Areas highlighted in green have been renamed, reorganized, or added as new topics to the CWNA-107 exam. Note that the old IEEE 802.11 RF Site Surveying knowledge domain has been renamed to RF Validation to reflect a significant change in focus. The CWNA-107 exam focuses primarily on using site design/survey software to validate an installation. Design topics are mostly reserved for CWDP. Additionally, a new knowledge domain, WLAN Troubleshooting, was added to gather the troubleshooting topics to one area rather than having them dispersed throughout.

CWNA-107 Objectives

Introduction

When you pass the CWNA exam, you earn credit towards the CWSP, CWDP, CWAP, and CWNE certifications and you earn the CWNA certification.

This exam measures the candidate's ability to understand the fundamentals of RF behavior and to describe the features and functions of WLAN components as they apply to WLAN administration. Also tested are the skills needed to install, configure, and troubleshoot WLAN hardware peripherals and protocols in small business and enterprise deployments.

The skills and knowledge measured by this examination are derived from a Job Task Analysis (JTA) involving wireless networking experts (CWNEs) and professionals. The results of this JTA were used in weighing the subject areas and ensuring that the weighting is representative of the relative importance of the content.

The following chart provides the breakdown of the exam as to the distribution of questions within each knowledge domain.

Knowledge Domain	Percentage
Radio Frequency (RF) Technologies	15%
WLAN Regulations and Standards	10%
WLAN Protocols and Devices	20%
WLAN Network Architecture	20%
WLAN Network Security	10%
RF Validation	10%
WLAN Troubleshooting	15%

CWNP Authorized Materials Use Policy

CWNP does not condone the use of unauthorized 'training materials' such as 'brain dumps'. Individuals who utilize such materials to pass CWNP exams will have their certifications revoked. In an effort to more clearly communicate CWNP's policy on use of unauthorized study materials, CWNP directs all certification candidates to the CWNP Candidate Conduct Policy at:

http://www.cwnp.com/wp-content/uploads/pdf/CWNPCandidateConductPolicy.pdf

Please review this policy before beginning the study process for any CWNP exam. Candidates will be required to state that they understand and have abided by this policy at the time of exam delivery. If a candidate has a question as to whether study materials are considered "brain dumps", he/she should perform a search using CertGuard's engine, found here: http://www.certguard.com/search.asp

Radio Frequency (RF) Technologies – 15%

1.1 Define and explain the basic characteristics of RF and RF behavior

- 1.1.1 Wavelength, frequency, amplitude, phase, sine waves
- 1.1.2 RF propagation and coverage
- 1.1.3 Reflection, refraction, diffraction and scattering
- 1.1.4 Multipath and RF interference
- 1.1.5 Gain and loss
- 1.1.6 Amplification
- 1.1.7 Attenuation
- 1.1.8 Absorption
- 1.1.9 Voltage Standing Wave Ratio (VSWR)
- 1.1.10 Return Loss
- 1.1.11 Free Space Path Loss (FSPL)
- 1.1.12 Delay Spread
- 1.1.13 Modulation (ASK and PSK)

1.2 Apply the basic concepts of RF mathematics and measurement

- 1.2.1 Watt and milliwatt
- 1.2.2 Decibel (dB)
- 1.2.3 dBm, dBd and dBi
- 1.2.4 Noise floor
- 1.2.5 SNR and SINR
- 1.2.6 RSSI
- 1.2.7 Signal metric conversions
- 1.2.8 System Operating Margin (SOM), fade margin and link budget calculations
- 1.2.9 Intentional Radiator compared with Equivalent Isotropically Radiated Power (EIRP)

1.3 Identify RF signal characteristics as they relate to antennas

- 1.3.1 RF and physical line of sight and Fresnel zone clearance
- 1.3.2 Beamwidths
- 1.3.3 Azimuth and Elevation charts
- 1.3.4 Passive gain vs. active gain
- 1.3.5 Isotropic radiator
- 1.3.6 Polarization
- 1.3.7 Antenna diversity types
- 1.3.8 Radio chains
- 1.3.9 Spatial multiplexing (SM)

1.3.10 Transmit Beam Forming (TxBF)
1.3.11 Maximal Ratio Combining (MRC)
1.3.12 MIMO and MU-MIMO

1.4 Explain and apply the functionality of RF antennas and antenna systems and the mounting options and antenna accessories available

