INDEX

Numerics

802.11 standards, 291
802.11a standard, 35–36
802.11g standard, preratification, 37
802.11i authentication standard, 224–226
802.1x authentication standard, 222–224

A

AAA (authentication, authorization, and accounting), 238
access, 269
access layer (hierarchical networks), 100
access points versus access layer, 102
access technologies, 26
accounting management, 257
ACS (Cisco Secure Access Control Servers), 296
ACU (Aironet Client Utility), 293
ad-hoc WLAN networks, 18
AES (Advanced Encryption Standard), 220
aggregate annualized monetary benefit, calculating, 78
alerts, 275–276
analytical processes, 43
application layer, 14
application matrices, 121–122
AP (access points)
client-to-AP ratio, 170, 172
configuring, 201
Griffith University case study, 345, 355
directional antennas, 237
installing, 200
Layer 2 address spoofing, preventing, 236
management policy, implementing, 234–235
outdoor coverage, 313
physical security, 237
rogue, 125, 218
detecting, 247, 262
responding to, 247–248
securing, 233–235, 237
signal strength, 293
minimizing, 236
SSID, 234
testing, 201–202
architectural guidelines, 161
checklist, 203
defining scope of WLAN, 164
deployment timeframe, 164–166
infrastructure requirements, 183
Lifespan case study, 318–319
operational support structure, establishing, 169

requirements, assessing
802.11 standards,, 291
assessing, 287
client-to-AP ratio, 292–293
global naming standards, 294
radio cell architecture, 294
roaming, 293
signal strength, 293
topology, 289–291
security posture, 166, 184
target audience of WLAN, 167–169
understanding goal of WLAN, 162–163
ASD (application specific devices), 115
assessing WLAN architecture requirements, 287
802.11 standards, 291
client-to-AP ratio, 292–293
global naming standards, 294
radio cell architecture, 294
roaming, 293
signal strength, 293
topology, 289–291
asset tags, 154, 263
battery life, 156
assets, TCO, 64
per-user, 66
Value Chain framework, 67–69
attenuation, 9
authentication, 61, 211
802.11i, 224–226
802.1x, 222–224
EAP, 227–228
machine-based, 214
mitigating security threats, 222, 225–226
user-based, 214
WPA, 224
automatic site surveys, 198
autonomous AP architecture, 259
availability of AAA, 238
average monthly benefit per user, calculating, 77

B

bandwidth
as limitation of WLANs, 54–55
factors influencing
antennas, 28–29
attenuation, 29
distortion, 29
interference, 29
modulation, 27
multipath, 29
path loss, 28–29
power, 28–29
base station model, 17
battery life of asset tags, 156
BBSM (Building Broadband Services Manager), 302
benchmarking, 171
benefits of global WLAN solution, 309–310
broadcasting video, 141
budgetary requirements, estimating, 126
building secure WLANs, best practices, 229–248
"built-in" traffic analysis tools, 281
bus topology, 8
business model
for WLAN deployment, 286–287
Griffith University education case study, 341
Lifespan case study, 316–318
manufacturing industry case study, 330–332

C

cabling, Griffith University case study, 355
CAGRs (compounded annual growth rates), 17
calculating
aggregate annualized monetary benefit of WLANs, 78
average monthly benefit per user, 77

daily organizational productivity, 76
IRR, 93
monetized productivity benefit per WLAN, 74
NPV, 89–90, 92
office employee productivity benefits, 77
payback period, 87–88
ROI, 86–87
total productivity benefit of WLANs, 72–73
traveling employee productivity benefits, 78

calculating location, methods of, 154–155

canned reports, 273

case studies
business model, 286–287
client management, 297
deployment issues, 305–308
education, Griffith University, 340
"Smart Zones," 340–342
AP configuration, 355
AP settings, 345
benefits, measuring, 360
best practices, 357–358
business model, 341
cabling, 355
challenges faced, 356
client management, 349
global naming standards, 346
network management, 347–348
phases of deployment, 351
project management, 355
radio cell architecture, 346
security, 350–351
signal strength, 346
site surveys, 353
three-tiered service and support system, 348–349
topology, 344
wireless equipment, 347
WLAN standards, 345
enhanced services, 301
wireless guest networking, 302–304
wireless voice services, 301
healthcare
architectural principles, 318–319
business model, 316–318
enterprise WLAN deployment, 325–326
network management, 323
patient tracking and telemetry, 327–328
RFID technology, 328
security, 324
site surveys, performing, 326
WLAN design, 320–322
manufacturing industry
business model, 330–332
coverage, 333–334
guest access, 336
rogue AP detection, 337
security concerns, 332
throughput, 334–335
VoIP, 337
WLAN deployment, 335
security, 304
technology considerations
architectural requirements, 287–294
client management, 297
network management, 296
service anad support, 298–300

