Vendor:CWNP

Exam Code:CWAP-404

Exam Name: Certified Wireless Analysis Professional

Version: Demo

QUESTION 1

How does a VoIP Phone, using WMM Power Save, request data frames buffered at the AP?

A. The VoIP phone transmits a PS-Poll frame

B. The VoIP phone sets the More Data bit in the MAC Header to 1

C. The VoIP phone transmits a WMM Action frame

D. The VoIP phone transmits a trigger frame, which is a QoS Null frame or a QoS Data frame

Correct Answer: D

Explanation: A VoIP phone, using WMM Power Save, requests data frames buffered at the AP by transmitting a trigger frame, which is a QoS Null frame or a QoS Data frame. WMM Power Save is a power saving mode that allows a STA (station) to conserve battery power by periodically sleeping and waking up. WMM Power Save is based on WMM (Wi-Fi Multimedia), which is a QoS (Quality of Service) enhancement that provides prioritized and differentiated access to the medium fordifferent types of traffic. 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 trigger frame to the AP, indicating its AC (Access Category), which is a logical queue that corresponds to its QoS level. A trigger frame can be either a QoS Null frame or a QoS Data frame, depending on whether it has any payload or not. The AP then responds with one or more data frames from the same AC as the trigger frame, followed by an ACK or BA (Block Acknowledgement) frame from the STA. The other options are not correct, as they are not used by a VoIP phone using WMM Power Save to request data frames buffered at the AP. A PS-Poll (Power Save Poll) frame is used by a STA using legacy power save mode, not WMM Power Save mode, to request data frames buffered at the AP. A PS-Poll frame does not indicate any AC or QoS information. Setting the More Data bit in the MAC header to 1 does not request any data frames from the AP, but indicates that there are more data frames to be sent by the STA or received by the STA. Transmitting a WMM Action frame does not request any data frames from the AP, but performs various management actions related to WMM features, such as admission control, parameter update, etc. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 7: QoS Analysis, page 198-199

QUESTION 2

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

Correct Answer: D

Explanation: The function of the PHY preamble is to allow the receiver to detect and synchronize with the signal. The PHY preamble is a part of the PPDU that is transmitted before the PHY header and the PSDU. The PHY preamble consists of a series of training fields that help the receiver to adjust its parameters, such as frequency, timing, and gain, to match the incoming signal. The PHY preamble also helps the receiver to estimate the channel conditions and noise level. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 99-100

QUESTION 3

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 4

When would you expect to see a Reassociation Request frame?

A. Every time a STA associates to an AP to which it has previously been associated

B. Only when a STA is using FT roaming

C. Only when a STA roams back to an AP it has previously been associated with

D. Every time a STA roams

Correct Answer: D

Explanation: A Reassociation Request frame is sent every time a STA roams from one AP to another within the same ESS. A Reassociation Request frame is similar to an Association Request frame, but it also contains the BSSID of the current AP that the STA is leaving. This allows the new AP to coordinate with the old AP and transfer the STA\\'s context information, such as security keys, QoS parameters, and buffered frames. This way, the STA can maintain its connectivity and session continuity during roaming . References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 195;CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 196.

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

QUESTION 6

What is the default 802.11 authentication method for a STA when using Pre-RSNA?

A. Open System

B. Shared Key

C. 4-Way Handshake

D. PSK

Correct Answer: A

Explanation: The default 802.11 authentication method for a STA when using Pre-RSNA is Open System. This is the simplest and most common authentication method, which does not provide any security or encryption. In Open System authentication, the STA sends an Authentication Request frame to the AP, and the AP responds with an Authentication Response frame with a status code of success. After this, the STA can proceed to association with the AP . References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 181; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter

6: MAC Sublayer Frame Exchanges, page 183.

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

Which one of the following should be the first step when troubleshooting a WLAN issue?

A. Identify probable causes

B. Identify capture locations

C. Perform an initial WLAN scan and see if any obvious issues stand out

D. Define the problem

Correct Answer: D

Explanation: The first step in any troubleshooting process is to define the problem. This involves gathering information from various sources, such as users, network administrators, network documentation, and network monitoring tools.

