - attack objectives, 128
 - enterprise guest, 300–303
 - multigroup, 259
- access control, 157
 - EAP-FAST, 187
 - frame format, 189
 - functional entities, 188
 - message exchange, 191
 - EAP protocols
 - EAP-MD5, 170
 - EAP-OTP, 171
 - EAP-TLS, 171, 174
 - EAP-TTLS, 176
 - frames, 163–168
 - layered framework, 159–162
 - three-party model, 158
 - LEAP, 185
 - PEAP, 176
 - frame format, 177–179
 - message exchange, 180–182
- access points. *See* APs
- accounting, 114
 - RADIUS protocol, 47
 - TACACS+ protocol, 44
- Ack (acknowledge), 36
- addresses (IPv6), 53
- ad-hoc mode security, 155
- administrator authentication, 346
- admission control, 282–283
- adoption (IPv6), 54
- AES CBC-MAC mode, 217
- AES counter mode, 216
- AH (Authentication Header), 55
- AirJack, 139, 399
- AirMagnet, 400
- airport WLAN hotspot deployment example, 394–395
- Airsnarf, 399
- AirSnort, 149, 399
- algorithms
 - Diffie-Hellman, 19, 30–31
 - encryption strengths/weaknesses, 23
 - MIC, 196
 - Michael algorithm, 204–205
- antennae, 6
- applications
 - MAC-based authentication, 116
 - open authentication, 114
 - shared-key authentication, 118
 - WLAN design considerations, 258
- APs (access points), 6–7, 14, 81
 - configuration for load balancing and failover, 294
 - rogue, 154
 - detecting, 287–291
 - SWAN, 243
 - WLAN design considerations, 258
- ArcFour algorithm, 402
- asymmetric encryption, 19–20
- attack trees, 126–127
 - access, 128
 - DoS, 128
- attacks, 288
 - asymmetric encryption, 22
 - authentication, 140
 - brute-force attacks, 23
 - DoS, 128, 138
 - disassociation and deauthentication, 139
 - transmit duration, 140
 - inductive attacks, 144
 - key recovery attacks, 146
 - dictionary-based, 146
 - EAP protocols, 150–153
 - Fuhrer-Mantin-Shamir attack, 147–149
 - keystream recovery, 142

attacks (*continued*)
 man-in-the-middle, 26
 objectives, 126
 access, 128
 attack trees, 126–128
 reaction attacks, 143–144
 reconnaissance, 127, 130
 sniffing, 130–132
 SSIDs, 130
 wardriving, 133–136
 reply attacks, preventing, 206
 rogue APs, 287

auditing, 114

authenticated data exchange, 22

authentication, 13, 34, 96–97
 administrator, 346
 attacks, 40
 CAs (certificate authorities), 32
 digital certificates, 31
 EAP protocols, 157
 EAP-MD5, 170
 EAP-OTP, 171
 EAP-TLS, 171, 174
 EAP-TTLS, 176
 frames, 163–168
 layered framework, 159–162
 three-party model, 158
 EAP-FAST, 187
 frame format, 189
 functional entities, 188
 message exchange, 191
 Kerberos, 48–49
 LEAP, 185
 MAC-based, 115–116
 mechanics, 111
 open, 113–114
 PEAP
 frame format, 177–179
 message exchange, 180–182
 PEAP, 176
 PPP, 34–35
 CHAP, 38
 EAP, 40–42
 link layer, 35
 negotiations, 35
 private key algorithms, 21
 RA, 45

 RADIUS protocol, 46
 shared-key, 116–118
 SWAN infrastructure authentication, 240
 TACACS+ protocol, 42–43
 WLAN design fundamentals, 257

Authentication Header (AH), 55

authentication servers, 48

authenticators, 40, 159

authorization, 13
 RADIUS, 46
 TACACS+ protocol, 43

availability, 13

B

BBSM (Building Broadband Service Manager), 374

beacon frames, 94

Bernard Aboba's "Unofficial 802.11 Security Web Page," 399

birthday paradox, 143

bridges, 6

brute-force attacks, 23

BSD UNIX, reconnaissance attacks, 137

bsd-airtools, 136, 399

BSS (Basic Service Set), 81

bug lightning, 288

Building Broadband Service Manager (BBSM), 374

C

Catalyst 6500 Wireless LAN Services Module, 310

CCK (Complementary Code Keying), 70

CCKM (Cisco Centralized Key Management), 246, 249

CCM algorithm, 215

CCMP, 196
 CCM algorithm, 215
 decapsulation, 214
 encapsulation, 212–213
 overview, 211

CCX (Cisco Client Extensions), 5, 309

central switching deployment mode (SWAN), 348–352

certificate authorities, 31

certificates, 31–32

CHAP (Challenge-Handshake Authentication Protocol), 37

- compatibility, 40
- EAP-MD5, 170
- vulnerabilities, 40

choreography. *See* exchanges

Cisco Aironet 802.11b/a/g, 309

Cisco Aironet AP350 AP, 308

Cisco Aironet AP1100 AP, 308

Cisco Aironet AP1200 AP, 308

Cisco Aironet BR350 AP, 309

Cisco Aironet BR1410 AP, 309

Cisco Client Extensions (CCX), 309

Cisco Compatible Extensions (CCX), 5

Cisco protocols, 226

Cisco Secure ACS, 310

Cisco Trust Agent (CTA), 283

Cisco Centralized Key Management (CCKM), 246, 249

Cisco Structured Wireless Aware Network.

