

## Numerics

---

### 100 Mbps WLANs, 233–234

#### 802.11 WLANs, 88

control frames, 54

*ACK frames*, 57

*CF-End frames*, 57–58

*CTS frames*, 56

*PS-Poll frames*, 54–55

*RTS frames*, 55–56

*DSSS*, 93–95

data frames, 76–78

fixed field elements, 63–66

frequency hopping, 88–93

MAC layer operations, 40–47, 50–78

*frame formats*, 50–78

*power save operations*, 47–50

*station connectivity*, 40–47

management frames, 58, 66

*association request frames*, 72

*association response frames*, 72

*ATM frames*, 76

*authentication frames*, 70–71

*beacon frames*, 67–68

*CF parameter set IE*, 61

*challenge text IE*, 62

*deauthentication frames*, 71

*disassociation frames*, 75

*DS parameter set IE*, 60–61

*FH parameter set IE*, 60

*IBSS parameter set IE*, 62

*probe request frames*, 67–70

*reassociation request frames*, 73

*reassociation response frames*, 74–75

*SSID IE*, 59

*supported rates IE*, 59–60

*TIM IE*, 61–62

medium access mechanisms, 24–36

*CSMA/CA*, 24–32

*frame fragmentation*, 32–33

*PCF*, 33–36

nonstandard devices, 36–39

*repeater APs*, 37

*universal clients*, 38

*wireless bridges*, 39

*workshop bridges*, 38

PHYs (physical layers), 81–83

*coding*, 84–85

*interleaving*, 85–86

*modulation*, 86–87

*scrambling*, 84

*symbol mapping*, 86–87

QoS (quality of service), 173–174

*cochannel overlap*, 174–175, 180–183

*EDCF (Enhanced DCF)*, 176–183

*half-duplex mediums*, 174

*hidden nodes*, 175

radio receivers, 194

roaming, 150

security, 21, 116–146

*authentication mechanisms*, 124–125

*encryption*, 121–123

*vulnerabilities*, 126–130

*wireless*, 117–146

topologies, 21

*BSSs (basic service sets)*, 23

*ESSs (extended service sets)*, 23–24

*IBSSs (independent basic service sets)*, 21–22

### **802.11a OFDM PMD, 106–110**

#### **802.11a WLANs, 102**

802.11a OFDM PLCP, 102–104

802.11j, 102

OFDM, 104–106

#### **802.11b HR-DSSS PLCP, 98–99**

#### **802.11b minimum radio performance, radio receivers, 193–194**

#### **802.11b PMD-CCK modulation, 100–101**

#### **802.11b WLANs, 98**

802.11b HR-DSSS PLCP, 98–99

802.11b PMD-CCK modulation, 100–101

PBCC modulation, 101–102

#### **802.11g WLANs, 111–113**

#### **802.1x authentication framework, 132**

#### **802.1x deployments, 220–222**

#### **802.3 Ethernet, 3**

addressing, 6–7

common media, 11–12

CSMA/CD architecture, 7

Ethernet slot time, 7–8

frames, 4–6

*broadcast frames*, 9–10

*multicast frames*, 9–10

*unicast frames*, 9–10

network diameter, 7–8

OSI (Open System Interconnect) model, 4–11, 14, 82–113

#### **802.3ab 1000BASE-T Ethernet, 15**

#### **802.3u Fast Ethernet, 12–13**

full-duplex operations, 13–14, 82–113

#### **802.3z 1000BASE-X Ethernet, 15–16**

---

## **A**

### **AARP (AppleTalk Address Resolution Protocol), 5**

**access layer (network hierarchy), 3**

**access points (APs). See APs (access points), 149**

**ACK frames, 57**

**acknowledgement frames, CSMA/CA, 29**

**active scanning, APs, 154**

**address fields (MAC frame), 53**

**Address Resolution Protocol (ARP), 5**

**addressing**

802.3 Ethernet, 6–7

broadcast addressing, 9

frames, stations, 9

**AES (Advanced Encryption Standard), 141, 146–147**

**agent discovery, Mobile IP, 163–165**

**AIFS (arbitration interframe space), 177**

**algorithms**

authentication, 131, 136–138

data integrity algorithms, 131

data privacy algorithms, 131

Michael MIC algorithm, 142

roaming algorithms, 153

**amplitude, data bits, applying to, 87**

**antennas**

- bandwidth, 191
- beamwidth, 188
- broadband, 191
- main lobes, 188
- minor lobes, 188
- radiation patterns, 187–189
- radios, 186–187
  - properties, 187–193, 197, 200–203*
  - types, 192–193*
- WLANs, 192

