Introduction

The CWAP™ certification, covering the current CWAP exam objectives, will certify that the successful candidate understands the frame structures and exchange processes for each of the 802.11 series of standards and how to use the tools that are available for analyzing and troubleshooting today's wireless LANs. This certification exam will cover the details of these topics in great depth and will have a strong inclination towards real-world applicability of this knowledge. The CWAP candidate must have obtained the CWNA certification prior to earning the CWAP certification. When you pass the CWAP exam, you earn credit towards the CWNE certification.

The skills and knowledge measured by this examination are derived from a survey of wireless networking professionals and analyzer product manufacturers from around the world. 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 CWAP exam as to the weight of each section of the exam.

Wireless LAN Analysis Subject Area	**% Of Exam**
802.11 Physical (PHY) Layer Frame Formats and Technologies	5%
802.11 MAC Layer Frame Formats and Technologies	20%
802.11 Operation and Frame Exchanges	40%
Spectrum Analysis and Troubleshooting	15%
Protocol Analysis and Troubleshooting	20%
Total	**100%**

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

802.11 Physical (PHY) Layer Frame Formats and Technologies – 5%

1.1 Understand the importance of each sublayer of the PHY Layer and differentiate between their functions:

1.1.1. PMD
1.1.2. PLCP

1.2 Describe PHY Layer terminology and understand PHY concepts found in the 802.11-2007 standard (as amended):

1.2.1. PSDU
1.2.2. PPDU
1.2.3. Header
1.2.4. Preambles
1.2.5. Frame Formatting
1.2.6. Frame Transmission
1.2.7. CCA
1.2.8. Subcarriers
1.2.9. Guard Intervals
1.2.10. Operating channels and channel widths
1.2.11. Modulation and Coding
1.2.12. Training Fields

1.3 Identify the frame format(s) of the PPDU for each PHY specification and specify the meaning of and purpose for its contents:

1.3.1. PLCP Preamble
1.3.2. PLCP Header
1.3.3. DATA Field

1.4 Describe PHY-specific operations and parameters for each the following 802.11 PHY specifications:

1.4.1. Clause 15 – DSSS
1.4.2. Clause 17 – OFDM
1.4.3. Clause 18 – HR/DSSS
1.4.4. Clause 19 – ERP
1.4.5. Clause 20 – HT

1.5 Understand the function of the primitives used for communication between the PMD and PLCP as well as the PLCP and MAC.

1.6 Demonstrate a detailed knowledge of PHY enhancements introduced by 802.11n:

1.6.1. 40 MHz channels
1.6.2. Additional subcarriers
1.6.3. Short Guard Intervals
1.6.4. Modulation rates
1.6.5. Antenna Selection

802.11 MAC Layer Frame Formats and Technologies – 20%

2.1. Describe MAC Layer terminology and concepts found in the 802.11-2007 standard (as amended):

2.1.1. MSDU
2.1.2. MPDU
2.1.3. A-MSDU
2.1.4. A-MPDU
2.1.5. Header
2.1.6. Trailer
2.1.7. Frame Formatting
2.1.8. Fixed Fields
2.1.9. Subfields
2.1.10. Information Element
2.1.11. Information Field

2.2. Compare and contrast the intended purposes of each 802.11 MAC layer frame type:

2.2.1. Control frame types and subtypes
2.2.2. Management frame types and subtypes, including Action frames
2.2.3. Data frame types and subtypes

2.3. Illustrate the general frame format structure for all frame types.

2.4. Understand and identify the specific frame format structure for each 802.11 MAC layer frame type and subtype:

2.4.1. Header fields and subfields
2.4.2. Information elements (IEs) and Information fields
2.4.3. Frames sizes and data rates
2.4.4. Frame body (payload) contents and sizes

802.11 Operation and Frame Exchanges – 40%

3.1. Identify and explain operational methods, modes, and technologies specific to each PHY, including a considerable emphasis on 802.11n enhancements:

3.1.1. SISO and MIMO
3.1.2. Transmit Beamforming
3.1.3. Spatial Multiplexing
3.1.4. Frame Aggregation
3.1.5. Block Acknowledgements
3.1.6. Space-Time Block Coding (STBC)
3.1.7. Cyclic Shift Diversity

3.2. Explain basic transmit and receive PHY operations.

3.3. Understand and illustrate the technologies related to 802.11 contention:

3.3.1. Demonstrate the use of CSMA/CA operations in 802.11 WLANs.
3.3.2. Explain the processes used for arbitration by DCF and HCF (i.e. EDCA) access methods.
3.3.3. Define Physical Carrier Sense (CCA), understand how it works, and differentiate between its two functional methods:

- Energy Detect
- Carrier Sense

3.3.4. Explain the purpose and detailed functionality of Virtual Carrier Sense (NAV).

3.3.5. Explain how Interframe Spacing (IFS) works, why it is used, and when each of the following IFS are used:

- SIFS
- PIFS
- DIFS
- EIFS
- AIFS
- RIFS

3.3.6. Describe the purpose, functionality, and selection of Contention Windows.

3.3.7. Describe how the Backoff Timer works and why it is used.

3.3.8. Define a Slot Time, calculate its value for each PHY specification, and understand how it is used.

3.3.9. Identify standards-based and non-standard methods used to manipulate 802.11 contention using EDCA Parameter Sets.

3.4. Illustrate the frame exchange processes involved in the following for both a QoS BSS and non-QoS BSS:

3.4.1. Active and Passive Scanning

3.4.2. Authentication, Association, and Reassociation

3.4.3. Disassociation and Deauthentication

3.4.4. Roaming within an ESS

3.4.5. Acknowledgements and Block Acknowledgements

3.4.6. Data frame forwarding

3.4.7. Data frame aggregation

3.4.8. Rate Selection

- Multirate support
- Basic rates
- Dynamic rate switching
- Modulation and Coding Schemes (MCSs)

3.5. Identify and illustrate the operation and frame exchange processes involved in 802.11 security:

3.5.1. 802.11 Authentication and Association

3.5.2. WEP

3.5.3. Shared Key Authentication

3.5.4. WPA-Personal and WPA2-Personal as described in 802.11-2007, Clause 8

3.5.5. 802.1X/EAP

3.5.6. 4-Way Handshake

3.5.7. Group Key Handshake

3.5.8. Robust Security Networks

3.5.9. 802.11n security requirements

3.5.10. 802.11w Protected Management Frames

3.5.11. WIPS rogue containment

3.6. Describe the methods and frame exchange processes used in 802.11 Fast/Secure Roaming within an RSN ESS:

3.6.1. Preauthentication
3.6.2. PMK Caching
3.6.3. Opportunistic Key Caching (OKC)
3.6.4. 802.11r Fast BSS Transition (FT)

- FT Initial Mobility Domain Association
- Over-the-Air Fast BSS Transition
- Over-the-DS Fast BSS Transition

3.6.5. Understand the basic functionality of common proprietary roaming mechanisms.

3.7. Understand and illustrate the following, related to 802.11 power management:

3.7.1. Understand how Active mode works as a basic 802.11 process.
3.7.2. Describe the processes and features of Legacy Power Save mode.
3.7.3. Illustrate a detailed knowledge of WMM Power Save and Unscheduled-Automatic Power Save Delivery (U-APSD), including:

- Effect on mobile device battery life and user experience
- Relationship with WMM QoS
- Power save behavior negotiation during association
- WMM AC transmit queue configuration using WMM-PS and legacy power save
- WMM-PS client initiation of queued data retrieval from QoS APs
- Downlink data frame transmission during an EDCA TXOP
- Application layer time sync functionality
- U-APSD/WMM operation
- The role of applications in specifying power save behavior

3.7.4. Identify and define the following terms and concepts related to 802.11 power management:

- APSD
- U-APSD
- S-APSD
- TIM
- DTIM
- ATIM
- AID

3.7.5. Demonstrate a thorough knowledge of 802.11n power save mechanisms, including:

- Power Save Multi-Poll (PSMP)
- Spatial Multiplexing Power Save (SMPS)

3.7.6. Compare and contrast each power save method, demonstrating a detailed knowledge of the following:

- Benefits and/or drawbacks of each, including efficiency and flexibility
- Operational differences between each process
- WMM-PS and Legacy Power-Save client compatibility and coexistence in a QoS BSS

3.8. Understand and explain the following, as related to 802.11 protection mechanisms:

3.8.1. Explain the frames and frame exchange processes included in mixed mode PHY environments.
3.8.2. Illustrate the operation of RTS/CTS and CTS-to-Self protection.
3.8.3. Describe the operation and uses for HT protection modes including:

- Mode 0 - Pure HT
- Mode 1 - HT non-Member Protection
- Mode 2 - HT 20 MHz Protection
- Mode 3 – non-HT Mixed Mode

3.8.4. Demonstrate an understanding of the functionality of HT protection/coexistence mechanisms and modes including:

- Dual-CTS
- L-Sig TXOP Protection
- Phased Coexistence Operation (PCO)
- 40 MHz Intolerant

3.8.5. Compare and contrast each type of protection mechanism and understand the benefits, drawbacks, and purpose for each.

3.9. Demonstrate a detailed understanding of the Wi-Fi Multimedia® (WMM®) certifications and QoS concepts, including the following:

3.9.1. Explain the terminology, purpose, and functionality of the WMM® certifications and how they relate to 802.11 QoS features:

- Use of Access Categories and User Priorities
- IEEE 802.1Q priority and DSCP tagging
- Relationship to 802.11 QoS features

3.9.2. Define QoS terminology and describe functionality relating to entities and coordination functions of QoS-enabled 802.11 networks:

- Quality of Service Station (QoS STA) and non-QoS STA
- Quality of Service Basic Service Set (QoS BSS) and non-QoS BSS
- Quality of Service Access Point (QoS AP) and non-QoS AP
- Service Period (SP), Scheduled Service Period, Unscheduled Service Period, and Service Interval (SI)
- Enhanced Distributed Channel Access (EDCA)
- Block Ack Procedures
- Controlled Access Phase (CAP)