- See* SWAN

Cisco Wireless LAN Solution Engine (WLSE), 310

CKIP (Cisco Key Integrity Protocol), 195, 246

client adapters, 6–7

clients, WLAN design recommendations, 260

coffee shop WLAN hotspot deployment example, 391–394

collisions, 143

communication, 48

compatibility (CHAP), 40

Complementary Code Keying (CCK), 70

Compound Session Key (CSK), 182

confidential messages, 24

confidentiality, 13–15

- CCMP, 212–213
- digital signatures, 29
- public key algorithms, 19–22
- symmetric key encryption, 16–17

configuring

- MAC address authentication, 316
- WLAN security
 - bridge-to-bridge links, 344–345
 - HTML GUI configuration pages, 311–312
 - IOS CLI configuration, 313–320, 324, 329–335
 - management configuration, 346–347

coverage areas, 81

creating digital signatures, 26

cryptography, 31

- asymmetric encryption, 19–20
- digital signatures, 26, 29
 - creating, 27
 - verifying, 28
- hash functions, 24–26
- keys
 - CAs (certificate authorities), 32
 - public, 31
 - resources, 400
 - symmetric encryption, 18–19

CSK (Compound Session Key), 182

CTA (Cisco Trust Agent), 283

cypher text, 22

D

data, 19

- frames, 104
- integrity, 20–22
- WEP, 121

Data Encryption Standard (DES), 19, 48

deauthentication, 99

deauthentication attacks, 139

decapsulation

- CCMP, 214
- TKIP, 211
- WEP, 202

decrypting

- cypher text, 22
- Kerberos, 51
- recovered keystreams, 146
- WEP, 123

demilitarized zones (DMZs), 114

deploying

- IPSec VPN over WLAN, 331
- SWAN central switching deployment mode, 281, 348–352
- SWAN nonswitching deployment mode, 336
 - fast secure roaming (CCKM) configuration, 337–339
 - local authentication configuration (RADIUS fall-back service), 343
 - RF aggregation configuration, 340–342
 - WDS configuration, 337–343

deploying (*continued*)

WLANs, 235

- embedded security solutions, 261–264
- financial WLAN examples, 376–379
- healthcare WLAN examples, 379–384
- integration with existing systems, 275–280
- large enterprise examples, 355–356, 358–364
- manufacturing WLAN examples, 386–388
- medium enterprise WLAN deployment example, 389
- security features, 239
- small office WLAN deployment example, 390
- SOHO WLAN deployment example, 391
- SWAN central switching deployment mode, 238
- SWAN nonswitching deployment mode, 235
- university example, 373–375
- vertical market examples, 365–371
- VPN overlays, 265–270

DES (Data Encryption Standard), 19, 48

designing

SWAN central switch design considerations, 281

WLANs

- admission control, 282–283
- AP management, 258
- AP recommendations, 259–260
- application support, 258
- authentication support, 257
- client recommendations, 260
- combined VPN/embedded security design, 271–274
- device support, 256
- embedded security solutions, 262–264
- fundamentals, 255
- infrastructure recommendations, 260
- integration with existing systems, 275–280
- mobility, 257
- multigroup access, 259
- network services placement, 257
- new deployments, 261
- radio coverage, 258
- security policies, 256
- VPN overlays, 265–270

