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.certbus.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

Prior to a retransmission what happens to the CWmax value?

A. Increases by 1

B. Reset to 0

C. Set to the value of the AIFSN

D. Doubles and increases by 1

Correct Answer: D

Explanation: Before a retransmission, the CWmax (Contention Window maximum) value doubles and increases by 1. The CWmax is a parameter that determines the upper limit of the random backoff time that a STA (station) has to wait before attempting to access the medium. The random backoff time is chosen from a range of values between CWmin (Contention Window minimum) and CWmax. The CWmin and CWmax values depend on the AC (Access Category) of the traffic and the PHY type of the STA. If a transmission fails due to a collision or an error, the STA has to retransmit the frame after waiting for another random backoff time. However, to reduce the probability of another collision, the STA increases its CWmax value by doubling it and adding 1. This increases the range of possible backoff values and spreads out the STAs more evenly. The STA resets its CWmax value to its original value after a successful transmission or after reaching a predefined limit. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 7: QoS Analysis, page 196-197

QUESTION 2

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 3

Which one of the following is not an 802.11 Management frame?

A. PS-Poll

B. Action

C. Beacon

D. Authentication

Correct Answer: A

Explanation: A PS-Poll (Power Save Poll) frame is not an 802.11 management frame. A PS-Poll frame is a type of control frame that is used by a STA in power save mode to request data frames from an AP. A STA in power save mode can conserve battery power by periodically sleeping and waking up. When a STA sleeps, it cannot receive any data frames from the AP, so it informs the AP of its power save status by setting a bit in its MAC header. The AP then buffers any data frames destined for the sleeping STA until it wakes up. When a STA wakes up, it sends a PS-Poll frame to the AP, indicating its association ID and requesting any buffered data frames. The AP thenresponds with one or more data frames, followed by an ACK or BA frame from the STA. The other options are not correct, as they are types of 802.11 management frames. An Action frame is used to perform various management actions, such as spectrum management, QoS management, radio measurement, etc. A Beacon frame is used to advertise the presence and capabilities of an AP or BSS. An Authentication frame is used to establish or terminate an authentication relationship between a STA and an AP. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 6: 802.11 Frame Exchanges, page 169-170

QUESTION 4

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

Correct Answer: C

Explanation: Display filters are applied after the capture is completed and they only hide the packets from view. The filtered packets are still present in the capture file and can be enabled for view later by changing or removing the display filter.

This is an advantage over capture-time filters, which discard the packets that do not match the filter criteria and cannot be recovered later34 References:

CWAP-403 Study Guide, Chapter 2: Protocol Analysis, page 37 CWAP-403 Objectives, Section 2.3: Apply display filters

QUESTION 5

Which one of the following is not a valid acknowledgement frame?

A. RTS

B. CTS

C. Ack

D. Block Ack

Correct Answer: A

Explanation: RTS is not a valid acknowledgement frame. RTS stands for Request To Send, and it is a control frame that is used to initiate an RTS/CTS exchange before sending a data frame. The purpose of an RTS/CTS exchange is to reserve the medium for a data transmission and avoid collisions with hidden nodes. An acknowledgement frame is a control frame that is used to confirm the successful reception of a data frame or a block of data frames. The valid acknowledgement frames are CTS (Clear To Send), Ack (Acknowledgement), and Block Ack (Block Acknowledgement) . References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 186; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 187; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 189; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 190.

QUESTION 6

What is used to respond with an uplink transmission to an MU-RTS trigger frame in the 802.11ax PHY?

A. HE SU PPDU

B. HE MU PPDU

C. HE TB PPDU

D. VHT PPDU

Correct Answer: C

Explanation: An HE TB PPDU (High Efficiency Trigger-Based Packet Data Unit) is used to respond with an uplink transmission to an MU-RTS trigger frame in the 802.11ax PHY (Physical Layer). An MU-RTS trigger frame is a frame that initiates a multi-user transmission opportunity (MU-TXOP) by requesting multiple stations (STAs) to send clear- to-send (CTS) frames on different spatial streams or resource units (RUs). An HE TB PPDU is a frame that contains data from multiple STAs that have been allocated RUs by an MU-RTS trigger frame or another type of trigger frame. An HE SU PPDU (High Efficiency Single User Packet Data Unit) is a frame that contains data from a single STA using all available spatial streams or RUs. An HE MU PPDU (High Efficiency Multi User Packet Data Unit) is a frame that contains data from multiple STAs using different spatial streams or RUs without being triggered by another frame. A VHT PPDU (Very High Throughput Packet Data Unit) is a frame that uses the 802.11ac PHY and does not support multi-user transmissions.References: CWAP-404 Study Guide, Chapter 3: 802.11 MAC Layer Frame Formats and Technologies, page 101 CWAP-404 Objectives, Section 3.4: Analyze multi-user transmissions CWAP-404 Study Guide, Chapter 3: 802.11 MAC Layer Frame Formats and Technologies, page 99

QUESTION 7

In which element of a Beacon frame would you look to identity the current HT protection mode in which an AP is

operating?

