

# Index

**Note to the reader:** Throughout this index **boldfaced** page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

## Numbers & Symbols

- 2.4 GHz ISM band (Scientific band), **166**
  - channel divisions, **172–175**
  - potential interference sources, **447**
- 4-way handshake, **371, 372**
- 5.8 GHz ISM band (Medical band), **166**
  - channel reuse patterns in, **336**
  - potential interference sources, **447**
- 6dB rule, **42, 66**
- 802 project, **5**
- 802.1X/EAP framework, **366–368, 367**
- 802.11 standards. *See* IEEE 802.11 standard
- 802.11 Working Group. *See* IEEE 802.11 Working Group
- 900 MHz ISM band, **165–166**
- $\lambda$  (lambda), for wavelength, **27**

## A

- absorption
  - of RF signal, **33–34, 34**
  - visual demonstration, **40**
- AC (alternating current) signal, **25**
  - transmitter generation, **57**
- access layer of network, **310**
- access point, dual radio cards, **138**
- access point-intelligent edge architecture, **284–285**
- access points, **198–199**
  - association with, **237, 237–238**
  - autonomous, **284**
  - collection in extended service set, **204**
  - configuration mode of, **208, 209**
  - discovery by scanning, **232**
  - maximum number of stations connected to, **312**
  - operational mode for 802.11g, **139**
  - physical security for, **375–376**
  - placement and configuration, **453–454**
  - in point coordinator role, **228**
  - power level for site survey, **449**
  - roaming and, **142**
  - rogue, **389–390**
  - station communication about power save mode, **261**
  - virtual, **297**
- ACK (acknowledgement) frame, **223–224, 252, 253**
  - for fragment transmission, **254**
  - over point-to-point links, **292**
- active gain, **46, 93–94**
- active manual coverage analysis, **460**
- active mode for power management, **261**
- active scanning, **201, 232, 233–234, 234**
- Ad-Hoc mode, **232**
  - for client stations, **209**
- ad-hoc network, **206. *See also* independent basic service set (IBSS)**
  - common use, **390**
  - security policy recommendations, **406**
  - as security risk, **389**
- adaptive rate selection, **329**
- Advanced Encryption Standard (AES)
  - algorithm, **146, 360, 373**
- African Telecommunications Union (ATU), **4**
- air stratification, impact on performance, **347**
- AirDefense Mobile, **403**
- AirDefense Personal, **407**
- AirMagnet Survey, **463**
- AirWave, Management Platform software, **286**
- Akin, Devin, **333**
- alignment of antenna, **116**
- all-band interference, **344**
- alternating current (AC) signal, **25**
  - transmitter generation, **57**
- amplification (gain), **46**
  - active vs. passive, **93–94**
- amplifiers, **120–121**
- amplitude, **30, 31**
  - phase effect on, **31**
  - and wavelength, **9, 9**
- Amplitude Shift Keying (ASK), **11–12, 12**
- amps, **61**

## 510 announcement traffic indication message – basic service set identifier

- announcement traffic indication message (ATIM), 263
  - antennas, 25, 58–59
    - accessories, 118–124
    - amplifiers, 120–121
    - attenuators, 121
    - cables, 118–119
    - connectors, 119–120
    - grounding rods and wires, 123–124, 124
    - lightning arrestors, 121–123, 122
    - splitters, 120
  - azimuth charts and elevation charts, 94–96, 95
  - beamwidth, 96–97, 97
  - connection and installation, 113–117
    - impact, 93
    - indoors, 99
    - maintenance, 117
    - mounting, 115–117
    - VSWR (voltage standing wave ratio), 113–114
  - diversity, 111–112, 112
  - exam essentials, 125–126
  - gain of power from
    - relative to dipole antenna, 65
    - relative to isotropic antenna, 64
  - height, earth bulge and, 110, 110
  - MIMO (Multiple Input Multiple Output), 113
  - on PCMCIA radio card, 277
  - plural, 98
  - polarity markings, 27
  - polarization, 111
  - types
    - highly-directional, 98, 103–104
    - omni-directional, 97, 98–100, 99
    - phased array, 104
    - sector, 104–105
    - semi-directional, 97, 100–102, 103, 453, 454
    - unidirectional, 44, 453, 455
  - and WLAN range, 345
  - Antheil, George, 169
  - AP mode for bridge, 292
  - appliances, Wi-Fi cards in, 279
  - application analysis, as site survey option, 454–455
  - Asia-Pacific Telecommunity (APT), 4
  - ASK (Amplitude Shift Keying), 11–12, 12
  - associated client stations, 199
  - association, 237, 237–238
    - terminating, 241
    - tracking station state, 238, 238–239
  - ATIM (announcement traffic indication message), 263
  - atmosphere, and refraction, 38, 38
  - attenuation (loss), 39–40
    - chart for coaxial cable, 119
    - due to free space path loss, 42
  - attenuators, 121
  - ATU (African Telecommunications Union), 4
  - authentication, 234–237, 361–362
    - 802.11 standards definition for, 145, 146
    - Open System, 235, 235
    - Shared Key, 236, 236–237
    - tracking station state, 238, 238–239
  - authentication and authorization, 366–370
    - 802.1X/EAP framework, 366–368, 367
    - dynamic encryption key generation, 369–370
    - Extensible Authentication Protocol (EAP) types, 368–369
  - authentication attacks, 393–394
  - authentication server in 802.1X framework, 367
  - authenticator in 802.1X framework, 366–367
  - AutoCell, 467
  - automatic rate selection, 329
  - autonomous access point, 284
  - azimuth charts, 94–96, 95
- 
- B**
- B/G mode, for 802.11g access point, 139
  - B Only mode, for 802.11g access point, 139
  - backbone, 310
  - background noise
    - and performance, 446
    - radio card differentiation of signal from, 43
  - background priority in WMM, 264
  - backward compatibility, 802.11b devices and legacy 802.11 devices, 136
  - bandwidth
    - for original 802.11 standard, 136
    - vs. throughput, 182–183
  - Barker Code, 137, 177
  - basic service area (BSA), 203, 204
  - basic service set (BSS), 198, 202–203
  - basic service set identifier (BSSID), 203, 203

battery pack, 456  
 battery time, 260  
 beacon management frame, 232  
 beacons, 141  
 beam divergence, 41  
 beamwidth, 96–97, 97  
 bel, 62  
 best effort priority in WMM, 264  
 bidirectional amplifiers, 120  
 binoculars, 458  
 Bird meter (wattmeter), 458  
 bit error rate, and receive sensitivity of wireless card, 78  
 bit-flipping attack, 365  
 blue sky phenomenon, 36  
 blueprints, 456  
 Bluetooth, 196, 197
 

- all-band interference from, 344

 bounded medium, 24  
 bridge mode, for access point, 208  
 Bridged Virtual Interface (BVI), 284  
 bridging, 314
 

