Exam Questions CWAP-404

Certified Wireless Analysis Professional

https://www.2passeasy.com/dumps/CWAP-404/

NEW QUESTION 1
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

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

NEW QUESTION 2
Where would you look in a packet trace file to identify the configured Minimum Basic Rate (MBR) of a BSS?

A. Supported Rates & 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

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 CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 123-124

NEW QUESTION 3
When performing protocol analysis, you notice a high number of RTS/CTS frames being transmitted on an HT network. You suspect this may be due to HT protection mechanisms. Where in the Beacon frame would you look to determine which one of the four HT protection modes the AP is operating in?

A. HT Protection Element
B. HT Information Element
C. HT Operation Element
D. Non-HT Present Element

Answer: B

Explanation:
When performing protocol analysis, you would look at the HT Information Element in the Beacon frame to determine which one of the four HT protection modes the AP is operating in. The HT Information Element contains various subfields that provide information about the HT network configuration and operation. One of these subfields is the HT Protection field, which indicates whether any protection mechanisms are required for mixed-mode operation with non-HT STAs. The four possible values for this field are:
? No Protection: No protection mechanisms are required.
? Non-member Protection: RTS/CTS or CTS-to-self protection is required for all HT transmissions.
? 20 MHz Protection: RTS/CTS or CTS-to-self protection is required for all HT transmissions using a 40 MHz channel.
? Non-HT Mixed Mode: All HT transmissions must use a non-HT preamble and header . References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 11: 802.11n/ac/ax PHYsical Layer Frame Exchanges, page 378; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 11: 802.11n/ac/ax PHYsical Layer Frame Exchanges, page 379.

NEW QUESTION 4
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

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

NEW QUESTION 5
You are troubleshooting a client that is experiencing slow WLAN performance. As part of the troubleshooting activity, you start a packet capture on your laptop close to the client device. While analyzing the packets, you suspect that you have not captured all packets transmitted by the client. By analyzing the trace file, how can you confirm if you have missing packets?

A. The missing packets will be shown as CRC errored packets
B. Protocol Analyzers show the number of missing packets in their statistics view
C. Look for gaps in the sequence number in MAC headers.
D. Retransmission are an indication of missing packets

Answer: C

Explanation:
One way to confirm if you have missing packets in your packet capture is to look for gaps in the sequence number in MAC headers. The sequence number is a 12-bit field in the MAC header that is used to identify and order data frames within a traffic stream. The sequence number is incremented by one for each new data frame transmitted by a STA, except for retransmissions, fragments, and control frames. The sequence number can range from 0 to 4095, and then wraps around to 0. If you see a jump or a gap in the sequence number between two consecutive data frames from the same STA, it means that you have missed some packets in between. The other options are not correct, as they do not confirm if you have missing packets in your packet capture. CRC errored packets are packets that have been corrupted during transmission and have failed the error detection check. Protocol analyzers may show the number of CRC errored packets in their statistics view, but not the number of missing packets. Retransmissions are an indication of packet loss or collision, but not necessarily of missing packets in your capture. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 114-115

NEW QUESTION 6
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

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

NEW QUESTION 7
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

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

NEW QUESTION 8
Why would a STA that supports 802.11k Radio Measurement send a Neighbor Request to an AP?

A. To learn about neighboring interference sources and tune its RF radio accordingly
B. To inform the current AP about the STA's intent to roam to a neighboring AP, ensuring a seamless handover
C. To request a list of neighboring APs which the STA can use as roaming candidates
D. To request a list of neighboring STAs which enables the STA to better pick the right protection mechanisms

Answer: C

Explanation:
A STA that supports 802.11k Radio Measurement would send a Neighbor Request to an AP to request a list of neighboring APs which the STA can use as roaming candidates. A Neighbor Request is an Action frame that contains a subelement specifying the type of information that the STA wants to receive from the AP. A Neighbor Report is an Action frame that contains a subelement with a list of neighboring APs that match the criteria specified in the Neighbor Request. The Neighbor Report provides information such as BSSID, channel, operating class, and PHY type of each neighboring AP. This information helps the STA to perform intelligent roaming decisions based on signal quality, load, and compatibility . References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 12: 802.11k/v/r/u/w/ai Amendments, page 434; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 12: 802.11k/v/r/u/w/ai Amendments, page 435.

NEW QUESTION 9
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

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

NEW QUESTION 10
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 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

NEW QUESTION 10
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

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.

NEW 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

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

NEW QUESTION 17
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:
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

NEW QUESTION 18
Protocol analyzers may present field values in either binary, decimal or hexadecimal. What preceeds a hexadecimal value to indicate it is hexadecimal?

A. 0x
B. 16x
C. %
D. HEX

Answer: A

Explanation:
A hexadecimal value is a value that uses base 16 notation, which means it can have digits from 0 to 9 and letters from A to F. A hexadecimal value is usually preceded by 0x to indicate that it is hexadecimal and not decimal or binary. For example, 0x0A is hexadecimal for 10 in decimal or 00001010 in binary. The other options are not valid prefixes for hexadecimal values.References:
? CWAP-404 Study Guide, Chapter 2: Protocol Analysis, page 35
? CWAP-404 Objectives, Section 2.2: Analyze field values

NEW QUESTION 23
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

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

NEW QUESTION 28
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CWAP-404 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CWAP-404 Product From:

https://www.2passeasy.com/dumps/CWAP-404/

Money Back Guarantee

CWAP-404 Practice Exam Features:

* CWAP-404 Questions and Answers Updated Frequently

* CWAP-404 Practice Questions Verified by Expert Senior Certified Staff

* CWAP-404 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CWAP-404 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year