Number: CWAP-404
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: CWAP-404

Exam Name: Certified Wireless Analysis Professional Exam

Exam A

QUESTION 1
The PHY layer provides framing by adding a header to create what type of data unit?

A. MPDU
B. PSDU
C. MSDU
D. PPDU

Correct Answer: D
Section:
Explanation:
The PHY layer provides framing by adding a header to create a PPDU. A PPDU (PHY Protocol Data Unit) is the data unit that is transmitted or received over the wireless medium by the PHY layer. A PPDU consists of a PSDU (PHY Service Data Unit) and a PHY header, which contains information such as modulation, coding, and data rate. The PHY layer adds the PHY header to the PSDU to create a PPDU for transmission, or removes the PHY header from the PPDU to extract the PSDU for reception. The other options are not correct, as they are not created by adding a header at the PHY layer. An MPDU (MAC Protocol Data Unit) is created by adding a MAC header and FCS to an MSDU (MAC Service Data Unit) at the MAC layer. An MSDU is the data unit that is passed from the LLC sublayer to the MAC sublayer or vice versa.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 97-98

QUESTION 2
What is the function of the PHY layer?

A. Convert PPDUs to PSDUs for transmissions and PSDUs to PPDUs for receptions
B. Convert MSDUs to PPDUs for transmissions and PPDUs to MSDUs for receptions
C. Convert PPDUs to MSDUs for transmissions and MSDUs to PPDUs for receptions
D. Convert PSDUs to PPDUs for transmissions and PPDUs to PSDUs for receptions

Correct Answer: D
Section:
Explanation:
The function of the PHY layer is to convert PSDUs to PPDUs for transmissions and PPDUs to PSDUs for receptions. A PSDU (PHY Service Data Unit) is the data unit that is passed from the MAC layer to the PHY layer for transmission, or from the PHY layer to the MAC layer for reception. A PPDU (PHY Protocol Data Unit) is the data unit that is transmitted or received over the wireless medium by the PHY layer. A PPDU consists of a PSDU and a PHY header, which contains information such as modulation, coding, and data rate. The PHY layer adds or removes the PHY header to or from the PSDU during the conversion process.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 97-98

QUESTION 3
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

Correct Answer: D
Section:

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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 99-100

QUESTION 4
Which one of the following should be the first step when troubleshooting a WLAN issue?

A. Identify probable causes
B. Identify capture locations
C. Perform an initial WLAN scan and see if any obvious issues stand out
D. Define the problem

Correct Answer: D
Section:
Explanation:
The first step in any troubleshooting process is to define the problem. This involves gathering information from various sources, such as users, network administrators, network documentation, and network monitoring tools.Defining the problem helps to narrow down the scope of the issue and identify the symptoms, causes, and effects of the problem12Reference:
CWAP-403 Study Guide, Chapter 1: Troubleshooting Methodology, page 7
CWAP-403 Objectives, Section 1.1: Define the problem

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

Correct Answer: C
Section:
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 later34Reference:
CWAP-403 Study Guide, Chapter 2: Protocol Analysis, page 37
CWAP-403 Objectives, Section 2.3: Apply display filters

QUESTION 6
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 ST

A. 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?
B. The portable analyzer is too close to the AP causing CCI, blinding the AP to the clients packets
C. The STA is transmitting data using more spatial streams than the potable analyzer can support
D. 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
E. 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

Correct Answer: D

Section:
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 AP5Reference:
CWAP-403 Study Guide, Chapter 4: PHY Layer Analysis, page 121
CWAP-403 Objectives, Section 4.3: Analyze PHY layer metrics

QUESTION 7
Given a protocol analyzer can decrypt WPA2-PSK data packets providing the PSK and SSID are configured in the analyzer software. When performing packet capture (in a non-FT environment) which frames are required in order for PSK frame decryption to be possible?

A. Authentication
B. 4-Way Handshake
C. Reassociation
D. Probe Response

Correct Answer: B
Section:
Explanation:
The 4-way handshake is the process that establishes the pairwise transient key (PTK) between the client and the AP in WPA2-PSK. The PTK is derived from the PSK, the SSID, and some random numbers exchanged in the handshake frames. The PTK is used to encrypt and decrypt the data frames between the client and the AP.Therefore, in order to decrypt WPA2-PSK data packets, a protocol analyzer needs to capture the 4-way handshake frames and have the PSK and SSID configured in the analyzer software12Reference:
CWAP-404 Study Guide, Chapter 3: 802.11 MAC Layer Frame Formats and Technologies, page 87
CWAP-404 Objectives, Section 3.5: Analyze security exchanges

QUESTION 8
When configuring a long-term, forensic packet capture and saving all packets to disk which of the following is not a consideration?