- outdoor link, 43
- wireless, 207
- wireless LAN, 290–292

 broadcast key, 370  
 broadcast traffic, DTIM and, 262  
 BSA (basic service area), 203, 204  
 BSSID (basic service set identifier), 203, 203  
 buildings, connections between, 314  
 BVI (Bridged Virtual Interface), 284

## C

cables, 118–119
 

- loss calculations, 459–460

 calculators, 458  
 captive portal, 318  
 carrier frequency, 173  
 carrier sense, 224–225  
 Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), 182, 346
 

- vs. CSMA/CD, 221–222

 carrier signals, 8–10, 58
 

- amplitude and wavelength, 9, 9

 casual eavesdropping, 391–392  
 CCA (clear channel assessment), 225, 338  
 CCK (Complementary Code Keying), 137, 177  
 CCMP (Cipher Block Chaining-Message Authentication Code), 145–146, 373  
 CD in book
 

- Beam patterns and Polarization of directional antennas* video, 111
- Ekahau Site Survey, 465, 466
- ENANIM, 31
- LinkBudget spreadsheet, 459
- Powerpoint animation, rule of 10s and 3s, 69

 cellular technologies
 

- networking card, 195
- for WWAN, 195

 centralized WLAN architecture, 286–287
 

- remote office WLAN switch, 288
- WLAN switch/controller, 287, 287–288

 CEPT (European Conference of Postal and Telecommunications Administrations), 4  
 certification of Wi-Fi products, 6  
 Certified Wireless Network Professional (CWNP) wireless certification program, 8  
 CF (Compact Flash) cards, 277  
 CFR (Code of Federal Regulations)
 

- intentional radiator (IR) definition, 59
- Title 47, 3

 channel reuse, 336, 337  
 channel statistics, 149  
 “chipping,” 177  
 chips, 177  
 chipsets, 280  
 cipher, 360  
 Cipher Block Chaining-Message Authentication Code Protocol (CCMP), 145–146, 373  
 Cisco Wireless LAN Solution Engine (WLSE), 285, 285  
 CITELE (Inter-American Telecommunication Commission), 4  
 clause 14 devices, 135  
 clause 15 devices, 135  
 clause 17 devices, 138  
 clause 18 devices, 136  
 clause 19 devices, 139  
 clear channel assessment (CCA), 225, 338  
 cleartext communication, capture by protocol analyzer, 392  
 client stations, 199
 

- configuration modes, 209, 209
- information retrieval methods, 153
- power management, 260–261
- roaming decision by, 332

 client statistics, 148

## 512 co-channel interference – digital camera

co-channel interference, 334–335, 335  
 co-location, 204, 206, 312  
 coaxial cable, attenuation chart, 119  
 Code of Federal Regulations (CFR), 3  
   intentional radiator (IR) definition, 59  
 Cognio, 404  
 collinear antennas, 99  
 collision  
   avoidance, 222  
   detection, 223–224  
   from hidden node transmission, 339, 339  
 communications  
   basic requirements, 56  
   fundamentals, 8–13  
     carrier signals, 8–10  
     keying methods, 11–13  
 Communications Act of 1934, 3  
 CommView, 243  
   installation, 239  
   packet capture, 239–240  
 Compact Flash (CF) cards, 277  
 comparison units of measurement, 60–66  
   decibels dipole (dBd), 65  
   decibels isotropic (dBi), 63–64  
   decibels relative to 1 milliwatt (dBm),  
     65–66  
 Complementary Code Keying (CCK), 137, 177  
 connectors, 119–120  
 Contention-Free Period (CFP), 229  
 contention window, 225, 226  
 control frames, 230–231  
 convolution coding, 180  
 cordless phones, interference from, 448  
 core of network, 310–311  
 Counter Mode with Cipher Block Chaining  
   Message Authentication Code Protocol  
   (CCMP), 145–146  
 coverage analysis  
   commercial applications, 461–462, 462  
   in site survey, 332, 460–467  
     assisted method, 464, 464  
     mandatory, 449–452  
     manual method, 460–464  
     predictive method, 465–466  
 CRC (cyclic redundancy check), 44, 364  
 CSMA/CA (Carrier Sense Multiple Access/  
   Collision Avoidance), 182, 346  
   vs. CSMA/CD, 221–222  
 CTS-to-Self, 260

Cuban Missile Crisis (1962), 169  
 current state techniques, 11  
 CWNP (Certified Wireless Network  
   Professional) wireless certification  
   program, 8  
 cyclic redundancy check (CRC), 44  
   by WEP, 364

**D**

data corruption from multipath, 44, 45  
 data frames, 231  
 data privacy, 145  
 data rate transmissions, impact of distance  
   between access point and client station, 329  
 data rates, for original 802.11 standard, 136  
 dB. *See* decibels (dB)  
 dBd (decibels dipole), 65  
 dBi (decibels isotropic), 63–64  
 dBm (decibels relative to 1 milliwatt), 65–66  
 DBPSK (Differential Binary Phase Shift  
   Keying), 177  
 DCF. *See* Distributed Coordination Function  
   (DCF)  
 DCF interframe space (DIFS), 223  
 deauthentication, 241  
 decibels (dB), 40, 61–63  
   comparison with milliwatt change, 63  
   loss and gain, 72–73  
   reason to use, 64  
 decibels dipole (dBd), 65  
 decibels isotropic (dBi), 63–64  
 decibels relative to 1 milliwatt (dBm), 65–66  
 Dedicated Short Range Communication  
   (DSRC), 150  
 degrees, for wavelength, 10, 10  
 delay spread, 43, 170, 345  
 delivery traffic indication message (DTIM),  
   262–263  
 denial of service attack, 396–398  
   protection against, 153  
 DFS (dynamic frequency selection), 144, 467  
 diagnostic maintenance for antennas, 117  
 dictionary attacks, 393–394  
 Differential Binary Phase Shift Keying  
   (DBPSK), 177  
 diffraction, 38–39, 39  
 digital camera, 456–457, 458

