

CWNA[®]

Certified Wireless Network Administrator

Official Study Guide

Fourth Edition



David A. Westcott, CWNE #7

David D. Coleman, CWNE #4



Contents at a Glance

<i>Foreword</i>		<i>xxvii</i>
<i>Introduction</i>		<i>xxix</i>
<i>Assessment Test</i>		<i>lix</i>
Chapter 1	Overview of Wireless Standards, Organizations, and Fundamentals	1
Chapter 2	Radio Frequency Fundamentals	31
Chapter 3	Radio Frequency Components, Measurements, and Mathematics	63
Chapter 4	Radio Frequency Signal and Antenna Concepts	107
Chapter 5	IEEE 802.11 Standards	161
Chapter 6	Wireless Networks and Spread Spectrum Technologies	199
Chapter 7	Wireless LAN Topologies	237
Chapter 8	802.11 Medium Access	263
Chapter 9	802.11 MAC Architecture	283
Chapter 10	WLAN Architecture	325
Chapter 11	WLAN Deployment and Vertical Markets	371
Chapter 12	WLAN Troubleshooting and Design	399
Chapter 13	802.11 Network Security Architecture	459
Chapter 14	Wireless Attacks, Intrusion Monitoring, and Policy	499
Chapter 15	Radio Frequency Site Survey Fundamentals	533
Chapter 16	Site Survey Systems and Devices	561
Chapter 17	Power over Ethernet (PoE)	595
Chapter 18	802.11n	621
Chapter 19	Very High Throughput (VHT) and 802.11ac	659
Chapter 20	Bring Your Own Device (BYOD)	697
Appendix A	Answers to Review Questions	735
Appendix B	Abbreviations and Acronyms	783
Appendix C	About the Additional Study Tools	797
<i>Index</i>		<i>801</i>

Contents

<i>Foreword</i>		<i>xxvii</i>
<i>Introduction</i>		<i>xxix</i>
<i>Assessment Test</i>		<i>lix</i>
Chapter 1	Overview of Wireless Standards, Organizations, and Fundamentals	1
	History of WLAN	2
	Standards Organizations	4
	Federal Communications Commission	5
	International Telecommunication Union Radiocommunication Sector	6
	Institute of Electrical and Electronics Engineers	7
	Internet Engineering Task Force	8
	Wi-Fi Alliance	10
	International Organization for Standardization	15
	Core, Distribution, and Access	16
	Communications Fundamentals	17
	Understanding Carrier Signals	18
	Understanding Keying Methods	20
	Summary	25
	Exam Essentials	25
	Review Questions	26
Chapter 2	Radio Frequency Fundamentals	31
	What Is a Radio Frequency Signal?	33
	Radio Frequency Characteristics	34
	Wavelength	34
	Frequency	39
	Amplitude	40
	Phase	41
	Radio Frequency Behaviors	42
	Wave Propagation	43
	Absorption	44
	Reflection	44
	Scattering	46
	Refraction	46
	Diffraction	48
	Loss (Attenuation)	49

	Free Space Path Loss	51
	Multipath	53
	Gain (Amplification)	56
	Summary	57
	Exam Essentials	57
	Review Questions	59
Chapter 3	Radio Frequency Components, Measurements, and Mathematics	63
	RF Components	66
	Transmitter	66
	Antenna	67
	Receiver	68
	Intentional Radiator (IR)	68
	Equivalent Isotropically Radiated Power	68
	Units of Power and Comparison	70
	Watt	71
	Milliwatt (mW)	71
	Decibel (dB)	72
	dBi	74
	dBd	74
	dBm	75
	Inverse Square Law	76
	RF Mathematics	77
	Rule of 10s and 3s	78
	Noise Floor	89
	Signal-to-Noise Ratio (SNR)	89
	Received Signal Strength Indicator	89
	Link Budget	94
	Fade Margin/System Operating Margin	97
	Summary	99
	Exam Essentials	100
	Review Questions	102
Chapter 4	Radio Frequency Signal and Antenna Concepts	107
	Azimuth and Elevation Charts (Antenna Radiation Envelopes)	110
	Interpreting Polar Charts	112
	Beamwidth	114
	Antenna Types	117
	Omnidirectional Antennas	118
	Semidirectional Antennas	121
	Highly Directional Antennas	123
	Sector Antennas	125