**AppleTalk Address Resolution Protocol (AARP), 5****AppleTalk over Ethernet, Ethertype value, 5****applications, operations, roaming, 150****APs (access points), 149**

- mobility, 149
- roaming, 149
  - 802.11 roaming, 150*
  - active scanning, 154*
  - application operations, 150*
  - duration, 152–153*
  - Layer 2 roaming, 153–160*
  - Layer 3 roaming, 160–161*
  - nomadic roaming, 149–150*
  - passive scanning, 154*
  - preemptive AP discovery, 155–156*
  - roaming domains, 151–152*
  - roam-time AP discovery, 155–157*
  - seamless roaming, 149*

**routing**

- Layer 3 routing, 151–152, 156–170*
- tunneling, 169–170*

**arbitration interframe space (AIFS), 177****ARP (Address Resolution Protocol), 5****association process, station connectivity, 45–47****association request frames, 72****association response frames, 72****ATM frames, 76****attacks, bit flipping attacks, 129****authentication**

- 802.11 standards, 124–125
- algorithms, 131, 136–138
- EAP (Extensible Authentication Protocol), 132–133
- framework, 131–136
- MAC address authentication, 125
  - vulnerabilities, 126*
- mutual authentication, 133
- one-way authentication, 133
- open authentication, 124
  - vulnerabilities, 126*
- shared key authentication, 125
  - vulnerabilities, 126–127*

**authentication frames, 70–71****authentication process, station connectivity, 44****auto negotiation, Gigabit Ethernet, 17–19****B****bandwidth, antennas, 191****Banyan Systems, Ethertype value, 5****basic service sets (BSSs), 23****beacon frames, 67–68**

beamwidth, antennas, 188  
bit flipping attacks, 129  
block ciphers, 119  
Bluetooth, 225–229  
“break before make” roaming, 150  
broadband, antennas, 191  
broadcast addressing, 9  
broadcast domains, 8, 151  
    frame collisions, 8  
broadcast packets, Mobile IP registration,  
    166  
BSSs (basic service sets), 23

## C

capacity-oriented WLANs, 211–212  
care-of address (CoA), Mobile IP, 162  
carrier sense, CSMA/CA, 25–26  
carrier sense multiple access/collision detect  
    (CSMA/CD), 21  
CCA modes, 2.4 GHz band, 114  
CCoA (co-located care-of address), Mobile  
    IP, 162  
cells, TDMA (time-division multiple access)  
    cells, 149  
CF parameter set IE, 802.11 management  
    frames, 61  
CF-End frames, 57–58  
CFP (Contention Free Period), 34  
Challenge Handshake Authentication  
    Protocol (CHAP), 134  
challenge text IE, 802.11 management  
    frames, 62

CHAP (Challenge Handshake  
    Authentication Protocol), 134  
CoA (care-of address), Mobile IP, 162  
cochannel overlap, QoS (quality of service),  
    174–175, 180–183  
coding, 802.11 PHYs, 84–85  
collisions  
    CSMA/CD (carrier sense multiple access/  
        collision detect), 21  
    Ethernet frames, 7  
colocated care-of address (CCoA), Mobile  
    IP, 162  
Contention Free Period (CFP), 34  
control frames  
    802.11 control frames, 54  
        ACK frames, 57  
        CF-End frames, 57–58  
        CTS frames, 56  
        PS-Poll frames, 54–55  
        RTS frames, 55–56  
    802.11 MAC, 50  
  
Core layer (network hierarchy), 3  
coverage-oriented WLANs, 210–211  
    phased AP deployment, 212–213  
CSMA/CA, 802.11 WLANs, 24–25  
    acknowledgment frame, 29  
    carrier sense, 25–26  
    DCF, 26–28  
    hidden node problem, 30–32  
    RTS/CTS, 30–32  
CSMA/CD (carrier sense multiple access/  
    collision detect), 7, 21  
CTS frames, 56