1.4.1 Omni-directional antennas
1.4.2 Semi-directional antennas
1.4.3 Highly directional antennas
1.4.4 Sectorized antennas and antenna arrays
1.4.5 Reading antenna charts for different antenna types
1.4.6 Pole/mast mount
1.4.7 Ceiling mount
1.4.8 Wall mount
1.4.9 Indoor vs. outdoor mounting
1.4.10 RF cables, connectors and splitters
1.4.11 Amplifiers and attenuators
1.4.12 Lightning arrestors and grounding rods/wires
1.4.13 Towers, safety equipment and related concerns

WLAN Regulations and Standards – 10%

2.1 Explain the roles of WLAN and networking industry organizations

2.1.1 IEEE
2.1.2 Wi-Fi Alliance
2.1.3 IETF
2.1.4 Regulatory domains and agencies

2.2 Explain the IEEE standard creation process including working groups, naming conventions, drafts and ratification

2.3 Explain and apply the various Physical Layer (PHY) solutions of the IEEE 802.11-2016 standard as amended including supported channel widths, spatial streams, data rates and supported modulation types

2.3.1 DSSS – 802.11
2.3.2 HR-DSSS – 802.11b
2.3.3 OFDM – 802.11a
2.3.4 ERP – 802.11g

2.3.5 HT – 802.11n
2.3.6 DMG – 802.11ad
2.3.7 VHT – 802.11ac
2.3.8 TVHT – 802.11af
2.3.9 S1G – 802.11ah

2.4 Identify and apply 802.11 WLAN functional concepts

2.4.1 Modulation and coding
2.4.2 Co-location interference
2.4.3 Channel centers and widths (all PHYs)
2.4.4 Primary channels
2.4.5 Adjacent overlapping and non-overlapping channels
2.4.6 Throughput vs. data rate
2.4.7 Bandwidth
2.4.8 Communication resilience

2.5 Describe the OSI model layers affected by the 802.11-2016 standard and amendments

2.6 Define the frequency bands used by the 802.11 PHYs

2.7 Identify and comply with regulatory domain requirements and explain how to determine constraints within a regulatory domain

2.7.1 Available channels
2.7.2 Output power constraints
2.7.3 Dynamic Frequency Selection (DFS)
2.7.4 Transmit Power Control (TPC)

2.8 Explain basic use case scenarios for 802.11 wireless networks

2.8.1 Wireless LAN (WLAN) – BSS and ESS
2.8.2 Wireless PAN (WPAN)
2.8.3 Wireless bridging
2.8.4 Wireless Ad-Hoc (IBSS)
2.8.5 Wireless Mesh (MBSS)

WLAN Protocols and Devices – 20%

3.1 Describe the components that make up an 802.11 wireless service set

- 3.1.1 Stations (STAs)
- 3.1.2 Basic Service Set (BSS)
- 3.1.3 Basic Service Area (BSA)
- 3.1.4 SSID
- 3.1.5 BSSID
- 3.1.6 Extended Service Set (ESS)
- 3.1.7 Ad Hoc mode and IBSS
- 3.1.8 Infrastructure mode
- 3.1.9 Distribution System (DS)
- 3.1.10 Distribution System Media (DSM)
- 3.1.11 Roaming (Layer 1 and Layer 2)

3.2 Identify and explain the basic frame types defined in the 802.11-2016 standard

- 3.2.1 General frame format
- 3.2.2 MAC addressing
- 3.2.3 Beacon frame
- 3.2.4 Association frames
- 3.2.5 Authentication frames
- 3.2.6 Data frames
- 3.2.7 Acknowledgement (ACK) frames
- 3.2.8 Block ACK frames

3.3 Explain the process used to locate and connect to a WLAN

- 3.3.1 Scanning (active and passive)
- 3.3.2 Authentication
- 3.3.3 Association
- 3.3.4 Open System Authentication and Shared Key authentication
- 3.3.5 802.1X/EAP and Pre-Shared Key authentication
- 3.3.6 BSS selection

3.4 Define terminology related to the 802.11 MAC and PHY

- 3.4.1 MSDU, MPDU, PSDU and PPDU
- 3.4.2 A-MSDU and A-MPDU

- 3.4.3 Guard Interval
- 3.4.4 Interframe spaces
- 3.4.5 Fragmentation
- 3.4.6 PHY preamble

3.5 Explain 802.11 channel access methods

- 3.5.1 DCF
- 3.5.2 EDCA
- 3.5.3 RTS/CTS
- 3.5.4 CTS-to-Self
- 3.5.5 NAV
- 3.5.6 Physical carrier sense and virtual carrier sense
- 3.5.7 Channel width operations
- 3.5.8 HT Operation Modes
- 3.5.9 VHT Operating Mode field
- 3.5.10 HT and VHT protection mechanisms
- 3.5.11 Power save modes

