Exam Questions CWAP-404

Certified Wireless Analysis Professional

https://www.2passeasy.com/dumps/CWAP-404/

NEW QUESTION 1
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 2
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 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
A PHY Header is added to the PSDU at which layer?

A. LLC
B. Network
C. PHY
D. MAC

Answer: C

Explanation:
A PHY header is added to the PSDU at the PHY layer. A PHY header is a part of the PPDU that contains information such as modulation, coding, and data rate. The PHY header is added by the PHY layer when it converts a PSDU to a PPDU for transmission, or removed by the PHY layer when it converts a PPDU to a PSDU for reception. The other layers do not add or remove a PHY header. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 97-98

NEW QUESTION 5
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 6
Which one of the following is required for Wi-Fi integration in laptop-based Spectrum Analyzer software in addition to the spectrum analysis adapter?

A. An 802.11 wireless adaptor
B. A firmware upgrade for the spectrum analysis adapter
C. A directional antenna
D. SNMP read credentials to the WLAN controller or APs

Answer: A

Explanation:
An 802.11 wireless adaptor is required for Wi-Fi integration in laptop-based spectrum analyzer software in addition to the spectrum analysis adapter. The spectrum analysis adapter is a hardware device that captures the RF signals in the wireless environment and sends them to the spectrum analyzer software for analysis and display. The 802.11 wireless adapter is a hardware device that connects the laptop to the wireless network and allows the spectrum analyzer software to correlate the RF data with the Wi-Fi data, such as SSID, channel, and BSSID. This enables the spectrum analyzer software to provide more context and insight into the spectrum activity and its impact on the Wi-Fi network. A firmware upgrade for the spectrum analysis adapter is not required for Wi-Fi integration, but it may be needed to fix bugs or add features to the device. A directional antenna is an antenna that focuses the RF energy in a specific direction and has a high gain and a narrow beamwidth. A directional antenna can be used with a spectrum analysis adapter to pinpoint the location or source of interference or noise in the wireless environment, but it is not required for Wi-Fi integration. SNMP read credentials to the WLAN controller or APs are not required for Wi-Fi integration, but they may be useful for obtaining additional information about the wireless network configuration and performance from the network devices.References:
? CWAP-404 Study Guide, Chapter 4: Spectrum Analysis and Troubleshooting, page 123
? CWAP-404 Objectives, Section 4.2: Integrate Wi-Fi data with spectrum analysis data
? CWAP-404 Study Guide, Chapter 4: Spectrum Analysis and Troubleshooting, page 131

NEW QUESTION 7
During a VHT Transmit Beamforming sounding exchange, the beamformee transmits a Compressed Beamforming frame to the beamformer. What is communicated within this Compressed Beamforming frame?

A. Steering Matrix
B. Beamforming Matrix
C. Feedback Matrix
D. Beamformee Matrix

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 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
How does a VoIP Phone, using WMM Power Save, request data frames buffered at the AP?

A. The VoIP phone transmits a PS-Poll frame
B. The VoIP phone sets the More Data bit in the MAC Header to 1
C. The VoIP phone transmits a WMM Action frame
D. The VoIP phone transmits a trigger frame, which is a QoS Null frame or a QoS Data frame

Answer: D

Explanation:
A VoIP phone, using WMM Power Save, requests data frames buffered at the AP by transmitting a trigger frame, which is a QoS Null frame or a QoS Data frame. WMM Power Save is a power saving mode that allows a STA (station) to conserve battery power by periodically sleeping and waking up. WMM Power Save is based on WMM (Wi-Fi Multimedia), which is a QoS (Quality of Service) enhancement that provides prioritized and differentiated access to the medium fordifferent types of traffic. 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 trigger frame to the AP, indicating its AC (Access Category), which is a logical queue that corresponds to its QoS level. A trigger frame can be either a QoS Null frame or a QoS Data frame, depending on whether it has any payload or not. The AP then responds with one or more data frames from the same AC as the trigger frame, followed by an ACK or BA (Block Acknowledgement) frame from the STA. The other options are not correct, as they are not used by a VoIP phone using WMM Power Save to request data frames buffered at the AP. A PS-Poll (Power Save Poll) frame is used by a STA using legacy power save mode, not WMM Power Save mode, to request data frames buffered at the AP. A PS-Poll frame does not indicate any AC or QoS information. Setting the More Data bit in the MAC header to 1 does not request any data frames from the AP, but indicates that there are more data frames to be sent by the STA or received by the STA. Transmitting a WMM Action frame does not request any data frames from the AP, but performs various management actions related to WMM features, such as admission control, parameter update, etc.
References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 7: QoS Analysis, page 198-199

NEW QUESTION 10
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 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 12
802.11k Neighbor Requests and Neighbor Reports are sent in what type of Management Frames?

A. RRM
B. Action
C. Beacon
D. Reassociation Request and Reassociation Response

Answer: B

Explanation:
802.11k Neighbor Requests and Neighbor Reports are sent in Action frames. An Action frame is a Management frame that is used to perform various operations or functions related to the operation or maintenance of a wireless network. An Action frame consists of a Category field that indicates the type of action being performed, and a variable-length Action Details field that contains specific information related to the action. For example, an Action frame with a Category field

value of 5 indicates a Radio
Measurement action, and the Action Details field may contain a Neighbor Request or a Neighbor Report subelement . References: CWAP-404 CertifiedWireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 207; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 208; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 12: 802.11k/v/r/u/w/ai Amendments, page 434.

NEW QUESTION 13
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 15
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 17
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 19
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 23
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 28
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 31
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 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 37
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 42
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, asthey 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 45
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 50
What is the function of 802.11 Management frames?

A. Prioritize network administration traffic
B. Communicate configuration changes between WLAN controller and APs
C. Manage the BSS
D. Manage the flow of data

Answer: C

Explanation:
The function of 802.11 management frames is to manage the BSS. A BSS (Basic Service Set) is a group of STAs (stations) that share a common SSID (Service Set Identifier) and communicate with each other through an AP (access point) or directly in an ad hoc mode. Management frames are one of the three types of 802.11 frames, along with control and data frames. Management frames are used to establish, maintain, and terminate associations between STAs and APs, as

well as to advertise and discover BSSs, exchange security information, report errors, and perform other management functions. The other options are not correct, as they are not functions of 802.11 management frames. Prioritizing network administration traffic, communicating configuration changes between WLAN controller and APs, and managing the flow of data are functions of other types of frames or protocols. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 120-121

NEW QUESTION 52
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 56
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CWAP-404 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CWAP-404 Product From:

https://www.2passeasy.com/dumps/CWAP-404/

Money Back Guarantee

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