CWNA Exam (CWNA-106) 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 survey of wireless networking experts and professionals. The results of this survey 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	**% of Exam**
Radio Frequency (RF) Technologies	21%
IEEE 802.11 Regulations and Standards	17%
IEEE 802.11 Protocols and Devices	17%
IEEE 802.11 Network Implementation	25%
IEEE 802.11 Network Security	8%
IEEE 802.11 RF Site Surveying	12%
Total	**100%**

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 – 21%

1.1. RF Fundamentals

1.1.1. Define and explain the basic concepts of RF behavior

- Gain and loss
- Reflection, refraction, diffraction, and scattering
- VSWR
- Return Loss
- Amplification
- Attenuation
- Absorption
- Wave propagation including Free Space Path Loss and Delay Spread

1.2. RF Mathematics

1.2.1. Understand and apply the basic components of RF mathematics and measurement

- Watt and milliwatt
- Decibel (dB)
- dBm, dBi and dBd
- SNR
- RSSI
- System Operating Margin (SOM), fade margin and link budget
- Intentional Radiator compared with Equivalent Isotropically Radiated Power (EIRP)

1.3. RF Signal and Antenna Concepts

1.3.1. Identify RF signal characteristics, the applications of basic RF antenna concepts, and the implementation of solutions that require RF antennas

- Line of Sight and Fresnel zone issues
- Beamwidths
- Azimuth & Elevation charts
- Passive gain vs. active gain
- Isotropic radiator
- Polarization
- Antenna diversity types
- Radio chains
- Spatial Multiplexing (SM)
- Transmit Beam Forming (TxBF) (as defined in the 802.11 standard)
- Maximal Ratio Combining (MRC)
- Space-Time Block Coding (STBC)
- Cyclic Shift Diversity (CSD)
- Multi-User MIMO (MU-MIMO)
- Wavelength, frequency, amplitude and phase

1.3.2. Explain the applications of physical RF antenna and antenna system types and identify their basic attributes, purpose, and function

- Omni-directional / Dipole antennas
- Semi-directional antennas
- Highly-direction antennas
- Sectorized antennas and Antenna arrays

1.3.3. Describe the proper locations and methods for installing RF antennas

- Pole/mast mount
- Ceiling mount
- Wall mount
- Outdoor/Indoor mounting considerations

1.4. RF Antenna Accessories

1.4.1. Identify the use of the following WLAN accessories.

- RF Cables, connectors and signal splitters
- Amplifiers and attenuators
- Lightning arrestors and grounding rods/wires
- Mounting Systems
- Towers, safety equipment, and related concerns

IEEE 802.11 Regulations and Standards – 17%

2.1. Spread Spectrum Technologies

2.1.1. Identify some of the uses for wireless networking technologies

- Wireless LANs
- Wireless PANs
- Wireless bridging

2.1.2. Comprehend the differences between, and explain the different types of spread spectrum technologies and how they relate to the IEEE 802.11-2012 standard's (as amended and including 802.11ac) PHY clauses

- DSSS
- HR-DSSS
- ERP
- OFDM
- HT
- VHT

2.1.3. Identify the basic characteristics underlying concepts of how spread spectrum technology works, including modulation and coding

2.1.4. Identify and apply the concepts that make up the functionality of spread spectrum technology

- Co-location
- Channel centers and widths (all PHYs)
- Primary and secondary channels
- Adjacent overlapping and non-overlapping channels
- Carrier frequencies
- Throughput vs. data rate
- Bandwidth
- Communication resilience
- Physical carrier sense (CSMA/CA)
- Virtual carrier sense (NAV)

2.2. IEEE 802.11-2012 Standard (as amended and including 802.11aa, 802.11ac, 802.11ad and 802.11ae))

2.2.1. Identify, explain, and apply the basic frame types and frame exchange sequences covered by the IEEE 802.11-2012 standard

2.2.2. Identify and apply regulatory domain requirements

- Dynamic Frequency Selection (DFS)
- Transmit Power Control (TPC)
- Available channels
- Output power

2.2.3. Understand the OSI model layers affected by the 802.11-2012 standard and amendments

2.2.4. Use of ISM, UNII, and licensed bands in Wi-Fi networks

2.2.5. Supported data rates for each IEEE 802.11-2012 (as amended to include 802.11ac) PHY

2.2.6. Understand the IEEE standard creation and ratification process and identify IEEE standard naming conventions

2.3. Industry Organizations and Their Roles

2.3.1. Define the roles of the following organizations in providing direction, cohesion, and accountability within the WLAN industry