- dipole antenna, 98  
 half-wave, 64, 100
- direct current, 25
- direct sequence spread spectrum (DSSS), 135, 176–178  
 data encoding, 176–177  
 modulation, 177–178
- disassociation, 241
- distributed antenna system, and hidden node problem, 340
- Distributed Coordination Function (DCF), 147, 222–228, 263–264  
 carrier sense, 224–225  
 collision detection, 223–224  
 duration/ID field, 224  
 flowchart, 226–228, 227  
 interframe space (IFS), 223  
 random backoff time, 225–226
- distributed WLAN architecture, 288–289
- distribution layer of network, 310
- distribution system (DS), 199–200  
 wireless vs. wired, 201
- distribution system medium (DSM), 199, 200
- distribution system services (DSS), 199
- downfade from multipath, 43
- drip loop, 117
- DSRC (Dedicated Short Range Communication), 150
- DSSS. *See* direct sequence spread spectrum (DSSS)
- DTIM (delivery traffic indication message), 262–263
- duration/ID field, 224
- dwel time, 171  
 significance, 172
- dynamic encryption key generation, 369–370
- dynamic frequency selection (DFS), 144, 467
- dynamic rate switching, 329, 329–331
- 
- E**
- E-field (electrical), 26
- E-plane of antenna element, 94, 95, 96, 98
- EAP (Extensible Authentication Protocol), 146, 367  
 types, 368–369
- earth bulge, 109–110
- eavesdropping, 390–392
- EDCA (Enhanced Distributed Channel Access), 147, 264
- educational/classroom use, of wireless network, 316
- EIFS (Extended interframe space), 223
- EIRP (equivalent isotropically radiated power), 3, 59–60
- Ekahau Site Survey, 465, 466
- electrical (E-) field, 26
- electrical power, for access points, 297
- electrical tape, 457
- elevation charts, 94–96, 95
- EMANIM, 31  
 exercise using, 40
- encryption, 360  
 and throughput, 183, 346  
 Wired Equivalent Privacy (WAP), 145
- encryption cracking, 393
- encryption key, dynamic generation, 369–370
- Endspan solution for PoE, 298
- Enhanced Distributed Channel Access (EDCA), 147, 264
- Enhanced Wireless Consortium (EWC), 150
- enterprise access point, dual radio card capabilities, 336
- enterprise encryption gateway, 295–297, 296
- enterprise environment, Wi-Fi client utility for, 282
- enterprise wireless gateway, 292–294, 293
- equivalent isotropically radiated power (EIRP), 3, 59–60
- ESSID (extended service set identifier), 206
- European Conference of Postal and Telecommunications Administrations (CEPT), 4
- European Radiocommunications Committee (ERC), 144
- evil twin attack, 395–396
- EWC (Enhanced Wireless Consortium), 150
- Extended interframe space (EIFS), 223
- Extended Rate Physical OFDM (ERP-OFDM) technology, 139
- extended service set (ESS), 198, 204–206, 205
- extended service set identifier (ESSID), 206
- Extensible Authentication Protocol (EAP), 146, 367  
 types, 368–369
- extension identifier, 229

**F**

fade margin, 80–81  
 calculating, 459  
 fast roaming amendment (802.11r), 150–151  
 fast secure roaming (FSR) solution, 332  
 Federal Communications Commission (FCC), 3  
 health and safety course on regulations, 117  
 Federal Information Processing Standards (FIPS), 405  
 FHSS (Frequency Hopping Spread Spectrum), 135, 170–172, 171  
 access point parameters, 141  
 communications, 344  
 firewall, personal, 390  
 security policy recommendations, 406  
 fixed-loss attenuator, 121  
 forward error correction (FEC), 180  
 4-way handshake, 371, 372  
 fragmentation, 253–255, 254  
 frame transmission time, 331  
 frame types in 802.11, 229–231  
 control frames, 230–231  
 data frames, 231  
 management frames, 230  
 free space path loss, 41–42, 66  
 calculating decibel loss, 64  
 and WLAN range, 346  
 frequency, 9  
 relationship to wavelength, 30  
 of RF signal, 29–30  
 and wavelength travel distance, 27, 28, 29  
 frequency band, 182  
 frequency domain tool (spectrum analyzer), 46, 46  
 Frequency Hopping Spread Spectrum (FHSS), 135, 170–172, 171  
 access point parameters, 141  
 frequency hopping spread spectrum (FHSS) communications, 344  
 frequency response, of cable, 118  
 Frequency Shift Keying (FSK), 12, 12  
 Fresnel zone, 105, 106–109  
 tree growth data for, 458  
 full-duplex communications, 198  
 functional security policy, 405

**G**

G Only mode, for 802.11g access point, 139  
 gain (amplification), 46  
 active vs. passive, 93–94  
 Gaussian Frequency Shift Keying (GFSK), 172  
 Generic Routing Encapsulation (GRE) tunnel, 286  
 gigahertz (GHz), 30  
 global spectrum management, 4  
 GMK (Group Master Key), 372  
 GPS, 458  
 Gramm-Leach-Bliley Act, 405–406  
 grid antenna, 103–104  
 grounding rods and wires, 123–124, 124  
 Group Master Key (GMK), 372  
 Group Temporal Key (GTK), 372  
 GSM (Global System for Mobile Communications) cellular phones, 165

**H**

H-field, 26  
 H-plane of antenna element, 26, 26, 94, 95, 96, 98  
 half-duplex communications, 198  
 half-wave dipole antenna, 64, 100  
 hallways, planar antennas for, 101  
 HCCA (Hybrid Coordination Function Controlled Access), 147, 264  
 HCF (Hybrid Coordination Function), 147, 264  
 Health Insurance Portability and Accountability Act (HIPAA), 405–406  
 healthcare, network design, 317  
 Helium Networks, 462  
 SiteScout, 463  
 hertz (Hz), 29  
 hidden node, 338–342, 339, 341  
 fixing, 342  
 High-Rate DSSS (HR-DSSS), 137, 176  
 highly-directional antenna, 98, 103–104  
 HIPAA (Health Insurance Portability and Accountability Act), 405–406  
 home wireless networks, security for, 407

- home wireless router, 294
  - HomeRF, 344
  - hop time, 171–172
  - hopping sequence, 170–171
  - horizontal polarization, 27
  - hospitals, network design, 317
  - hotspots, 317–318
    - malicious eavesdropping attacks at, 392
    - and security, 376
    - security policy recommendations, 406
  - “housekeeping” for 802.11, 149
  - human adult, water in, 34
  - Hybrid Coordination Function (HCF), 147, 264
  - Hybrid Coordination Function Controlled Access (HCCA), 147, 264
  - Hz (hertz), 29
- 
- I**
- IAPP (Inter Access Point Protocol), 142, 143
  - IBSS (independent basic service set), 198, 206–207, 207, 390
  - ICV (Integrity Check Value), 362
  - IEEE (Institute of Electrical and Electronics Engineers), 2, 5, 134
  - IEEE 802.3 frame format, vs. 802.11 frame format, 229
  - IEEE 802.1X standard, 366–368, 367
  - IEEE 802.11 standard, 2, 170, 255
    - amendment comparison, 140–141
    - configuration modes, 208–209
      - for access points, 208, 209
      - for client stations, 209, 209
    - draft amendments, 148–153
      - 802.11k, 148–149
      - 802.11m, 149
      - 802.11n, 149–150
      - 802.11p, 150
      - 802.11r, 150–151
      - 802.11s, 151
      - 802.11T, 151–152
      - 802.11u, 152
      - 802.11v, 153
      - 802.11w, 153, 398
    - exam essentials, 154–155
    - fragmentation, 253–255, 254
    - frame format, vs. 802.3 frame format, 229
    - frame types, 229–231
      - control frames, 230–231
      - data frames, 231
      - Layer 3 integration with, 231
      - management frames, 230
    - nonstandard topologies, 207
    - overview, 135–136
    - ratified amendments, 136–147
      - 802.11a amendment, 137–138, 166, 178, 180
      - 802.11b amendment, 136–137, 170, 173
      - 802.11d amendment, 141
      - 802.11e amendment, 147, 263–265
      - 802.11F recommended practice, 142
      - 802.11g amendment, 139–140, 170, 175, 178, 180, 255–256, 334
      - 802.11h amendment, 144–145
      - 802.11i amendment, 145–146, 370–371
      - 802.11j amendment, 146
    - topologies, 197–207
  - IEEE 802.11 Working Group, 134
    - MAC Task Group, 135
    - PHY Task Group, 135
  - IEEE 802.15 Working Group, 196
  - IEEE 802.16 standard, 195–196
  - IETF (Internet Engineering Task Force),
    - request for comment (RFC) 3344, 334
  - IFS (interframe space), 223
  - impedance, 113
  - in phase, 31, 32
  - inclinometer, 458
  - independent basic service set (IBSS), 198, 206–207, 207, 390
  - indoor installation of antenna, 99
    - mounting options, 116
  - industrial environment, network design, 316–317
  - Industrial, Scientific, and Medical (ISM) bands, 135, 165–166
    - exam essentials, 184
  - Infrared Data Association, 135
  - infrared technology, 196
    - PHY Task Group work on specifications, 135
  - infrastructure equipment protection, 375–376
    - interface security, 376
    - physical security, 375–376

