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.leads4pass.com/cwap-404.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

As a wireless network consultant you have been called in to troubleshoot a high-priority issue for one of your customers. The customer\\'s office is based on two floors within a multi- tenant office block. On one of these floors (floor 5) users cannot connect to the wireless network. During their own testing the customer has discovered that users can connect on floor 6 but not when they move to the floor 5. This issue is affecting all users on floor 5 and having a negative effect on productivity.

To troubleshoot this issue, you perform both Spectrum and Protocol Analysis. The Spectrum Analysis shows the presence of Bluetooth signals which you have identified as coming from wireless mice. In the protocol analyzer you see the top frame on the network is Deauthentication frames. On closer investigation you see that the Deauthentication frames\\' source addresses match the BSSIDs of your customers APs and the destination address is FF:FF:FF:FF:FF:FF:FF.

What do you conclude from this troubleshooting exercise?

A. The customer should replace all their Bluetooth wireless mice as they are stopping the users on floor 5 from connecting to the wireless network

B. The users on floor 5 are being subjected to a denial of service attack, as this is happening across the entire floor it is likely to be a misconfigured WIPS solution belonging to the tenants on the floor below

C. The customers APs are misbehaving and a technical support case should be open with the vendor

D. The CCI from the APs on the floor 4 is the problem and you need to ask the tenant below to turn down their APs Tx power

Correct Answer: B

Explanation: The users on floor 5 are being subjected to a denial of service attack, as this is happening across the entire floor it is likely to be a misconfigured WIPS solution belonging to the tenants on the floor below. This is because the

Deauthentication frames have a source address that matches the BSSIDs of the customer\\'s APs and a destination address that is a broadcast address (FF:FF:FF:FF:FF:FF). This indicates that someone is sending spoofed Deauthentication

frames to all STAs associated with the customer\\'s APs, causing them to disconnect from the wireless network. This is a common type of DoS attack on wireless networks, and it could be caused by a rogue device or a WIPS solution that is

configured to protect the wireless network of another tenant on the floor below12. References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 13: Troubleshooting Common Wi-Fi Issues, page 4961;

CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 14:

Troubleshooting Tools, page 5272.

QUESTION 2

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

Correct 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

QUESTION 3

In what scenario is Open Authentication without encryption not allowed based on the 802.11 standard?

A. When operating a BS5 in the CBRS band

B. When operating a BSS in FIPS mode

C. When operating a BSS in a government facility

D. When operating a BSS in the 6 GHz band

Correct Answer: D

Explanation: Open Authentication without encryption is not allowed when operating a BSS in the 6 GHz band, according to the 802.11 standard. Open Authentication is a type of authentication method that does not require any credentials or security information from a STA (station) to join a BSS (Basic Service Set). Open Authentication can be used with or without encryption, depending on the configuration of the BSS and the STA. Encryption is a technique that scrambles the data frames using an algorithm and a key to prevent unauthorized access or eavesdropping. However, in the 6 GHz band, which is a newly available frequency band for WLANs, OpenAuthentication without encryption 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. The other options are not correct, as they do not describe scenarios where Open Authentication without encryption is not allowed by the 802.11 standard. When operating a BSS in the CBRS band, which is another newly available frequency band for WLANs, Open Authentication without encryption is allowed, but not recommended, as it also poses security and interference risks for other users and services in the band. When operating a BSS in FIPS mode, which is a mode that complies with the Federal Information Processing Standards for cryptographic security, Open Authentication without encryption is allowed, but not compliant, as it does

not meet the FIPS requirements for encryption algorithms and keys. When operating a BSS in a government facility, Open Authentication without encryption is allowed, but not advisable, as it may violate the government policies or regulations for wireless security. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 8: Security Analysis, page 220-221

QUESTION 4

When configuring a long-term, forensic packet capture and saving all packets to disk which of the following is not a consideration?

A. Real-time packet decodes

B. Analyzer location

C. Total capture storage space

D. Individual trace file size

Correct Answer: A

Explanation: Real-time packet decodes are not a consideration when configuring a long- term, forensic packet capture and saving all packets to disk. Real-time packet decodes are useful for live analysis and troubleshooting, but they consume CPU and memory resources that could affect the performance of the capture process. For a long-term, forensic packet capture, it is more important to consider the analyzer location, the total capture storage space, and the individual trace file size. These factors affect the quality and quantity of the captured packets and the ease of post-capture analysis34 References: CWAP-404 Study Guide, Chapter 2: Protocol Analysis, page 49 CWAP-404 Objectives, Section 2.1: Configure protocol analyzers

QUESTION 5

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 6

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

Correct Answer: C

Explanation: One of the information that is communicated by bits in the PHY header is data rate. Data rate is the speed at which data is transmitted or received over the wireless medium. Data rate depends on factors such as modulation, coding, channel width, spatial streams, and guard interval. Data rate is indicated by bits in different fields of the PHY header, depending on the type of PPDU (e.g., OFDM, HT, VHT, HE). The receiver uses these bits to determine how to decode and demodulate the rest of the PPDU. The other options are not correct, as they are not communicated by bits in the PHY header. SNR (Signal-to-Noise Ratio), noise, and signal strengthare measured by the receiver based on its own capabilities and environment. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 101-105

QUESTION 7

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 8

Which piece of information is not transmitted in an HT PPDU header?

A. Number of Spatial Streams

B. PPDU length

C. MCS index

D. Channel number

Correct Answer: D

Explanation: The channel number is not transmitted in an HT PPDU header. An HT PPDU header is a part of the PPDU that contains information such as modulation, coding, data rate, and number of spatial streams for an 802.11n transmission. The channel number is not included in the HT PPDU header, as it is determined by the frequency band and channel width that are used by the transmitter and receiver. The channel number can be inferred from the frequency band and channel width, which are indicated by bits in different fields of the HT PPDU header, such as HT-SIG and HT-LTF. The other options are not correct, as they are transmitted in an HT PPDU header. The number of spatial streams, PPDU length, and MCS index are indicated by bits in the HT-SIG field of the HT PPDU header. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 4:

802.11 Physical Layer, page 108-109

QUESTION 9

You have installed a new 802.1 lac WLAN configured with 80 MHz channels. Users in one area are complaining about poor performance. This area is currently served by a single AP. You take a spectrum analysis capture in the poor performing area. While examining the waterfall plot you notice the airtime utilization is higher on the first 20 MHz of the 80 MHz channel when compared to the rest of the channel. What do you conclude?

A. The AP is misconfigured and needs to be reconfigured to 80 MHz operation

B. Non-Wi-Fi interference is preventing the APs 80 MHz operation

C. The first 20 MHz is the AP\\'s primary channel and higher airtime utilization on the primary channel is normal when an AP is configured for 80 MHz operation

D. RRM is enabled and has dynamically picked a 20 MHz channel

Correct Answer: B

Explanation: The most likely cause of higher airtime utilization on the first 20 MHz of the 80 MHz channel is non-Wi-Fi interference. Non-Wi-Fi interference can prevent an AP from using its full channel width, as it will degrade the signal quality and increase the noise floor on some parts of the channel. This will force the AP to fall back to a narrower channel width, such as 20 MHz or 40 MHz, to maintain communication with its clients. The waterfall plot can help identify non-Wi-Fi interference by showing spikes or bursts of RF energy on specific frequencies or sub-channels. The other options are not correct, as they do not explain why only the first 20 MHz of the channel has higher airtime utilization. References: [Wireless Analysis Professional Study Guide], Chapter 3: Spectrum Analysis, page 74-75

QUESTION 10

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.