DFS (Dynamic Frequency Selection), 62, 76

dictionary-based attacks, 146

LEAP, 151

Diffie-Hellman algorithm, 19, 30–31

digital certificates, 31–32

Digital Signature Standard (DSS), 29

digital signatures, 13, 26–29

confidentiality, 29

verifying, 28

disassociation attacks, 139

disassociations frames, 102

distributing public keys, 31

distribution service (DS), 82

DMZs (demilitarized zones), 114

DoS (denial-of-service) attacks, 128, 138

disassociation and authentication, 139

IEEE 802.11i, 227

transmit duration, 140

DS (distribution service), 82

DSS (Digital Signature Standard), 29

Dynamic Frequency Selection (DFS), 62, 76

E

EAP (Extensible Authentication Protocol), 40, 163

802.1x, 150

attacks, 150

dictionary attacks, 151

PEAP man-in-the-middle attacks, 153

authentication mechanisms

EAP-MD5, 170

EAP-OTP, 171

EAP-TLS, 171, 174

EAP-TTLS, 176

flexibility, 42

frames, 163

request/response, 165

success/failure, 167–168

LEAP. *See* LEAP

packet types assigned by IANA, 166–167

security, 229

Tunneled EAP (TEAP), 187

vulnerabilities, 176

with dynamic WEP configuration, 317–319

EAP over LAN protocol. *See* EAPOL

- EAP-FAST, 187
 - client configuration, 320
 - frame format, 189
 - functional entities, 188
 - message exchange, 191
 - with WPA client configuration, 326
 - EAP-GTC, 171
 - EAPOL (EAP over LAN protocol), 183–185
 - master key establishment, 218
 - EAPOL Key Confirmation Key (KCK), 220
 - EAPOL Key Encryption Key (KEK), 220
 - EAP-OTP, 171
 - EAP-TLS, 171, 174
 - client configuration, 322
 - EAP-TTLS, 176
 - ECP chaining mechanism, 17
 - e-dictation, 381
 - embedded security
 - central switch design, 281
 - combined with VPN overlay security solutions, 271–274
 - design fundamentals, 264
 - threat mitigation, 262
 - EMSK (Extended Master Session Key), 182
 - Encapsulating Security Payload (ESP), 55
 - encapsulation
 - CCMP, 212–213
 - TKIP, 210
 - WEP, 200–201
 - encryption, 14, 52
 - algorithms, 23
 - asymmetric encryption, 19–20
 - digital signatures, 26–29
 - hash functions, 24–26
 - private key, 20
 - symmetric encryption, 18–19
 - symmetric key encryption, 15
 - encryption protocols
 - CCMP, 211
 - CCM algorithm, 215
 - decapsulation, 214
 - encapsulation, 212–213
 - TKIP
 - decapsulation, 211
 - encapsulation, 210
 - key mixing algorithm, 207
 - Michael MIC, 204–205
 - overview, 203
 - packet construction, 209
 - preventing reply attacks, 206
 - WEP, 197–198
 - decapsulation, 202
 - encapsulation, 200–201
 - RC4, 198–199
 - enterprise guest access, 300–303
 - ERO (European Radiocommunications Office), 76
 - ESP (Encapsulating Security Payload), 55
 - Ethereal, 132, 399
 - ETSI (European Standard Organizations and Regulations), 77
 - European Radiocommunications Office (ERO), 76
 - exchanges
 - association frames, 100–102
 - authentication, 96–97
 - data frames, 104
 - deauthentication, 99
 - disassociation frames, 102
 - reassociation frames, 102
 - exclusive OR (XOR), 202
 - Extended Master Session Key (EMSK), 182
 - Extensible Authentication Protocol. *See* EAP
- ## F
-
- failover (AP configuration), 294
 - fakeap, 400
 - fast secure roaming (CCKM), 338–339
 - FCC regulations, 67
 - FCS (frame check sequence), 198
 - financial WLAN deployment examples, 376–379
 - Fluhrer-Mantin-Shamir attack, 147
 - FMS (Fluhrer-Mantin-Shamir) attack, 147, 228
 - frame check sequence (FCS), 198
 - frame types
 - CHAP (Challenge-Handshake Authentication Protocol), 38
 - PAP (Password Authentication Protocol), 35
 - frames, 89
 - association frames, 100–102
 - beacon frames, 94
 - data frames, 104
 - deauthentication frames, 99
 - disassociation frames, 102

frames (*continued*)
EAP, 163
 request/response, 165
 success/failure frames, 167–168
EAP-FAST, 189
FCS, 198
MAC frame, 90
management, 90
PEAP, 177–179
probe request frames, 95
probe response frames, 95
reassociation frames, 102
functions (hash functions), 24–26

G

GMK (Group Master Key), 218
Goonda.com, 399
group key handshake, 223
group key hierarchy, 221
Group Master Key (GMK), 218
GTKSA (Group Transient Key Security Association), 225
guest services (large enterprise WLAN deployment), 360

H

handshakes (CHAP), 37
hash functions, 24–26
headers
 AH (Authentication Header), 55
 ESP (Encapsulating Security Payload), 55
healthcare WLAN deployment examples, 379–384
hotspot WLAN deployment examples, 391–395
HTML GUI configuration pages, 312

I–J

IANA (Internet Assigned Numbers Authority), 166–167
IAPP (Inter-Access Point Protocol), 73

iBSS (independent basic service set)
 mode, 83
 network configuration, 289
ICV (Integrity Check Vector), 143, 198
IDEA (International Data Encryption Algorithm), 19
identity protocols, 34
IEEE (Institute of Electrical and Electronic Engineers), 60
 802 standard, 60–63
 online resources, 401
IEEE 802.11, 69, 84
 authentication, 111
 compared to WPA, 66
 services, 88
IEEE 802.11a, 70–71
IEEE 802.11b, 70
IEEE 802.11e, 73–75
IEEE 802.11f, 73
IEEE 802.11h, 76–78
IEEE 802.11i, 195–196
 CCMP, 211
 CCM algorithm, 215
 decapsulation, 214
 encapsulation, 212–213
 development, 225
 dictionary-based WEP key recovery, 228
 key management, 217
 key exchange, 222–223
 key hierarchy, 218–221
 master key establishment, 218
 security associations (SAs), 224–225
 message modification and replay, 228
 rogue APs, 229
 security problems addressed, 227
TKIP, 203
 decapsulation, 211
 encapsulation, 210
 key mixing algorithm, 207
 Michael MIC, 204–205
 packet construction, 209
 preventing reply attacks, 206
WEP, 197–198
 decapsulation, 202
 encapsulation, 200–201
 RC4, 198–199
 WEP keystream recovery, 228
IEEE 802.11k, 75