## 516 Infrastructure mode – lightning arrestors

- Infrastructure mode, for client stations, 209
- Initialization Vector (IV), 363  
static WEP encryption key and, 363
- Institute of Electrical and Electronics Engineers (IEEE), 2, 5, 134. *See also* IEEE 802.11 standard
- integrated WIDS, 401
- Integrity Check Value (ICV), 362
- intelligent edge access point, 284
- Intelligent Transportation Systems (ITS), 150
- intentional radiator (IR), 59
- Inter Access Point Protocol (IAPP), 142, 143
- Inter-American Telecommunication Commission (CITEL), 4
- inter-symbol interference, 344–345
- interference  
devices causing, 345  
locating, 255  
potential sources for, 447–448  
troubleshooting, 343–345
- interframe space (IFS), 223
- International Organization for Standardization (ISO), 3, 7
- International Telecommunication Union  
Radiocommunication Sector (ITU-R), 2, 4
- Internet Engineering Task Force (IETF),  
request for comment (RFC) 3344, 334
- Internet Protocol Security (IPSec), 377
- Internet service providers, wireless (WISP), 315
- intersymbol interference (ISI), 44, 45, 170
- intrusion monitoring, 398–404  
mobile WIDS, 402–403  
spectrum analyzer (frequency domain tool),  
403–404  
wireless intrusion detection system (WIDS),  
398–401, 399  
wireless intrusion prevention system  
(WIPS), 401–402
- inverse square law, 81
- IPSec (Internet Protocol Security), 377
- ISI (intersymbol interference), 44, 45, 170
- ISM (Industrial, Scientific, and Medical) band,  
135
- ISO (International Organization for  
Standardization), 3, 7
- isotropic radiator, 58
- ITS (Intelligent Transportation Systems), 150
- ITU-R (International Telecommunication  
Union Radiocommunication Sector), 2, 4  
ISM bands defined by, 165
- IV (Initialization Vector), 363  
static WEP encryption key and, 363
- IV collisions attack, 364
- IXIA, 455
- 
- ## J
- jamming, 397, 403  
narrowband vs. spread spectrum signal,  
168
- Japan, IEEE Task Group j and regulatory  
approval, 146
- Juniper Networks Odyssey Access Client, 282
- 
- ## K
- k-factor, 37
- keying methods, 11–13  
Amplitude Shift Keying (ASK), 11–12, 12  
Frequency Shift Keying (FSK), 12, 12  
Phase Shift Keying (PSK), 13, 13
- kilohertz (KHz), 30
- Kismet, 393
- 
- ## L
- lambda ( $\lambda$ ), for wavelength, 27
- laptop computers, same radio card for  
multiple, 279
- laser distance measuring tool, 457
- last-mail of service, 314–315
- latency, 332
- layer 2 DoS attacks, 398
- Layer 3 integration, with 802.11 frames, 231
- Layer 3 roaming, 333, 333–334
- Layer 3 VPNs, 376–378
- LEAP (Lightweight Extensible Authentication  
Protocol), 368, 393
- legacy security issues  
authentication, 361–362  
MAC Filters, 365  
SSID cloaking, 365–366  
static WEP encryption, 362–365
- legislative compliance, 405–406
- licensed wireless communications, 3
- lightning arrestors, 121–123, 122

lightning, damage risks, 346  
 Lightweight Extensible Authentication Protocol (LEAP), 368, 393  
 line of sight  
   earth bulge and, 109–110  
   RF, 105  
   visual, 105  
 link analysis software, 458  
 link budget, 43. *See also* system operating margin (SOM)/link budget  
   calculating, 459  
 LinkBudget.xls spreadsheet, 459  
 local area network, wireless. *See* wireless LAN  
 logarithms, 62–63  
   rule of 10s and 3s as alternative, 67  
 loss (attenuation), 39–40  
 lower band (UNII-1), 167

## M

MAC (media access control), 221  
   address fields in 802.3 and 802.11 frames, 229  
   header of 802.11 frame, 224, 253  
 MAC address, of BSS access point, 203  
 MAC Filters, 365  
 MAC Service Data Unit (MSDU), 199  
 MAC spoofing, 394  
   software utility, 395  
 MAC Task Group (IEEE 802.11), 135  
 MacStumbler, 393  
 MAHO (Mobile Assisted Hand-Over), 149  
 maintenance of antennas, 117  
 malicious eavesdropping, 392  
 man-in-the-middle attack, 396, 397  
 management console in WIDS, 399, 400  
 management frames, 230  
 management interface exploits, 395  
 management, of access points, 285–286  
 mandatory coverage analysis, in site survey, 449–452  
 mandatory spectrum analysis, in site survey, 445–449  
 manufacturing, network design, 316–317  
 Markey, Hedy Kiesler, 169  
 matched cable, 114  
 materials, attenuation (loss) comparison, 40–41

mathematics  
   Fresnel zone, 106–108  
   radio frequency, 66–81  
     exam essentials, 83  
     fade margin, 80–81  
     inverse square law, 81  
     received signal strength indicator (RSSI), 76–77  
   rule of 10s and 3s, 67–76  
   system operating margin (SOM)/link budget, 77–79