CBC-MAC (Cipher Block Chaining Message Authentication Code), 220

CCX (Cisco Client Extensions), 121, 297

CCX (Cisco Compatible Extension) program, 324

CDMA (Code Division Multiple Access), 22

cellular telephone networks, LBS, 151

centralized management model versus distributed management model, 258
centralized self-service model, 272
centrally funded deployment strategies, 106
Christensen, Clayton, 4
Cisco Aironet 350 Series Access Point, 294
Cisco four-tier support model, 299–300
Cisco NexGen WLAN project, 310–314
Cisco Wireless IP Phone 7920, 302
client management, 191, 265–267, 297
Griffith University case study, 349
manual client configuration, 272
client security, 243–245
client software, 202
client to access point ratio, 184
client-based reporting, 246
client-funded deployment strategies, 107–108
clients checklist, 206
client-to-AP ratio, 170–172, 292–293
coexistence of IEEE standards, 37
collaborative processes, 43
communication plan, implementing, 189
comparing
centralized and distributed management models, 258
in-house deployment versus outsourced deployment, 181
wired and wireless LANs, 51–52, 55
complementary services (WLANs), 130–131
compute assets, 49
configuration management, 257
manual client configuration, 272
configuring APs, 201
consumer retail industry, identifying key application areas in Value Chain framework, 68
convenience as benefit of WLANs, 53
core layer (hierarchical networks), 100
CoS (class of service), 55
cost of support, 300
cost savings of WLANs, 309–310
cost-benefit analysis, 64
of hybrid wired and wireless LANs, 59
of wired-only LANs, 57
of wireless-only LANs, 58
CPOM (Computer Physician Order Management) application, 318
CSMA (Carrier Sense Multiple Access), 19
CSMA/CA (Carrier Sense Muliple Access/Collision Avoidance), 26

D

Daemen, Joan, 221
daily organizational productivity, calculating, 76
data link layer, 12–13
defining
home wireless networking policies, 240, 243
security policy, 233
deploying
enterprise WLANs
AAA architecture dependencies, 186
architecture scalability, 122–123
business model, 286–287
case study, 305–308
communication plan, 189
impact on application portfolio, 121–122
in manufacturing setting, 335
Lifespan healthcare case study, 325–326
methodology and project planning checklist, 205

planning phase, 109–118, 123–127
preparation phase, 98–100, 103–108
regulatory issues, 190
security standards, 186
support plan, 187
timeframe as architectural component, 164–166
guest networks, 149–150
reasons for, 143–144
WLAN location services, 152
in transport and shipping companies, 154
deployment checklist, 203, 207–208
for architecture, 203
for clients, 206
for deployment methodology and project planning, 205
for infrastructure, 207
design considerations
client-to-AP ratio, 170–172
roaming, 172–174
detecting rogue APs, 247
developing project plan, 125
directional antennas, 237
discount rate, selecting, 89
disruptive technology, 4
distortion, 10
distributed management model versus centralized management model, 258
distribution layer (hierarchical networks), 100
distribution mechanism of video traffic, 138–139
DMZ, 302
documents, developing project plan, 125
DSSS (Direct Sequence Spread Spectrum), 24, 26
dual-band devices, 32
duplex technologies, 26

