CWNP

Exam Questions CWAP-404

Certified Wireless Analysis Professional

NEW QUESTION 1
How many frames are exchanged for 802.11 authentication in the 6 GHz band when WPA3-Enterprise is not used, and a passphrase is used instead?

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

Answer: B

Explanation:
Two frames are exchanged for 802.11 authentication in the 6 GHz band when WPA3-Enterprise is not used, and a passphrase is used instead. Authentication is a process that establishes an identity relationship between a STA (station) and an AP (access point) before joining a BSS (Basic Service Set). There are two types of authentication methods defined by 802.11: Open System Authentication and Shared Key Authentication. Open System Authentication does not require any credentials or security
information from a STA to join a BSS, and it consists of two frames: an Authentication Request frame sent by the STA to the AP, and an Authentication Response frame sent by the AP to the STA. Shared Key Authentication requires a shared secret key from a STA to join a BSS, and it consists of four frames: two challenge-response frames in addition to the request-response frames. However, Shared Key Authentication uses WEP (Wired Equivalent Privacy) as its encryption algorithm, which is insecure and deprecated. In the 6 GHz band, which is a newly available frequency band for WLANs, Shared Key Authentication 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. WPA3-Personal uses a passphrase to derive a PMK (Pairwise Master Key), while WPA3-Enterprise uses an authentication server to obtain a PMK. Both methods use SAE (Simultaneous Authentication of Equals) as their authentication protocol, which replaces PSK (Pre-Shared Key) or EAP (Extensible Authentication Protocol). SAE consists of two frames: an SAE Commit frame sent by both parties to exchange elliptic curve parameters and nonces, and an SAE Confirm frame sent by both parties to verify each other??s identities and generate a PMK. Therefore, when WPA3-Enterprise is not used, and a passphrase is used instead in the 6 GHz band, only two frames are exchanged for 802.11 authentication: an SAECommit frame and an SAE Confirm frame. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 8: Security Analysis, page 220-221

NEW QUESTION 2
Prior to a retransmission what happens to the CWmax value?

A. Increases by 1
B. Reset to 0
C. Set to the value of the AIFSN
D. Doubles and increases by 1

Answer: D

Explanation:
Before a retransmission, the CWmax (Contention Window maximum) value doubles and increases by 1. The CWmax is a parameter that determines the upper limit of the random backoff time that a STA (station) has to wait before attempting to access the medium. The random backoff time is chosen from a range of values between CWmin (Contention Window minimum) and CWmax. The CWmin and CWmax values depend on the AC (Access Category) of the traffic and the PHY type of the STA. If a transmission fails due to a collision or an error, the STA has to retransmit the frame after waiting for another random backoff time. However, to reduce the probability of another collision, the STA increases its CWmax value by doubling it and adding 1. This increases the range of possible backoff values and spreads out the STAs more evenly. The STA resets its CWmax value to its original value after a successful transmission or after reaching a predefined limit. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 7: QoS Analysis, page 196-197

NEW QUESTION 3
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 4
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

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

NEW QUESTION 5
What does the value of the Listen Interval field in an Association Request frame indicate?

A. How long a STA performing active scanning will listen for Probe Responses before changing channels
B. How often a STA will go off channel to look for other BSSs
C. How often a STA in power save mode wakes up to listen to Beacon frames
D. How long a STA waits for an Ack before retransmitting the frame

Answer: C

Explanation:
The value of the Listen Interval field in an Association Request frame indicates how often a STA in power save mode wakes up to listen to Beacon frames. The Listen Interval is expressed in units of Beacon Intervals (typically 100 TU or 102.4 ms). For example, if the Listen Interval is set to 10, it means that the STA will wake up every 10 Beacon Intervals (or about 1 second) to check for buffered frames at the AP. The Listen Interval is used by the AP to determine how long it can hold frames for a STA in power save mode before discarding them . References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 197; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 198.

NEW QUESTION 6
Which common feature of a Spectrum Analyzer would be the best to help you locate a non-802.11 interference source?

A. Max hold
B. Min hold
C. Location filter
D. Device finder

Answer: D

Explanation:
The device finder is a common feature of a spectrum analyzer that helps locate a non-802.11 interference source. The device finder uses a directional antenna to measure the signal strength of a specific frequency or signal source. By pointing the antenna in different directions, the device finder can indicate the direction and distance of the interference source. The device finder can also filter out other signals that are not related to the interference source. The other options are not correct, as they do not help locate a non-802.11 interference source. Max hold and min hold are features that show the maximum and minimum RF power levels over time,respectively. Location filter is a feature that filters out signals that are not from a specific location or area. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 3: Spectrum Analysis, page 77-78

NEW QUESTION 7
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 8
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 9
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 10
When performing protocol analysis, you capture an 802.1 lac data frame on channel 52, transmitted at MCS 8. At what data rate was the PHY Preamble transmitted?