maximum transmission unit, for TCP/IP, 253  
 measuring wheel, 457  
 media access control (MAC), 221. *See also* MAC entries  
 Medical band (5.8 GHz ISM band), 165  
 megahertz (MHz), 30  
 mesh networking, 151  
   wireless LAN mesh routers, 295, 296  
 Message Integrity Check (MIC), 373  
 metal, and reflection, 36  
 microwave ovens  
   interference from, 447  
   spectrum use, 448  
 microwave reflection, 35  
 middle band (UNII-2), 167  
 Midspan solution for PoE, 298  
 milliwatts (mW), 61  
   comparison with decibel change, 63  
 MIMO (Multiple Input Multiple Output), 36, 113, 149  
 Mini PCI, 277, 278  
 MiniStumbler, 393  
 mixed mode, 255, 256  
   for 802.11g access point, 139  
 Mobile Assisted Hand-Over (MAHO), 149  
 Mobile IP standard, 231, 334  
 mobile office networking, 315–316  
 mobile WIDS, 402–403  
 mobility of user, 313  
 modulation for data transmission, 8  
 modulation techniques. *See* keying methods  
 mounting antennas, 115–116  
 mounting gear, temporary, 456  
 MPSK (Multiple Phase Shift Keying), 13, 14  
 MSDU (MAC Service Data Unit), 199  
 multicast traffic, DTIM and, 262  
 multipath  
   interference, 168–169

## 518 multiple access – passive scanning

MIMO and, 113  
 of RF signal, 42–44, 45  
   visual demonstration, 44–45  
 multiple access, 222  
 Multiple Input Multiple Output (MIMO), 36, 113, 149  
 Multiple Phase Shift Keying (MPSK), 13, 14

**N**

narrowband, 135, 168–170, 169  
   interference, 344  
 National Institute of Standards and Technologies (NIST), 404, 405  
 NAV (network allocation vector), 224, 256  
 near/far problem, 343, 343  
 NetStumbler, 365–366, 391, 391–392, 393, 460  
 network allocation vector (NAV), 224, 256  
 network design  
   bridging, 314  
   capacity vs. coverage, 311, 311–312, 312  
   core, distribution and access, 310–311  
   corporate data access and end user mobility, 313  
   educational/classroom use, 316  
   exam essentials, 319  
   extension to remote areas, 313–314  
   healthcare, 317  
   industrial warehousing and manufacturing, 316–317  
   mobile office networking, 315–316  
   public network access, 317–318  
   SOHO (small office, home office), 315  
   wireless networking in, 311  
   WISP (wireless ISP), 314–315  
 networks, interworking between different, 152  
 Newton, Isaac, Inverse Square Law, 81  
 NIST (National Institute of Standards and Technologies), 404, 405  
 noise floor, 43  
 nomadic roaming, 204, 205  
 non-overlapping DSSS channels, 173–174  
 non-root bridge, 290  
   with clients, 292  
 null frames, 231  
 nulling from multipath, 43

**O**

Occupational Safety and Health Administration, 117  
 OFDM. *See* Orthogonal Frequency Division Multiplexing (OFDM)  
 ohm, 113  
 Ohm, Georg, 113  
 omni-directional antenna, 97, 98–100, 99  
   beamwidth, 97  
   placement of, 115  
   vertical radiation patterns, 99  
 Open System authentication, 145, 235, 235, 361–362  
 Open Systems Interconnection (OSI) model, 7  
   IEEE 802.11 standard and, 135  
 Organizational Unique Identifier (OUI), 229  
 Orthogonal Frequency Division Multiplexing (OFDM), 138, 149, 178–180, 179  
   convolution coding, 180  
 oscillation, 26  
 oscilloscope (time domain tool), 46, 46  
 OSI. *See* Open Systems Interconnection (OSI) model  
 out of phase, 31, 32  
   and primary signal degradation, 109  
 outdoor bridge link, 43  
 overlapping channels  
   in 2.4 GHz ISM band, 172–175, 173  
   avoiding, 450  
 overlay WIDS, 401

**P**

Packet Binary Convolutional Coding (PBCC), 140, 178  
 Pairwise Master Key (PMK), 372  
 Pairwise Transient Key (PTK), 372  
 panel antenna, 101  
   beamwidth, 97  
   radiation patterns, 103  
 parabolic dish antenna, 103–104  
   beamwidth, 97  
 parallel plane of antenna element, 26, 26  
 passive gain, 46, 93–94  
 passive manual coverage analysis, 460  
 passive scanning, 201, 232, 233

- patch antenna, 101, 102
    - beamwidth, 97
  - PBCC. *See* Packet Binary Convolutional Coding (PBCC)
  - PC Card, 277, 277
  - PCF (Point Coordination Function), 147, 222, 228–229, 264
  - PCF interframe space (PIFS), 223
  - PCI (Peripheral Component Interconnect) bus technology, 277, 278
  - PCMCIA client adapter, 277, 277
  - PEAP (Protected Extensible Authentication Protocol), 368
  - peer-to-peer attacks, 390
  - Peer-to-Peer mode, for client stations, 209
  - peer-to-peer network, 206. *See also* independent basic service set (IBSS)
    - security policy recommendations, 406
  - per session per user key generation, 370
  - performance issues
    - 802.11b devices on 802.11g networks, 256
    - background noise, 446
    - troubleshooting, 345–346
  - Peripheral Component Interconnect (PCI) bus technology, 277, 278
  - personal firewall, 390
    - security policy recommendations, 406
  - phase, 10, 10, 31, 32
    - visual demonstration, 44–45
  - Phase Shift Keying (PSK), 13, 13
  - phased array antenna, 104
  - phishing attacks, 396
  - PHY Task Group (IEEE 802.11), 135
  - physical carrier sense, 225
  - physical interference, 344
  - physical security for network hardware, 375–376
  - pigtail cables, 119
  - pilot carriers, 180
  - placement of antennas, 115
  - planar antennas, 101
  - PMK (Pairwise Master Key), 372
  - PoE (Power over Ethernet), 297–298
  - Point Coordination Function (PCF), 147, 222, 228–229, 264
  - point coordinator, 228
  - point source, 58
  - point-to-multipoint bridge, 291, 291, 341
    - for connecting buildings, 314
  - point-to-point bridge, 291, 291
    - for connecting buildings, 314
  - Point-to-Point Tunneling Protocol (PPTP), 377
  - polarity, 26, 26–27
  - polarization of antennas, 111
  - polling by mainframes, 221
  - port-based access control standard, 366
  - power level of access point, for site survey, 449
  - power management, 260–261
  - power output from antenna, increasing, 58
  - Power over Ethernet (PoE), 297–298
  - power save mode, 261
  - Power Sourcing Equipment (PSE), 297
  - power splitters, 120
  - power units of measure, 60–66
    - decibel (dB), 61–63
    - milliwatt (mW), 61
    - watt, 61
  - PPTP (Point-to-Point Tunneling Protocol), 377
  - preshared key (PSK), 146, 372
  - preventive maintenance of antennas, 117
  - probe requests, 141, 233
  - probe response, 233
  - processing gain, 177
  - propagation behaviors for RF signals, 25
  - Protected Extensible Authentication Protocol (PEAP), 368
  - protection mechanism, from 802.11g
    - amendment, 140
  - protocol analyzer, 340
    - laptop versions, 402–403, 403
    - unauthorized use, 392
  - PS-Poll frame, 262
  - PSE (Power Sourcing Equipment), 297
  - PSK (Phase Shift Keying), 13, 13
  - PSK (preshared key), 146, 372
  - PSPF (Public Secure Packet Forwarding), 390, 391
  - PTK (Pairwise Transient Key), 372
  - public network access, 317–318
  - Public Secure Packet Forwarding (PSPF), 390, 391
  - “Pure G” network, 255
- 
- Q**
- Quality of Service Basic Service Set (QBSS), 263

