Certified Wireless Analysis Professional (CWAP-404) Objectives

Introduction

When you pass the CWAP exam and hold a valid CWNA certification, you earn the CWAP certification and credits towards the CWNE certification should you choose to pursue it.

The Certified Wireless Analysis Professional (CWAP) is responsible for the capture and analysis of data related to Wireless LANs following troubleshooting principles and methodologies. This professional has an in-depth understanding of protocols, frame exchanges, and standards at the Physical layer and MAC sublayer. A CWAP is proficient in the use of spectrum and protocol analysis tools.

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 table provides the breakdown of the exam as to the distribution of questions within each knowledge domain.

Knowledge Domain	**Percentage**
Protocol Analysis	15%
Spectrum Analysis	10%
PHY Layers and Technologies	10%
MAC Sublayer and Functions	25%
WLAN Medium Access	10%
802.11 Frame Exchanges	30%

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

1.0 Protocol Analysis – 15%

1.1 Capture 802.11 frames using the appropriate methods

- 1.1.1 Select capture devices
  - Laptop protocol analyzers
  - APs, controllers, and other management solutions
  - Specialty devices (hand-held analyzers and custom-built devices)
- 1.1.2 Install monitor mode drivers
- 1.1.3 Select capture location(s)
- 1.1.4 Capture sufficient data for analysis
- 1.1.5 Capture all channels or capture on a single channel as needed
- 1.1.6 Capture roaming events

1.2 Understand and apply the common capture configuration parameters available in protocol analysis tools

- 1.2.1 Save to disk
- 1.2.2 Packet slicing
- 1.2.3 Event triggers
- 1.2.4 Buffer options
- 1.2.5 Channels and channel widths
- 1.2.6 Capture filters
- 1.2.7 Channel scanning and dwell time

1.3 Analyze 802.11 frame captures to discover problems and find solutions

- 1.3.1 Use appropriate display filters to view relevant frames and packets
- 1.3.2 Use colorization to highlight important frames and packets
- 1.3.3 Configure and display columns for analysis purposes
- 1.3.4 View frame and packet decodes while understanding the information shown and applying it to the analysis process
- 1.3.5 Use multiple adapters and channel aggregation to view captures from multiple channels
- 1.3.6 Implement protocol analyzer decryption procedures
- 1.3.7 View and use a capture's statistical information for analysis
- 1.3.8 Use expert mode for analysis
- 1.3.9 View and understand peer maps as they relate to communications analysis

1.4 Utilize additional tools that capture 802.11 frames for analysis and troubleshooting

- 1.4.1 WLAN scanners and discovery tools
- 1.4.2 Protocol capture visualization and analysis tools

1.4.3 Centralized monitoring, alerting, and forensic tools

1.5 Ensure appropriate troubleshooting methods are used with all analysis types

1.5.1 Define the problem
1.5.2 Determine the scale of the problem
1.5.3 Identify probable causes
1.5.4 Capture and analyze the data
1.5.5 Observe the problem
1.5.6 Choose appropriate remediation steps
1.5.7 Document the problem and resolution

2.0 Spectrum Analysis – 10%

2.1 Capture RF spectrum data and understand the common views available in spectrum analyzers

2.1.1 Install, configure, and use spectrum analysis software and hardware
2.1.2 Capture RF spectrum data using handheld, laptop-based, and infrastructure spectrum capture solutions
2.1.3 Understand and use spectrum analyzer views
- Real-time FFT
- Waterfall, swept spectrogram, density, and historic views
- Utilization and duty cycle
- Detected devices
- WLAN integration views

2.2 Analyze spectrum captures to identify relevant RF information and issues

2.2.1 RF noise floor in an environment
2.2.2 Signal-to-Noise Ratio (SNR) for a given signal
2.2.3 Sources of RF interference and their locations
2.2.4 RF channel utilization
2.2.5 Non-Wi-Fi transmitters and their impact on WLAN communications
2.2.6 Overlapping and non-overlapping adjacent channel interference
2.2.7 Poor performing or faulty radios

2.3 Analyze spectrum captures to identify various device signatures

2.3.1 Identify various 802.11 PHYs
- DSSS
- OFDM

- OFDMA
- Channel widths
- Primary channel

2.3.2 Identify non-802.11 devices based on RF behaviors and signatures

- Frequency hopping devices
- IoT devices
- Microwave ovens
- Video devices
- RF Jammers
- Cordless phones

