



CWNP

Exam Questions CWAP-404

Certified Wireless Analysis Professional

NEW QUESTION 1

ABC International has installed a new smart ZigBee controlled lighting system. However, the network team is concerned that this new system will interfere with the existing WLAN and has asked you to investigate the impact of the two systems operating simultaneously in the 2.4 GHz band. When performing Spectrum Analysis, which question could you answer by looking at the FFT plot?

- A. Do the ZigBee channels used by the lighting system overlap with the WLAN channels?
- B. Is the ZigBee system using more than 50% of the available airtime?
- C. Is the WLAN corrupting ZigBee system messages?
- D. Is the ZigBee system causing an increase in WLAN retries?

Answer: A

Explanation:

The FFT plot is a spectrum analysis plot that shows the RF power present at a particular frequency over a short period of time. It can help identify the sources and characteristics of RF signals in the spectrum. By looking at the FFT plot, you can determine which ZigBee channels are used by the lighting system and whether they overlap with the WLAN channels in the 2.4 GHz band. ZigBee channels are 5 MHz wide and WLAN channels are 20 MHz or 40 MHz wide, so there is a possibility of overlap and interference between them. The other questions cannot be answered by looking at the FFT plot alone, as they require other types of plots or analysis tools, such as duty cycle plot, airtime utilization plot, or protocol analyzer. References: [Wireless Analysis Professional Study Guide], Chapter 3: Spectrum Analysis, page 69-70

NEW QUESTION 2

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

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

NEW QUESTION 3

When a data frame is encrypted with WPA2, to which portion of the frame is the encryption applied?

- A. Frame body and MAC Header
- B. Frame body excluding the LLC PDU
- C. Frame body including the LLC PDU
- D. The whole MPDU

Answer: C

Explanation:

When a data frame is encrypted with WPA2, the encryption is applied to the frame body including the LLC PDU. The LLC PDU (Logical Link Control Protocol Data Unit) is a part of the frame body that contains information such as protocol type, source and destination service access points (SAPs), and control fields. The LLC PDU is added by the LLC (Logical Link Control) sublayer to provide multiplexing and flow control functions for different upper layer protocols. When a data frame is encrypted with WPA2, which uses AES-CCMP as its encryption algorithm, both the payload and the LLC PDU are encrypted as a single unit. The MAC header and FCS are not encrypted, as they are needed for addressing and error detection purposes. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 115-116

NEW QUESTION 4

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

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.

NEW QUESTION 5

Which one of the these is the most important in the WLAN troubleshooting methodology among those listed?

- A. Obtain detailed -knowledge of the wireless vendors debug and logging options
- B. Interview the network manager about the issues being experienced
- C. Observe the problem
- D. Talk to the end users about their experiences

Answer: C

Explanation:

Observing the problem is the most important step in the WLAN troubleshooting methodology among those listed. This step involves capturing and analyzing the relevant data from the wireless network, such as packets, frames, spectrum, and performance metrics. Observing the problem helps to verify the existence and scope of the issue, identify the root cause and possible solutions, and validate the results of any actions taken. The other steps are also important, but they are not as critical as observing the problem¹² References:

? CWAP-404 Study Guide, Chapter 1: Troubleshooting Methodology, page 15

? CWAP-404 Objectives, Section 1.2: Observe the problem

NEW QUESTION 6

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

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

NEW QUESTION 7

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

- A. RTS
- B. CTS
- C. Ack
- D. Block Ack

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.

NEW QUESTION 8

What interframe space would be expected between a CTS and a Data frame?

- A. PIFS
- B. AIFS
- C. DIFS
- D. SIFS

Answer: D

Explanation:

The interframe space that would be expected between a CTS (Clear to Send) and a Data frame is SIFS (Short Interframe Space). A SIFS is the shortest interframe space that is used for high-priority transmissions, such as ACKs (Acknowledgements), CTSs, or data frames that are part of a fragmentation or aggregation process. A SIFS is a fixed value that depends on the PHY type and channel width. A CTS and a Data frame are part of a virtual carrier sense mechanism called RTS/CTS (Request to Send/Clear to Send), which is used to avoid collisions and hidden node problems in wireless transmissions. When a STA (station) wants to send a data frame, it first sends an RTS frame to the intended receiver, indicating the duration of the transmission. The receiver then responds

with a CTS frame, also indicating the duration of the transmission. The other STAs in the vicinity hear either the RTS or the CTS frame and update their NAV (Network Allocation Vector) timers accordingly, deferring their access to the medium until the transmission is over. The sender then sends the data frame after waiting for a SIFS, followed by an ACK frame from the receiver after another SIFS. The other options are not correct, as they are not used between a CTS and a Data frame. A PIFS (PCF Interframe Space) is used for medium access by the PCF (Point Coordination Function), which is an optional and rarely implemented polling-based mechanism that provides contention-free service for time-sensitive traffic. An AIFS (Arbitration Interframe Space) is used for medium access by different ACs (Access Categories), which are logical queues that correspond to different QoS (Quality of Service) levels for different types of traffic. An AIFS is a variable interframe space that depends on the AIFSN (Arbitration Interframe Space Number) value of each AC. A DIFS (Distributed Interframe Space) is used for medium access by the DCF (Distributed Coordination Function), which is the default and mandatory contention-based mechanism that provides best-effort service for normal traffic. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 6: 802.11 Frame Exchanges, page 166-167; Chapter 7: QoS Analysis, page 194-195