## D

**data bits, amplitude, applying to, 87**

**data encryption, 118–119, 139–141**

802.11 standards, 121–123

block ciphers, 119

feedback modes, 121

initialization vectors, 120

stream ciphers, 119

WEP, 121

*static WEP key management, 130*

*vulnerabilities, 128–130*

**data field (Ethernet frames), 6**

**data frames**

802.11 data frames, 76–78

802.11 MAC, 50

**data integrity, 131, 141–144**

**data link layer (OSI), 4**

**data privacy, 139–141**

**data privacy algorithms, 131**

**DBPSK modulation, DSSS WLANs, 82–113**

**DCF, CSMA/CA, 26–28**

**deauthentication frames, 71**

**decapsulation, Mobile IP registration, 166**

**decibel values, radios, 186**

**deployments, 207–209**

802.1x, 220–222

management, 222–223

methodologies, 209–213, 218–222

*capacity-oriented WLANs, 211–212*

*coverage-oriented WLANs, 210–211*

*phased AP deployment, 212–213*

site surveys, 213–216

*conducting, 218–219*

*tools, 217*

upper-layer considerations, 219

**design, WLANs, 237**

enterprise branch offices, 242–246

healthcare, 241–242

public access, 247–249

public safety, 249–251

retail stores, 237–241

schools, 246–247

telecommunication, 242–246

**destination MAC address field (Ethernet frames), 5**

**dipole antennas, 192**

**direct sequence spread spectrum (DSSS).**

*See DSSS WLANs*

**directional antennas, 192**

**disassociation frames, 75**

**Distribution layer (network hierarchy), 3**

**domains**

broadcast domains, 8, 151

roaming between, 160–161

roaming domains, 151–152

**DQPSK modulation, DSSS WLANs, 97–98**

**DS parameter set IE, 802.11 management frames, 60–61**

**DSSS WLANs, 93–96**

802.11 DSSS, 93–95

DBPSK modulation, 82–113

DQPSK modulation, 97–98

**duration, roaming, 152–153**

**duration/ID field (MAC frame), 53**

## E

**EAP (Extensible Authentication Protocol), 132–133**

**EAP-MD5 (EAP-Message Digest 5), 134**

**EAP-Message Digest 5 (EAP-MD5), 134**

**EAP-PEAP (EAP-Transport Layer Security), 133**

**EAP-Transport Layer Security (EAP-PEAP), 133**

**EDCF (Enhanced DCF), 176–183**

**education, WLAN design, 246–247**

**effective radiated power (ERP), 189**

**EIRP (effective isotropic radiated power), 189**

**electromagnetic transmissions, 185**

**encapsulation, IP packets, 169**

**encryption, 118–119, 139–141**

802.11 standards, 121–123

AES (Advanced Encryption Standard), 141, 146–147

block ciphers, 119

feedback modes, 121

initialization vectors, 120

stream ciphers, 119

TKIP encryption, 142

WEP, 121

*static WEP key management, 130*

*vulnerabilities, 128–130*

**enhanced keys, managing, 144–146**

**enterprise branch offices, WLAN design, 242–246**

**ERP (effective radiated power), 189**

**ESSs (extended service sets), 802.11**

**WLANs, 23–24**

## Ethernet

802.3 Ethernet, 3

*addressing, 6–7*

*common media, 11–12*

*CSMA/CD architecture, 7*

*Ethernet slot time, 7–8*

*frames, 4–6, 9–10*

*network diameter, 7–8*

*OSI (Open System Interconnect)*

*model, 4–14, 82–113*

802.3u Fast Ethernet, 12–13

*full-duplex operations, 13–14, 82–113*

common media, 11–12

frames, collisions, 7

Gigabit Ethernet, 15

*802.3ab 1000BASE-T Ethernet, 15*

*802.3z 1000BASE-X Ethernet, 15–16*

*auto negotiation, 17–19*

*slot time, 4–11, 14–17, 82–113*

## Ethernet slot time

802.3 Ethernet, 7–8

Gigabit Ethernet, 4–11, 14–17, 82–113

## EtherTalk, Ethertype value, 5

## Ethertype values, 5

## Europe, frequency hopping patterns, 89

## extended service sets (ESSs), 802.11 WLANs, 23–24

## Extensible Authentication Protocol (EAP), 132–133

## F

- FA (foreign agent), Mobile IP, 162**
- far field, antennas, 187**
- FCS (frame check sequence) field**
  - (Ethernet frames), 6
- FCS field (MAC frame), 53**
- FDD (frequency division duplex), 185**
- feedback modes, encryption, 121**
- FH parameter set IE, 802.11 management frames, 60**
- FHSS PLCP, 90–91**
- FHSS PMD-GFSK modulation, 91–93**
- FHSS WLANs, 88–89**
  - FHSS PLCP, 90–91
  - FHSS PMD-GFSK modulation, 91–93
  - patterns, 89
- fire departments, WLAN design, 249–251**
- fixed field elements, 802.11 fixed field elements, 63–66**
- foreign agent (FA), Mobile IP, 162**
- formats, frames, 802.11 WLANs, 50–78**
- four-way handshakes, 145**
- fragmentations, frames, 802.11 WLANs, 32–33**
- frame control field (MAC frame), 51**
- frames**
  - 802.3 Ethernet, 4–6
  - 802.11 control frames, 54
    - ACK frames*, 57
    - CF-End frames*, 57–58
    - CTS frames*, 56
    - PS-Poll frames*, 54–55
    - RTS frames*, 55–56
  - 802.11 data frames, 76–78
  - 802.11 fixed field elements, 63–66
  - 802.11 management frames, 58, 66
    - association request frames*, 72
    - association response frames*, 72
    - ATM frames*, 76
    - authentication frames*, 70–71
    - beacon frames*, 67–68
    - CF parameter set IE*, 61
    - challenge text IE*, 62
    - deauthentication frames*, 71
    - disassociation frames*, 75
    - DS parameter set IE*, 60–61
    - FH parameter set IE*, 60
    - IBSS parameter set IE*, 62
    - probe request frames*, 67, 69–70
    - reassociation request frames*, 73
    - reassociation response frames*, 74–75
    - SSID IE*, 59
    - supported rates IE*, 59–60
    - TIM IE*, 61–62
  - acknowledgment frames, 29
  - addressing stations, 9
  - collisions, broadcast domains, 8
  - Ethernet
    - broadcast frames*, 9–10
    - collisions*, 7
    - multicast frames*, 9–10
    - unicast frame*, 9–10
  - fragmentations
    - 802.11 WLANs, 32–33
  - per-frame keying, 139
  - SIFS (short interframe space), 29
- framework, authentication, 131–136**
- free space optics (FSO), 231–233**