E

EAP (Extensible Authentication Protocol), 227–228
EAP-FAST (Flexible Authentication via Secure Tunneling), 305, 313
EAP-LEAP (Lightweight Extensible Authentication Protocol), 227
edge devices, 258
edge layer (hierarchical networks), 100
education case study, 340
"Smart Zones," 340–342
AP configuration, 355
AP settings, 345
benefits, measuring, 360
best practices, 357–358
business model, 341
cabling, 355
challenges faced, 356
client management, 349
global naming standards, 346
network management, 347–348
phases of deployment, 351
project management, 355
radio cell architecture, 346
security, 350–351
signal strength, 346
site surveys, 353
three-tiered service and support system, 348–349
topology, 344
wireless equipment, 347
WLAN standards, 345
employee productivity, impact of WLANs, 309–310
encoding methods, 22
encryption, 62
AES, 220
mitigating security threats, 219–220
WEP, 220

enhanced services, 301
wireless guest networking, 302–304
wireless voice services, 301
entertainment/leisure industries, deploying WLAN location services, 153
environmental factors affecting WLAN deployment, 104–105
governmental, 176–177
physical attributes of surroundings, 175
RF environment, 176
estimating
budgetary requirements, 126
resource requirements, 126
ETSI (European Telecommunications Standards Institute), 190
extending coverage outdoors, 313

F

facilitating value creation process, top-down approach, 44–49
fan-out ratio, 53
fast Layer 2 roaming, 135
fast roaming, 173
FCAPS
accounting management, 257
configuration management, 257
limitations of, 258
performance management, 257
security management, 258
FCC (Federal Communications Commission), 190
FDMA (Frequency Division Multiple Access), 23
financial services industry, identifying key application areas in Value Chain framework, 68
four-tier support model, 299–300
frequency division duplexing, 26
friendly rogues, 337
FUD (Fear, Uncertainty, Doubt) factor, 124
funding strategies
centrally funded, 106
client-funded, 107–108
group funded, 106
subscription funded, 108
future of WLANs, 310–314

G

global naming standards, 294
Griffith University case study, 346
goal of WLANs as architectural component, 162–163
Gore, Rich, 292
governmental considerations, 176–177
GRE, 303
"gray IT" deployments, 286
Griffith University case study, 340
"Smart Zones," 340–342
AP configuration, 355
AP settings, 345
benefits, measuring, 360
best practices, 357–358
business model, 341
cabling, 355
challenges faced, 356
client management, 349
global naming standards, 346
network management, 347–348
phases of deployment, 351
project management, 355
radio cell architecture, 346
security, 350–351
signal strength, 346
site surveys, 353
three-tiered service and support system, 348–349
topology, 344
wireless equipment, 347
WLAN standards, 345

group-funded deployment strategies, 106
guest access on manufacturing company enterprise WLAN, 336
guest networking
implementing, 149–150
reasons for deploying, 143–144
requirements for, 145, 148
SSIDs, 145
guest user class, 117

H

hackers, profile of, 216
hashing, 62
TKIP, 221
HCF (Hybrid Coordination Function), 132
healthcare industry, deploying WLAN location services, 152
heat maps, 263
Hemendinger, David, 316
hierarchical network model, 100
hierarchy of organizational needs, 82–84
"high bandwidth" applications, 120
HIPAA (Health Insurance Portability and Accountability Act of 1996), 325
history of WLANs, 14
home wireless networking policies, defining, 240, 243
host management, 265
hot-desk user class, 116

I

identifying risks, 79, 81
IDS (intrusion detection systems), 248
IEEE (Institute for Electrical and Electronics Engineers), 15
coexistence, 37
IEEE 802.11b standard, 33
IEEE 802.11g standard, 33, 35
implementing
AP management policies, 234–235
communication plan, 189
guest networks, 149–150
voice on WLANs, 134–137
WLAN video, 140–142
implementing enterprise WLANs
case study, 305–308
infrastructure checklist, 207
infrastructure layer, 49
asset classes, 50
security
authentication, 61
encryption, 62
hashing, 62
network admission control, 61
infrastructure management, 191
infrastructure mode, 19
infrastructure requirements for WLAN deployment
connectivity, 103
console access, 104
power, 103–104
in-house deployment versus outsourced deployment, 181
in-house management, 254
installing APs, 200
interception of transmitted data, 217
interference, 11
medical field standards, 322
intermittent connectivity of mobile endpoints, 269
internally developed tools, 282
inventory taking, enhancing effectiveness through WLAN location services, 153
investment in IT infrastructure, 41
investments
IRR, calculating, 93
NPV, calculating, 89–90, 92
payback period, calculating, 87–88
ROI, 86
calculating, 87

IRR (internal rate of return), 85
calculating, 93
isotropic antennae, 29
IT infrastructure, investment in, 41