**R**

- ρ (rho) for voltage reflection coefficient, 113
- radiation patterns, 94
- radio cards
  - chipsets, 280
  - formats, 276–280
  - receiver sensitivity level, 43
- radio frequency (RF)
  - communications, 24
  - components, 57
    - antenna, 58–59
      - EIRP (equivalent isotropically radiated power), 59–60
    - intentional radiator (IR), 59
    - receiver, 59
    - transmitter, 57–58
  - interference. *See* interference
  - line of sight, 105
  - mathematics, 66–81
    - exam essentials, 83
    - fade margin, 80–81
    - inverse square law, 81
    - received signal strength indicator (RSSI), 76–77
    - rule of 10s and 3s, 67–76
    - system operating margin (SOM)/link budget, 77–79
  - shadow, 39
  - transmission methods, 168–170
- radio frequency (RF) signal
  - behavior identification
    - absorption, 33–34, 34
    - diffraction, 38–39, 39
    - free space path loss, 41–42
    - gain (amplification), 46
    - loss (attenuation), 39–40
    - multipath, 42–44, 45
    - reflection, 35, 35–36
    - refraction, 37–38, 38
    - scattering, 36–37, 37
    - wave propagation, 32–33
  - characteristics, 25–31
    - amplitude, 30, 31
    - frequency, 29–30
    - phase, 31, 32
    - polarity, 26, 26–27
    - wavelength, 27–29, 28
      - exam essentials, 47
      - what it is, 25
- Radio Frequency Spectrum Management (RFSM), 466
- radio resource measurement, 802.11k for, 148–149
- RADIUS (Remote Authentication Dial-In User Service) server, 367
- random backoff time, 225–226
- range of WLAN, variables affecting, 345–346
- Rayleigh fading, 43
- Rayleigh scattering, 36
- RBAC (role-based access control), 374–375
- RC4 (Rivest's Cipher) algorithm, 360
- RCC (Regional Commonwealth in the field of Communications), 4
- re-injection attack, 365
- reassociation, 240–241
- receive sensitivity level, 77
- received signal strength
  - measurement tool, 449, 456
  - measurements recorded, 451
- received signal strength indicator (RSSI), 76–77
  - thresholds, 330
- receiver, 59
  - receiver sensitivity level, of radio cards, 43
- recommendations, 406–407
  - from IEEE on practices, 142
- reflection, 35, 35–36, 109
- refraction, 37–38, 38
- Regional Commonwealth in the field of Communications (RCC), 4
- relative measurement units, 60
- remote areas, wireless for extending network to, 313–314
- Remote Authentication Dial-In User Service (RADIUS) server, 367
- remote office WLAN switch, 288
- repeater, 207
  - repeater mode
    - for access point, 208
    - for bridge, 292
- request to send/clear to send (RTS/CTS), 257–260, 258, 340
  - hidden node and, 342
- residential wireless gateway, 294
- resilience of communications, 183
- return loss, 113
- RF. *See* radio frequency (RF)

RFSM (Radio Frequency Spectrum Management), 466

roaming, 143, 144, 240

- access point support for, 142
- fast roaming amendment (802.11r), 150–151
- nomadic, 204, 205
- seamless, 204, 205
- troubleshooting, 331–333

roaming site reports, 149

Robust Security Network (RSN), 146, 371

robust security network associations (RSNAs), 371

- dynamic encryption key generation, 372

rogue access point, 389–390

rogue AP policy, security policy recommendations, 406

role-based access control (RBAC), 374–375

root bridge, 290

- with clients, 292

root mode for access point, 208

router

- VPN wireless, 295
- wireless for home, 294

RSN Information Element, 371

RSNAs (robust security network associations), 371

- dynamic encryption key generation, 372

RSSI (received signal strength indicator), 76–77

RSSI\_Max, 76

RTS/CTS (request to send/clear to send), 257–260, 258, 340

- data transfer between 2 wireless PCs, 259
- data transfer between wired PC and wireless PC using, 259
- hidden node and, 342

“rubber duck” antenna, 98

rule of 10s and 3s, 67–76

## S

safety, for antenna installation, 116–117

SANS Institute, 404

Sarbanes-Oxley Act of 2002, 405–406

scanner mode, for access point, 208

scattering, of RF signal, 36–37, 37

Scientific band (2.4 GHz ISM band), 165

- channel divisions, 172–175

script kiddies, 366

SD (Secure Digital) cards, 277

SDR (software defined radio), 280

seamless roaming, 204, 205

sector antenna, 104–105

- beamwidth, 97

Secure Digital (SD) cards, 277

security

- authentication and authorization, 366–370
  - 802.1X/EAP framework, 366–368, 367
  - dynamic encryption key generation, 369–370
  - Extensible Authentication Protocol (EAP) types, 368–369
- basics, 359–361
  - AAA (authentication, authorization, accounting), 360–361
  - encryption, 360
  - segmentation, 361
- exam essentials, 378–379, 408
- hotspots and, 318
- infrastructure equipment protection, 375–376
  - interface security, 376
  - physical security, 375–376
- intrusion monitoring, 398–404
  - mobile WIDS, 402–403
  - spectrum analyzer (frequency domain tool), 403–404
  - wireless intrusion detection system (WIDS), 398–401, 399
  - wireless intrusion prevention system (WIPS), 401–402
- legacy issues
  - authentication, 361–362
  - MAC Filters, 365
  - SSID cloaking, 365–366
  - static WEP encryption, 362–365
- segmentation, 374–375
  - RBAC (role-based access control), 374–375
  - VLANs, 374, 375
- and throughput, 183
- virtual private network (VPN), 376–378
- wireless attacks, 388–398
  - authentication attacks, 393–394
  - denial of service attack, 396–398
  - eavesdropping, 390–392
  - encryption cracking, 393