- Regulatory domain governing bodies
- IEEE
- Wi-Fi Alliance
- IETF

IEEE 802.11 Protocols and Devices – 17%

3.1. IEEE 802.11 Protocol Architecture

3.1.1. Summarize the processes involved in authentication and association

- The IEEE 802.11 State Machine
- Open System Authentication, Shared Key Authentication, and Deauthentication
- Association, reassociation, and disassociation

3.1.2. Define, describe, and apply the following concepts associated with WLAN service sets

- Stations
- BSSs
- Basic Service Area (BSA)
- Starting and joining a BSS
- BSSID
- SSID
- Ad Hoc mode and IBSS
- Infrastructure mode and ESS
- Distribution System (DS)
- Distribution System Media (DSM)
- Layer 2 and Layer 3 roaming

3.1.3. Explain and apply the following power management features of WLANs

- Active Mode
- Power Save Mode
- Unscheduled Automatic Power Save Delivery (U-APSD)
- WMM Power-Save (WMM-PS)
- Power Save Multi-Poll (PSMP)
- Spatial Multiplexing Power Save (SMPS)
- TIM/DTIM/ATIM
- VHT TXOP

3.2. IEEE 802.11 MAC & PHY Layer Technologies

3.2.1. Describe and apply the following concepts surrounding WLAN frames

- IEEE 802.11 Frame Format vs. IEEE 802.3 Frame Format
- Define terminology related to the MAC & PHY
  - Guard Interval (GI)
  - PSDU, PPDU, and PPDU Formats
  - MSDU and MPDU
  - A-MPDU vs. A-MSDU
  - 802.11 Frame Format and Types
  - Interframe spaces (RIFS, SIFS, PIFS, DIFS, AIFS, EIFS)
  - Block acknowledgements
  - Fragmentation
- Jumbo frame support (Layer 2)
- MTU discovery and functionality (Layer 3)

3.2.2. Identify methods described in the IEEE 802.11-2012 standard for locating, joining, and maintaining connectivity with an IEEE 802.11 WLAN

- Active scanning (Probes)
- Passive scanning (Beacons)
- Dynamic Rate Switching (DRS)

3.2.3. Define, describe, and apply IEEE 802.11 coordination functions and channel access methods and features available for optimizing data flow across the RF medium

- DCF and HCF coordination functions
- EDCA channel access method
- RTS/CTS and CTS-to-Self protocols
- HT channel width operation
- HT protection mechanisms
- HT Operation Modes (0, 1, 2, 3)
- VHT channel width operation
- VHT protection mechanisms
- VHT Operating Mode field

3.3. WLAN Infrastructure and Client Devices

3.3.1. Identify the purpose of the following WLAN infrastructure devices and describe how to install, configure, secure, and manage them

- Autonomous access points
- Controller-based access points

- Mesh access points / routers
- Enterprise WLAN controllers
- Distributed WLAN architectures
- Remote office WLAN controllers and/or APs
- PoE injectors (single and multi-port) and PoE-enabled Ethernet switches
- WLAN bridges
- Home WLAN router (teleworker)

3.3.2. Describe the purpose of the following WLAN client adapters and explain how to install, configure, secure, and manage them

- PC cards (ExpressCard, CardBus, and PCMCIA)
- USB2/3
- PCI, Mini-PCI, Mini-PCIe, and Half Mini PCIe cards
- Workgroup bridges

IEEE 802.11 Network Implementation – 25%

4.1. IEEE 802.11 Network Design, Implementation, and Management

4.1.1. Identify technology roles for which WLAN technology is appropriate and describe implementation of WLAN technology in those roles

- Corporate data access and end-user mobility
- Network extension to remote areas
- Building-to-building connectivity - Bridging
- Last-mile data delivery – Wireless ISP
- Small Office / Home Office (SOHO) use
- Mobile office networking
- Educational / classroom use
- Industrial – warehousing and manufacturing
- Healthcare – hospitals and offices
- Hotspots – public network access
- Transportation networks (trains, planes, automobiles)
- Law enforcement networks

4.2. IEEE 802.11 Network Troubleshooting

4.2.1. Identify and explain how to solve the following WLAN implementation challenges using features available in enterprise class WLAN equipment.

- System throughput
- Co-channel and adjacent-channel interference
- RF noise and noise floor
- Narrowband and wideband RF interference
- Multipath (in SISO and MIMO environments)
- Hidden nodes, near/far, weather and possible solutions

4.3. Power over Ethernet (PoE)

4.3.1. IEEE 802.3-2012, Clause 33

4.3.2. Powering 802.11 devices
- Proprietary midspan & endpoint PSEs
- IEEE 802.3 midspan & endpoint PSEs

4.4. WLAN Architectures – Configuration, Installation and Management

4.4.1. Define, describe, and implement autonomous APs with network connectivity and common features including control, management and data planes

4.4.2. Define, describe, and implement WLAN controllers that use centralized and/or distributed forwarding with network connectivity and common features including control, management and data planes