Antenna Arrays	126
Visual Line of Sight	129
RF Line of Sight	129
Fresnel Zone	129
Earth Bulge	134
Antenna Polarization	135
Antenna Diversity	136
Multiple-Input, Multiple-Output	137
MIMO Antennas	138
Antenna Connection and Installation	139
Voltage Standing Wave Ratio	139
Signal Loss	141
Antenna Mounting	141
Antenna Accessories	147
Cables	147
Connectors	148
Splitters	149
Amplifiers	149
Attenuators	150
Lightning Arrestors	150
Grounding Rods and Wires	152
Regulatory Compliance	154
Summary	155
Exam Essentials	155
Review Questions	157
Chapter 5	IEEE 802.11 Standards
	161
Original IEEE 802.11 Standard	164
IEEE 802.11-2007 Ratified Amendments	166
802.11b-1999	166
802.11a-1999	167
802.11g-2003	169
802.11d-2001	172
802.11h-2003	172
802.11i-2004	174
802.11j-2004	175
802.11e-2005	175
IEEE Std 802.11-2012	176
802.11r-2008	179
802.11k-2008	179
802.11y-2008	181
802.11w-2009	181
802.11n-2009	182
802.11p-2010	182

802.11z-2010	183
802.11u-2011	183
802.11v-2011	183
802.11s-2011	184
Post-2012 Ratified Amendments	185
802.11ae-2012	185
802.11aa-2012	185
802.11ad-2012	185
802.11ac-2013	186
802.11af-2014	187
IEEE 802.11 Draft Amendments	188
802.11ah	188
802.11ai	189
802.11aj	189
802.11ak	189
802.11aq	189
Defunct Amendments	189
802.11F	189
802.11T	192
802.11m Task Group	193
Summary	193
Exam Essentials	194
Review Questions	195

Chapter 6 Wireless Networks and Spread Spectrum Technologies 199

Industrial, Scientific, and Medical Bands	201
900 MHz ISM Band	202
2.4 GHz ISM Band	202
5.8 GHz ISM Band	203
Unlicensed National Information Infrastructure Bands	203
U-NII-1 (Lower Band)	204
U-NII-2 (Middle Band)	204
U-NII-2 Extended	204
U-NII-3 (Upper Band)	205
Future U-NII Bands	206
3.6 GHz Band	208
4.9 GHz Band	208
Future Wi-Fi Frequencies	208
60 GHz	208
White-Fi	209
Narrowband and Spread Spectrum	210

Multipath Interference	211
Frequency Hopping Spread Spectrum	212
Hopping Sequence	213
Dwell Time	213
Hop Time	214
Modulation	214
Direct Sequence Spread Spectrum	215
DSSS Data Encoding	216
Modulation	217
Packet Binary Convolutional Code	217
Orthogonal Frequency Division Multiplexing	218
Convolutional Coding	219
Modulation	220
2.4 GHz Channels	221
5 GHz Channels	224
Adjacent, Nonadjacent, and Overlapping Channels	229
Throughput vs. Bandwidth	230
Communication Resilience	231
Summary	231
Exam Essentials	232
Review Questions	233
Chapter 7	
 Wireless LAN Topologies	237
Wireless Networking Topologies	238
Wireless Wide Area Network (WWAN)	238
Wireless Metropolitan Area Network (WMAN)	239
Wireless Personal Area Network (WPAN)	240
Wireless Local Area Network (WLAN)	240
802.11 Topologies	241
Access Point	242
Client Station	242
Integration Service	243
Distribution System	243
Wireless Distribution System	244
Service Set Identifier	247
Basic Service Set	248
Basic Service Set Identifier	248
Basic Service Area	249
Extended Service Set	250
Independent Basic Service Set	253
Mesh Basic Service Set	253
QoS Basic Service Set	255