A. HT Protection Element

B. HT Operations Element

C. ERP Information Element

D. HT Capabilities Element

Correct Answer: B

Explanation: The HT protection mode in which an AP is operating can be identified by looking at the HT Operations element in a Beacon frame. The HT Operations element is a part of the Beacon frame that contains information about the High Throughput (HT) capabilities and operation of an 802.11n BSS. The HT Operations element has a field called HT Protection, which indicates how the BSS protects its HT transmissions from interference or collisions with non-HT devices or BSSs. The HT Protection field can have four values: No Protection, Nonmember Protection, 20 MHz Protection, or Non-HT Mixed Mode. The other options are not correct, as they do not contain information about the HT protection mode. The HT Protection element does not exist, the ERP Information element is used for Extended Rate PHY (ERP) protection mode for 802.11g devices, and the HT Capabilities element is used for indicating the supported HT features of an individual device. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 5:

802.11 MAC Sublayer, page 125-126

QUESTION 8

Given a protocol analyzer can decrypt WPA2-PSK data packets providing the PSK and SSID are configured in the analyzer software. When performing packet capture (in a non- FT environment) which frames are required in order for PSK frame decryption to be possible?

A. Authentication

B. 4-Way Handshake

C. Reassociation

D. Probe Response

Correct Answer: B

Explanation: The 4-way handshake is the process that establishes the pairwise transient key (PTK) between the client and the AP in WPA2-PSK. The PTK is derived from the PSK, the SSID, and some random numbers exchanged in the handshake frames. The PTK is used to encrypt and decrypt the data frames between the client and the AP. Therefore, in order to decrypt WPA2-PSK data packets, a protocol analyzer needs to capture the 4-way handshake frames and have the PSK and SSID configured in the analyzer software12 References: CWAP-404 Study Guide, Chapter 3: 802.11 MAC Layer Frame Formats and Technologies, page 87 CWAP-404 Objectives, Section 3.5: Analyze security exchanges

QUESTION 9

Using a portable analyzer you perform a packet capture next to a client STA and you can see that the STA is associated to a BSS. You observe the STA sending packets to the AP and the AP sending packets to the STA. Less than 2% of all packets are retransmissions. You move to capture packets by the AP and, while the retry rate is still less than 2%, you

now only see unidirectional traffic from the AP to the client. How do you explain this behavior?

A. The portable analyzer is too close to the AP causing CCI, blinding the AP to the clients packets

B. The STA is transmitting data using more spatial streams than the potable analyzer can support

C. There is a transmit power mismatch between the client and the AP and while the client can hear the APs traffic, the AP cannot hear the client

D. The portable analyzer has a lower receive sensitivity than the AP and while it can\\'t capture the packets from the client STA, the AP can receive them OK

Correct Answer: D

Explanation: Receive sensitivity is the minimum signal level that a receiver can detect and decode. Different devices may have different receive sensitivity levels depending on their hardware specifications and antenna configurations. In this scenario, the portable analyzer has a lower receive sensitivity than the AP, meaning that it requires a stronger signal to capture the packets from the client STA. The AP, on the other hand, has a higher receive sensitivity and can receive the packets from the client STA even if they have a weaker signal. This explains why the portable analyzer can only see unidirectional traffic from the AP to the client when capturing near the AP5 References: CWAP-403 Study Guide, Chapter 4: PHY Layer Analysis, page 121 CWAP-403 Objectives, Section 4.3: Analyze PHY layer metrics

QUESTION 10

What does the value of the Listen Interval field in an Association Request frame indicate?

A. How long a STA performing active scanning will listen for Probe Responses before changing channels

B. How often a STA will go off channel to look for other BSSs

C. How often a STA in power save mode wakes up to listen to Beacon frames

D. How long a STA waits for an Ack before retransmitting the frame

Correct Answer: C

Explanation: The value of the Listen Interval field in an Association Request frame indicates how often a STA in power save mode wakes up to listen to Beacon frames. The Listen Interval is expressed in units of Beacon Intervals (typically 100 TU or 102.4 ms). For example, if the Listen Interval is set to 10, it means that the STA will wake up every 10 Beacon Intervals (or about 1 second) to check for buffered frames at the AP. The Listen Interval is used by the AP to determine how long it can hold frames for a STA in power save mode before discarding them . References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 197; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 198.