

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 to the 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 SAE Commit 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

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 piece of information is not transmitted in an HT PPDU header?

- A. Number of Spatial Streams
- B. PPDU length
- C. MCS index
- D. Channel number

Answer: D

Explanation:

The channel number is not transmitted in an HT PPDU header. An HT PPDU header is a part of the PPDU that contains information such as modulation, coding, data rate, and number of spatial streams for an 802.11n transmission. The channel number is not included in the HT PPDU header, as it is determined by the frequency band and channel width that are used by the transmitter and receiver. The channel number can be inferred from the frequency band and channel width, which are indicated by bits in different fields of the HT PPDU header, such as HT-SIG and HT-LTF. The other options are not correct, as they are transmitted in an HT PPDU header. The number of spatial streams, PPDU length, and MCS index are indicated by bits in the HT-SIG field of the HT PPDU header. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 108-109

NEW QUESTION 6

You are analyzing a packet decode of a Probe Request and notice the SSID element has a length of zero. What do you conclude about the transmitting STA?

- A. The WLAN adaptor is configured in promiscuous mode
- B. The STA is operating in Ad-Hoc mode
- C. The STA's WLAN adaptor is disabled
- D. The STA is discovering a list of available BSSs

Answer: D

Explanation:

The STA is discovering a list of available BSSs by sending a Probe Request with an empty SSID element. This is also known as a broadcast Probe Request, as it does not specify any particular SSID to probe for. Any AP that receives this Probe Request will respond with a Probe Response containing its own SSID and other information about its BSS. This way, the STA can learn about all the BSSs in its vicinity and choose which one to associate with. References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 191; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 193.

NEW QUESTION 7

What is an AIFS?

- A. A medium access method introduced by 802.11n, but never implemented
- B. A variable Interframe Space introduced by 802.11e to help prioritize medium access for different Access Categories
- C. A form of aggregation performed at the PHY layer based on 802.11e 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. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 7: QoS Analysis, page 194-195

NEW QUESTION 8

The network administrator at ABC Engineering has taken a large packet capture from one of their APs running in monitor mode. She has very little knowledge of 802.11 protocols but would like to use the capture file to evaluate the overall health and performance of their wireless network. When she asks your advice, which tool do you recommend she opens the packet capture file with?

- A. Spectrum analyzer
- B. Python
- C. Capture visualization tool
- D. WLAN scanner

Answer: C

Explanation:

A capture visualization tool is a software application that can open a packet capture file and display various graphs, charts, tables, and statistics that illustrate the characteristics and behavior of the wireless network. A capture visualization tool can help a network administrator with little knowledge of 802.11 protocols to evaluate the overall health and performance of their wireless network by providing a visual and intuitive representation of the captured data. A spectrum analyzer is

a hardware device that measures the radio frequency signals in a given frequency range and displays their amplitude, frequency, and modulation. A spectrum analyzer can help identify sources of interference and noise in the wireless environment, but it cannot open a packet capture file. Python is a programming language that can be used to write scripts or applications that manipulate or analyze packet capture files, but it requires coding skills and knowledge of 802.11 protocols. A WLAN scanner is a software application that scans for available wireless networks and displays information such as SSID, BSSID, channel, signal strength, security type, and vendor. A WLAN scanner can help discover wireless networks and their basic parameters, but it cannot open a packet capture file. 345

References:

- ? CWAP-404 Study Guide, Chapter 2: Protocol Analysis, page 63
- ? CWAP-404 Objectives, Section 2.5: Use capture visualization tools
- ? CWAP-404 Study Guide, Chapter 4: Spectrum Analysis and Troubleshooting, page 117
- ? CWAP-404 Objectives, Section 4.1: Use spectrum analysis tools
- ? CWAP-404 Study Guide, Chapter 2: Protocol Analysis, page 33
- ? CWAP-404 Objectives, Section 2.2: Analyze field values

NEW QUESTION 9

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 Certified Wireless 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 10

When performing protocol analysis, you capture an 802.11lac 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 802.11lac data frame on channel 52, which uses VHT PPDUs, the data rate for the PHY preamble is 6 Mbps. This data rate does not depend on MCS (Modulation and Coding Scheme), which only affects the data rate for the PSDU. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 99-100

NEW QUESTION 10

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, 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. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 8: Security Analysis, page 220-221

NEW QUESTION 13

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 15

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 then responds 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 16

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 21

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 below. 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 22

Where, in a protocol analyzer, would you find an indication that a frame was transmitted as part of an A-MPDU?

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

Answer: D

Explanation:

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

NEW QUESTION 26

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

CWAP-404 Practice Exam Features:

- * CWAP-404 Questions and Answers Updated Frequently
- * CWAP-404 Practice Questions Verified by Expert Senior Certified Staff
- * CWAP-404 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CWAP-404 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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