	802.11 Configuration Modes	255
	Access Point Modes	256
	Client Station Modes	257
	Summary	257
	Exam Essentials	258
	Review Questions	259
Chapter 8	802.11 Medium Access	263
	CSMA/CA vs. CSMA/CD	264
	Collision Detection	265
	Distributed Coordination Function	266
	Interframe Space (IFS)	266
	Duration/ID Field	267
	Carrier Sense	268
	Random Backoff Timer	270
	Point Coordination Function	271
	Hybrid Coordination Function	272
	Enhanced Distributed Channel Access	272
	HCF Controlled Channel Access	273
	Block Acknowledgment	274
	Wi-Fi Multimedia	275
	Airtime Fairness	276
	Summary	278
	Exam Essentials	278
	Review Questions	279
Chapter 9	802.11 MAC Architecture	283
	Packets, Frames, and Bits	285
	Data-Link Layer	286
	MAC Service Data Unit	286
	MAC Protocol Data Unit	286
	Physical Layer	287
	PLCP Service Data Unit	287
	PLCP Protocol Data Unit	287
	802.11 and 802.3 Interoperability	288
	Three 802.11 Frame Types	290
	Management Frames	291
	Control Frames	291
	Data Frames	292
	Beacon Management Frame	293
	Passive Scanning	294
	Active Scanning	295

Authentication	297
Open System Authentication	297
Shared Key Authentication	298
Association	299
Authentication and Association States	300
Basic and Supported Rates	300
Roaming	301
Reassociation	301
Disassociation	303
Deauthentication	304
ACK Frame	304
Fragmentation	305
Protection Mechanism	307
RTS/CTS	309
CTS-to-Self	310
Data Frames	311
Power Management	312
Active Mode	313
Power Save Mode	313
Traffic Indication Map	313
Delivery Traffic Indication Message	314
Announcement Traffic Indication Message	315
WMM Power Save and U-APSD	315
802.11n Power Management	318
Summary	318
Exam Essentials	319
Review Questions	321
Chapter 10	WLAN Architecture
	325
Wireless LAN Client Devices	326
802.11 Radio Form Factors	326
802.11 Radio Chipsets	333
Client Utilities	333
Management, Control, and Data Planes	337
Management Plane	338
Control Plane	338
Data Plane	339
WLAN Architecture	339
Autonomous WLAN Architecture	339
Centralized Network Management Systems	341
Cloud Networking	343
Centralized WLAN Architecture	343
Distributed WLAN Architecture	351

	Unified WLAN Architecture	353
	Hybrid Architecture	353
	Specialty WLAN Infrastructure	354
	Wireless Workgroup Bridge	354
	Wireless LAN Bridges	354
	Enterprise WLAN Routers	357
	Wireless LAN Mesh Access Points	358
	WLAN Array	359
	Virtual AP System	360
	Real-Time Location Systems	361
	VoWiFi	362
	Summary	364
	Exam Essentials	364
	Review Questions	366
Chapter 11	WLAN Deployment and Vertical Markets	371
	Deployment Considerations for Commonly Supported	
	WLAN Applications and Devices	373
	Data	373
	Voice	374
	Video	374
	Real-Time Location Services	375
	Mobile Devices	376
	Corporate Data Access and End-User Mobility	377
	Network Extension to Remote Areas	378
	Bridging: Building-to-Building Connectivity	378
	Wireless ISP: Last-Mile Data Delivery	379
	Small Office/Home Office	379
	Mobile Office Networking	380
	Branch Offices	381
	Educational/Classroom Use	381
	Industrial: Warehousing and Manufacturing	382
	Retail	382
	Healthcare: Hospitals and Offices	384
	Municipal Networks	385
	Hotspots: Public Network Access	385
	Stadium Networks	387
	Transportation Networks	387
	Law Enforcement Networks	388
	First-Responder Networks	389
	Fixed Mobile Convergence	389
	WLAN and Health	390
	WLAN Vendors	391

	Summary	393
	Exam Essentials	393
	Review Questions	394
Chapter 12	WLAN Troubleshooting and Design	399
	Layer 2 Retransmissions	401
	RF Interference	403
	Multipath	407
	Adjacent Channel Interference	408
	Low SNR	409
	Mismatched Power Settings	411
	Near/Far	413
	Hidden Node	414
	802.11 Coverage Considerations	418
	Dynamic Rate Switching	419
	Roaming	422
	Layer 3 Roaming	426
	Co-channel Interference	428
	Channel Reuse/Multiple-Channel Architecture	430
	Channel Reuse/Channel Bonding	434
	Single-Channel Architecture	437
	Capacity vs. Coverage	440
	Band Steering	442
	Load Balancing	443
	High-Density WLANs	444
	Oversized Coverage Cells	447
	Physical Environment	447
	Voice vs. Data	447
	Performance	449
	Weather	450
	Upper-Layer Troubleshooting	451
	Summary	452
	Exam Essentials	453
	Review Questions	454
Chapter 13	802.11 Network Security Architecture	459
	802.11 Security Basics	461
	Data Privacy and Integrity	462
	Authentication, Authorization, and Accounting	463
	Segmentation	464
	Monitoring and Policy	464
	Legacy 802.11 Security	465
	Legacy Authentication	465