A. Real-time packet decodes
B. Analyzer location
C. Total capture storage space
D. Individual trace file size

Correct Answer: A
Section:
Explanation:
Real-time packet decodes are not a consideration when configuring a long-term, forensic packet capture and saving all packets to disk. Real-time packet decodes are useful for live analysis and troubleshooting, but they consume CPU and memory resources that could affect the performance of the capture process. For a long-term, forensic packet capture, it is more important to consider the analyzer location, the total capture storage space, and the individual trace file size.These factors affect the quality and quantity of the captured packets and the ease of post-capture analysis34Reference:
CWAP-404 Study Guide, Chapter 2: Protocol Analysis, page 49
CWAP-404 Objectives, Section 2.1: Configure protocol analyzers

QUESTION 9
You are performing a multiple adapter channel aggregation capture to troubleshoot a VoIP roaming problem and would like to measure the roaming time from the last VoIP packet sent on the old AP's channel to the first VoIP packet sent on the new AP's channel. Which timing column in the packet view would measure this for you?

A. Roaming

B. Relative
C. Absolute
D. Delta

Correct Answer: D
Section:
Explanation:
Delta is the timing column in the packet view that measures the time difference between two consecutive packets in a capture file. Delta can be used to measure the roaming time from the last VoIP packet sent on the old AP's channel to the first VoIP packet sent on the new AP's channel by selecting these two packets and looking at their delta values. The other timing columns are not suitable for this measurement because they do not show the time difference between two specific packets. Roaming is a column that shows whether a packet belongs to a roaming event or not. Relative is a column that shows the time elapsed since the beginning of the capture file.Absolute is a column that shows the date and time when a packet was captured5Reference:
CWAP-404 Study Guide, Chapter 2: Protocol Analysis, page 57
CWAP-404 Objectives, Section 2.4: Analyze timing values

QUESTION 10
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

Correct Answer: A
Section:
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.
Reference:
CWAP-404 Study Guide, Chapter 2: Protocol Analysis, page 35
CWAP-404 Objectives, Section 2.2: Analyze field values

QUESTION 11
Which one of the these is the most important in the WLAN troubleshooting methodology among those listed?

A. Obtain detailed -knowledge of the wireless vendors debug and logging options
B. Interview the network manager about the issues being experienced
C. Observe the problem
D. Talk to the end users about their experiences

Correct Answer: C
Section:
Explanation:
Observing the problem is the most important step in the WLAN troubleshooting methodology among those listed. This step involves capturing and analyzing the relevant data from the wireless network, such as packets, frames, spectrum, and performance metrics. Observing the problem helps to verify the existence and scope of the issue, identify the root cause and possible solutions, and validate the results of any actions taken.The other steps are also important, but they are not as critical as observing the problem12Reference:
CWAP-404 Study Guide, Chapter 1: Troubleshooting Methodology, page 15
CWAP-404 Objectives, Section 1.2: Observe the problem

QUESTION 12
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

Correct Answer: C
Section:
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 file345Reference:
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

QUESTION 13
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

Correct Answer: C
Section:
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.
Reference:
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

QUESTION 14
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

Correct Answer: D
Section:
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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 3: Spectrum Analysis, page 77-78

QUESTION 15
A manufacturing facility has installed a new automation system which incorporates an 802.11 wireless network. The automation system is controlled from tablet computers connected via the WLAN. However, the automation system has not gone live due to problem with the tablets connecting to the WLAN. The WLAN vendor has been onsite to perform a survey and confirmed good primary and secondary coverage across the facility. As a CWAP you are called in to perform Spectrum Analysis to identify any interference sources. From the spectrum analysis, you did not identify any interference sources but were able to correctly identify the issue. Which of the following issues did you identify from the spectrum analysis?

A. The tablets are connecting to the wrong SSID
B. The tablets are entering power save mode and failing to wake up to receive the access points transmissions
C. A high noise floor has resulted in a SNR of less than 20dB
D. There is a power mismatch between the APs and the clients

Correct Answer: D
Section:
Explanation:
The most likely issue that can be identified from the spectrum analysis is a power mismatch between the APs and the clients. A power mismatch occurs when the APs transmit at a higher power level than the clients, or vice versa. This can cause asymmetric communication, where one side can hear the other, but not vice versa. This can result in poor performance, disconnections, or packet loss. A spectrum analysis can reveal a power mismatch by showing different signal amplitudes or RSSI values for the APs and the clients on the same channel or frequency. The other options are not correct, as they cannot be identified from the spectrum analysis alone. The tablets' SSID, power save mode, and noise floor can be determined by using other tools or methods, such as protocol analysis, site survey, or device configuration.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 3: Spectrum Analysis, page 79-80

QUESTION 16
Finish the statement:
It is possible to distinguish between_____22 MHz transmissions and_____20 MHz transmissions when looking at an FFT plot.

A. HR/DSSS and ERP
B. OFDM and HT
C. ERP and VHT
D. HT and VHT

Correct Answer: B
Section:
Explanation:
It is possible to distinguish between OFDM 20 MHz transmissions and HT 20 MHz transmissions when looking at an FFT plot. OFDM and HT are two different modulation schemes used by 802.11 WLANs. OFDM is used by legacy 802.11a/g devices, while HT is used by newer 802.11n/ac devices. OFDM and HT have different spectral characteristics that can be observed on an FFT plot. OFDM transmissions have a flat spectrum with sharp edges, while HT transmissions have a tapered spectrum with rounded edges. This is because HT uses guard intervals and cyclic prefixes to reduce inter-symbol interference and improve performance. The other options are not

correct, as they do not describe different modulation schemes or channel widths that can be distinguished on an FFT plot.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 3: Spectrum Analysis, page 70-71

QUESTION 17
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

Correct Answer: A
Section:
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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 97-98

QUESTION 18
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

Correct Answer: A
Section:
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 and Extended 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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 123-124

QUESTION 19
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
Section:

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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 122-123

QUESTION 20
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

Correct Answer: A
Section:
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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 6: 802.11 Frame Exchanges, page 167-168

QUESTION 21
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

Correct Answer: B
Section:
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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 125-126

QUESTION 22
When a data frame is encrypted with WPA2, to which portion of the frame is the encryption applied?