3.9.3. Define 802.11 terminology relating to QoS features of QoS-enabled 802.11 networks:

- Access Category (AC)
- Traffic Specification (TSPEC)
- Traffic Classification (TCLAS)
- Differentiated Services Code Point (DSCP)
- Admission Control
- Automatic Power Save Delivery (APSD)
- Traffic Category (TC)
- User Priority (UP)
- Traffic Stream (TS)
- Traffic Identifier (TID)
- Traffic Stream Identifier (TSID)
- Transmission Opportunity (TXOP)
- TXOP Holder

3.9.4. Illustrate the use of end-to-end QoS in an enterprise network.

3.10. Describe mechanisms related to spectrum and transmit power management:

- Transmit Power Control (TPC) procedures and frame exchanges
- Dynamic Frequency Selection (DFS) procedures and frame exchanges

3.11. Define terms and concepts and illustrate procedures related to 802.11s mesh networks:

3.11.1. Mesh BSS
3.11.2. Mesh Coordination Function (MCF)
3.11.3. Simultaneous Authentication of Equals (SAE)
3.11.4. Abbreviated Handshake

3.12. Understand the basic differences between the frame exchange processes in a BSS and an IBSS.

Spectrum Analysis and Troubleshooting – 15%

4.1. Demonstrate appropriate use, features, and configuration of professional spectrum analysis tools, including the following:

4.1.1. Locate and identify RF sources
4.1.2. Interpret and quantify the results of a spectrum analyzer trace
4.1.3. Analyzer bandwidth resolution
4.1.4. Comparison of spectrum analyzer types

- Purpose-built spectrum analyzer chipsets
- Wi-Fi chipsets with spectrum capabilities

4.2. Identify common RF device signatures, their operating frequencies, behaviors, and impact on WLAN operations:

4.2.1. 802.11 PHYs
4.2.2. Microwave ovens
4.2.3. Analog transmitters (video, voice, etc.)
4.2.4. Cordless phones
4.2.5. Bluetooth and other frequency hopping devices
4.2.6. Baby monitors
4.2.7. Signal generators and antenna test tools
4.2.8. Telemetry and other healthcare RF devices
4.2.9. Radar
4.2.10. RF-producing lighting systems

4.3. Define and describe common terms and concepts related to RF spectrum analysis:

4.3.1. Signal strength
4.3.2. SNR
4.3.3. Channel utilization
4.3.4. Duty cycle
4.3.5. Sweep cycles
4.3.6. Narrow band interference
4.3.7. Wide band interference
4.3.8. Resolution Bandwidth

4.4. Identify the purpose and illustrate proper interpretation of common types of spectrum measurement:

4.4.1. Swept Spectrograph
4.4.2. Real Time FFT
4.4.3. Utilization
4.4.4. Duty Cycle

4.5. Describe the features, purpose, and deployment strategies of distributed spectrum analyzers.

4.6. Demonstrate effective use of spectrum analyzers for network troubleshooting.

Protocol Analysis and Troubleshooting – 20%

5.1 Demonstrate appropriate application, configuration, and basic use of an 802.11 protocol analyzer:

5.1.1. Install and configure an 802.11 protocol analyzer:

- Channel selection, scanning, or multichannel support
- Define and enable appropriate filters

5.1.2. Performance optimization
5.1.3. Advanced troubleshooting
5.1.4. Security protocol and intrusion analysis

5.2 Describe features common to most 802.11 protocol analyzers:

5.2.1. Protocol decodes
5.2.2. Peer map functions
5.2.3. Conversation analysis
5.2.4. Filtering: capture and display
5.2.5. Expert functions

5.3 Demonstrate expert-level network troubleshooting using an 802.11 protocol analyzer:

5.3.1. Understand the sequence of events for expected network behavior and identify aberrations.
5.3.2. Understand the 802.11 WLAN frame structure and fields, and apply this knowledge to protocol analysis.
5.3.3. Perform event correlation.
5.3.4. Interpret and identify frame exchange processes.
5.3.5. Interpret and understand data presented by a protocol analyzer and apply this knowledge to network troubleshooting.

5.4 Explain the benefits and interpret the results of multiple-channel protocol analysis using multiple adapters and aggregation software.

5.5 Perform roaming and VoWiFi analysis using a protocol analyzer.

5.6 Describe the features, purpose, and deployment strategies of distributed protocol analyzers.

5.7 Demonstrate appropriate use, configuration, and features of wired protocol analyzers for WLAN troubleshooting.

5.8 Perform end-to-end QoS troubleshooting and analysis for WLAN optimization.

5.9 Identify common challenges related to protocol analysis:

5.9.1. PHY compatibility
5.9.2. Roaming analysis
5.9.3. Time synchronization with distributed analysis
5.9.4. Location limitations with laptop-based tools

5.10 Describe the use of syslog messages in troubleshooting network problems.

5.11 Identify common client problems and use client logs and statistics to resolve connectivity problems.