A. 54 Mbps
B. 86.7 Mbps
C. 6 Mbps
D. 78 Mbps

Answer: C

Explanation:
The data rate at which the PHY preamble was transmitted is 6 Mbps. 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 detect and synchronize with the signal. The PHY preamble is always transmitted at a fixed data rate that depends on the type of PPDU (e.g., OFDM, HT, VHT, HE). For an 802.1 lac data frame on channel 52, which uses VHT PPDUs, the data rate for the PHY preamble is 6 Mbps. This data rate does not depend on MCS (Modulation and Coding Scheme), which only affects the data rate for the PSDU. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 99-100

NEW 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

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

NEW QUESTION 11
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

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

NEW QUESTION 12
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

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

NEW QUESTION 16
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 17
What interframe space would be expected between a CIS 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 20
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

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.

NEW QUESTION 24
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 27
Which one of the following is not an 802.11 Management frame?

A. PS-Poll
B. Action
C. Beacon
D. Authentication

Answer: A

Explanation:
A PS-Poll (Power Save Poll) frame is not an 802.11 management frame. A PS-Poll frame is a type of control frame that is used by a STA in power save mode to request data frames from an AP. A STA in power save mode can conserve battery power by periodically sleeping and waking up. 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 PS-Poll frame to the AP, indicating its association ID and requesting any buffered data frames. The AP thenresponds with one or more data frames, followed by an ACK or BA frame from the STA. The other options are not correct, as they are types of 802.11 management frames. An Action frame is used to perform various management actions, such as spectrum management, QoS management, radio measurement, etc. A Beacon frame is used to advertise the presence and capabilities of an AP or BSS. An Authentication frame is used to establish or terminate an authentication relationship between a STA and an AP. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 6: 802.11 Frame Exchanges, page 169-170

NEW QUESTION 31
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 33
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 38
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 41
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 44
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

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

NEW QUESTION 46
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 50
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 51
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 54
Where, in a protocol analyzer, would you find an indication that a frame was transmitted as part of an A-MPDU?

A. The HT Operation Element
B. A-MPDU flag in the QoS Control Field
C. A-MPDU flag in the Frame Control Field
D. The Aggregation flag in the Radio Tap Header

Answer: D

Explanation:
In a protocol analyzer, you would find an indication that a frame was transmitted as part of an A-MPDU by looking at the Aggregation flag in the Radio Tap Header. The Radio Tap Header is a pseudo-header that is added by some wireless capture devices to provide additional information about the physical layer characteristics of a frame. The Aggregation flag is one of the fields in this header, and it indicates whether the frame belongs to an A-MPDU or not. If the flag is set to 1, it means that the frame is part of an A- MPDU; if it is set to 0, it means that the frame is not part of an A-MPDU . References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 9: PHY Layer Frame Formats andTechnologies, page 303; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 9: PHY Layer Frame Formats and Technologies, page 304.

NEW QUESTION 57
What is the difference between a Data frame and a QoS-Data frame?

A. QoS Data frames include a DSCP control field
B. QoS Data frames include a QoS information element
C. QoS Data frames include an 802.1Q VLAN tag
D. QoS Data frames include a QoS control field

Answer: D

Explanation:
The difference between a Data frame and a QoS-Data frame is that QoS Data frames include a QoS control field. A Data frame is a type of data frame that is used to carry user data or upper layer protocol data between STAs and APs. A QoS Data frame is a type of data frame that is used to carry user data or upper layer protocol data between STAs and APs that support QoS (Quality of Service) features. QoS features allow different types of traffic to be prioritized and handled differently according to their QoS requirements, such as delay, jitter, throughput, etc. QoS Data frames include a QoS control field in their MAC header, which contains information such as traffic identifier (TID), queue size (TXOP), acknowledgment policy (ACK), etc., that are used for QoS purposes. The other options are not correct, as they do not describe the difference between Data and QoS Data frames. QoS Data frames do not include a DSCP (Differentiated Services Code Point) control field, which is part of the IP header in the network layer, not the MAC header in the data link layer. QoS Data frames do not include a QoS information element (IE), which is part of some management frames that indicate QoS capabilities or parameters, not data frames. QoS Data frames do not include an 802.1Q VLAN tag, which is part of some Ethernet frames that indicate VLAN membership or priority, not wireless frames. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 118-119

NEW QUESTION 58
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

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 63
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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