CWNP

Exam Questions CWAP-404

Certified Wireless Analysis Professional

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
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 2
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 3
Which one of the statements regarding the Frame Control field in an 802.11 MAC header is true?

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

Answer: C

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

NEW QUESTION 4
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 5
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 6
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 7
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 8
You have installed a new 802.1 lac WLAN configured with 80 MHz channels. Users in one area are complaining about poor performance. This area is currently served by a single AP. You take a spectrum analysis capture in the poor performing area. While examining the waterfall plot you notice the airtime utilization is higher on the first 20 MHz of the 80 MHz channel when compared to the rest of the channel. What do you conclude?

A. The AP is misconfigured and needs to be reconfigured to 80 MHz operation
B. Non-Wi-Fi interference is preventing the APs 80 MHz operation
C. The first 20 MHz is the AP's primary channel and higher airtime utilization on the primary channel is normal when an AP is configured for 80 MHz operation
D. RRM is enabled and has dynamically picked a 20 MHz channel

Answer: B

Explanation:
The most likely cause of higher airtime utilization on the first 20 MHz of the 80 MHz channel is non-Wi-Fi interference. Non-Wi-Fi interference can prevent an AP from using its full channel width, as it will degrade the signal quality and increase the noise floor on some parts of the channel. This will force the AP to fall back to a narrower channel
width, such as 20 MHz or 40 MHz, to maintain communication with its clients. The waterfall plot can help identify non-Wi-Fi interference by showing spikes or bursts of RF energy on specific frequencies or sub-channels. The other options are not correct, as they do not explain why only the first 20 MHz of the channel has higher airtime utilization. References: [Wireless Analysis Professional Study Guide], Chapter 3: Spectrum Analysis, page 74-75

NEW QUESTION 9
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 10
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 10
Which one of the following is not an 802.11 Management frame?

A. PS-Poll
B. Action
C. Beacon
D. Authentication

Answer: A

Explanation:
A PS-Poll (Power Save Poll) frame is not an 802.11 management frame. A PS-Poll frame is a type of control frame that is used by a STA in power save mode to request data frames from an AP. A STA in power save mode can conserve battery power by periodically sleeping and waking up. When a STA sleeps, it cannot receive any data frames from the AP, so it informs the AP of its power save status by setting a bit in its MAC header. The AP then buffers any data frames destined for the sleeping STA until it wakes up. When a STA wakes up, it sends a PS-Poll frame to the AP, indicating its association ID and requesting any buffered data frames. The AP thenresponds with one or more data frames, followed by an ACK or BA frame from the STA. The other options are not correct, as they are types of 802.11 management frames. An Action frame is used to perform various management actions, such as spectrum management, QoS management, radio measurement, etc. A Beacon frame is used to advertise the presence and capabilities of an AP or BSS. An Authentication frame is used to establish or terminate an authentication relationship between a STA and an AP. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 6: 802.11 Frame Exchanges, page 169-170

NEW QUESTION 14
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 16
What is the function of the PHY Preamble?

A. To terminate a conversation between transmitter and receiver
B. To set the modulation method for the MPDU
C. Carries the NDP used in Transmit Beamforming and MU-MIMO
D. Allows the receiver to detect and synchronize with the signal

Answer: D

Explanation:
The function of the PHY preamble is to allow the receiver to detect and synchronize with the signal. The PHY preamble is a part of the PPDU that is transmitted before the PHY header and the PSDU. The PHY preamble consists of a series of training fields that help the receiver to adjust its parameters, such as frequency, timing, and gain, to match the incoming signal. The PHY preamble also helps the receiver to estimate the channel conditions and noise level. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 99-100

NEW QUESTION 17
When would you expect to see a Reassociation Request frame'

A. Every time a STA associates to an AP to which it has previously been associated
B. Only when a STA is using FT roaming
C. Only when a STA roams back to an AP it has previously been associated with
D. Every time a STA roams

Answer: D

Explanation:
A Reassociation Request frame is sent every time a STA roams from one AP to another within the same ESS. A Reassociation Request frame is similar to an Association Request frame, but it also contains the BSSID of the current AP that the STA is leaving. This allows the new AP to coordinate with the old AP and transfer the STA??s context information, such as security keys, QoS parameters, and buffered frames. This way, the STA can maintain its connectivity and session continuity during roaming . References: CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 195;CWAP-404 Certified Wireless Analysis Professional Study and Reference Guide, Chapter 6: MAC Sublayer Frame Exchanges, page 196.

NEW QUESTION 18
What is used to respond with an uplink transmission to an MU-RTS trigger frame in the 802.11ax PHY?