L

launching production services, 203
Law of Large Numbers, 75
Layer 1, 7–9
Layer 2, 12–13
address spoofing, preventing, 236
Layer 3, 13
Layer 4, 13
Layer 5, 14
Layer 6, 14
Layer 7, 14
layers of hierarchical network model, 100
LBS (location-based services), 150, 263, 313
legal liability protection as motivation for guest networks, 144
legislation, Sarbanes-Oxley Act, 325
Lifespan healthcare case study, 318
architectural principals, 318–319
business model, 316–318
CPOM, 318
enterprise WLAN deployment, 325–326
network management, 323
patient tracking and telemetry, 327–328
RFID technology, 328
security, 324
site surveys, performing, 326
WLAN design, 320
distaster recovery, 322
guest networking, 321
RF and interference, 322
limitations of FCAPS, 258
LLC sublayer, 12
location, methods of calculating, 154–155
location tags, 154
"low bandwidth" applications, 120
LWAPP (Lightweight Access Point Protocol), 291

M

MAC sublayer, 12
machine-based authentication, 214
malicious hackers, profile of, 216
management strategies, 253
for clients, 191
for infrastructure, 191
in-house management, 254
outsourced management, 255
user expectations of WLAN video, 142
management tools
third-party WLAN management tools, 278
vendor-specific WLAN management tools, 277–278
man-in-the-middle attacks, 217
manual site surveys, 199
manufacturing industry
case study
business model, 330, 332
coverage, 333–334
guest access, 336
rogue AP detection, 337
security concerns, 332
throughput, 334–335
VoIP, 337
WLAN deployment, 335
deploying WLAN location services, 153
Value Chain framework, identifying key application areas, 67
Maslow, Abraham, 81
measuring benefits of WLAN deployment on university setting, 360

medical industry, interference standards, 322
Meetinghouse Data Communications, 266
mesh topology, 8
Microsoft Excel, calculating NPV, 92
minimizing AP signal strength, 236
mitigating security threats, 219
with authentication, 222, 225–226
802.11i standard, 224–226
802.1x, 222–224
WPA, 224
with encryption, 219–220
with hashing, TKIP, 221
mobile devices, securing, 243
mobile endpoints, 268
intermittent connectivity, 269
mobile user class, 115
mobility
as benefit of WLANs, 52
value of, 2, 5
modulation, 27
monetized productivity benefit per WLAN, calculating, 74
multipath, 29
multiple access WLAN technologies, 22
multiplex technologies, DSSS, 24–26
OFDM, 25–26

N

Negroponte, Nicholas, 3
NEMA (National Electrical Manufacturers Association) enclosures, 105
NetFlow, 281
network admission control, 61
network layer, 13
network management, 296
Griffith University case study, 347–348
Lifespan case study, 323
platforms, 279
tools
built-in tools, 281
internally developed tools, 282
NetFlow, 281
RADIUS accounting, 281
SNMP, 280
syslog, 280
unique challenges to
dynamic nature of transport medium, 267–268
intermittent connectivity of mobile endpoints, 269
mobile nature of wireless endpoints, 269
mobility of endpoints, 268
network-based rogue AP detection, 247
NexGen WLAN project, 310–314
noise, 11
non-overlapping channels, 25
NPV (net present value), 85
calculating, 89–92

O

OFDM (Orthogonal Frequency Division Multiplexing), 25–26
office employee productivity benefits, calculating, 77
office space, security, 239
on-demand viewing, 140
operational support structure, establishing, 169
organizational ecosystem, 42
OSI reference model, 6
application layer, 14
data link layer, 12–13
network layer, 13
physical layer, 7–9
presentation layer, 14
session layer, 14
transport layer, 13
out-of-band management, 104

outdoor coverage, 313
outsourced deployment versus in-house deployment, 181
outsourced WLAN management, 255
overlay security solutions, 215