IEEE 802.1x
 EAPOL, 184–185
 overview, 183

IETF, 402

IKE (Internet Key Exchange), 56

IKMP (Internet Key Management Protocol), 56

independent basic service set (iBSS)
 mode, 83
 network configuration, 289

indexes (SPI), 55

inductive attacks, 144

initialization vectors. *See* IVs

Institute of Electrical and Electronic Engineers.
See IEEE

integrating WLAN deployments, 275–280, 357

integrity, 13, 24–26
 CCMP, 212–213
 ICV, 143, 198
 public key algorithms, 19–22
 WEP, 121

Inter-Access Point Protocol (IAPP), 73

International Data Encryption Algorithm (IDEA), 19

Internet Assigned Numbers Authority (IANA), 166–167

Internet Key Exchange (IKE), 56

Internet Key Management Protocol (IKMP), 56

intrusion detection (SWAN), 243

IOS CLI configuration, 313–320
 IPSec VPN over WLAN configuration, 329–331
 multiple security profiles configuration, 332–335
 WPA-DOT1x configuration, 324

IP, 55

IPng (IP: The Next Generation), 52

IPSec, 54
 authentication header (AH), 55
 external load balancers, 299
 key management, 56

IPSec VPN clustering, 296–297

IPSec VPN over WLAN configuration, 329–331

IPSec VPNs, 267

IPv6, 52
 address structure and representation, 53
 headers, 53
 scalability, 54

ISPs, 47

IV (initialization vectors), 17, 143, 197
 generating (WEP), 122
 inductive attacks, 144
 traffic injection, 145

K

KCK (EAPOL Key Confirmation Key), 220

KDC (key distribution center), 48–50

KEK (EAPOL Key Encryption Key), 220

Kerberos
 authentication, 48–49
 replies, 51
 requests, 51

key exchange, 222
 4-way handshake, 222
 group key handshake, 223

key management, 15, 29, 217

IPSec, 56
 key exchange, 222–223
 key hierarchy, 218
 CCKM, 249
 group key hierarchy, 221
 Pairwise key hierarchy, 220
 master key establishment (EAPOL), 218
 PEAP, 182

key mixing algorithm (TKIP), 207

key pairs, 23

key recovery attacks, 146
 dictionary-based, 146
 EAP protocols, 150–153
 Fluhrer-Mantin-Shamir attack, 147–149

Key Scheduling Algorithm (KSA), 147, 199

keylength (WEP), 121

keys
 CAs (certificate authorities), 32
 cryptography, 31
 digital certificates, 31
 hierarchy, 218–220, 249
 key management. *See* key management
 secret keys, 30
 WEP, 197

keyspace, 23

- keystream recovery
 - keystream dictionaries, 141
 - RC4, 142
 - reaction attacks, 143
 - uses for recovered keystreams, 145
- KisMAC, 399
- Kismet, 135, 399
- KSA (Key Scheduling Algorithm), 147, 199

L

- LAN/MAN RM (Reference Model), 60
- LAN/MAN standards, 60
- large enterprise WLAN deployment, 355–356
 - AAA and external user database infrastructure implementation, 358–359
 - deployment challenges, 364
 - security deployment, 363
 - security details, 356
 - VoIP and guest services, 360
 - wired/wireless LAN integration, 357
- layered framework for authentication, 159–162
- LEAP, 185
 - client configuration, 319
 - dictionary-based attacks, 151
 - EAP-FAST. *See* EAP-FAST
- legacy devices/systems, 276
- Libradiate, 399
- Light Weight Access Point Protocol (LWAPP), 79
- link layer (PPP), 35
- Linux reconnaissance attacks, 137
- LLC (Logical Link Control), 61
- load balancing
 - AP configuration, 294
 - IPSec external load balancers, 299
 - IPSec VPN clustering, 297
 - RADIUS, 292
 - site-based VPN, 296
 - SSL external load balancers, 299
- local authentication configuration (RADIUS fall-back service), 343
- Logical Link Control (LLC), 61
- LOGIN port (TACACS protocol), 42
- LWAPP (Light Weight Access Point Protocol), 79