**frequency division duplex (FDD).** *See* FDD  
(frequency division duplex)

**frequency hopping**

802.11 WLANs, 88–93

patterns, 89

**frequency hopping spread spectrum  
(FHSS).**

*See* FHSS WLANs

**from DS field (MAC frame),** 53

**front-to-back ratio radiation pattern,**  
189–190

**FSO (free space optics),** 231–233

**full-duplex operations, 802.3u Fast**

Ethernet,

13–14, 82–113

## G

---

**Generic Routing Encapsulation (GRE),** 166

**Gigabit Ethernet, 15**

802.3ab 1000BASE-T Ethernet, 15

802.3z 1000BASE-X Ethernet, 15–16

auto negotiation, 17–19

slot time, 4–17, 82–113

**global system for mobile (GSM)**

communications, 149

**group addressing, 9**

**GSM (global system for mobile)**

communications, 149

## H

---

**HA (home agent), Mobile IP, 162**

**half-duplex mediums, QoS (quality of  
service), 174**

**half-power beamwidth, antennas, 189**

**HCF (hybrid coordination function),  
176–183**

**healthcare, WLAN design, 241–242**

**hidden nodes**

CSMA/CA, 30–32

QoS (quality of service), 175

**hierarchies, networks, logical units, 3**

**home agent (HA), Mobile IP, 162**

**hospitals, WLAN design, 249–251**

**hybrid coordination function (HCF),  
176–183**

## I–K

---

**IBM Systems Network Architecture (SNA)  
Services over Ethernet, 5**

**IBSSs (independent basic service sets), 21–22**  
management frames, 62

**idealized nonrealizable antennas, 192**

**impedance, RF devices, 191**

**initialization vectors, 120**

**in-phase components (sinusoids), 87**

**integrity (data), 141–144**

**interleaving, 802.11 PHYs, 85–86**

**Internetwork Packet Exchange (IPX), 5**

**IP (Internet Protocol), 5**

packets, encapsulation, 169

**IP Version 6, Ethertype value, 5**



**IPX (Internetwork Packet Exchange), 5**  
**ISM band frequencies, unlicensed wireless, 199–201**

2.4 GHz power levels, 201

**isotropic radiators, 187**

**IVs (initialization vectors), 120–121**

**Japan, frequency hopping patterns, 89**

**key streams, deriving, 127**

**keys**

enhanced keys, managing, 144–146

master keys, 144

per-frame keying, 140

static WEP keys, managing, 130

## L

**LANs, 3**

*See also* WLANs

design, 237

QoS, 173–183

**LAT (Local Area Transport), 5**

**Layer 2 roaming, 153, 157–160**

locations, determining, 154–157

roaming algorithms, 153

**Layer 3 roaming, 160–161**

**Layer 3 routing**

Mobile IP, 151–152, 156–170

tunneling, 169–170

**Lifetime field (Mobile IP registration), 166**

**linear polarization, WLANs, 190**

**Local Area Transport (LAT), 5**

**logical link (LLC) sublayer (OSI), 4**

**logical units, network hierarchies, 3**

## M

**MAC**

address authentication, 125

address tables, updating, 160

layer operations, 40

*frame formats, 50–78*

*power save operations, 47–50*

*standards, 126*

*station connectivity, 40–47*

**main lobes, antennas, 188**

**management frames**

802.11 MAC, 50

802.11 management frames, 58, 66

*association request frames, 72*

*association response frames, 72*

*ATM frames, 76*

*authentication frames, 70–71*