2.4 Use centralized spectrum analysis solutions

2.4.1 AP-based spectrum analysis
2.4.2 Sensor-based spectrum analysis

3.0 PHY Layers and Technologies – 10%

3.1 Understand and describe the functions of the PHY layer and the PHY protocol data units (PPDUs)

3.1.1 DSSS (Direct Sequence Spread Spectrum)
3.1.2 HR/DSSS (High Rate/Direct Sequence Spread Spectrum)
3.1.3 OFDM (Orthogonal Frequency Division Multiplexing)
3.1.4 ERP (Extended Rate PHY)
3.1.5 HT (High Throughput)
3.1.6 VHT (Very High Throughput)
3.1.7 HE (High Efficiency)

- HE SU PPDU
- HE MU PPDU
- HE ER SU PPDU
- HE TB PPDU
- HE NULL data packets

3.2 Apply the understanding of PHY technologies, including PHY headers, preambles, training fields, frame aggregation, and data rates, to captured data

3.3 Identify and use PHY information provided within pseudo-headers in protocol analyzers

3.3.1 Pseudo-Header formats

- Radiotap
- Per Packet Information (PPI)

3.3.2 Key pseudo-header content
- Guard intervals
- Resource units allocation
- PPDU formats
- Signal strength
- Noise
- Data rate and MCS index
- Length information
- Channel center frequency or received channel
- Channel properties

3.4 Recognize the limits of protocol analyzers to capture PHY information including NULL data packets and PHY headers

3.5 Use appropriate capture devices based on proper understanding of PHY types

3.5.1 Supported PHYs
3.5.2 Supported spatial streams

4.0 MAC Sublayer and Functions – 25%

4.1 Understand frame encapsulation and frame aggregation

4.1.1 Frame aggregation (A-MSDU and A-MPDU)

4.2 Identify and use MAC information in captured data for analysis

4.2.1 Management, Control, and Data frames
4.2.2 MAC frame formats and contents
- Frame Control field
- To DS and From DS fields
- Address fields
- Frame Check Sequence (FCS) field

4.2.3 802.11 Management frame formats
- Information Elements
- Authentication
- Association and Reassociation
- Beacon
- Prove Request and Probe Response

4.2.4 Data and QoS Data frame formats
4.2.5 802.11 Control frame formats

- Acknowledgement (ACK)
- Request to Send/Clear to Send (RTS/CTS)
- Block Acknowledgement and related frames
- Trigger frames
- VHT/HE NDP announcements
- Multiuser RTS

4.3 Validate BSS configuration through protocol analysis

4.3.1 Country code
4.3.2 Minimum basic rate
4.3.3 Supported rates and coding schemes
4.3.4 Beacon interval
4.3.5 WMM settings
4.3.6 RSN settings
4.3.7 HT/VHT/HE operations
4.3.8 Channel width
4.3.9 Primary channel
4.3.10 Hidden or non-broadcast SSIDs

4.4 Identify and analyze CRC error frames and retransmitted frames

5.0 WLAN Medium Access – 10%

5.1 Understand 802.11 contention algorithms in-depth and know how they impact WLANs

5.1.1 Distributed Coordination Function (DCF)
- Carrier Sense (CS) and Energy Detect (ED)
- Network Allocation Vector (NAV)
- Contention Windows (CW) and random backoff
- Interframe spacing

5.1.2 Enhanced Distributed Channel Access (EDCA)
- EDCA Function (EDCAF)
- Access Categories and Queues
- Arbitration Interframe Space Number (AIFSN)

5.1.3 Wi-Fi Multimedia (WMM)
- WMM parameters
- WMM-Power Save
- WMM-Admission Control

5.2 Analyze QoS configuration and operations

5.2.1 Verify QoS parameters in capture files
5.2.2 Ensure QoS is implemented end-to-end

6.0 802.11 Frame Exchanges – 30%

6.1 Capture, understand, and analyze BSS discovery and joining frame exchanges

6.1.1 BSS discovery
6.1.2 802.11 Authentication and Association
6.1.3 802.1X/EAP exchanges
6.1.4 Pre-Shared Key authentication
6.1.5 Four-way handshake
6.1.6 Group key exchange
6.1.7 Simultaneous Authentication of Equals (SAE)
6.1.8 Opportunistic Wireless Encryption (OWE)
6.1.9 WPA2 and WPA3
6.1.10 Fast secure roaming mechanisms
- Fast BSS Transition (FT) roaming exchanges
- Pre-FT roaming exchanges

6.1.11 Neighbor discovery (802.11k/v)
6.1.12 Hotspot 2.0 protocols and operations from the client access perspective
- ANQP
- Initial access

