CWAP-404$^{Q\&As}$

Certified Wireless Analysis Professional

Pass CWNP CWAP-404 Exam with 100% Guarantee

QUESTION 1

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

Correct 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

QUESTION 2

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

Correct 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.

QUESTION 3

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

Correct Answer: D

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

9: PHY Layer Frame Formats andTechnologies, page 303; CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 9: PHY Layer Frame Formats and Technologies, page 304.

QUESTION 4

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

Correct 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

QUESTION 5

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

Correct 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

QUESTION 6

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

Correct 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

QUESTION 7

An RTS frame should be acknowledged by which frame?

A. CTS

B. Ack

C. RTS-Ack

D. Block Ack

Correct 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

QUESTION 8

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

Correct 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

QUESTION 9

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

Correct 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

QUESTION 10

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

Correct 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