- MAC spoofing, 394
- MAC spoofing software utility, 395
- man-in-the-middle attack, 397
- management interface exploits, 395
- peer-to-peer attacks, 390
- rogue access point, 389–390
- wireless hijacking, 395–396
- wireless policy, 404–407
  - functional policy, 405
  - general policy, 404–405
  - legislative compliance, 405–406
  - recommendations, 406–407
- WPA (Wi-Fi Protected Access), 370–373
  - 4-way handshake, 372
  - CCMP, 373
  - robust security network, 371
  - Temporal Key Integrity Protocol (TKIP), 373
  - WPA/WPA2 Personal, 372–373
- SEEMesh (Simple, Efficient and Extensible Mesh), 151
- segmentation, 361, 374–375
  - RBAC (role-based access control), 374–375
  - VLANs, 374, 375
- self-organizing wireless LANs, 466–467
- semi-directional antenna, 97, 100–102, 103
  - radiation patterns, 103
  - in WLAN design, 453
- sensors in WIDS, 399, 400
- service set identifier (SSID), 201–202, 202
  - vs. BSSID, 203
  - cloaking, 365–366
- service sets, 194
  - basic (BSS), 198, 202–203
  - components
    - access points, 198–199
    - client stations, 199
    - distribution system (DS), 199–200
    - service set identifier (SSID), 201–202, 202
    - wireless distribution system (WDS), 200–201
    - wireless distribution system (WDS), dual radios, 202
    - wireless distribution system (WDS), single radio, 201
  - exam essentials, 210
  - extended (ESS), 198, 204–206, 205
  - independent basic (IBSS), 198, 206–207, 207
  - Shared Key authentication, 145, 236, 236–237, 361–362
  - short interframe space (SIFS), 223, 252
  - sideband lobes, in transmit spectrum mask, 175, 175, 176
  - signal generator, 458
  - signal loss, 58
    - from cable, 118
    - from VSWR (voltage standing wave ratio), 114
  - signal splitters, 120
  - signal-to-noise ratio, 452
  - Simple, Efficient and Extensible Mesh (SEEMesh), 151
  - Simple Network Management Protocol (SNMP), 376, 402
  - simplex communications, 198
  - sine wave, 25, 25
  - site survey, 29
    - coverage analysis, 332, 460–467
      - assisted method, 464, 464
      - manual method, 460–464
      - predictive method, 465–466
    - defined, 444–455
      - AP placement and configuration, 453–454
      - mandatory coverage analysis, 449–452
      - mandatory spectrum analysis, 445–449
      - optional application analysis, 454–455
    - exam essentials, 467–468
    - for multiple floors in building, 336
    - tools, 455–460
      - indoor site, 456–457
      - outdoor site, 457–459
      - prepackaged kits, 455
  - sky wave reflection, 35
  - slot time, 225
  - small office, home office (SOHO), 315
    - client utilities, 281
    - security for, 407
  - SNMP (Simple Network Management Protocol), 376, 402
  - software defined radio (SDR), 280
  - SOHO (small office, home office), 315
    - client utilities, 281
    - security for, 407
  - SOM (system operating margin)/link budget, 77–79
    - components, 77

gain and loss, 79  
   point-to-point gain and loss, 80  
 space diversity, 111  
 Spanning Tree Protocol (STP), 290  
 spectrum analysis in site survey, 445–449  
 spectrum analyzer (frequency domain tool), 46,  
   46, 345, 403–404, 456  
   for interference detection, 397  
 splitters, 120  
 spread spectrum signal, 135, 168–170, 169  
   invention of, 169  
   “spreading,” 177  
 SSID (service set identifier), 201–202, 202  
   cloaking, 365–366  
 standards organizations, 2–7  
 state transition techniques, 11  
 static WEP encryption, 362–365  
 station (STA), 197  
 STP (Spanning Tree Protocol), 290  
 streaming cipher, 360  
 supplicant in 802.1X framework, 366  
 swarm logic, 467  
 system operating margin (SOM)/link budget,  
   77–79  
   components, 77  
   gain and loss, 79  
   point-to-point gain and loss, 80

## T

target beacon transmission time (TBTT), 262  
 Task Group n-Sync, 150  
 task groups in IEEE, 5, 134  
 TCP/IP, maximum transmission unit for, 253  
 temperature of air, change, and performance,  
   347  
 Temporal Key Integrity Protocol (TKIP), 146,  
   373  
 third-party client utility for wireless  
   configuration, 281, 283  
 three-dimensional channel reuse, 336, 338  
 through loss, 120  
 throughput, 152  
   for 802.11g access point, 139  
   802.11n for increasing, 149–150  
   vs. bandwidth, 182–183  
   degradation, 340

  frame fragmentation and, 254  
   variables affecting, 346  
 TIM (traffic indication map), 261–262  
 time, and phase, 10  
 time domain tool (oscilloscope), 46, 46  
 Time Microwave Systems, attenuation  
   calculator, 459  
 TKIP (Temporal Key Integrity Protocol), 146,  
   373  
 topologies, 194  
   for IEEE 802.11 standard, 197–207  
 topology map, 458  
 TPC (transmit power control), 148, 467  
 traffic indication map (TIM), 261–262  
 transceiver (transmitter/receiver), 58  
 transition security network (TSN), 371  
 transmission diversity, 111  
 transmit power control (TPC), 144, 145, 148,  
   467  
 transmit spectrum mask, 173, 175, 175  
   802.11a, 182  
 transmitter, 57–58  
 troubleshooting  
   coverage considerations, 328–343  
   channel reuse, 336, 337  
   co-channel interference, 334–335, 335  
   dynamic rate switching, 329, 329–331  
   hidden node, 338–342, 339, 341  
   Layer 3 roaming, 333, 333–334  
   near/far problem, 343, 343  
   roaming, 331–333  
   three-dimensional channel reuse, 336,  
     338  
   interference, 343–345  
   performance issues, 345–346  
   weather impact, 346–347  
 TSN (transition security network), 371

## U

unbounded medium, 24  
 unicast key, 370  
 unidirectional amplifiers, 120  
 unidirectional antenna, 44, 453, 454, 455  
 unified WLAN architecture, 289  
 UNII. *See* Unlicensed National Information  
   Infrastructure (UNII) frequency bands

## 524 unintentional jamming – wind

unintentional jamming, 397  
 United Nations, 4  
 Unlicensed National Information  
   Infrastructure (UNII) frequency bands,  
   166–168  
 allocation, 137  
 exam essentials, 184  
 overview, 181, 181  
 potential interference sources, 447–448  
 unlicensed wireless communications, 3  
 upfade from multipath, 43  
 upper band (UNII-3), 167–168  
 USB 802.11 radio adapter, 279, 279  
 user density, and absorption, 34  
 utilities, for client card configuration, 281  
 UV rays, cable damage from, 347

