# Free Questions for CWAP-404 by certsdeals

## Shared by Wolf on 15-04-2024

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

As a wireless network consultant you have been called in to troubleshoot a high-priority issue for one of your customers. The customer's office is based on two floors within a multi-tenant office block. On one of these floors (floor 5) users cannot connect to the wireless network. During their own testing the customer has discovered that users can connect on floor 6 but not when they move to the floor 5. This issue is affecting all users on floor 5 and having a negative effect on productivity.

To troubleshoot this issue, you perform both Spectrum and Protocol Analysis. The Spectrum Analysis shows the presence of Bluetooth signals which you have identified as coming from wireless mice. In the protocol analyzer you see the top frame on the network is Deauthentication frames. On closer investigation you see that the Deauthentication frames' source addresses match the BSSIDs of your customers APs and the destination address is FF:FF:FF:FF:FF:FF:FF.

What do you conclude from this troubleshooting exercise?

## Options:

**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. Reference: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 13: Troubleshooting Common Wi-Fi Issues, page 4961; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 14: Troubleshooting Tools, page 5272.

## Question 2

**Question Type:** MultipleChoice

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?

## Options:

**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 SAE Commit frame and an SAE Confirm frame.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 8: Security Analysis, page 220-221

# Question 3

**Question Type:** MultipleChoice

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

## Options:

**A-** PMK

**B-** PTK

**C-** GMK

**D-** GTK

## Answer:

D

## Explanation:

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

The PTK is a key that is derived from the PMK, the ANonce, and the SNonce, and it is not transmitted in any message of the 4-Way Handshake. The GMK (Group Master Key) is a key that is generated by the AP and used to derive the GTK, and it is not transmitted in any message of the 4-Way Handshake.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 8: Security Analysis, page 211-213

# Question 4

**Question Type:** MultipleChoice

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

## Options:

**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 for different 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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 7: QoS Analysis, page 198-199

## Question 5

**Question Type:** MultipleChoice

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

## Options:

**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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 6: 802.11 Frame Exchanges, page 166-167; Chapter 7: QoS Analysis, page 194-195

# Question 6

**Question Type:** **MultipleChoice**

Prior to a retransmission what happens to the CWmax value?

## Options:

**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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 7: QoS Analysis, page 196-197

## Question 7

**Question Type:** MultipleChoice

In what scenario is Open Authentication without encryption not allowed based on the 802.11 standard?

## Options:

**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, Open Authentication 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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 8: Security Analysis, page 220-221

# Question 8

**Question Type:** **MultipleChoice**

What is an AIFS?

## Options:

**A-** A medium access method introduced by 802.lln, but never implemented

**B-** A variable Interframe Space introduced by 802.lie to help prioritize medium access for different Access Categories

**C-** A form of aggregation performed at the PHY layer based on 802.lie UP values interpreted from DSCP values

**D-** The shortest period of time a STA can sleep

## Answer:

B

## Explanation:

An AIFS is a variable interframe space introduced by 802.11e to help prioritize medium access for different Access Categories (ACs). An interframe space is a period of time that a STA (station) has to wait before attempting to access the medium. An AIFS is a type of interframe space that varies depending on the AC of the traffic. An AC is a logical queue that corresponds to a QoS (Quality of Service) level for different types of traffic. There are four ACs defined by 802.11e: AC_VO (Voice), AC_VI (Video), AC_BE (Best Effort), and AC_BK (Background). Each AC has a different AIFSN (Arbitration Interframe Space Number) 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 other options are not correct, as they do not describe what an AIFS is. An AIFS is not a medium access method introduced by 802.11n, but never implemented, as it is part of the 802.11e standard and widely used in QoS-enabled WLANs. An AIFS is not a form of aggregation performed at the PHY layer based on 802.11e UP values interpreted from DSCP values, as aggregation is a technique that combines multiple frames into one larger frame to improve efficiency and throughput, not prioritization or medium access. An AIFS is not the shortest period of time a STA can sleep, as sleeping is a power saving mode that allows a STA to conserve battery power by periodically turning off its radio, not accessing the medium.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 7: QoS Analysis, page 194-195

# Question 9

**Question Type:** MultipleChoice

How is the length of an AIFS calculated?

## Options:

**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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 7: QoS Analysis, page 194-195

# Question 10

**Question Type:** MultipleChoice

Which one of the statements regarding the Frame Control field in an 802.11 MAC header is true?

## Options:

**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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 113-114

## Question 11

**Question Type:** MultipleChoice

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

## Options:

**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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 118-119