A. Frame body and MAC Header
B. Frame body excluding the LLCPD U
C. Frame body including the LLCPDU
D. The whole MPDU

Correct Answer: C
Section:
Explanation:
When a data frame is encrypted with WPA2, the encryption is applied to the frame body including the LLCPDU. The LLCPDU (Logical Link Control Protocol Data Unit) is a part of the frame body that contains information such as protocol type, source and destination service access points (SAPs), and control fields. The LLCPDU is added by the LLC (Logical Link Control) sublayer to provide multiplexing and flow control functions for different upper layer protocols. When a data frame is encrypted with WPA2, which uses AES-CCMP as its encryption algorithm, both the payload and the LLCPDU are encrypted as a single unit. The MAC header and FCS are not encrypted, as they are needed for addressing and error detection purposes.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 115-116

QUESTION 23
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
Section:
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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 123-124

QUESTION 24
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

Correct Answer: C
Section:
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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 5: 802.11 MAC Sublayer, page 114-115

QUESTION 25
Which one of the following portions of information is communicated by bits in the PHY Header?

A. SNR
B. Noise
C. Data rate
D. Signal strength

Correct Answer: C
Section:
Explanation:
One of the information that is communicated by bits in the PHY header is data rate. Data rate is the speed at which data is transmitted or received over the wireless medium. Data rate depends on factors such as modulation, coding, channel width, spatial streams, and guard interval. Data rate is indicated by bits in different fields of the PHY header, depending on the type of PPDU (e.g., OFDM, HT, VHT, HE). The receiver uses these bits to determine how to decode and demodulate the rest of the PPDU. The other options are not correct, as they are not communicated by bits in the PHY header. SNR (Signal-to-Noise Ratio), noise, and signal strength are measured by the receiver based on its own capabilities and environment.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 101-105

QUESTION 26
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

Correct Answer: C
Section:
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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 99-100

QUESTION 27
A PHY Header is added to the PSDU at which layer?

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

Correct Answer: C
Section:
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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 97-98

QUESTION 28
ABC International has installed a new smart ZigBee controlled lighting system. However, the network team is concerned that this new system will interfere with the existing WLAN and has asked you to investigate the impact of the two systems operating simultaneously in the 2.4 GHz band. When performing Spectrum Analysis, which question could you answer by looking at the FFT plot?

A. Do the ZigBee channels used by the lighting system overlap with the WLAN channels?
B. Is the ZigBee system using more than 50% of the available airtime?
C. Is the WLAN corrupting ZigBee system messages?
D. Is the ZigBee system causing an increase in WLAN retries?

Correct Answer: A
Section:
Explanation:
The FFT plot is a spectrum analysis plot that shows the RF power present at a particular frequency over a short period of time. It can help identify the sources and characteristics of RF signals in the spectrum. By looking at the FFT plot, you can determine which ZigBee channels are used by the lighting system and whether they overlap with the WLAN channels in the 2.4 GHz band. ZigBee channels are 5 MHz wide and WLAN channels are 20 MHz or 40 MHz wide, so there is a possibility of overlap and interference between them. The other questions cannot be answered by looking at the FFT plot alone, as they require other types of plots or analysis tools, such as duty cycle plot, airtime utilization plot, or protocol analyzer.Reference:[Wireless Analysis Professional Study Guide], Chapter 3: Spectrum Analysis, page 69-70

QUESTION 29
In a Spectrum Analyzer the Swept Spectrogram plot displays what information?

A. RF power present at a particular frequency over the course of time
B. Reductions in frame transmissions
C. Wi-Fi Device information
D. The RF time domain

Correct Answer: A
Section:
Explanation:
The Swept Spectrogram plot is a spectrum analysis plot that shows the RF power present at a particular frequency over the course of time. It can help identify trends and patterns in the RF spectrum over a longer period of time. It can also show how the RF environment changes over time and how different sources of RF signals affect each other. The other options are not correct, as they describe different types of plots or information that are not related to the Swept Spectrogram plot.Reference:[Wireless Analysis Professional Study Guide], Chapter 3: Spectrum Analysis, page 72-73

QUESTION 30
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 are a. 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

Correct Answer: B
Section:
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.Reference:[Wireless Analysis Professional Study Guide], Chapter 3: Spectrum Analysis, page 74-75

QUESTION 31
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
Section:
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.Reference:[Wireless Analysis Professional Study Guide CWAP-404], Chapter 4: 802.11 Physical Layer, page 108-109