M

- MAC address authentication, configuring, 316
- MAC address spoofing, 141, 227
- MAC frame, 90
- MAC Protocol Data Unit (MPDU) 184, 203
- MAC Service Data Unit (MSDU), 203
- MAC-based authentication, 115–116
- MacStumbler, 135, 399
- management frames, 90
- man-in-the-middle attacks, 26, 153
- manual rogue AP detection, 289
- manufacturing WLAN deployment examples, 386–388
- master keys, 218
- Master Session Key (MSK), 182
- medium enterprise WLAN deployment example, 389
- message digest, 24
- messages
 - authentication, 113
 - exchanges, 93
 - EAP-FAST, 188, 191
 - LEAP, 185
 - PEAP, 180–182
 - TLS, 172
- MIC (Message Integrity Check) algorithm, 196
- Michael algorithm, 204–205
- Michael MIC, 204–205
- Mini Stumbler, 134
- mobility, WLAN design considerations, 257
- monkey_jack, 139, 399
- MPDU (MAC Protocol Data Unit), 184, 203
- MSDU (MAC Service Data Unit), 203
- MSK (Master Session Key), 182
- multiple security profiles (SSIDs/VLANs), 332–335

N

- NAD (network access device), 283
- Nak (negative acknowledge), 36
- negotiations (PPP), 35
- Network Stumbler, 134, 400
- network-based rogue AP detection, 291
- networks
 - Robust Security Network, 196
 - wireless. *See* wireless networks
- NICs, 6

NMS (network management servers), 6
 nonswitching deployment mode (SWAN), 336
 fast secure roaming (CCKM) configuration, 337–339
 local authentication configuration, 343
 RF aggregation configuration, 340–342
 WDS configuration, 337–343

O

Omerta, 139, 400
 open authentication, 113–114
 open authentication guest VLAN, 301
 open/no WEP configuration, 313
 open/with WEP (static WEP) configuration, 313

P–Q

PAC TLV frame format (EAP-FAST), 189
 packets
 EAP packet types assigned by IANA, 166–167
 PAP, 36
 TKIP, 209
 Pairwise key hierarchy, 220
 Pairwise Master Key (PMK), 218
 Pairwise Master Key Security Association (PMKSA), 225
 Pairwise Transient Key (PTK), 220
 Pairwise Transient Key Security Association (PTKSA), 225
 PAP (Password Authentication Protocol), 35–37
 passwords, 34–35
 PEAP (Protected EAP), 64
 arbitrary parameter exchange, 178
 client configuration, 320
 configuration on a third-party EAP supplicant, 322
 frames, 177–179
 key management, 182
 man-in-the-middle attacks, 153
 message exchange, 180, 182
 plaintext attacks, 142
 PLCP (Physical Layer Convergence Protocol), 70
 PMK (Pairwise Master Key), 218

PMKSA (Pairwise Master Key Security Association), 225
 PPDU (PLCP Protocol Data Unit), 70
 PPP (Point-to-Point Protocol), 34
 link layer, 35
 negotiations, 35
 online resources, 402
 Preshared Key (PSK), 218
 pre-WeP devices, 275
 PRGA (Pseudorandom Generation Algorithm), 199
 Prismdump, 132, 400
 privacy, 119–122
 private key encryption, 20
 probe request frames, 95
 probe response frames, 95
 processing WEP, 120–122
 Protected EAP (PEAP), 64
 protocols
 CHAP, compatibility, 40
 Cisco, 226
 IKE (Internet Key Exchange), 56
 IPSec, 54–55
 IPv6, 52
 address structure and representation, 53
 headers, 53
 scalability, 54
 Kerberos
 authentication, 48–49
 replies, 51
 requests, 51
 PPP, 34
 CHAP, 38
 EAP, 40–42
 link layer, 35
 negotiations, 35
 PAP, 35–36
 RADIUS (Remote Address Dial-In User Service), 45
 accounting, 47
 authentication, 46
 authorization, 46
 transactions, 47
 shared-key authentication, 117
 TACACS+, 42
 accounting, 44
 authentication, 43
 authorization, 43

- transactions, 44
- Pseudorandom Generation Algorithm (PRGA), 199
- PSK (Preshared Key), 218
- PSPF (Public Secure Packet Forwarding), 347
- PTK (Pairwise Transient Key), 220
- PTKSA (Pairwise Transient Key Security Association), 225
- public keys
 - creating, 31
 - distributing, 31
 - encryption, 22
- Public Secure Packet Forwarding (PSPF), 347
- public WAN deployment examples, 391–395
- public WLAN (PWLAN), 85

