CWAP-404 $^{Q\&As}$

Certified Wireless Analysis Professional

Pass CWNP CWAP-404 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/cwap-404.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CWNP Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

A client is operating in an unstable RF environment. Out of five data frames transmitted to the client it only receives four. The client sends a Block Ack to acknowledge the receipt of these four frames but due to frame corruption the Block Ack

is not received by the AP.

Which frames will be retransmitted?

A. All data frames

B. Both the corrupted data and Block Ack

C. Only the data frame which was corrupted

D. Only the Block Ack

Correct Answer: A

Explanation: All data frames will be retransmitted in this scenario. This is because the AP uses a Block Ack (BA) mechanism to acknowledge the receipt of multiple data frames from a client in a single frame. The BA contains a bitmap that indicates which data frames were received correctly and which were not. If the BA is not received by the AP due to frame corruption, the AP will assume that none of the data frames were received by the client and will retransmit all of them. The other options are not correct, as they do not account for the loss of the BA or the use of the bitmap. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 6: 802.11 Frame Exchanges, page 167-168

QUESTION 2

How many frames are exchanged for 802.11 authentication in the 6 GHz band when WPA3-Enterprise is not used, and a passphrase is used instead?

A. 1

B. 2

C. 3

D. 4

Correct Answer: B

Explanation: Two frames are exchanged for 802.11 authentication in the 6 GHz band when WPA3-Enterprise is not used, and a passphrase is used instead. Authentication is a process that establishes an identity relationship between a STA (station) and an AP (access point) before joining a BSS (Basic Service Set). There are two types of authentication methods defined by 802.11: Open System Authentication and Shared Key Authentication. Open System Authentication does not require any credentials or security information from a STA to join a BSS, and it consists of two frames: an Authentication Request frame sent by the STA to the AP, and an Authentication Response frame sent by the AP to the STA. Shared Key Authentication requires a shared secret key from a STA to join a BSS, and it consists of four frames: two challenge-response frames in addition to the request-response frames. However, Shared Key Authentication uses WEP (Wired Equivalent Privacy) as its encryption algorithm, which is insecure and deprecated. In the 6 GHz band, which is a newly available frequency band for WLANs, Shared Key Authentication is prohibited by the 802.11 standard, as it poses security and interference risks for other users and services in the band. The 6 GHz band requires all WLANs

to use WPA3-Personal or WPA3-Enterprise encryption methods, which are more secure and robust than previous encryption methods such as WPA2 or WEP. WPA3-Personal uses a passphrase to derive a PMK (Pairwise Master Key), while WPA3-Enterprise uses an authentication server to obtain a PMK. Both methods use SAE (Simultaneous Authentication of Equals) as their authentication protocol, which replaces PSK (Pre-Shared Key) or EAP (Extensible Authentication Protocol). SAE consists of two frames: an SAE Commit frame sent by both parties to exchange elliptic curve parameters and nonces, and an SAE Confirm frame sent by both parties to verify each other\\'s identities and generate a PMK. Therefore, when WPA3-Enterprise is not used, and a passphrase is used instead in the 6 GHz band, only two frames are exchanged for 802.11 authentication: an SAECommit frame and an SAE Confirm frame. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 8: Security Analysis, page 220-221

QUESTION 3

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

Correct Answer: B

Explanation: In the 2.4 GHz band, probe requests are usually sent at the minimum basic rate from an unassociated STA. A probe request is a type of management frame that is transmitted by a STA to discover available BSSs in its vicinity. A probe request can be sent on one or more channels in either passive or active scanning mode. In passive scanning mode, a STA listens for beacon frames from APs on each channel. In active scanning mode, a STA sends probe requests on each channel and waits for probe responses from APs. A probe request is usually sent at the minimum basic rate, which is the lowest data rate among the supported rates that is required for all STAs to join and communicate with a BSS. The minimum basic rate can vary depending on the configuration of each BSS, but it is typically one of these values: 1 Mbps, 2 Mbps, 5.5 Mbps, or 11 Mbps in the 2.4 GHz band. The other options are not correct, as they do not reflect how probe requests are usually sent in the 2.4 GHz band. MCS 0 is a modulation and coding scheme used by 802.11n/ac devices in either band, but it is not a data rate per se. 6 Mbps is a data rate used by OFDM devices in either band, but it is not usually configured as a minimum basic rate in the 2.4 GHz band. References: [Wireless Analysis Professional Study Guide CWAP- 404], Chapter 5: 802.11 MAC Sublayer, page 123-124

QUESTION 4

Where, in a protocol analyzer, would you find an indication that a frame was transmitted as part of an A-MPDU?

A. The HT Operation Element

B. A-MPDU flag in the QoS Control Field

C. A-MPDU flag in the Frame Control Field

D. The Aggregation flag in the Radio Tap Header

Correct Answer: D

Explanation: In a protocol analyzer, you would find an indication that a frame was transmitted as part of an A-MPDU by looking at the Aggregation flag in the Radio Tap Header. The Radio Tap Header is a pseudo-header that is added by

some wireless capture devices to provide additional information about the physical layer characteristics of a frame. The Aggregation flag is one of the fields in this header, and it indicates whether the frame belongs to an A-MPDU or not. If the flag is set to 1, it means that the frame is part of an A- MPDU; if it is set to 0, it means that the frame is not part of an A-MPDU . References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter

9: PHY Layer Frame Formats andTechnologies, page 303; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 9: PHY Layer Frame Formats and Technologies, page 304.

QUESTION 5

After examining a Beacon frame decode you see the SSID Element has a length of 0. What do you conclude about this frame?

A. The frame is corrupted

B. SSID elements always have a length of 0

C. This is a common attack on WISP backend SQL databases

D. The beacon is from a BSS configured to hide the SSID

Correct Answer: D

Explanation: If the SSID element has a length of 0 in a Beacon frame decode, it means that the beacon is from a BSS configured to hide the SSID. The SSID element is a part of the Beacon frame that contains the name or identifier of the BSS. The SSID element has two fields: length and value. The length field indicates how many bytes are used for the value field, which contains the actual SSID string. If the length field is 0, it means that there is no value field or SSID string in the element. This is a common technique used by some APs to hide their SSID from passive scanning clients or potential attackers. However, this technique does not provide much security, as there are other ways to discover or reveal the hidden SSID, such as active scanning or capturing probe response or association frames. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 5:

802.11 MAC Sublayer, page 122-123

CWAP-404 VCE Dumps   CWAP-404 Study Guide   CWAP-404 Exam Questions