

Introduction

The CWNE certification covering the current objectives will certify that the successful candidate has a firm grasp on the fundamentals of advanced WLAN troubleshooting, Quality of Service (QoS), and spectrum management, can describe the features and functions of the IEEE 802.11 standard as amended, and has the skills needed to design, install, configure, secure, and troubleshoot an advanced 802.11 WLAN enterprise installation. A typical candidate should have a solid understanding of WLAN administration and security.

The skills and knowledge measured by this examination are derived from a survey of wireless networking experts and professionals. The subject areas below provide the breakdown of the main objectives of the PW0-300 exam.

CWNP Authorized Materials Use Policy

CWNP does not condone the use of unauthorized 'training materials', aka '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/exams/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>

Subject Areas

- 802.11 Physical Layer Technologies
- 802.11 MAC Frames and Exchange Processes
- 802.11 Spectrum Management
- 802.11 QoS Terms and Features
- WMM Certifications, Features, and Configuration
- Designing, Managing, and Troubleshooting Wireless Voice/Data Networks
- 802.11 WLAN Protocol Analyzer Use and Trace Interpretation

802.11 Physical Layer Technologies

- 1.1. Describe PHY Layer terminology and PLCP Sublayer found in the 802.11 standard, Clause 3 (as amended)
 - 1.1.1. PSDU
 - 1.1.2. PPDU
 - 1.1.3. Header
 - 1.1.4. Preambles
 - 1.1.5. Frame Formatting
 - 1.1.6. Purpose
 - 1.1.7. Transmission
- 1.2. Explain how Interframe Spacing works, why it is used, and when each of the following IFS is used:
 - 1.2.1. SIFS
 - 1.2.2. PIFS
 - 1.2.3. DIFS
 - 1.2.4. EIFS
 - 1.2.5. AIFS
- 1.3. Describe Slot Time procedure, channel widths, and other parameters for each 802.11 PHY specification
 - 1.3.1. Clause 15 – DSSS
 - 1.3.2. Clause 17 – OFDM
 - 1.3.3. Clause 18 – HR-DSSS
 - 1.3.4. Clause 19 – ERP
- 1.4. Explain 802.11 contention procedure
 - 1.4.1. CSMA/CA
 - 1.4.2. Backoff timer operation
 - 1.4.3. Virtual Carrier Sense (NAV)
 - 1.4.4. Physical Carrier Sense (CCA)
 - 1.4.5. Contention Window operation

802.11 MAC Frames and Exchange Processes

- 2.1. Compare and contrast the intended purposes of each 802.11 MAC layer frame type
 - 2.1.1. Control frame types and subtypes
 - 2.1.2. Management frame types and subtypes
 - 2.1.3. Data frame types and subtypes
- 2.2. Illustrate the structure of each 802.11 MAC layer frame type
 - 2.2.1. MAC Layer terminology used in the 802.11 standard (as amended)
 - 2.2.2. Header fields and subfields
 - 2.2.3. Control, Management, and Data frame payload contents and sizes
 - Information fields
 - Information elements

- 2.2.4. Frames sizes and data rates
- 2.2.5. MAC layer addressing
- 2.3. Illustrate the frame exchange processes involved in following for both a QoS BSS and non-QoS BSS:
 - 2.3.1. Authentication, Association, and Reassociation
 - 2.3.2. Disassociation and Deauthentication
 - 2.3.3. Acknowledgements
 - 2.3.4. Active and Passive Scanning
 - 2.3.5. 802.11 Fast/Secure Roaming within an RSN ESS
 - 2.3.6. 802.11 Power-Save operation
 - 2.3.7. Fragmentation
 - 2.3.8. Protection Mechanisms
 - 2.3.9. Data frame forwarding
 - 2.3.10. Security mechanisms
 - WEP
 - WPA / WPA2 / 802.11 Clause 8
 - 802.1X/EAP
 - 4-Way Handshake
 - Direct Link / PeerKey
 - Preauthentication
- 2.4. Contrast the differences between the frame exchange processes in:
 - 2.4.1. BSS vs. IBSS

802.11 Spectrum Management

- 3.1. Describe Spectrum and Transmit Power Management Extensions in the 5 GHz band, including functionality of:
 - 3.1.1. Transmit Power Control (TPC) procedures and frame exchanges
 - 3.1.2. Dynamic Frequency Selection (DFS) procedures and frame exchanges

802.11 QoS Terms and Features

- 4.1. Define QoS terminology and describe functionality relating to entities and coordination functions of QoS-enabled 802.11 networks
 - 4.1.1. Quality of Service Station (QoS STA) and non-QoS STA
 - 4.1.2. Quality of Service Basic Service Set (QoS BSS) and non-QoS BSS
 - 4.1.3. Quality of Service Access Point (QoS AP) and non-QoS AP
 - 4.1.4. Service Period (SP), Scheduled Service Period, Unscheduled Service Period, and Service Interval (SI)
 - 4.1.5. Contention Period (CP) and Contention-Free Period (CFP)
 - 4.1.6. Uplink, Downlink, and Direct Link
 - 4.1.7. Hybrid Coordination Function (HCF) and Hybrid Coordinator (HC)
 - 4.1.8. Enhanced Distributed Channel Access (EDCA)
 - 4.1.9. HCF Controlled Channel Access (HCCA)
 - 4.1.10. Block Ack Procedures
 - 4.1.11. Controlled Access Phase (CAP)
 - 4.1.12. Arbitration Interframe Space (AIFS)