A. HE SU PPDU
B. HE MU PPDU
C. HE TB PPDU
D. VHT PPDU

Answer: C

Explanation:
An HE TB PPDU (High Efficiency Trigger-Based Packet Data Unit) is used to respond with an uplink transmission to an MU-RTS trigger frame in the 802.11ax PHY (Physical Layer). An MU-RTS trigger frame is a frame that initiates a multi-user transmission opportunity (MU-TXOP) by requesting multiple stations (STAs) to send clear- to-send (CTS) frames on different spatial streams or resource units (RUs). An HE TB PPDU is a frame that contains data from multiple STAs that have been allocated RUs by an MU-RTS trigger frame or another type of trigger frame. An HE SU PPDU (High Efficiency Single User Packet Data Unit) is a frame that contains data from a single STA using all available spatial streams or RUs. An HE MU PPDU (High Efficiency Multi User Packet Data Unit) is a frame that contains data from multiple STAs using different spatial streams or RUs without being triggered by another frame. A VHT PPDU (Very High Throughput Packet Data Unit) is a frame that uses the 802.11ac PHY and does not support multi-user transmissions.References:
? CWAP-404 Study Guide, Chapter 3: 802.11 MAC Layer Frame Formats and Technologies, page 101
? CWAP-404 Objectives, Section 3.4: Analyze multi-user transmissions
? CWAP-404 Study Guide, Chapter 3: 802.11 MAC Layer Frame Formats and Technologies, page 99

NEW QUESTION 21
In the 2.4 GHZ band, what data rate are Probe Requests usually sent at from an unassociated STA?

A. 1 Mbps
B. The minimum basic rate
C. MCS 0
D. 6 Mbps

Answer: B

Explanation:
In the 2.4 GHz band, probe requests are usually sent at the minimum basic rate from an unassociated STA. A probe request is a type of management frame that is transmitted by a STA to discover available BSSs in its vicinity. A probe request can be sent on one or more channels in either passive or active scanning mode. In passive scanning mode, a STA listens for beacon frames from APs on each channel. In active scanning mode, a STA sends probe requests on each channel and waits for probe responses from APs. A probe request is usually sent at the minimum basic rate, which is the lowest data rate among the supported rates that is required for all STAs to join and communicate with a BSS. The minimum basic rate can vary depending on the configuration of each BSS, but it is typically one of these values: 1 Mbps, 2 Mbps, 5.5 Mbps, or 11 Mbps in the 2.4 GHz band. The other options are not correct, as they do not reflect how probe requests are usually

sent in the 2.4 GHz band. MCS 0 is a modulation and coding scheme used by 802.11n/ac devices in either band, but it is not a data rate per se. 6 Mbps is a data rate used by OFDM devices in either band, but it is not usually configured as a minimum basic rate in the 2.4 GHz band. References: [Wireless Analysis Professional Study Guide CWAP- 404], Chapter 5: 802.11 MAC Sublayer, page 123-124

NEW QUESTION 22
Protocol analyzers may present field values in either binary, decimal or hexadecimal. What preceeds a hexadecimal value to indicate it is hexadecimal?

A. 0x
B. 16x
C. %
D. HEX

Answer: A

Explanation:
A hexadecimal value is a value that uses base 16 notation, which means it can have digits from 0 to 9 and letters from A to F. A hexadecimal value is usually preceded by 0x to indicate that it is hexadecimal and not decimal or binary. For example, 0x0A is hexadecimal for 10 in decimal or 00001010 in binary. The other options are not valid prefixes for hexadecimal values.References:
? CWAP-404 Study Guide, Chapter 2: Protocol Analysis, page 35
? CWAP-404 Objectives, Section 2.2: Analyze field values

NEW QUESTION 24
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 andTechnologies, 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
In which element of a Beacon frame would you look to identity the current HT protection mode in which an AP is operating?

A. HT Protection Element
B. HT Operations Element
C. ERP Information Element
D. HT Capabilities Element

Answer: B

Explanation:
The HT protection mode in which an AP is operating can be identified by looking at the HT Operations element in a Beacon frame. The HT Operations element is a part of the Beacon frame that contains information about the High Throughput (HT) capabilities and operation of an 802.11n BSS. The HT Operations element has a field called HT Protection, which indicates how the BSS protects its HT transmissions from interference or collisions with non-HT devices or BSSs. The HT Protection field can have four values: No Protection, Nonmember Protection, 20 MHz Protection, or Non-HT Mixed Mode. The other options are not correct, as they do not contain information about the HT protection mode. The HT Protection element does not exist, the ERP Information element is used for Extended Rate PHY (ERP) protection mode for 802.11g devices, and the HT Capabilities element is used for indicating the supported HT features of an individual device. References: [Wireless Analysis Professional Study Guide CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 125-126

NEW QUESTION 27
.....

Relate Links

100% Pass Your CWAP-404 Exam with Exambible Prep Materials

https://www.exambible.com/CWAP-404-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/