Certified Wireless Analysis Professional

CWNP CWAP-405

Version Demo

Total Demo Questions: 10

Total Premium Questions: 106

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, 802.11 Physical (PHY) Layer Frame Formats and Technologies	17
Topic 2, 802.11 MAC Layer Frame Formats and Technologies	31
Topic 3, 802.11 Operation and Frame Exchanges	27
Topic 4, Spectrum Analysis and Troubleshooting	27
Topic 5, Mix Questions	4
Total	106

QUESTION NO: 1

What is the Extended IFS used in 802.11 contention?

A. When the higher data rates are used and you want the fastest medium access times

B. When the lower data rates are used and you want the fastest medium access times

C. When 802.11ac must coexist with 802.11n

D. When a frame reception begins but the received frame is incomplete or corrupted based on the FCS

ANSWER: D

Explanation:

“When a frame reception begins but the received frame is incomplete or corrupted based on the FCS” is correct. Extended Interframe Space (EIFS) is a recovery interval used by 802.11 stations after the station has detected a received frame that it cannot decode successfully, including a frame that fails its Frame Check Sequence validation. Rather than immediately contending for the medium using the normal post-frame timing, the station defers for the longer EIFS period. This gives time for the exchange that may be occurring on the wireless medium to finish, particularly because the station may have been unable to correctly interpret the frame and therefore cannot reliably determine all of the normal timing context. After the EIFS defer interval, normal contention procedures, including backoff where required, apply. EIFS is therefore associated with reception-error handling and medium protection, not with selecting higher or lower PHY data rates or with coexistence between specific Wi-Fi amendments. The IEEE 802.11 standard defines the MAC timing and interframe-space behavior that governs this process; see the IEEE 802.11 standard overview. CWNP’s CWAP certification overview also identifies MAC-layer analysis as a core area of wireless analysis expertise.

QUESTION NO: 2

How many frames make up the Group Key Handshake excluding any Ack frames that may be required?

A. 1

B. 2

C. 3

D. 4

ANSWER: B

Explanation:

2 is correct. The IEEE 802.11 Group Key Handshake is a two-message exchange used by the authenticator, normally the AP, to install or update a station’s group temporal key material. The AP first sends Group Key Handshake Message 1 as an EAPOL-Key frame. This message delivers the new GTK securely, along with key-information fields and integrity protection needed for the station to validate and install the group key. The station then returns Group Key Handshake Message 2, also an EAPOL-Key frame, acknowledging successful receipt and installation of the key material. Therefore, the handshake itself comprises two EAPOL-Key frames. This count does not include IEEE 802.11 MAC-layer acknowledgment control frames, which may be transmitted as part of reliable unicast delivery but are not Group Key Handshake messages. The GTK installed through this exchange protects group-addressed traffic, including broadcast and multicast frames, for the applicable basic service set. The exchange may occur after initial key establishment or later when the AP rekeys the group key. The Wi-Fi Alliance’s Wi-Fi security overview describes WPA security’s protection of wireless traffic, and the IEEE 802.11 working group provides access to the 802.11 standards program governing these MAC and security mechanisms.

QUESTION NO: 3

You are using a swept spectrum analyzer to distinguish two low-power interferers that are very close in frequency. The signals appear as one broad peak with the current resolution bandwidth setting.

What change is most appropriate?

A. Reduce the resolution bandwidth

B. Increase the resolution bandwidth

C. Increase the capture adapter's channel width

D. Enable MAC-layer decryption

ANSWER: A

Explanation:

Reduce the resolution bandwidth. A narrower RBW improves frequency resolution, allowing closely spaced signals to be separated into distinct spectral components. It also reduces the noise power admitted to each measurement bin.

The trade-off is that a narrower RBW generally increases sweep time. Increasing RBW can make the sweep faster, but it reduces the analyzer's ability to distinguish signals that are close together in frequency.

QUESTION NO: 4

Which one of the following portions of information is communicated by bits in the PHY Header?

A. SNR

B. Noise

C. Data rate

D. Signal strength

ANSWER: C

Explanation:

Data rate is communicated in PHY-layer signaling so that a receiving station can correctly interpret and decode the transmitted PPDU. In classic ERP/OFDM PHYs, the PLCP header includes a RATE field that identifies the modulation and coding rate used for the PSDU portion of the transmission. The receiver must decode this initial PHY information before it can determine the expected transmission duration and apply the appropriate demodulation and decoding parameters to the remainder of the frame.