**V**

variable-loss attenuator, 121, 458  
 vertical polarization, 26  
 video priority in WMM, 264  
 virtual access points, in predicted coverage  
   analysis, 465  
 virtual AP system, 297  
 virtual carrier sense, 224–225  
 virtual local area networks (VLANs), 374, 375  
 virtual private network (VPN), 376–378  
 visual light of sight, 105  
 Voice over IP (VoIP), quality of service  
   procedures for, 147  
 Voice over Wi-Fi (VoWiFi), 147  
   cell recommendations, 453  
   packet loss limits, 446  
 Voice over Wireless IP (VoWIP), 147  
 Voice over Wireless Lan (VoWLAN), 147  
 voice priority in WMM, 264  
 voltage reflection coefficient, 113  
 voltage standing wave ratio (VSWR), 113–114  
   signal loss from, 114  
 volts, 61  
 VPN wireless router, 295

**W**

walkie-talkies, 456, 458  
 wardriving, 391–392  
   tools for, 393

warehousing, network design, 316–317  
 water damage prevention, 347  
   to antenna, 117  
 water, in adult body, 34  
 water vapor, and refraction, 37  
 watt, 61  
 Watt, James, 61  
 wattmeter, 458  
 WAVE (Wireless Access and Vehicular  
   Environment), 150  
 wave propagation, 32–33  
 waveform, 25  
 wavelength  
   and amplitude, 9, 9  
   relationship to frequency, 30  
   of RF signal, 27–29, 28  
   and WLAN range, 345  
 WDS (wireless distribution system), 151  
 weak key attack in WEP, 364  
 weather impact, troubleshooting, 346–347  
 web resources  
   on chipsets, 280  
   on IEEE 802.11 Working Group, 134  
   Wi-Fi Alliance white papers, 265  
 WECA (Wireless Ethernet Compatibility  
   Alliance), 6  
 WEP. *See* Wired Equivalent Privacy (WEP)  
 WGB mode for bridge, 292  
 Wi-Fi Alliance, 2, 6  
   white papers, 265  
   Wi-Fi Protected Access (WPA) certification,  
   370  
 Wi-Fi Multimedia (WMM), 147  
 Wi-Fi networks, citywide deployments, 196  
 Wi-Fi phishing attack, 396  
 Wi-Fi Protected Access (WPA2), 146  
 Wi-Mesh Alliance (WiMA), 151  
 wideband interference, 344  
 WIDS (wireless intrusion detection system),  
   398–401, 399  
 WIEN (Wireless InterWorking with External  
   Networks), 152  
 WIGLE (Wireless Geographic Logging  
   Engine), 393  
 WiMA (Wi-Mesh Alliance), 151  
 WiMAX (Worldwide Interoperability for  
   Microwave Access), 195  
 wind  
   impact on performance, 346–347  
   preventing damage to antenna, 117

- wind load
  - and antenna mounting, 115
  - grid antennas and, 104
- WIPS (wireless intrusion prevention system), 401–402
- wired communications, 24
- Wired Equivalent Privacy (WEP), 145, 210, 362
  - attacks, 364–365
  - encryption process, 364
  - and Open System authentication, 235
  - and Shared Key authentication, 236–237
  - static encryption, 362–365
- wired network jacks, installation costs, 313
- Wireless Access and Vehicular Environment (WAVE), 150
- wireless attacks, 388–398
  - authentication attacks, 393–394
  - denial of service attack, 396–398
  - eavesdropping, 390–392
  - encryption cracking, 393
  - MAC spoofing, 394
  - MAC spoofing software utility, 395
  - man-in-the-middle attack, 397
  - management interface exploits, 395
  - peer-to-peer attacks, 390
  - rogue access point, 389–390
  - wireless hijacking, 395–396
- wireless bridging, 207, 311
- wireless distribution system (WDS), 151, 200–201
- wireless distribution system (WDS), dual radios, 202
- wireless distribution system (WDS), single radio, 201
- Wireless Ethernet Compatibility Alliance (WECA), 6
- Wireless Fidelity (Wi-Fi) standard, 2. *See also* IEEE 802.11 standard
- Wireless Geographic Logging Engine (WIGLE), 393
- wireless hijacking, 395–396
- Wireless InterWorking with External Networks (WIEN), 152
- wireless intrusion detection system (WIDS), 398–401, 399
- wireless intrusion prevention system (WIPS), 401–402
- wireless ISP (WISP), 314–315
- wireless LAN, 197
  - bridges, 290–292, 291
  - client devices, 276–281
  - client utilities, 281
  - radio card chipsets, 280
  - radio card formats, 276–280
- design
  - reflection and performance issues, 36
  - site survey, 29. *See also* site survey
- mesh routers, 295, 296
- self-organizing, 466–467
- specialty infrastructure devices, 289–297
  - enterprise encryption gateway, 295–297, 296
  - enterprise wireless gateway, 292–294, 293
  - residential wireless gateway, 294
  - virtual AP system, 297
  - VPN wireless router, 295
  - wireless LAN bridges, 290–292, 291
  - wireless LAN mesh routers, 295, 296
  - wireless workgroup bridge, 289, 290
- switch, 148–149
  - switch/controller, 287, 287–288
- wireless LAN architecture
  - access point-intelligent edge, 284–285
  - centralized, 286–287
    - remote office WLAN switch, 288
    - WLAN switch/controller, 287, 287–288
  - distributed, 288–289
  - progression, 284
  - unified, 289
  - wireless network management system (WNMS), 285–286
- wireless metropolitan area network (WMAN), 195–196
- wireless multimedia (WMM), 263–265
- wireless network management system (WNMS), 285–286
- wireless network topologies, 194
- Wireless Performance Prediction (WPP), 152
- wireless personal area network (WPAN), 196
- wireless policy, 404–407
  - functional security policy, 405
  - general security policy, 404–405
  - legislative compliance, 405–406
  - recommendations, 406–407
- wireless wide area network (WWAN), 195
- wireless workgroup bridge, 289, 290
- Wireless Zero Configuration (WZC) service, 281, 283, 407, 461
- WISP (wireless ISP), 314–315

**526** WLAN – zones of useable signal coverage

WLAN. *See* wireless LAN

WMAN (wireless metropolitan area network),  
195–196

WMM (wireless multimedia), 263–265  
access categories, 264

WMM-PS (Power Save), 265

WMM-SA (Scheduled Access), 265

workgroup bridge (WGB), 207

as access point mode, 208

wireless, 289, 290

working groups in IEEE, 5

World-Wide Spectrum Efficiency (WWiSE), 150

Worldwide Interoperability for Microwave  
Access (WiMAX), 195

WPA (Wi-Fi Protected Access), 370–373

4-way handshake, 372

CCMP, 373

robust security network, 371

Temporal Key Integrity Protocol (TKIP),  
373

WPA/WPA2 Personal, 372–373

WPA/WPA2 Personal, 372–373

WPAN (wireless personal area network), 196

WPP (Wireless Performance Prediction), 152

WWAN (wireless wide area network), 195

WWiSE (World-Wide Spectrum Efficiency),  
150

WZC (Wireless Zero Configuration) service,  
281, 283, 407, 461

---

**Y**

yagi antenna, 101, 102

beamwidth, 97

---

**Z**

ZigBee, 196

zones of useable signal coverage, 29