- Core, Distribution, and Access layer forwarding
- Controller-based, mesh, and portal APs
- Scalability
- Intra- and Inter-controller station handoffs
- Advantages and limitations
- Tunneling, QoS, and VLANs

4.4.3. Define, describe, and implement distributed and controller-less WLAN architectures with network connectivity and common features including control, management and data planes

- Scalability
- Inter-AP handoffs
- Advantages and limitations
- Tunneling, QoS, and VLANs

4.4.4. Define, describe, and implement a WNMS that manages APs and WLAN controllers with network connectivity and common features including control, management and data planes

4.4.5. Define, describe, and implement a multiple channel architecture (MCA) network model

- BSSID / ESSID configuration
- Site surveying methodology
- Network throughput capacity
- Co-channel and adjacent channel interference
- Cell sizing (including micro-cell)

4.4.6. Define, describe, and implement a single channel architecture (SCA) network model

- BSSID / ESSID configuration (including Virtual BSSIDs)
- Site surveying methodology
- Network throughput capacity
- Co-channel and adjacent channel interference
- Cell sizing
- Transmission coordination

4.4.7. Define and describe alternative WLAN architectures including control, management and data planes

- WLAN arrays
- Mesh networks
- Cloud management

4.5. WLAN Deployment Types

4.5.1. Understand WLAN design and deployment considerations for commonly supported WLAN applications and devices

- Data
- Voice
- Video
- Real-Time Location Services (RTLS)
- Mobile devices (tablets and smartphones)
- High density
- AirTime Fairness
- Band steering

4.6. WLAN Access and Deployment Technologies

- BYOD
- Guest access
- Mobile device management (MDM)
- Network Access Control (NAC)

IEEE 802.11 Network Security – 8%

5.1. IEEE 802.11 Network Security Architecture

5.1.1. Identify and describe the strengths, weaknesses, appropriate uses, and implementation of the following IEEE 802.11 security-related items:

- Weak Security Mechanisms
  - WEP cipher suite
  - Open System Authentication
  - Shared Key Authentication
  - MAC filtering
  - SSID hiding
- Effective Security Mechanisms
  - WPA- / WPA2-Enterprise
  - WPA- / WPA2-Personal
  - TKIP and CCMP cipher suites
  - 802.1X / EAP framework
  - Preshared Key (PSK) / passphrase authentication
  - Per-user Preshared Keys (PPSK)
  - Wi-Fi Protected Setup (WPS)
- Additional Mechanisms
  - Secure device management protocols (HTTPS, SNMPv3, SSH2)
  - Role Based Access Control (RBAC)
  - Captive portals and guest networks (BYOD)
  - Protected management frames
  - Fast Secure Roaming methods

5.2. IEEE 802.11 Network Security Analysis, Performance Analysis, and Troubleshooting

5.2.1. Describe, explain, and illustrate the appropriate applications for the following wireless security solutions from a monitoring, containment and reporting perspective

- Wireless Intrusion Protection System (WIPS)
- Protocol and spectrum analyzers

IEEE 802.11 RF Site Surveying – 12%

6.1. IEEE 802.11 Network Site Survey Fundamentals

6.1.1. Explain the importance of and the processes involved in information collection for manual and predictive RF site surveys.

- Gathering business requirements
- Interviewing managers and users
- Defining physical and data security requirements
- Gathering site-specific documentation
- Documenting existing network characteristics
- Gathering permits and zoning requirements
- Indoor- or Outdoor-specific information
- Identifying infrastructure connectivity and power requirements
- Understanding RF coverage requirements
- Understanding data capacity and client density requirements
- VoWiFi considerations for delay and jitter
- Client connectivity requirements
- Antenna use considerations
- Aesthetics requirements
- Tracking system considerations
- WIPS sensor considerations

6.1.2. Explain the technical aspects involved in performing manual and predictive RF site surveys.

- Locating and identifying RF interference sources
- Defining AP and antenna types to be used
- Defining AP and antenna placement locations
- Defining AP output power and channel assignments
- Defining co-channel and adjacent-channel interference
- Testing applications for proper operation
- Measuring performance metrics according to design requirements

6.1.3. Describe site survey reporting and follow-up procedures for manual and predictive RF site surveys.

- Reporting methodology
- Customer reporting requirements
- Hardware recommendations and bills of material
- Application analysis for capacity and coverage verification

6.2. IEEE 802.11 Network Site Survey Systems and Devices

6.2.1. Identify the equipment, applications, and system features involved in performing predictive site surveys

6.2.2. Identify the equipment, applications, and methodologies involved in performing manual site surveys

6.2.3. Identify the equipment, applications, and methodologies involved in self-managing RF technologies (automated RF resource management)