NEW QUESTION 9

Given: The Frame Check Sequence (FCS) is a 32 CRC used for error detection. The CRC is calculated over what?

- A. Mac Header and Frame Body only
- B. Frame Body only
- C. PHY Header, MAC Header and Frame Body
- D. PHY Header and Mac Header only

Answer: A

Explanation:

The CRC is calculated over the MAC Header and Frame Body only. The CRC (Cyclic Redundancy Check) is a 32-bit value that is used for error detection in wireless transmissions. The CRC is calculated over the MAC Header and Frame Body of a PSDU, which are the parts of the data unit that contain information such as source and destination addresses, frame type, frame control, sequence number, payload, etc. The CRC is appended to the end of the PSDU as a FCS (Frame Check Sequence) field. The CRC is not calculated over the PHY Header or PHY Preamble, which are parts of the PPDU that contain information such as modulation, coding, data rate, etc. The PHY Header and PHY Preamble are added or removed by the PHY layer during the conversion between PSDU and PPDU. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 97-98

NEW QUESTION 10

How many frames make up the Group Key Handshake excluding any Ack frames that may be required?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: B

Explanation:

The Group Key Handshake consists of two frames excluding any Ack frames that may be required. The Group Key Handshake is used to distribute and update the Group Temporal Key (GTK) for encrypting broadcast and multicast traffic. The AP initiates the Group Key Handshake by sending a Group Key Message 1 frame to a STA, which contains the new GTK and other information. The STA responds with a Group Key Message 2 frame to the AP, which confirms the receipt of the GTK and other information. After this, both the AP and the STA can use the new GTK for encryption and decryption of broadcast and multicast traffic. References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 7: 802.11 Security, page 246; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 7: 802.11 Security, page 247.

NEW QUESTION 10

A manufacturing facility has installed a new automation system which incorporates an 802.11 wireless network. The automation system is controlled from tablet computers connected via the WLAN. However, the automation system has not gone live due to problem with the tablets connecting to the WLAN. The WLAN vendor has been onsite to perform a survey and confirmed good primary and secondary coverage across the facility. As a CWAP you are called in to perform Spectrum Analysis to identify any interference sources. From the spectrum analysis, you did not identify any interference sources but were able to correctly identify the issue. Which of the following issues did you identify from the spectrum analysis?

- A. The tablets are connecting to the wrong SSID
- B. The tablets are entering power save mode and failing to wake up to receive the access points transmissions
- C. A high noise floor has resulted in a SNR of less than 20dB
- D. There is a power mismatch between the APs and the clients

Answer: D

Explanation:

The most likely issue that can be identified from the spectrum analysis is a power mismatch between the APs and the clients. A power mismatch occurs when the APs transmit at a higher power level than the clients, or vice versa. This can cause asymmetric communication, where one side can hear the other, but not vice versa. This can result in poor performance, disconnections, or packet loss. A spectrum analysis can reveal a power mismatch by showing different signal amplitudes or RSSI values for the APs and the clients on the same channel or frequency. The other options are not correct, as they cannot be identified from the spectrum analysis alone. The tablets' SSID, power save mode, and noise floor can be determined by using other tools or methods, such as protocol analysis, site survey, or device configuration. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 3: Spectrum Analysis, page 79-80

NEW QUESTION 12

What is the function of the PHY layer?

- A. Convert PPDU to PSDU for transmissions and PSDU to PPDU for receptions
- B. Convert MSDU to PPDU for transmissions and PPDU to MSDU for receptions
- C. Convert PPDU to MSDU for transmissions and MSDU to PPDU for receptions
- D. Convert PSDU to PPDU for transmissions and PPDU to PSDU for receptions

Answer: D

Explanation:

The function of the PHY layer is to convert PSDUs to PPDU for transmissions and PPDU to PSDUs for receptions. A PSDU (PHY Service Data Unit) is the data unit that is passed from the MAC layer to the PHY layer for transmission, or from the PHY layer to the MAC layer for reception. A PPDU (PHY Protocol Data Unit) is the data unit that is transmitted or received over the wireless medium by the PHY layer. A PPDU consists of a PSDU and a PHY header, which contains information such as modulation, coding, and data rate. The PHY layer adds or removes the PHY header to or from the PSDU during the conversion process. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 97-98

NEW QUESTION 14

Which one of the following statements is not true concerning DTIMs?