3.6 Describe features of, select and install WLAN infrastructure devices

- 3.6.1 Autonomous Access Points (APs)
- 3.6.2 Controller-based APs
- 3.6.3 Cloud-based APs
- 3.6.4 Distributed APs
- 3.6.5 Management systems
- 3.6.6 Mesh APs and routers
- 3.6.7 WLAN controllers
- 3.6.8 Remote office controllers and/or APs
- 3.6.9 PoE injectors and PoE-enabled Ethernet switches
- 3.6.10 WLAN bridges
- 3.6.11 Home WLAN routers

3.7 Identify the features, purpose, and use of the following WLAN client devices and adapters

- 3.7.1 USB adapters
- 3.7.2 PCI, Mini-PCI, Mini-PCIe and Half Mini-PCIe cards
- 3.7.3 Laptops, tablets and mobile phones
- 3.7.4 802.11 VoIP handsets
- 3.7.5 Specialty devices (handheld scanners, push-to-talk, IoT)

3.7.6 Configure Windows, Linux, Chrome OS, and macOS clients

WLAN Network Architecture – 20%

4.1 Identify technology roles for which WLAN solutions are appropriate and describe the typical use of WLAN solutions in those roles

- 4.1.1 Corporate data access and end-user mobility
- 4.1.2 Enterprise network extension
- 4.1.3 WLAN bridging
- 4.1.4 Last-mile data delivery – Wireless ISP
- 4.1.5 Small Office/Home Office (SOHO) use
- 4.1.6 Mobile offices
- 4.1.7 Educational/classroom use
- 4.1.8 Industrial
- 4.1.9 Healthcare
- 4.1.10 Hotspots
- 4.1.11 Hospitality
- 4.1.12 Conference/convention/arena/stadium and large high density deployments
- 4.1.13 Transportation networks (trains, planes, automobiles)
- 4.1.14 Law enforcement networks

4.2 Describe and implement Power over Ethernet (PoE)

- 4.2.1 IEEE 802.3-2012, Clause 33, including 802.3af-2003 and 802.3at-2009
- 4.2.2 Power Source Equipment
- 4.2.3 Powered Device
- 4.2.4 Midspan and endpoint PSEs
- 4.2.5 Power levels
- 4.2.6 Power budgets and powered port density

4.3 Define and describe controller-based, distributed, cloud-based, and controller-less WLAN architectures

- 4.3.1 Core, Distribution and Access layer forwarding
- 4.3.2 Centralized data forwarding
- 4.3.3 Distributed data forwarding
- 4.3.4 Control, Management and Data planes
- 4.3.5 Scalability and availability solutions
- 4.3.6 Intra- and Inter-controller STA roaming handoffs (OKC and FT)
- 4.3.7 Advantages and limitations of each technology

4.3.8 Tunneling, QoS and VLANs

4.4 Define and describe a multiple channel architecture (MCA) network model and contrast it with a single channel architecture (SCA) model

4.4.1 BSSID and ESS configuration
4.4.2 Channel selection
4.4.3 AP placement
4.4.4 Co-channel and adjacent channel interference
4.4.5 Cell sizing (output power, antenna selection)

4.5 Match WLAN deployment requirements commonly specified to technology solutions

4.5.1 Data
4.5.2 Voice
4.5.3 Video
4.5.4 Real-Time Location Services (RTLS)
4.5.5 Mobile devices (tablets and smartphones)
4.5.6 High density
4.5.7 AirTime Fairness
4.5.8 Band steering
4.5.9 HotSpot 2.0/Passpoint certification
4.5.10 Radio Resource Management (RRM) and Adaptive Radio Management (ARM)
4.5.11 BYOD
4.5.12 Guest access
4.5.13 Mobile device management (MDM)
4.5.14 Network Access Control (NAC)

4.6 Determine and document required network services supporting the WLAN

4.6.1 DHCP
4.6.2 DNS
4.6.3 NTP
4.6.4 VLANs
4.6.5 RADIUS
4.6.6 Access Control Lists
4.6.7 Wired network capacity requirements
4.6.8 Cable lengths
4.6.9 Cable types