Static WEP Encryption	466
MAC Filters	469
SSID Cloaking	469
Robust Security	470
Robust Security Network (RSN)	472
Authentication and Authorization	472
PSK Authentication	472
Proprietary PSK Authentication	474
802.1X/EAP Framework	475
EAP Types	477
Dynamic Encryption-Key Generation	478
4-Way Handshake	480
WPA/WPA2-Personal	481
TKIP Encryption	481
CCMP Encryption	482
Traffic Segmentation	484
VLANs	484
RBAC	486
Infrastructure Security	487
Physical Security	487
Interface Security	487
VPN Wireless Security	488
Layer 3 VPNs	488
SSL VPN	489
VPN Deployment	489
Guest WLAN Security	490
Captive Portal	491
Summary	493
Exam Essentials	493
Review Questions	495
Chapter 14	Wireless Attacks, Intrusion Monitoring, and Policy
	499
Wireless Attacks	500
Rogue Wireless Devices	501
Peer-to-Peer Attacks	503
Eavesdropping	505
Encryption Cracking	508
Authentication Attacks	509
MAC Spoofing	511
Management Interface Exploits	512
Wireless Hijacking	512
Denial of Service (DoS)	514

	Vendor-Specific Attacks	515
	Social Engineering	516
	Intrusion Monitoring	516
	Wireless Intrusion Detection System	516
	Wireless Intrusion Prevention System (WIPS)	519
	Mobile WIDS	521
	Spectrum Analyzer	522
	Wireless Security Policy	523
	General Security Policy	524
	Functional Security Policy	524
	Legislative Compliance	524
	802.11 Wireless Policy Recommendations	526
	Summary	527
	Exam Essentials	527
	Review Questions	528
Chapter 15	Radio Frequency Site Survey Fundamentals	533
	WLAN Site Survey Interview	534
	Customer Briefing	534
	Business Requirements	535
	Capacity and Coverage Requirements	536
	Existing Wireless Network	539
	Infrastructure Connectivity	541
	Security Expectations	543
	Guest Access	543
	Documents and Reports	544
	Forms and Customer Documentation	544
	Deliverables	547
	Additional Reports	547
	Vertical Market Considerations	549
	Outdoor Surveys	549
	Aesthetics	550
	Government	550
	Education	551
	Healthcare	552
	Hotspots	552
	Retail	553
	Warehouses	553
	Manufacturing	553
	Multitenant Buildings	554
	Summary	554
	Exam Essentials	554
	Review Questions	556

Chapter 16	Site Survey Systems and Devices	561
	Site Survey Defined	562
	Protocol and Spectrum Analysis	563
	Spectrum Analysis	564
	Coverage Analysis	568
	AP Placement and Configuration	574
	Application Analysis	574
	Site Survey Tools	575
	Indoor Site Survey Tools	576
	Outdoor Site Survey Tools	579
	Coverage Analysis	581
	Manual	582
	Predictive	584
	Dynamic RF	585
	Wireless Network Validation	586
	Summary	587
	Exam Essentials	588
	Review Questions	589
Chapter 17	Power over Ethernet (PoE)	595
	History of PoE	596
	Nonstandard PoE	596
	IEEE 802.3af	597
	IEEE Std 802.3-2005, Clause 33	597
	IEEE 802.3at-2009	597
	IEEE Std 802.3-2012, Clause 33	597
	An Overview of PoE Devices	598
	Powered Device	598
	Power-Sourcing Equipment	600
	Endpoint PSE	601
	Midspan PSE	602
	Power-Sourcing Equipment Pin Assignments	605
	Planning and Deploying PoE	609
	Power Planning	609
	Redundancy	612
	802.11n or 802.11ac and PoE	613
	Summary	614
	Exam Essentials	615
	Review Questions	616
Chapter 18	802.11n	621
	802.11n-2009 Amendment	623
	Wi-Fi Alliance Certification	624