6.2 Analyze roaming behavior and resolve problems related to roaming

6.2.1 Sticky clients
6.2.2 Excessive roaming
6.2.3 Channel aggregation for roaming analysis

6.3 Analyze data frame exchanges

6.3.1 Data frames and acknowledgement frames
6.3.2 RTS/CTS data frame exchanges
6.3.3 QoS Data frame exchanges
6.3.4 Block Acknowledgement exchanges

6.4 Analyze MIMO and multiuser-specific transmission methods

6.4.1 MIMO
- Transmit Beamforming (TxBF)
- MU-MIMO

6.4.2 OFDMA
- Scheduling and trigger frames

6.5 Analyze behavior and solve problems related to MAC layer operations

6.5.1 Power Save operations
6.5.2 Protection mechanisms
6.5.3 Load balancing
6.5.4 Band Steering

CWAP-403 Exam Acronyms

For the CWAP-403 exam, you should be able to understand clearly define the following acronyms in relation to 802.11 WLAN operations and analysis. Such acronyms shall be used on the CWAP-403 exam without definition.

AAA	Authentication, Authorization, and Accounting
ACI	Adjacent Channel Interference
AD DS	Active Directory Domain Services
AES	Advanced Encryption Standard
AP	Access Point
ARM	Adaptive Radio Management
ASK	Amplitude Shift Keying
BPSK	Binary Phase Shift Keying
BSA	Basic Service Area
BSS	Infrastructure Basic Service Set
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CCI	Co-Channel Interference
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Protocol
CIA	Confidentiality, Integrity, and Availability
CRC	Cyclic Redundancy Check
CTS	Clear to Send
dB	Decibel
dBi	Decibel to Isotropic
dBm	Decibel to Milliwatt
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol

DMG	Directional Multi-Gigabit
DMZ	Demilitarized Zone
DNS	Domain Name System
DRS	Dynamic Rate Switching
DS	Distribution System
DSM	Distribution System Medium
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EIRP	Equivalent Isotropically Radiated Power
ERP	Extended Rate PHY
ESS	Extended Service Set
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
FSK	Frequency Shift Keying
FSR	Fast Secure Roaming
FT	Fast BSS Transition
FTP	File Transfer Protocol
Gbps	Gigabits Per Second
GBps	Gigabytes Per Second
GHz	Gigahertz
GI	Guard Interval
GTK	Group Temporal Key
HR/DSSS	High Rate DSSS
HT	High Throughput
HTTP	Hypertext Transfer Protocol

Hz	Hertz
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IR	Intentional Radiator
ISP	Internet Service Provider
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Medium Access Control
Mbps	Megabits Per Second
MBps	Megabytes Per Second
MBSS	Mesh Basic Service Set
MCA	Multiple Channel Architecture
MCS	Modulation and Coding Scheme
MDM	Mobile Device Management
MHz	Megahertz
MIMO	Multiple-Input/Multiple-Output
MOS	Mean Opinion Score
MSK	Master Session Key
MU-MIMO	Multi-User MIMO
mW	Milliwatt
NAC	Network Access Control

NIC	Network Interface Card
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OKC	Opportunistic Key Caching
OTA	Over-the-Air
PCI-DSS	Payment Card Industry Data Security Standard
PD	Powered Device
PHY	Physical Layer
PIN	Personal identification Number
PKI	Public Key Infrastructure
PoE	Power over Ethernet
PPDU	Physical Layer Protocol Data Unit
PSE	Power Source Equipment
PSK	Pre-Shared Key or Phase Shift Keying
PTK	Pairwise Transient Key
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-Based Access Control
RC4	Rivest Cipher 4
RF	Radio Frequency
RFC	Request for Comments
RRM	Radio Resource Management
RSNA	Robust Security Network Association

RSNA	Robust Security Network
RSSI	Received Signal Strength Indicator
RTS	Request to Send
Rx	Receive or Receiver
S1G	Sub-1 GHz
SCA	Single Channel Architecture
SINR	Signal-to-Interference plus Noise Ratio
SISO	Single-Input/Single-Output
SNR	Signal-to-Noise Ratio
SOHO	Small Office Home Office
SS	Spatial Streams
SSH	Secure Shell
SSID	Service Set Identifier
STA	Station
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TVHT	Television Very High Throughput
Tx	Transmit or Transmitter
UDP	User Datagram Protocol
VHT	Very High Throughput
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VoWLAN	Voice over WLAN
VPN	Virtual Private Network

W	Watt
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area network
WNMS	Wireless Network Management System
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access version 2
WPA3	Wi-Fi Protected Access version 3