- A. Buffered Broadcast and Multicast traffic will be transmitted following a DTIM
- B. The DTIM interval can dictate when an STA will wake up to listen to beacon frames
- C. DTIM stands for Delivery Traffic Indication Map
- D. Every Beacon frame must contain a DTIM

Answer: D

Explanation:

Every Beacon frame must contain a DTIM is not a true statement concerning DTIMs. DTIM stands for Delivery Traffic Indication Message, and it is a subfield within the TIM (Traffic Indication Map) element in a Beacon frame. The DTIM indicates how many Beacon frames (including the current one) will appear before the next DTIM. For example, if the DTIM interval is set to 3, it means that every third Beacon frame will contain a DTIM. Buffered broadcast and multicast traffic will be transmitted following a DTIM, so that STAs in power save mode can wake up and receive them. The DTIM interval can also dictate when an STA will wake up to listen to Beacon frames, as some STAs may choose to only listen to Beacon frames that contain a DTIM. References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 200; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 201.

NEW QUESTION 19

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 20

What is encrypted within the third message of the 4-Way Handshake?

- A. PMK
- B. PTK
- C. GMK
- D. GTK

Answer: D

Explanation:

The GTK (Group Temporal Key) is encrypted within the third message of the 4-Way Handshake. The 4-Way Handshake is a process that establishes a secure connection between a STA (station) and an AP (access point) using WPA2 (Wi-Fi Protected Access 2), which is a security protocol that uses AES-CCMP (Advanced Encryption Standard-Counter Mode CBC-MAC Protocol) as its encryption algorithm. The 4-Way Handshake consists of four messages that are exchanged between the STA and the AP. The first message is sent by the AP to the STA, containing the ANonce (Authenticator Nonce), which is a random number generated by the AP. The second message is sent by the STA to the AP, containing the SNonce (Supplicant Nonce), which is a random number generated by the STA, and the MIC (Message Integrity Code), which is a value that verifies the integrity of the message. The third message is sent by the AP to the STA, containing the GTK, which is a key that is used to encrypt and decrypt multicast and broadcast data frames, and the MIC. The GTK is encrypted with the KEK (Key Encryption Key), which is derived from the PTK (Pairwise Temporal Key). The PTK is a key that is used to encrypt and decrypt unicast data frames, and it is derived from the PMK (Pairwise Master Key), the ANonce, and the SNonce. The fourth message is sent by the STA to the AP, containing only the MIC, to confirm the completion of the 4-Way Handshake. The other options are not correct, as they are not encrypted within the third message of the 4-Way Handshake. The PMK is a key that is derived from a passphrase or obtained from an authentication server, and it is not transmitted in any message of the 4-Way Handshake. The PTK is a key that is derived from the PMK, the ANonce, and the SNonce, and it is not transmitted in any message of the 4-Way Handshake. The GMK (Group Master Key) is a key that is generated by the AP and used to derive the GTK, and it is not transmitted in any message of the 4-Way Handshake. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 8: Security Analysis, page 211-213

NEW QUESTION 21

An RTS frame should be acknowledged by which frame?

- A. CTS
- B. Ack
- C. RTS-Ack
- D. Block Ack

Answer: A

Explanation:

An RTS (Request to Send) frame should be acknowledged by a CTS (Clear to Send) frame. An RTS and CTS frame are types of control frames that are used to implement a virtual carrier sense mechanism called RTS/CTS. RTS/CTS is a technique that helps to avoid collisions and hidden node problems in wireless transmissions. When a STA (station) wants to send a data frame, it first sends an RTS frame to the intended receiver, indicating the duration of the transmission. The receiver then responds with a CTS frame, also indicating the duration of the transmission. The other STAs in the vicinity hear either the RTS or the CTS frame and update their NAV (Network Allocation Vector) timers accordingly, deferring their access to the medium until the transmission is over. The sender then sends the data frame, followed by an ACK (Acknowledgement) frame from the receiver. The other options are not correct, as they are not used to acknowledge an RTS frame. An ACK frame is used to acknowledge a data frame, not an RTS frame. An RTS-Ack frame does not exist, as there is no such type of control frame in 802.11. A Block Ack (BA) frame is used to acknowledge multiple data frames in a single frame, not an RTS frame. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 6: 802.11 Frame Exchanges, page 166-167

NEW QUESTION 25

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 26

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 30

In which element of a Beacon frame would you look to identify 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

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

NEW QUESTION 33

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The CWAP-404 Practice Test Here](#)