R

- radio coverage design, 258
- radio management
 - enabling on a Cisco client, 342
 - SWAN, 242–243
- Radio Manager Assisted Site-Survey wizard, 341
- radio technologies in, 802.11, 68
- RADIUS (Remote Address Dial-In User Service)
 - protocol, 45–46
 - accounting, 47
 - authentication, 46
 - authorization, 46
 - best practices, 292–293
 - EAP parameter configuration on RADIUS server, 323
 - Local authentication configuration (RADIUS fallback service), 343
 - server load balancing, 292
 - SWAN, 250
 - transactions, 47
- RC4 (Rivest Cipher 4), 19, 198
 - history of, 121
 - keystream dictionaries, 141
 - keystream recovery, 142
 - KSA, 147
 - two phases, 121
- reaction attacks, 143
- reason codes, 104–105
- reconnaissance, 127
- reconnaissance attacks, 130
 - sniffing, 130–132
 - SSIDs, 130
 - wardriving, 133–136
- refresh number (RN), 248
- Remote Address Dial-In User Service. *See* RADIUS
- removing certificates, 32
- replies (Kerberos protocol), 51
- reply attacks, preventing, 206
- REPLY message, 43
- reply packets (PAP), 36
- request packets (PAP), 36
- request/response frames (EAP), 165
- requests (Kerberos protocol), 51
- resolves, 21
- response, 40
- retail WLAN deployment
 - example 1, 366
 - challenges, 370
 - security, 367
 - WDS and AAA infrastructure, 369
 - example 2, 371
- revoking certificates, 32
- RF aggregation configuration, 340–342
- Rivest Cipher 4 (RC4), 19
- RN (refresh number), 248
- Robust Security Network, 196
- rogue APs, 154
 - detecting, 287
 - manually, 289
 - network-based, 291
 - SWAN, 288–289
 - IEEE 802.11i, 229
 - SWAN, 243
- routers, wireless aware, 6

S

- SAs (security associations), 55, 224–225
- scalability
 - IPv6, 54
 - RADIUS best practices, 292–293

- VPN best practices, 296–299
- security, 8, 13
 - access control, 157
 - EAP frames, 163–168
 - EAP-FAST, 187–191
 - EAP-MD5, 170
 - EAP-OTP, 171
 - EAP-TLS, 171, 174
 - EAP-TTLS, 176
 - layered framework, 159–162
 - LEAP, 185
 - PEAP, 176–180, 182
 - three-party model, 158
 - accounting, 44
 - ad-hoc mode, 155
 - attacks
 - access, 128
 - authentication, 140
 - DoS, 128, 138–140
 - key recovery attacks, 146–153
 - objectives, 126–128
 - reaction attacks, 143
 - reconnaissance, 127, 130–136
 - authentication
 - Kerberos, 48–49
 - MAC-based, 115–116
 - mechanics, 111
 - open, 113–114
 - PAP, 35–36
 - PPP, 35
 - shared-key, 116–118
 - TACACS, 42
 - TACACS+ protocol, 42
 - authorization, 43
 - bridge-to-bridge links, 344–345
 - brute-force attacks, 23
 - CAs (certificate authorities), 32
 - confidentiality, 15–17
 - configuring, 307
 - cryptography
 - asymmetric encryption, 19–20
 - digital signatures, 26–29
 - hash functions, 24–26
 - symmetric encryption, 18–19
 - digital certificates, 31
 - digital signatures, 13
 - EAP, 229
 - embedded security solutions
 - design fundamentals, 264
 - threat mitigation, 262
 - encryption, 14
 - HTML GUI configuration pages, 311–312
 - IOS CLI configuration, 313–320
 - IPSec VPN over VLAN configuration, 329–331
 - multiple security profiles configuration, 332–335
 - WPA-DOT1x configuration, 324
 - Kerberos protocol, 51
 - key management, 29, 217
 - key exchange, 222–223
 - key hierarchy, 218–220
 - master key establishment, 218
 - SAs, 224–225
 - protocols, 38
 - retail WLAN deployment, 367
 - rogue APs, 154, 287–291
 - SWAN, 233–234
 - 802.11x RADIUS authentication service, 250
 - fast secure roaming, 246
 - infrastructure authentication, 240
 - radio management, 242–243
 - rogue APs, 243
 - WLAN deployment, 239
 - threat mitigation
 - combined VPN/embedded security design, 273
 - integration with legacy devices, 278–279
 - VPN overlays, 265
 - design fundamentals, 270
 - technologies, 267–269
 - threat mitigation, 266
 - WEP, 123
 - key recovery attacks, 146–153
 - keystream and plaintext recovery, 141, 143–145
 - WLAN design concerns
 - AP recommendations, 259–260
 - client recommendations, 260
 - infrastructure recommendations, 260

