CWNP

Exam Questions CWAP-404

Certified Wireless Analysis Professional

NEW QUESTION 1
You're the WLAN administrator for a large retailer based at the HQ in New York. The London-based office has been complaining about WLAN disconnections around lunch time each day. You suspect this might be interference from the staff microwave, how might you test your theory from the New York office?

A. Ask a local member of staff to change the frequency of the microwave and see if the disconnections stop
B. Ask a local member of staff to take some pictures of the microwave, including some close-ups of the door seal so that you can assess it
C. Access the microwave remotely and run a diagnostic check
D. Place one of the London APs into spectrum analyzer mode and monitor the situation over lunch time

Answer: D

Explanation:
The best way to test the theory of microwave interference from the New York office is to use a remote spectrum analyzer. By placing one of the London APs into spectrum analyzer mode, you can capture and analyze the RF spectrum in the London office over lunch time. You can then look for any signs of microwave interference, such as high duty cycle, high amplitude, or frequency hopping on the 2.4 GHz band. This method does not require any physical access tothe microwave or any changes to its
frequency. References: [Wireless Analysis Professional Study Guide], Chapter 3: Spectrum Analysis, page 64

NEW QUESTION 2
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 3
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 4
Using a portable analyzer you perform a packet capture next to a client STA and you can see that the STA is associated to a BSS. You observe the STA sending packets to the AP and the AP sending packets to the STA. Less than 2% of all packets are retransmissions. You move to capture packets by the AP and, while the retry rate is still less than 2%, you now only see unidirectional traffic from the AP to the client. How do you explain this behavior?

A. The portable analyzer is too close to the AP causing CCI, blinding the AP to the clients packets
B. The STA is transmitting data using more spatial streams than the potable analyzer can support
C. There is a transmit power mismatch between the client and the AP and while the client can hear the APs traffic, the AP cannot hear the client
D. The portable analyzer has a lower receive sensitivity than the AP and while it can't capture the packets from the client STA, the AP can receive them OK

Answer: D

Explanation:

Receive sensitivity is the minimum signal level that a receiver can detect and decode. Different devices may have different receive sensitivity levels depending on their hardware specifications and antenna configurations. In this scenario, the portable analyzer has a lower receive sensitivity than the AP, meaning that it requires a stronger signal to capture the packets from the client STA. The AP, on the other hand, has a higher receive sensitivity and can receive the packets from the client STA even if they have a weaker signal. This explains why the portable analyzer can only see unidirectional traffic from the AP to the client when capturing near the AP5 References:
? CWAP-403 Study Guide, Chapter 4: PHY Layer Analysis, page 121
? CWAP-403 Objectives, Section 4.3: Analyze PHY layer metrics

NEW QUESTION 5
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 6
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 7
Which one of the statements regarding the Frame Control field in an 802.11 MAC header is true?

A. Only Control frames have a Frame Control field
B. The Frame Control field is used to communicate the duration value
C. The Frame Control field contains subfields, and soma in 1-bit flags
D. The Frame Control field is always set to 0

Answer: C

Explanation:
The statement that the Frame Control field contains subfields, and some 1- bit flags is true. The Frame Control field is a 2-byte field in the MAC header that contains information about the type, subtype, and characteristics of a frame. The Frame Control field is divided into several subfields, each with a specific function and length. Some of these subfields are 1-bit flags, which can be set to 0 or 1 to indicate a certain condition or status. For example, the To DS and From DS subfields are 1-bit flags that indicate whether a frame is destined for or originated from the DS (Distribution System). The other statements are not true, as they do not describe the Frame Control field correctly. All types of frames (management, control, and data) have a Frame Control field, not just control frames. The Frame Control field is not used to communicate the duration value, which is a separate field in the MAC header. The Frame Control field is not always set to 0, as it varies depending on the type, subtype, and characteristics of each frame. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 113-114

NEW QUESTION 8
When performing protocol analysis, you notice a high number of RTS/CTS frames being transmitted on an HT network. You suspect this may be due to HT protection mechanisms. Where in the Beacon frame would you look to determine which one of the four HT protection modes the AP is operating in?

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

Answer: B

Explanation:

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

NEW QUESTION 9
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 10
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 11
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 16
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 21
Given a protocol analyzer can decrypt WPA2-PSK data packets providing the PSK and SSID are configured in the analyzer software. When performing packet capture (in a non- FT environment) which frames are required in order for PSK frame decryption to be possible?

A. Authentication
B. 4-Way Handshake
C. Reassociation
D. Probe Response

Answer: B

Explanation:
The 4-way handshake is the process that establishes the pairwise transient key (PTK) between the client and the AP in WPA2-PSK. The PTK is derived from the PSK, the SSID, and some random numbers exchanged in the handshake frames. The PTK is used to encrypt and decrypt the data frames between the client and the AP. Therefore, in order to decrypt WPA2-PSK data packets, a protocol analyzer needs to capture the 4-way handshake frames and have the PSK and SSID configured in the analyzer software12 References:
? CWAP-404 Study Guide, Chapter 3: 802.11 MAC Layer Frame Formats and Technologies, page 87
? CWAP-404 Objectives, Section 3.5: Analyze security exchanges

NEW QUESTION 23
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 24
After examining a Beacon frame decode you see the SSID Element has a length of 0. What do you conclude about this frame?

A. The frame is corrupted

B. SSID elements always have a length of 0
C. This is a common attack on WISP backend SQL databases
D. The beacon is from a BSS configured to hide the SSID

Answer: D

Explanation:
If the SSID element has a length of 0 in a Beacon frame decode, it means that the beacon is from a BSS configured to hide the SSID. The SSID element is a part of the Beacon frame that contains the name or identifier of the BSS. The SSID element has two fields: length and value. The length field indicates how many bytes are used for the value field, which contains the actual SSID string. If the length field is 0, it means that there is no value field or SSID string in the element. This is a common technique used by some APs to hide their SSID from passive scanning clients or potential attackers. However, this technique does not provide much security, as there are other ways to discover or reveal the hidden SSID, such as active scanning or capturing probe response or association frames. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 122-123

NEW QUESTION 28
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 33
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 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 40
What is the function of the PHY layer?

A. Convert PPDUs to PSDUs for transmissions and PSDUs to PPDUs for receptions
B. Convert MSDUs to PPDUs for transmissions and PPDUs to MSDUs for receptions
C. Convert PPDUs to MSDUs for transmissions and MSDUs to PPDUs for receptions
D. Convert PSDUs to PPDUs for transmissions and PPDUs to PSDUs for receptions

Answer: D

Explanation:
The function of the PHY layer is to convert PSDUs to PPDUs for transmissions and PPDUs 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 43
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 48
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 CertifiedWireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 201.

NEW QUESTION 49
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 53
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

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

NEW QUESTION 56
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 57
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 58
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.
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

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.

NEW QUESTION 61
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 64
Which one of the following should be the first step when troubleshooting a WLAN issue?

A. Identify probable causes
B. Identify capture locations
C. Perform an initial WLAN scan and see if any obvious issues stand out
D. Define the problem

Answer: D

Explanation:
The first step in any troubleshooting process is to define the problem. This involves gathering information from various sources, such as users, network administrators, network documentation, and network monitoring tools. Defining the problem helps to narrow down the scope of the issue and identify the symptoms, causes, and effects of the problem12 References:
? CWAP-403 Study Guide, Chapter 1: Troubleshooting Methodology, page 7
? CWAP-403 Objectives, Section 1.1: Define the problem

NEW QUESTION 65
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 70
......