*beacon frames, 67–68*

*CF parameter set IE, 61*

*challenge text IE, 62*

*deauthentication frames, 71*

*disassociation frames, 75*

*DS parameter set IE, 60–61*

*FH parameter set IE, 60*

*IBSS parameter set IE, 62*

*probe request frames, 67–70*

*reassociation request frames, 73*

*reassociation response frames, 74–75*

*SSID-IE, 59*

*support rate IE, 59–60*

*TIM IE, 61–62*

- master keys, 144**
- media, 802.3 Ethernet, 11–12**
- medium access mechanisms, 802.11**
  - WLANs, 24**
    - CSMA/CA, 24–32
    - frame fragmentations, 32–33
    - PCF, 33–36
- message integrity check (MIC), 139**
- MIC (message integrity check), 139**
- Michael MIC algorithm, 142**
- minimal encapsulation, Mobile IP**
  - registration, 166
- minor lobes, antennas, 188**
- MN (mobile node), Mobile IP registration, 151–156**
- Mobile IP, 151–170**
  - agent discovery, 163–165
  - CCoA (co-located care-of address), 162
  - CoA (care-of address), 162
  - FA (foreign agent), 162
  - HA (home agent), 162
  - MN (mobile node), 162
  - registration, 151–156
- mobility, 149**
- modulation, 802.11 PHYs, 86–87**
- more data field (MAC frame), 53**
- more fragments field (MAC frame), 53**
- multicast addressing, 9**
- mutual authentication, one-way**
  - authentication, compared, 133

## N–O

---

- near field, antennas, 187**
- negotiation, auto negotiation, Gigabit Ethernet, 17–19**
- network diameter, 802.3 Ethernet, 7–8**
- network hierarchies, logical units, 3**
- nomadic roaming, 149–150**
- North America, frequency hopping patterns, 89**
  
- OFDM, 104–106**
- omnidirectional antennas, 192**
- one-way authentication, mutual**
  - authentication, compared, 133
- open authentication, 124–126**
- Open System Interconnect (OSI). *See* OSI (Open System Interconnect)**
- order field (MAC frame), 53**
- OSI (Open System Interconnect), 4**
  - 802.3 Ethernet, 4–14, 82–113

## P–Q

---

- packets, IP packet encapsulation, 169**
- passive scanning, APs, 154**
- patch antennas, 192**
- payload field (Ethernet frames), 6**
- PBCC modulation, 101–102**
- PCF, 802.11 WLANs, 33–36**
  - CFP (Contention Free Period), 34
  - PIFS (priority interframe space), 34–35
- per-frame keying, 139–140**
- phased AP deployment, 212–213**

**PHYs (physical layers), 802.11, 81–83**

- coding, 84–85
- interleaving, 85–86
- modulation, 86–87
- scrambling, 84
- symbol mapping, 86–87

**PIFS (priority interframe space), 34–35****police departments, WLAN design, 249–251****power limitations, U-NII bands, 204****power management field (MAC frame), 53****power save operations, 802.11 WLANs, 47–50****preamble field (Ethernet frames), 5****preemptive AP discovery, 153–156****priority interframe space (PIFS), 34****probe process, station connectivity, 40–44****probe request frames, 67–70****properties, radio antennas, 187–193, 197, 200–203****protocol version field (MAC frame), 51****PS-Poll frames, 54–55****public access, WLAN design, 247–249****public safety, WLAN design, 249–251****QoS (quality of service), 802.11 WLANs, 173–174**