- WLAN management configuration, 346–347
- WLANs standards, 65
- security associations. *See* SAs
- security domain conceptual model, 8
- security parameter index (SPI), 55
- security policies (WLAN design), 256
- Security Wizards, 400
- seeds (WEP), 121, 197
- sender authentication, 22
- Service Set Identifier (SSID), 114
- services, 87
 - IEEE 802.11, 88
 - state transitions, 92
- shared-key authentication, 116–118
- shared-key authentication attacks, 140, 227
- sign, 29
- signatures, digital, 26–28
- site-based VPN load balancing, 296
- small office WLAN deployment example, 390
- Sniffer Wireless, 400
- sniffing, 130–132
- SOA (services-oriented architecture) paradigms, 53
- SOHO (small office, home office), 389
- SOHO WLAN deployment example, 391
- SPI (security parameter index), 55
- spoofing
 - IEEE 802.11i, 227
 - MAC addresses, 141
- SSH, 269
- SSID (Service Set Identifier), 114, 130, 287
- SSL, 269
- SSL external load balancing, 299
- STA (station), 7, 81
- standards
 - ERO, 76
 - ETSI, 77
 - FCC regulations, 67
 - IEEE 802, 60
 - IEEE 802.11, 69
 - IEEE 802.11a, 70–71
 - IEEE 802.11b, 70
 - channel allocation, 70
 - IEEE 802.11e, 73–75
 - IEEE 802.11f, 73
 - IEEE 802.11h, 76–78
 - IEEE 802.11k, 75
 - LAN/MAN, 60
 - layered framework for authentication, 160–162

- WLANs, 7, 59, 62–63
- WPA, 65
- START message, 43
- state diagrams, 91–93
- state transitions, 92
- static WEP configuration, 313
- status codes, 106–107
- stickiness, 293
- Structured Wireless Aware Network. *See* SWAN
- success/failure frames (EAP), 167–168
- suplicants, 159
 - third-party, 322
- SWAN (Cisco Structured Wireless Aware Network), 4, 233
 - 802.11x RADIUS authentication service, 250
 - central switching deployment, 281, 348–352
 - fast secure roaming, 246
 - infrastructure authentication, 240
 - nonswitching deployment, 336–343
 - radio management, 242–243
 - rogue AP detection, 243, 288–289
 - security, 233–234
 - WLAN deployment, 235
 - central switching deployment mode, 238
 - nonswitching deployment mode, 235
 - security features, 239
- switches (wireless aware), 6
- symmetric encryption, 18–19
- symmetric key encryption, 15–17

T

- TACACS, administrator authentication, 346
- TACACS+ protocol, 42
 - accounting, 44
 - authentication, 43
 - authorization, 43
 - transactions, 44
- Task Group i (TGi), 195
- tcpdump, 132, 400
- TEAP (Tunneled EAP), 187
- TEK (Temporal Encryption Key), 207
- Temporal Encryption Key (TEK), 207
- Temporal Key (TK), 220

TGi (Task Group i), 195
 third-party supplicants, 322
 threat mitigation

- combined VPN/embedded security design, 273
- integration with legacy devices, 278–279
- VPN overlays, 266

 three-party model, 158
 three-way handshakes (CHAP), 37
 timing, 37
 TK (Temporal Key), 220
 TKIP

- decapsulation, 211
- encapsulation, 210
- key mixing algorithm, 207
- Michael MIC, 204–205
- overview, 203
- packet construction, 209
- preventing reply attacks, 206

 TKIP Sequence Counter (TSC), 206
 TLS (Transport Level Security), 64, 172

- EAP-TLS, 174
- EAP-TTLS, 176

 TLV frame format (PEAP), 178
 TPC (Transmit Power Control), 62, 76
 traffic injection, 145
 transactions

- RADIUS protocol, 47
- TACACS+ protocol, 44

 Transmit Power Control (TPC), 62, 76
 trees. *See* attack trees
 troubleshooting

- rogue APs, 287
 - manually, 289
 - network-based, 291
 - SWAN, 288–289
- WDS server configuration, 337

 trust model (open authentication), 114
 TSC (TKIP Sequence Counter), 206
 Tunneled EAP (TEAP), 187

U–V

university WLAN deployment example, 373–375

upgrading, integrating design with existing WLAN deployments, 275
 vertical market WLAN deployment, 365

- financial WLAN deployment examples, 376–379
- healthcare WLAN deployment examples, 379–384
- manufacturing WLAN deployment examples, 386–388
- retail WLAN example 1, 366
 - challenges, 370
 - security, 367
 - WDS and AAA infrastructure, 369
 - retail WLAN example 2, 371
 - university WLAN deployment example, 373–375

 void11, 139, 400
 VoIP (Voice over IP), large enterprise WLAN deployment, 360
 VPNs (virtual private networks)

- IPSec, 54
 - overlays, 265
 - best practices, 296–299
 - central switch design, 281
 - combined with embedded security design, 271–274
 - design fundamentals, 270
 - technologies, 267–269
 - threat mitigation, 266

 vulnerabilities

- EAP, 176
- MAC-based authentication, 116
- open authentication, 114
- shared-key authentication, 118
- WEP, 123
- wireless networks, 125

W

WarBSD, 137, 400
 wardriving, 133–136
 WarLinux, 137, 400
 WDS (Wireless Domain Services), 289
 websites