- 4.2. Define 802.11 terminology and describe functionality relating to QoS features of QoS-enabled 802.11 networks
 - 4.2.1. Access Category (AC)
 - 4.2.2. Traffic Specification (TSPEC)
 - 4.2.3. Traffic Classification (TCLAS)
 - 4.2.4. Differentiated Services Code Point (DSCP)
 - 4.2.5. Admission Control
 - 4.2.6. Automatic Power Save Delivery (APSD)
 - 4.2.7. Traffic Category (TC)
 - 4.2.8. User Priority (UP)
 - 4.2.9. Traffic Stream (TS)
 - 4.2.10. Traffic Identifier (TID)
 - 4.2.11. Traffic Stream Identifier (TSID)
 - 4.2.12. Transmission Opportunity (TXOP)
 - 4.2.13. TXOP Holder

WMM Certifications, Features, and Configuration

- 5.1. Explain the terminology, purpose, and functionality of the Wi-Fi Multimedia® (WMM®) certifications and how they relate to 802.11 QoS features
 - 5.1.1. Use of Access Categories and User Priorities (including Annex G of 802.1D-2004)
 - 5.1.2. IEEE 802.1Q priority (802.1Q-2004, Clause 9) and DSCP tagging (RFC 2474)
 - 5.1.3. The role of applications in specifying power save behavior
 - 5.1.4. Relationship to 802.11 QoS features
- 5.2. Explain the purpose and functionality of WMM Power Save® (WMM-PS®)
 - 5.2.1. Effect on mobile device battery life and user experience
 - 5.2.2. Power save behavior negotiation during association
 - 5.2.3. WMM AC transmit queue configuration using WMM-PS and legacy power save
 - 5.2.4. WMM-PS client initiation of retrieving queued data at QoS APs
 - 5.2.5. Comparison between WMM-PS and Legacy Power-Save for downlink buffered data transmission
 - 5.2.6. Downlink data frame transmission during an EDCA TXOP
 - 5.2.7. Application layer time sync functionality
 - 5.2.8. U-APSD/WMM operation
 - 5.2.9. WMM, WMM-PS, and legacy power save client coexistence in a QoS BSS
- 5.3. Describe and configure equipment required for enterprise-class WLAN QoS
 - 5.3.1. WMM-enabled client devices and client/server applications
 - 5.3.2. WMM-enabled WLAN infrastructure devices that support wired-side QoS tagging
 - 5.3.3. Role Based Access Control (RBAC) filtering for voice-only, voice/video, and voice/data enabled WLAN client devices

Designing, Managing, and Troubleshooting Wireless Voice/Data Networks

- 6.1. Design Optimized Wireless Voice/Data Networks

- 6.1.1. Site survey and deployment differences for data-only versus voice+data WLANs
- 6.1.2. Site survey and deployment differences between 802.11a/g and 802.11n networks
- 6.1.3. Site survey and deployment considerations for mixed 802.11a/b/g/n networks
- 6.1.4. Design and implement real-time, location-based WLAN tracking services
- 6.1.5. Describe implementation of multicast features in a VoWiFi system
- 6.1.6. Describe effects of layer 3 boundaries on end-to-end QoS
- 6.1.7. Describe design problems for VoWiFi implementations
- 6.1.8. Implement VoWiFi systems with fast BSS transition and RSNA security mechanisms
- 6.1.9. Install and configure advanced WLAN infrastructure systems
- 6.1.10. Redesign an 802.11 WLAN based on an updated set of design criteria

6.2. Manage Wireless Voice/Data Networks

- 6.2.1. Understand operation of voice-aware WLAN controllers with features that optimize connectivity for voice clients

6.3. Troubleshoot Wireless Voice/Data Networks

- 6.3.1. Locate, identify, and mitigate RF interference sources with a spectrum analyzer
- 6.3.2. Implement MAC-layer performance and security monitoring to aid in resolution of problems that affect voice connectivity
- 6.3.3. Troubleshoot end-to-end latency, jitter, and frame loss problems caused by propagation, congestion, interference, queuing, and wired infrastructure performance problems
- 6.3.4. Use an 802.11 VoWiFi protocol analyzer

802.11 Wireless LAN Protocol Analyzer Use and Trace Interpretation

7.1. Demonstrate appropriate application of and interpret protocol traces from an 802.11 protocol analyzer

- 7.1.1. Install and configure an 802.11 protocol analyzer
- 7.1.2. Performance optimization and QoS troubleshooting
- 7.1.3. Security protocol and intrusion analysis

7.2. Demonstrate generic features common to most 802.11 protocol analyzers

- 7.2.1. Protocol decodes
- 7.2.2. Peer map functions
- 7.2.3. Conversation analysis
- 7.2.4. Expert functions