MIMO	626	
Radio Chains	627	
Spatial Multiplexing (SM)	628	
MIMO Diversity	630	
Space-Time Block Coding (STBC)	631	
Cyclic Shift Diversity (CSD)	631	
Transmit Beamforming (TxBF)	632	
HT Channels	634	
20 MHz Non-HT and HT Channels	634	
40 MHz Channels	636	
Forty MHz Intolerant	638	
Guard Interval (GI)	638	
Modulation and Coding Scheme (MCS)	640	
HT PHY	643	
Non-HT Legacy	643	
HT Mixed	644	
HT Greenfield	645	
HT MAC	645	
A-MSDU	645	
A-MPDU	646	
Block Acknowledgment	647	
Reduced Interframe Space	648	
HT Power Management	648	
HT Operation	649	
20/40 Channel Operation	650	
HT Protection Modes (0–3)	650	
RTS/CTS and CTS-to-Self	651	
Summary	652	
Exam Essentials	652	
Review Questions	654	
Chapter 19	Very High Throughput (VHT) and 802.11ac	659
802.11ac-2013 Amendment	662	
5 GHz Only	663	
20, 40, 80, and 160 MHz Channels	663	
256-QAM Modulation	669	
Modulation and Coding Schemes	672	
Single-User MIMO	673	
802.11ac Data Rates	674	
VHT MAC	676	
A-MPDU	677	
RTS/CTS	677	

	Beamforming	680
	Explicit Beamforming	680
	Multiuser MIMO	681
	Multiuser Beamforming	682
	Quality of Service	684
	Infrastructure Requirements	685
	Ethernet	685
	Power	687
	802.11ac in a SOHO or Home	688
	Device Radios	688
	Data Flow/Usage	688
	Spatial Streams	689
	Wider 802.11ac Channels	689
	MU-MIMO	689
	Wi-Fi Alliance Certification	689
	Summary	690
	Exam Essentials	691
	Review Questions	692
Chapter 20	Bring Your Own Device (BYOD)	697
	Mobile Device Management	699
	Company-Issued Devices vs. Personal Devices	701
	MDM Architecture	701
	MDM Enrollment	703
	MDM Profiles	706
	MDM Agent Software	709
	Over-the-Air Management	710
	Application Management	712
	Wi-Fi Client Onboarding	713
	Guest WLAN Access	714
	Guest SSID	714
	Guest VLAN	715
	Guest Firewall Policy	715
	Captive Web Portals	717
	Client Isolation, Rate Limiting, and Web Content Filtering	719
	Guest Management	719
	Guest Self-Registration	721
	Employee Sponsorship	721
	Social Login	723
	Encrypted Guest Access	724
	Network Access Control (NAC)	725
	Posture	725
	NAC and BYOD	726

	OS Fingerprinting	726
	AAA	727
	RADIUS Change of Authorization	727
	Summary	728
	Exam Essentials	728
	Review Questions	730
Appendix A	Answers to Review Questions	735
	Chapter 1: Overview of Wireless Standards, Organizations, and Fundamentals	736
	Chapter 2: Radio Frequency Fundamentals	738
	Chapter 3: Radio Frequency Components, Measurements, and Mathematics	740
	Chapter 4: Radio Frequency Signal and Antenna Concepts	742
	Chapter 5: IEEE 802.11 Standards	744
	Chapter 6: Wireless Networks and Spread Spectrum Technologies	746
	Chapter 7: Wireless LAN Topologies	748
	Chapter 8: 802.11 Medium Access	750
	Chapter 9: 802.11 MAC Architecture	752
	Chapter 10: WLAN Architecture	754
	Chapter 11: WLAN Deployment and Vertical Markets	757
	Chapter 12: WLAN Troubleshooting and Design	759
	Chapter 13: 802.11 Network Security Architecture	762
	Chapter 14: Wireless Attacks, Intrusion Monitoring, and Policy	764
	Chapter 15: Radio Frequency Site Survey Fundamentals	767
	Chapter 16: Site Survey Systems and Devices	770
	Chapter 17: Power over Ethernet (PoE)	772
	Chapter 18: 802.11n	774
	Chapter 19: Very High Throughput (HT) and 802.11ac	777
	Chapter 20: Bring Your Own Device (BYOD)	779
Appendix B	Abbreviations and Acronyms	783
	Certifications	784
	Organizations and Regulations	784
	Measurements	785
	Technical Terms	786
Appendix C	About the Additional Study Tools	797
	<i>Index</i>	801