In newer 802.11 PHY amendments, the exact representation has evolved. Rather than always expressing a simple legacy rate value, signaling fields can communicate parameters such as an MCS index, channel bandwidth, guard interval, coding, and spatial-stream information. Those parameters collectively identify the transmission’s effective data rate and the PHY processing required by the receiver. This is why data rate is the appropriate answer: it is explicitly conveyed or derivable from bits carried in the PHY preamble/header signaling fields, not merely observed after reception. The IEEE 802.11 working group maintains the standard family at IEEE 802.11; an overview of 802.11 PHY operation is also available from CWNP CWAP.

QUESTION NO: 5

Which one of the following is an advantage of using display filters that is not an advantage of capture-time filters?

A. They allow for focused analysis on just the packets of interest

B. Once created they are reusable for later captures

C. They only hide the packets from view and the filtered packets can be enabled for view later

D. Multiple of them can be applied simultaneously

ANSWER: C

Explanation:

They only hide the packets from view and the filtered packets can be enabled for view later is correct because display filtering operates on packets that have already been captured and retained in the packet list or capture file. A display filter changes the analyst's current view, allowing attention to be focused on packets matching a particular protocol, address, frame type, management-information element, or other decoded field. Crucially, packets that do not match the active display-filter expression have not been removed from the capture. The analyst can clear the filter, revise it, or apply a different expression and immediately inspect those previously hidden frames. This preserves the ability to pursue new hypotheses during troubleshooting or forensic analysis without having to repeat the capture. In contrast, capture filters are evaluated while traffic is being acquired; frames excluded by that filter are not written into the capture and therefore cannot be displayed or analyzed later. Wireshark's documentation explicitly distinguishes capture filters, which control what is captured, from display filters, which control what is shown after capture. See the Wireshark filter documentation and the Wireshark User's Guide: Building Display Filters.

QUESTION NO: 6

In the 2.4 GHZ band, what data rate are Probe Requests usually sent at from an unassociated STA?

A. 1 Mbps

B. The minimum basic rate

C. MCS 0

D. 6 Mbps

ANSWER: B

Explanation:

The minimum basic rate is correct. Probe Requests are management frames used during active scanning, when a client station has not yet associated with an access point and is attempting to discover available wireless networks. In 2.4 GHz operation, these broadcasts are ordinarily transmitted using a low basic rate so that nearby access points and stations can reliably decode the frame, including devices at the edge of coverage. Basic rates are mandatory rates advertised by a BSS and are used for traffic that must be broadly understood, such as many broadcast and management transmissions.

Although the exact configured minimum basic rate can differ by WLAN design, legacy 2.4 GHz deployments commonly use a low DSSS basic rate such as 1 Mbps, 2 Mbps, 5.5 Mbps, or 11 Mbps. The key point is that the frame is normally sent at the applicable minimum basic rate, rather than at a particular fixed rate that would be universal to every network. This behavior aids discovery compatibility and reflects the importance of management-frame decodability before a client has completed association. CWNP's CWAP certification scope includes analysis of 802.11 management operations and client scanning behavior; see CWNP Certified Wireless Analysis Professional. For protocol-level context on active scanning and Probe Request management frames, see Wireshark IEEE 802.11 protocol reference.

QUESTION NO: 7

What is the function of the PHY Preamble?

A. To terminate a conversation between transmitter and receiver

B. To set the modulation method for the MPDU

C. Carries the NDP used in Transmit Beamforming and MU-MIMO

D. Allows the receiver to detect and synchronize with the signal

ANSWER: D

Explanation:

The PHY Preamble “Allows the receiver to detect and synchronize with the signal.” It is the initial portion of an IEEE 802.11 PHY Protocol Data Unit (PPDU), sent before the PHY header and the data portion. Its training sequences let a receiving radio recognize that a valid 802.11 transmission is present, establish timing and frequency synchronization, and perform channel estimation needed to reliably demodulate the remainder of the frame. Depending on the PHY amendment, the preamble contains training fields such as short and long training fields; these support functions including automatic gain control, coarse and fine frequency-offset estimation, symbol timing, and channel estimation. The receiver must complete these physical-layer acquisition tasks before it can interpret the signal field and decode the PSDU that carries the MAC frame. This synchronization role is fundamental across 802.11 PHY types, even though the exact preamble fields and formats vary among legacy, HT, VHT, HE, and EHT transmissions. The IEEE 802.11 working group maintains the family of standards governing WLAN PHY operation at IEEE 802.11 Working Group. For a practical technical discussion of 802.11 frame transmission and the PLCP/PPDU structure, see MRN-CCIEW: 802.11 Physical Layer.