WLAN Network Security – 10%

5.1 Identify weak security options that should not be used in enterprise WLANs

- 5.1.1 WEP
- 5.1.2 Shared Key authentication
- 5.1.3 SSID hiding
- 5.1.4 MAC filtering
- 5.1.5 Improper use of WPA (TKIP/RC4)
- 5.1.6 Open System authentication alone, with the exception of intentional public networks
- 5.1.7 Wi-Fi Protected Setup (WPS)

5.2 Identify and configure effective security mechanisms for enterprise WLANs

- 5.2.1 WPA2 (CCMP/AES)
- 5.2.2 WPA2-Personal
- 5.2.3 WPA2-Enterprise
- 5.2.4 802.1X/EAP framework
- 5.2.5 RADIUS servers
- 5.2.6 EAP methods
- 5.2.7 Effective pre-shared key (PSK) and passphrase usage
- 5.2.8 Per-User PSK (PPSK)

5.3 Describe and select common security enhancements and tools used in WLANs

- 5.3.1 Captive portals
- 5.3.2 BYOD and guest networks
- 5.3.3 Protected management frames
- 5.3.4 Fast Secure Roaming methods
- 5.3.5 Wireless Intrusion Prevention System (WIPS)
- 5.3.6 Protocol and spectrum analyzers

5.4 Explain and use secure management protocols

- 5.4.1 HTTPS
- 5.4.2 SNMPv3
- 5.4.3 SSH2
- 5.4.4 VPN

RF Validation – 10%

6.1 Explain the importance of and the process of a post-implementation validation survey

- 6.1.1 Verify design requirements
  - 6.1.1.1 Coverage
  - 6.1.1.2 Capacity
  - 6.1.1.3 Throughput
  - 6.1.1.4 Roaming
  - 6.1.1.5 Delay
  - 6.1.1.6 Jitter
  - 6.1.1.7 Connectivity
  - 6.1.1.8 Aesthetics
- 6.1.2 Document actual WLAN implementation results

6.2 Locate and identify sources of RF interference

- 6.2.1 WLAN devices
  - 6.2.1.1 Co-Channel Interference (CCI)
  - 6.2.1.2 Adjacent Channel Interference (ACI)
- 6.2.2 Non-Wi-Fi devices
  - 6.2.2.1 Airtime utilization
  - 6.2.2.2 Frequencies used
- 6.2.3 Interference solutions
- 6.2.4 Spectrum analysis

6.3 Perform application testing to validate WLAN performance

- 6.3.1 Network and service availability
- 6.3.2 VoIP testing
- 6.3.3 Real-time application testing
- 6.3.4 Throughput testing
- 6.3.5 Load testing

6.4 Understand and use the basic features of validation tools

- 6.4.1 Throughput testers (iPerf, TamoSoft Throughput Tester, etc.)
- 6.4.2 Wireless design software (Ekahau Site Survey, iBwave Wi-Fi, AirMagnet Survey Pro, TamoSoft Survey, Aruba RFPLan)
- 6.4.3 Protocol analyzers

6.4.4 Spectrum analyzers

WLAN Troubleshooting – 15%

7.1 Define and apply industry and vendor recommended troubleshooting processes to resolve common 802.11 wireless networking problems

- 7.1.1 Identify the problem
- 7.1.2 Discover the scale of the problem
- 7.1.3 Define possible causes
- 7.1.4 Narrow to the most likely cause
- 7.1.5 Create a plan of action or escalate the problem
- 7.1.6 Perform corrective actions
- 7.1.7 Verify the solution
- 7.1.8 Document the results

7.2 Describe and apply common troubleshooting tools used in WLANs

- 7.2.1 Protocol analyzer
- 7.2.2 Spectrum analyzer
- 7.2.3 Centralized management consoles
- 7.2.4 WLAN monitoring solutions

7.3 Identify and explain how to solve the following WLAN implementation challenges using features available in enterprise class WLAN equipment and troubleshooting tools

- 7.3.1 System throughput
- 7.3.2 CCI and ACI
- 7.3.3 RF noise and noise floor
- 7.3.4 RF interference
- 7.3.5 Hidden nodes
- 7.3.6 Insufficient PoE power
- 7.3.7 Lack of coverage

7.4 Troubleshoot common connectivity problems in WLANs (both WLAN connectivity and network connectivity for wireless clients)

- 7.4.1 No signal or weak signal
- 7.4.2 Security configuration mismatch
- 7.4.3 Improper AP configuration
- 7.4.4 Improper client configuration

7.4.5 Faulty drivers/firmware
7.4.6 Hardware failure
7.4.7 DHCP issues
7.4.8 Captive portal issues