- cochannel overlap, 174–175, 180–183
- EDCF (enhanced DCF), 176–183
- half-duplex mediums, 174
- hidden nodes, 175

**quadrature components (sinusoids), 87****R****radiation patterns, antennas, 186–189****radios, 185**

## antennas, 186–187

*bandwidth, 191**beamwidth, 188**main lobes, 188**minor lobes, 188**properties, 187–193, 197, 200–203**radiation patterns, 187–189**types, 192–193**WLANs, 192*

## decibel values, 186

## electromagnetic transmissions, 185

## power, 186

## receivers, 193

*802.11a minimum radio performance, 194**802.11b minimum radio performance, 193–194**sensitivity calculation, 193*

## system performance, 195–198

## two-way radios, 185

*FDD (frequency division duplex), 185**TDD (time division duplex), 185*

## U-NII band frequencies, 201–202

*power limitations, 204**spectral masks, 202–203*

## unlicensed wireless, 198–199

*2.4 GHz ISM band transmit power levels, 201**ISM band frequencies, 199–201*

## watts, 186

**reassociation request frames, 73**

**reassociation response frames, 74–75**

**receivers**

radios, 193

*802.11a minimum radio performance,*  
*194*

*802.11b minimum radio performance,*  
*193–194*

*sensitivity calculation, 193*

**registration, MN (mobile node), 151–170**

**repeater APs, 37**

**retail stores, WLAN design, 237–241**

**retry field (MAC frame), 53**

**reverse tunneling, 170**

Mobile IP registration, 166

**RF devices, impedance, 191**

**roaming, 149, 248**

802.11 roaming, 150

active scanning, 154

application operations, 150

between subnets, 161

Layer 2 roaming, 153, 157–160

*locations, 154–157*

*roaming algorithms, 153*

Layer 3 roaming, 160

*between domains, 160–161*

nomadic roaming, 149–150

preemptive roaming, 155–156

roaming domains, 151–152

roaming duration, 152–153

roam-time AP discovery, 155, 157

seamless roaming, 149

**roam-time AP discovery, 153–157**

**routing, Layer 3 routing**

Mobile IP, 151–152, 156–170

tunneling, 169–170

**RTS frames, 55–56**

**RTS/CTS frames, 30–32**

---

## S

**scanning**

active scanning, 154

passive scanning, 154

**schools, WLAN design, 246–247**

**scrambling, 802.11 PHYs, 84**

**seamless roaming, 149**

**security, 118–146**

802.11 specifications, 116–117

*authentication mechanisms, 124–125*

*encryption, 121–123*

*vulnerabilities, 126–130*

*wireless, 117–146*

attacks, bit flipping attacks, 129

authentication

*algorithms, 131, 136–138*

*EAP (Extensible Authentication*  
*Protocol), 132–133*

*framework, 131–136*

data integrity, 131, 141–144

data privacy algorithms, 131

encryption, 118–119, 139–141

*802.11 standards, 121–123*

*AES (Advanced Encryption*  
*Standard), 141, 146–147*

- block ciphers*, 119
- feedback modes*, 121
- initialization vectors*, 120
- stream ciphers*, 119
- TKIP encryption*, 142
- enhanced key management, 144–146
- keys
  - master keys*, 144
  - per-frame keying*, 139–140
- mutual authentication, 133
- one-way authentication, 133
- vulnerabilities
  - MAC address authentication*, 126
  - open authentication*, 126
  - shared key authentication*, 126–127
  - WEP*, 128–130
- sensitivity calculation, radio receivers**, 193
- sequence field (MAC frame)**, 53
- service sets**, 21
  - BSSs (basic service sets), 23
  - ESSs (extended service sets), 23
  - IBSSs (independent service sets), 21
- SFD (start of frame delimiter) field (Ethernet frames)**, 5
- shared key authentication**, 125–127
- short interframe space (SIFS)**, 29
- simultaneous bindings, Mobile IP registration**, 166
- sinusoids**, 87
- site surveys**, 213–216
  - conducting, 218–219
  - tools, 217
- slot time (Gigabit Ethernet)**, 4–17, 82–113