Defining the problem helps to narrow down the scope of the issue and identify the symptoms, causes, and effects of the problem12 References:

CWAP-403 Study Guide, Chapter 1: Troubleshooting Methodology, page 7 CWAP-403 Objectives, Section 1.1: Define the problem

---

QUESTION 9

Where would you look in a packet trace file to identify the configured Minimum Basic Rate (MBR) of a BSS?

A. Supported Rates and Extended Supported Rates elements in a Beacon frame

B. In the MBR Action frame

C. In the MBR Information Element in an Association Response frame

D. In the Minimum Basic Rate Element in a Beacon frame

Correct Answer: A

Explanation: The configured Minimum Basic Rate (MBR) of a BSS can be identified by looking at the Supported Rates and Extended Supported Rates elements in a Beacon frame. A Beacon frame is a type of management frame that is transmitted by an AP to advertise its presence and capabilities to potential clients. A Beacon frame contains various information elements (IEs) that provide details about the BSS configuration and operation. The Supported Rates andExtended Supported Rates IEs list the data rates that are supported by the AP for data transmission. The MBR is the lowest data rate among these supported rates that is required for all clients to join and communicate with the BSS. The MBR is usually marked with a flag bit in these IEs to indicate its mandatory status. The other options are not correct, as they do not exist or do not indicate the MBR of a BSS. References: [Wireless Analysis Professional Study Guide CWAP404], Chapter 5:

802.11 MAC Sublayer, page 123-124

QUESTION 10

You are performing a multiple adapter channel aggregation capture to troubleshoot a VoIP roaming problem and would like to measure the roaming time from the last VoIP packet sent on the old AP\\'s channel to the first VoIP packet sent on the new AP\\'s channel. Which timing column in the packet view would measure this for you?

A. Roaming

B. Relative

C. Absolute

D. Delta

Correct Answer: D

Explanation: Delta is the timing column in the packet view that measures the time difference between two consecutive packets in a capture file. Delta can be used to measure the roaming time from the last VoIP packet sent on the old AP\\'s channel to the first VoIP packet sent on the new AP\\'s channel by selecting these two packets and looking at their delta values. The other timing columns are not suitable for this measurement because they do not show the time difference between two specific packets. Roaming is a column that shows whether a packet belongs to a roaming event or not. Relative is a column that shows the time elapsed since the beginning of the capture file. Absolute is a column that shows the date and time when a packet was captured5 References: CWAP-404 Study Guide, Chapter 2: Protocol Analysis, page 57 CWAP-404 Objectives, Section 2.4: Analyze timing values

---

QUESTION 11

During a VHT Transmit Beamforming sounding exchange, the beamformee transmits a Compressed Beamforming frame to the beamformer. What is communicated within this Compressed Beamforming frame?

A. Steering Matrix

B. Beamforming Matrix

C. Feedback Matrix

D. Beamformee Matrix

Correct Answer: C

Explanation: The beamformee transmits a Feedback Matrix within the Compressed Beamforming frame to the beamformer. The Feedback Matrix contains information about the channel state between the beamformee and each spatial stream of the beamformer. This information is used by the beamformer to adjust its transmit weights and optimize its signal for the beamformee34. References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 11: 802.11n/ac/ax PHYsical Layer Frame Exchanges, page 4033; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 11: 802.11n/ac/ax PHYsical Layer Frame Exchanges, page 4064.

QUESTION 12

Finish the statement:

It is possible to distinguish between_____22 MHz transmissions and_____20 MHz transmissions when looking at an FFT plot.

A. HR/DSSS and ERP

B. OFDM and HT

C. ERP and VHT

D. HT and VHT

Correct Answer: B

Explanation: It is possible to distinguish between OFDM 20 MHz transmissions and HT 20 MHz transmissions when looking at an FFT plot. OFDM and HT are two different modulation schemes used by 802.11 WLANs. OFDM is used by legacy 802.11a/g devices, while HT is used by newer 802.11n/ac devices. OFDM and HT have different spectral characteristics that can be observed on an FFT plot. OFDM transmissions have a flat spectrum with sharp edges, while HT transmissions have a tapered spectrum with rounded edges. This is because HT uses guard intervals and cyclic prefixes to reduce inter-symbol interference and improve performance. The other options are not correct, as they do not describe different modulation schemes or channel widths that can be distinguished on an FFT plot. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 3: Spectrum Analysis, page 70-71