- cryptography and cryptoanalysis, 401

- general tools, 399–400
- IEEE resources, 401
- websites (*continued*)
 - IETF resources, 402
 - WiFi Alliance, 226, 401
- Wellenreiter, 135, 400
- WEP (Wired Equivalent Privacy), 18, 65, 108–109, 197–198
 - CCMP, 211
 - CCM algorithm, 215
 - decapsulation, 214
 - encapsulation, 212–213
 - decapsulation, 202
 - encapsulation, 200–201
 - ICV, 143
 - IEEE 802.11i, 195–196
 - IVs, 24
 - keys, 197
 - key management, 122
 - key recovery attacks, 146
 - dictionary-based, 146
 - EAP protocols, 150–153
 - Fluhrer-Mantin-Shamir attack, 147–149
 - keystream and plaintext recovery, 141–143
 - uses for recovered keystreams, 145
 - pre-WEP devices, 275
 - privacy mechanics, 119
 - processing model, 120–122
 - RC4, 199
 - seed, 197
 - TKIP, 203
 - decapsulation, 211
 - encapsulation, 210
 - key mixing algorithm, 207
 - Michael MIC, 204–205
 - packet construction, 209
 - preventing reply attacks, 206
 - vulnerabilities, 123
 - WEP-only devices, 275
- wep_crack and wep_decrypt, 400
- WEPCrack, 149, 400
- WGBs (workgroup bridges), 6
- Wi-Fi Alliance, 65
 - websites, 226, 401
- Wi-Fi Protected Access. *See* WPA
- wireless-aware routers, 6
- wireless-aware switches, 6
- Wireless Domain Services (WDS), 289
- Wireless LAN Association (WLANA), 67
- Wireless LAN Services Module (WLSM), 4, 303
- Wireless LAN Solution Engine (WLSE), 357
- wireless LANs. *See* WLANs
- wireless networks
 - security
 - ad-hoc mode, 155
 - authentication attacks, 140
 - DoS attacks, 138
 - disassociation and deauthentication, 139
 - transmit duration, 140
 - reconnaissance attacks, 130–136
 - rogue APs, 154
 - supplicants, 159
 - vulnerabilities, 125
- wireless service provider (WSP), 82
- WLANA (Wireless LAN Association), 67
- WLANs (wireless LANs), 3
 - authentication, 96–97
 - basic topology, 84
- Cisco Enterprise class, 307–308
 - Catalyst 6500 Wireless LAN Services Module, 310
 - Cisco Aironet 802.22b/a/g, 309
 - Cisco Aironet AP350 AP, 308
 - Cisco Aironet AP1100 AP, 308
 - Cisco Aironet AP1200 AP, 308
 - Cisco Aironet BR350 AP, 309
 - Cisco Aironet BR1410 AP, 309
 - Cisco Secure ACS, 310
 - WLSE, 310
- components, 6
- deauthentication, 99
- deploying
 - financial WLAN examples, 376–379
 - healthcare WLAN examples, 379–384
 - large enterprise examples, 355–364
 - manufacturing WLAN examples, 386–388
 - university example, 373–375
 - vertical market examples, 365–371
- deployment modes, 235
 - security features, 239
 - SWAN central switching deployment mode, 238
 - SWAN nonswitching deployment mode, 235
- designing

- admission control, 282–283
- AP management, 258
- AP recommendations, 259–260
- application support, 258
- authentication support, 257
- client recommendations, 260
- combined VPN/embedded security design, 271–274
- device support, 256
- embedded security solutions, 262–264
- infrastructure recommendations, 260
- mobility, 257
- multigroup access, 259
- network services placement, 257
- new deployments, 261
- radio coverage, 258
- security policies, 256
- VPN overlays, 265–270
- elements and characteristics, 81
- enterprise guest access, 300–303
- frames, 89, 102–104
 - associations frames, 100–102
 - beacon frames, 94
 - MAC frame, 90
 - management, 90
 - probe request frames, 95
 - probe response frames, 95
 - reassociations frames, 102
- integration with existing systems, 275–280
- limitations, 4
- medium enterprise deployment example, 389
- public, 85
- reason codes, 104–105
- security, 8
 - bridge-to-bridge links, 344–345
 - HTML GUI configuration pages, 311–312
 - IOS CLI configuration, 313–324, 329–335
 - management configuration, 346–347
 - standards, 64
 - security domain conceptual model, 8
 - services, 87
 - IEEE 802.11, 88
 - state transitions, 92
 - services scaling
 - RADIUS best practices, 292–293
 - VPN best practices, 296–299
 - small office deployment example, 390
 - SOHO deployment example, 391
 - standards, 7, 59, 62–63
 - state diagram, 91–93
 - status codes, 106–107
 - SWAN, 4
 - WEP, 108–109
- WLSE (Cisco Wireless LAN Solution Engine), 310, 357
- WLSM (Wireless LAN Services Module), 4, 303
- WPA (Wi-Fi Protected Access), 65, 226, 261
 - compared to IEEE 802.11, 66
 - WPA upgradeable devices, 275
- WPA-DOT1x configuration
 - debug information, 328
- WPA-PSK configuration, 315
- WSP (wireless service provider), 82

X–Z

- XOR (exclusive OR), 202
- XTACACS protocol, 42