P

patient tracking and telemetry, Lifespan healthcare case study, 327–328
"pay as you go" deployment strategy, 108
payback period, 85
calculating, 87–88
PCAOB (Public Company Accounting Oversight Board), 325
peer layers, 6
performance management, 257
performing site surveys for Lifespan healthcare WLAN, 326
per-user TCO, 66
phases of deployment, Griffith University case study, 351
physical layer, 7–9
physical locations, 175
physical security of office space, 239
placement of WLANs, 175
planning phase of solutions lifecycle, 109–110
architecture scalability, 122–123
defining high-level program plan, 125–127
design considerations, 170
documenting project stakeholders, 111–114
environmental considerations, 175
governmental regulations, 176–177
identifying users, 114–118
impact on application portfolio, 121–122
security strategy, 123–125
PMBOK (Project Management Body of Knowledge), 109–111
PoE (Power over Ethernet), 103
Porter, Michael E., 67
Post Implementation Review, 358
post-installation acceptance test, 201
PPDIOO solutions lifecycle, 96, 253
planning phase, 109–110
architectural considerations, 122–123, 161, 165–169
defining high-level program plan, 125–127
design considerations, 170
documenting project stakeholders, 111–114
environmental considerations, 175
governmental regulations, 176–177
identifying users, 114–119
impact on application portfolio, 121–122
security strategy, 123–125
preparation phase, 98
environmental factors, 104–105
funding strategies, 106–108
identifying scope of deployment, 99
infrastructure requirements, 100, 103–104
pre-deployment tasks, 194
preparation phase of solutions lifecycle, 98
environmental factors, 104–105
funding strategies, 106–108
identifying scope of deployment, 99
infrastructure requirements, 100
connectivity, 103
console access, 104
power, 103–104
presentation layer, 14
preventing Layer 2 address spoofing, 236

primary users, 118
probabilistic nature of WLANs, 267
product demonstrations, accessing through guest networks, 144
production services, launching, 203
productivity
average monthly benefit per user, calculating, 77
daily organizational productivity, calculating, 76
impact of WLANs, 309–310
monetized productivity benefit per WLAN, calculating, 74
office employee benefits, calculating, 77
total productivity benefit of WLANs, calculating, 72–73
traveling employee benefits, calculating, 78
profiles, 270–271
project board, 111
project management, Griffith University case study, 355
project plan, developing, 125

R

radio cell architecture, 294
Griffith University case study, 346
radio side protection, 221
radio-based rogue AP detection, 246
RADIUS accounting, 281
real-time video streaming applications, 139
regulatory agencies, 190
regulatory requirements, 31–32
restrictions on enterprise WLANs, 105
remote access, defining home wireless networking policies, 240, 243
Renaud, David, 353
requirements for guest networking, 145, 148
resource requirements, estimating, 126
responding to rogue APs, 247–248
RF devices, regulations, 31–32
RF environment, 176
RF fingerprinting, 155
RF management, 261–262
RF Prediction, 198
RF triangulation, 155
RFID (Radio Frequency Identification), 263
Lifespan healthcare case study, 328
Rijmen, Vincent, 221
Rijndael, 221
ring topology, 8
risks, identifying, 79–81
road warriors, 116
roaming, 172–174, 293
fast Layer 2 roaming, 135
roaming user class, 116
rogue APs, 125, 218, 337
responding to, 247–248
detecting, 247, 262
on manufacturing company enterprise WLAN, 337
ROI (return on investment), 40, 63, 85–87

S

scalability of AAA, 238
scope of WLAN as architectural component, 164
Scott, Bruce, 347, 356
secondary users, 118
security, 304
alerts, 275–276
as architectural component, 166
as reason for guest network deployment, 144
authentication, 61, 211
EAP, 227–228
client security, 243–245
encryption, 62

Griffith University case study, 350–351
hashing, 62
IDSs, 248
Lifespan case study, 324
manufacturing industry case study, 332
mobile devices, 243
network admission control, 61
security management, 258
security models
encryption and authentication with overlay security solutions, 215
machine-based authentication, 214
native authentication only, 213–214
native encryption and authentication, 215
native encryption only, 213
no authentication, encryption, or hashing, 212
user-based authentication, 214
security policies, defining, 233
security settings management
centralized self-service model, 272
manual client configuration, 272
profiles, 270–271
standardization, 272
third-party wireless software, 271
selecting
discount rate, 89
inhouse versus outsourced deployment, 181
self-actualization, 82
self-healing WLANs, 261
self-throttling throughput strategy, 30
service and support, 298
Cisco four-tier support model, 299–300
cost of, 300
session layer, 14
signal strength, Griffith University education case study, 346
signal strength requirements, assessing, 293
single points of failure, effect on scalability, 123
site surveys, 198
Griffith University case study, 353
Lifespan healthcare case study, 326
"Smart Zones," 340–341
Griffith University education case study, 341–342
sniffing, 262
SNMP (Simple Network Management Protocol), 280
soft benefits, 78–79
software, third-party, 271
solutions lifecycle, 96
planning phase, 109–110
architecture scalability, 122–123
defining high-level program plan, 125–127
documenting project stakeholders, 111–114
identifying users, 114–119
impact on application portfolio, 121–122
security strategy, 123–125
preparation phase, 98
environmental factors, 104–105
funding, 106–108
identifying scope of deployment, 99
infrastructure requirements, 100, 103–104
SOX (Sarbanes-Oxley Act), 325
SSIDs (Service Set Identifiers), 234
on guest networks, 145
SSO (single sign-on), 296
stakeholders, 111
standard business applications, 120
standard user class, 114
standardization, 272