QUESTION NO: 8

Given: The Frame Check Sequence (FCS) is a 32 CRC used for error detection.

The CRC is calculated over what?

A. Mac Header and Frame Body only

B. Frame Body only

C. PHY Header, MAC Header and Frame Body

D. PHY Header and Mac Header only

ANSWER: A

Explanation:

The correct answer is **Mac Header and Frame Body only**. In an IEEE 802.11 MAC frame, the Frame Check Sequence is a 32-bit CRC value carried as the final field of the MAC Protocol Data Unit. The transmitting MAC calculates this CRC across the MAC header and the frame body, then appends the resulting FCS. A receiving station performs the same CRC calculation on the received MAC header and frame body and compares its result with the received FCS. A mismatch identifies that the MPDU was corrupted in transit, allowing the receiver to discard the frame rather than pass corrupted content to upper MAC processing. This scope is important during packet analysis because the FCS validates the integrity of the MAC-layer frame fields, including addressing, control, sequence-related fields, and any payload contained in the frame body. PHY preamble and PHY header fields are not part of the MAC frame data covered by the MAC FCS; those fields belong to the PHY-layer PPDU encapsulation and are processed separately. IEEE 802.11 defines the MAC service and frame structure, while CWNP’s CWAP curriculum expects analysts to distinguish MAC-layer integrity checking from PHY-layer signaling. See the IEEE 802.11 standard overview and the CWNP CWAP certification page.

QUESTION NO: 9

ABC Company requires the ability to identify and quickly locate rogue devices. ABC has chosen an overlay WIPS solution with Wi-Fi sensors that use dipole antennas to perform this task. No other sensors are included. Use your knowledge of location tracking techniques to answer the question.

Which one of the following location methods is not available in the described system?

A. GPS Positioning

B. Time Difference of Arrival (TDoA)

C. RF Fingerprinting

D. Trilateration of RSSI measurements

ANSWER: A

Explanation:

GPS Positioning is not available because the described deployment contains only Wi-Fi WIPS sensors with dipole antennas and explicitly includes no other sensor type. GPS-based positioning depends on receiving GPS satellite signals through a GPS receiver and deriving a position from those satellite measurements. A conventional Wi-Fi sensor and its dipole antenna are intended to receive and analyze 802.11 RF transmissions; that equipment alone does not provide a GPS receiver or GPS satellite-signal capability. Consequently, the system can observe rogue-device Wi-Fi transmissions and use the measurements made by its distributed Wi-Fi sensor infrastructure, but it cannot obtain a rogue device's location from GPS coordinates in the stated design. This distinction matters especially for an overlay WIPS: its sensor placement and RF observations support wireless-security monitoring and RF-based location workflows, whereas GPS is a separate positioning technology requiring dedicated GPS-capable hardware and usable satellite reception. CWNP's CWAP certification scope includes WLAN analysis, troubleshooting, and security-oriented analysis concepts relevant to WIPS deployments: CWNP CWAP certification. The U.S. government's GPS overview also describes GPS positioning as based on signals from GPS satellites received by GPS equipment: GPS.gov: The Global Positioning System.

QUESTION NO: 10

What is encrypted within the third message of the 4-Way Handshake?

A. PMK

B. PTK

C. GMK

D. GTK

ANSWER: D

Explanation:

GTK is encrypted within message 3 of the IEEE 802.11i/WPA2 4-Way Handshake when the authenticator distributes or updates the group key material. Once both parties have derived the Pairwise Transient Key from the Pairwise Master Key, the nonces, and their MAC addresses, the PTK's Key Encryption Key component protects the GTK carried in the EAPOL-Key Key Data field. This prevents a passive observer from learning the key that stations use to protect broadcast and multicast traffic. Message 3 also includes key-installation and handshake-confirmation information, protected with a message integrity code derived from the PTK, allowing the supplicant to validate the authenticator and safely install its keys. The GTK is generated by the authenticator's group-key management process and is subsequently used with the group cipher to secure group-addressed frames. The 4-Way Handshake's key distribution and confirmation process is specified by IEEE 802.11 and summarized in the Wi-Fi Alliance's WPA3 security overview. See IEEE 802.11 standard information and Wi-Fi Alliance security resources.