- source address field (Ethernet frames)**, 5
- spectral masks, U-NII bands**, 202–203
- spurious emissions, U-NII bands**, 202–203
- SSID-IE, 802.11 management frames**, 59
- static WEP keys, managing**, 130
- station connectivity, 802.11 WLANs**, 40–47
- stations, frames, addressing**, 9
- stream ciphers**, 119
- subnets, roaming between**, 161
- subtype field (MAC frame)**, 51
- supported rate IE, 802.11 management frames**, 59–60
- symbol mapping, 802.11 PHYs**, 86–87
- system performance, radios**, 195–198

## T

- TDD (time division duplex)**, 185
- TDMA (time-division multiple access) cells**, 149
- telecommunication, WLAN design**, 242–246
- TIM IE, 802.11 management frames**, 61–62
- TKIP encryption**, 142
- TLV (type/length value) field (Ethernet frames)**, 5
- topologies, 802.11 WLANs**, 21–24
- transmissions, electromagnetic transmissions**, 185
- transmit opportunity (TXOP)**, 177
- tunneling**
  - Layer 3 routing, 169–170
  - reverse tunneling, 170

two-way radios, 185  
TXOP (transmit opportunity), 177  
type field (MAC frame), 51

## U–V

---

UDP (User Datagram Protocol), 150  
ultra wide band (UWB), 229–231  
unicast addressing, 9  
unicast power save operations, 802.11  
    WLANs, 47–50  
U-NII band frequencies, 201–204  
universal clients, 802.11 WLANs, 38  
unlicensed wireless, 198–199  
    2.4 GHz ISM band transmit power levels,  
    201  
    ISM band frequencies, 199–201  
upper layers, deployments, 219  
User Datagram Protocol (UDP), 150  
UWB (ultra wide band), 229–231  
  
vertical polarization, 190  
voltage standing wave ratio (VSWR), 191  
VSWR (voltage standing wave ratio), 191  
vulnerabilities  
    802.11 security, 126–130  
    security  
        MAC address authentication, 126  
        open authentication, 126  
        shared key authentication, 126–127  
        WEP, 128–130

## W–Z

---

watts, radios, 186  
WEP (Wired Equivalent Privacy), 116  
    frame encryption, 121  
    static WEP keys, managing, 130  
    vulnerabilities, 128–130  
WEP field (MAC frame), 53  
whitening. *See* scrambling  
Wired Equivalent Privacy (WEP). *See* WEP  
    (Wired Equivalent Privacy)  
wireless bridges, 802.11 WLANs, 39  
WLANs (Wireless LANs), 3  
    802.11, 21, 36, 88  
        *frequency hopping, 88–93*  
        *MAC layer operations, 40–78*  
        *medium access mechanisms, 24–36*  
        *QoS (quality of service), 173–183*  
        *repeater APs, 37*  
        *security, 118–125, 127, 129–146*  
        *topologies, 21–24*  
        *universal clients, 38*  
        *wireless bridges, 39*  
        *workshop bridges, 38*  
    802.11a, 102  
        802.11a OFDM PLCP, 102–104  
        802.11j, 102  
        OFDM, 104–106  
    802.11b, 98  
        802.11b HR-DSS PLCP, 98–99  
        802.11b PMD-CCK modulation,  
        100–101  
        PBCC modulation, 101–102  
    802.11g WLANs, 111–113

- 
- antennas, 192
  - capacity-oriented WLANs, 211–212
  - coverage-oriented WLANs, 210–211
  - deployments, 207–209
    - methodologies*, 209–213, 218–222
  - design, 237
    - enterprise branch offices*, 242–246
    - healthcare*, 241–242
    - public access*, 247–249
    - public safety*, 249–251
    - retail stores*, 237–241
    - schools*, 246–247
    - telecommunication*, 242–246
  - DSSS WLANs, 93–96
    - 802.11 DSSS*, 93–95
    - DBPSK modulation*, 82–113
    - DQPSK modulation*, 97–98
  - FHSS WLANs, 88–89
    - FHSS PLCP*, 90–91
    - FHSS PMD-GFSK modulation*, 91–93
    - patterns*, 89
  - linear polarization, 190
  - U-NII band frequencies, 201–202
    - power limitations*, 204
    - spectral masks*, 202–203
  - unlicensed wireless, 198–199
    - 2.4 GHz ISM band transmit power levels*, 201
    - ISM band frequencies*, 199–201
  - workshop bridges, 38**
  
  - Yagi antennas, 192**
  - Yagi-Uda antennas, 192**