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

QUESTION 1

How is the length of an AIFS calculated?

A. DIFS + SIFS + AIFSN

B. SIFS + AIFS * Time Unit

C. SIFS * Slot Time + AIFSN

D. AIFSN * Slot Time + SIFS

Correct Answer: D

Explanation: The length of an AIFS (Arbitration Interframe Space) is calculated by multiplying the AIFSN (Arbitration Interframe Space Number) by the Slot Time and adding the SIFS (Short Interframe Space). An AIFS is a variable interframe space introduced by 802.11e to help prioritize medium access for different Access Categories (ACs). An AC is a logical queue that corresponds to a QoS (Quality of Service) level for different types of traffic. Each AC has a different AIFSN value, which determines how long it has to wait before attempting to access the medium. A lower AIFSN value means a higher priority and a shorter waiting time. The Slot Time is a fixed value that depends on the PHY type and channel width. The SIFS is the shortest interframe space that is used for high-priority transmissions, such as ACKs or CTSs. The formula for calculating the AIFS length is: AIFS = AIFSN * Slot Time + SIFS. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 7: QoS Analysis, page 194-195

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

The network administrator at ABC Engineering has taken a large packet capture from one of their APs running in monitor mode. She has very little knowledge of 802.11 protocols but would like to use the capture file to evaluate the overall health and performance of their wireless network. When she asks your advice, which tool do you recommend she opens the packet capture file with?

A. Spectrum analyzer

B. Python

C. Capture visualization tool

D. WLAN scanner

Correct Answer: C

Explanation: A capture visualization tool is a software application that can open a packet capture file and display various graphs, charts, tables, and statistics that illustrate the characteristics and behavior of the wireless network. A capture visualization tool can help a network administrator with little knowledge of 802.11 protocols to evaluate the overall health and performance of their wireless network by providing a visual and intuitive representation of the captured data. A spectrum analyzer is a hardware device that measures the radio frequency signals in a given frequency range and displays their amplitude, frequency, and modulation. A spectrum analyzer can help identify sources of interference and noise in the wireless environment, but it cannot open a packet capture file. Python is a programming language that can be used to write scripts or applications that manipulate or analyze packet capture files, but it requires coding skills and knowledge of 802.11 protocols. A WLAN scanner is a software application that scans for available wireless networks and displays information such as SSID, BSSID, channel, signal strength, security type, and vendor. A WLAN scanner can help discover wireless networks and their basic parameters, but it cannot open a packet capture file345 References: CWAP-404 Study Guide, Chapter 2: Protocol Analysis, page 63 CWAP-404 Objectives, Section 2.5: Use capture visualization tools CWAP-404 Study Guide, Chapter 4: Spectrum Analysis and Troubleshooting, page 117 CWAP-404 Objectives, Section 4.1: Use spectrum analysis tools CWAP-404 Study Guide, Chapter 2: Protocol Analysis, page 33 CWAP-404 Objectives, Section 2.2: Analyze field values

QUESTION 4

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 5

What should the To DS and From DS flags be to set to in an Association Response frame?

A. To DS = 1, From DS = 1

B. To DS - 1, From DS = 0

C. To DS - 0, From DS = 0

D. To DS = 0, From DS = 1

Correct Answer: C

Explanation: The To DS and From DS flags should be set to 0 in an Association Response frame. An Association Response frame is a type of management frame that is transmitted by an AP to accept or reject an association request from a STA. The To DS (To Distribution System) and From DS (From Distribution System) flags are two bits in the Frame Control field of the MAC header that indicate whether a frame is destined for or originated from the DS (Distribution System), which is a system that connects multiple BSSs together. The To DS and From DS flags can have four possible combinations: 00, 01, 10, or 11. For an Association Response frame, which is sent from an AP to a STA within a BSS, both flags should be set to 0. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 121-122