standards
IEEE 802.11a, 35–36
IEEE 802.11b, 33
IEEE 802.11g, 33–35
pre-ratification, 37
coexistence, 37
star topology, 8
storage assets, 49
strategic value of wireless networking, 287
subscription-funded deployment strategies, 108
sunk costs, 41
supplementary services, 130
video, 137–139
voice, 131–137
syslog, 280

T

target audience of WLAN as architectural component, 167–169
TCO (total cost of ownership), 64
per user, 66
Value Chain framework, 67
identifying key application areas, 67
identifying secondary application areas, 69
TDMA (Time Division Multiple Access), 23
technical support, 192
tertiary institutions, 340
testing APs, 201–202
third-party tools
wireless client software, 271
WLAN management tools, 278
threats to security
interception, 217
mitigating, 219
with authentication, 222, 225–226
with encryption, 219–220
with hashing, 221
rogue APs, 218
three-tiered service and support system, Griffith University case study, 348–349
throughput, self-throttling strategy, 30
tiered support structure, 188, 192
time division duplexing, 26
TKIP (Temporal Key Integrity Protocol), 221
top-down approach to facilitating value creation process, 44, 47–49
topological considerations for WLAN deployment, 289–291
topologies, Griffith University education case study, 344
total productivity benefit of WLANs, calculating, 72–73
tracking and telemetry, Lifespan healthcare case study, 327–328
traffic, sniffing, 262
transactional processes, 43
transmit channels, 25
transport and shipping companies, deploying WLAN location services, 154
transport assets, 49
transport layer, 13
traveling employee productivity benefits, calculating, 78
trend reporting, 257, 274–275
trusted WLANs, 124, 228–229
types of WLAN users, 168

U

unaware employees as security threat, 216
unfriendly rogues, 337
UNII (Unlicensed National Information Infrastructure) band, 26
unique challenges to WLAN management
dynamic nature of transport medium, 267–268

intermittent connectivity of mobile endpoints, 269
mobile nature of wireless endpoints, 268–269
untrusted wireless networks, 124, 228–229
user-based authentication, 214

V

Value Chain framework, 67
identifying key application areas, 67
identifying secondary application areas, 69
value creation process, facilitating with top-down approach, 44, 47–49
vendor-specific WLAN management tools, 277–278
video technologies, 137
broadcasting, 141
distribution mechanism, 138–139
implementing, 140–142
on-demand, 140
real-time streaming applications, 139
user expectations, managing, 142
visualization tools, 263
voice technologies, 131–132
WLAN voice, implementing, 134–137
VoIP, implementing on manufacturing company enterprise WLAN, 337

W-X-Y-Z

WACC (Weighted Average Cost of Capital), 89
war driving, 217
WECA (Wireless Ethernet Compatibility Alliance), 16
WEP (Wired Equivalent Privacy), 220
WIDS (wireless intrusion detection system), 263
wired networks, 313
wireless equipment, Griffith University case study, 347
wireless guest networking, 302–304
wireless voice services, 301
WLAN location services, 150, 154
asset tags, 154–156
components of, 154
deploying, 152–154
inventory taking, 153
methods of calculating location, 154–155
privacy issues, 155
rationale for, 151
WLANs
complementary services, 131
history of, 14
standards, Griffith University education case study, 345
topology, Lifespan case study, 320–322
video, managing user expectations, 142
voice devices, 132
voice implementation, 134–137
WLSE (Cisco Wireless LAN Solution Engine), 305, 347
WMM (WiFi Multimedia) standard, 121, 132
workgroup switches, 101
working groups (IEEE), 15
WPA (Wi-Fi Protected Access), 224