CWNP CWNA-109 Practice Questions

Shared by Mcclain on 06-11-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You are reporting on the RF environment in your facility. The manager asks you to describe the noise floor noted in the report. Which of the following is the best explanation?

Options:

A- The noise caused by elevators, microwave ovens, and video transmitters.
B- The extra energy radiated by access points and client devices beyond that intended for the signal.
C- The energy radiated by flooring materials that causes interference in the 2.4 GHz and 5 GHz bands.
D- The RF energy that exists in the environment from intentional and unintentional RF radiators that forms the baseline above which the intentional signal of your WLAN must exist.

Answer:

D

Explanation:

The RF energy that exists in the environment from intentional and unintentional RF radiators that forms the baseline above which the intentional signal of your WLAN must exist is the best explanation of the noise floor noted in the report. The noise floor is a term that describes the level of background noise or interference in a wireless channel or band. The noise floor is measured in dBm (decibel-milliwatts) and it represents the minimum signal strength that can be detected or received by a wireless device. The noise floor is influenced by various factors, such as the sensitivity of the receiver, the antenna gain, the cable loss, and the ambient RF environment. The ambient RF environment consists of intentional and unintentional RF radiators that emit RF energy in the wireless spectrum. Intentional RF radiators are devices that are designed to transmit RF signals for communication purposes, such as Wi-Fi access points, Bluetooth devices, microwave ovens, or cordless phones. Unintentional RF radiators are devices that are not designed to transmit RF signals but generate electromagnetic radiation as a by-product of their operation, such as USB 3 devices, PC power supplies, or fluorescent lights. The noise floor affects WLAN performance and quality because it determines the minimum signal-to-noise ratio (SNR) that is required for a successful wireless transmission. SNR is the difference between the signal strength of the desired signal and the noise floor of the channel. SNR is also measured in dB and it indicates how much the signal stands out from the noise. A higher SNR means a better signal quality and a lower bit error rate. A lower SNR means a worse signal quality and a higher bit error rate. Therefore, to achieve a reliable WLAN connection, the intentional signal of your WLAN must exist above the noise floor by a certain margin that depends on the data rate and modulation scheme used. The other options are not accurate or complete explanations of the noise floor noted in the report. The noise caused by elevators, microwave ovens, and video transmitters is not the noise floor but rather examples of

interference sources that contribute to the noise floor. The extra energy radiated by access points and client devices beyond that intended for the signal is not the noise floor but rather an example of spurious emissions that cause interference to other devices or channels. The energy radiated by flooring materials that causes interference in the 2.4 GHz and 5 GHz bands is not the noise floor but rather an example of attenuation or reflection that reduces or changes the direction of the signal.Reference:CWNA-109 Study Guide, Chapter 5: Radio Frequency Signal and Antenna Concepts, page 139

Question 2

Question Type: MultipleChoice

What common feature of MDM solutions can be used to protect enterprise data on mobile devices?

Options:

A- Over-the-air registration
B- Onboarding
C- Containerization
D- Self-registration

Answer:

C

Explanation:

A common feature of MDM solutions that can be used to protect enterprise data on mobile devices iscontainerization. Containerization is a technique that creates a separate and secure environment on the mobile device where enterprise data and applications are stored and accessed. Containerization isolates the enterprise data from the personal data and prevents unauthorized access, leakage, or loss of sensitive information. Containerization can also enforce security policies, encryption, authentication, and remote wipe on the enterprise data and applications. Over-the-air registration, onboarding, and self-registration are features of MDM solutions that facilitate the enrollment and management of mobile devices, but they do not directly protect enterprise data on mobile devices.Reference:[CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 336; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 326.

Question 3

Question Type: MultipleChoice

In an 802.11n (H T) 2.4 GHz BSS, what prevents each station from using all the airtime when other client stations are actively communicating in the same BSS?

Options:

A- 802.11 DOS prevention
B- OFDMA
C- CSMA/CD
D- CSMA/CA

P2P exams

Answer:

D

Explanation:

What prevents each station from using all the airtime when other client stations are actively communicating in the same BSS isCSMA/C

A . CSMA/CA stands for Carrier Sense Multiple Access with Collision Avoidance and is a media access control method used by WLAN devices to share the wireless medium. CSMA/CA works by having each station sense the medium before transmitting a frame. If the medium is busy (i.e., another station is transmitting), the station defers its transmission until the medium is idle. If the medium is idle, the station waits for a random backoff period before transmitting. This way, CSMA/CA reduces the chances of collisions and ensures fair access to the medium for all stations. CSMA/CA also uses positive acknowledgements to confirm successful transmissions and retransmissions to recover from errors. CSMA/CD, DOS prevention, and OFDMA are not used by WLAN devices in a BSS.Reference:[CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 108; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 98.

Question 4

Question Type: MultipleChoice

Three access points are used within a facility. One access point is on channel 11 and the other two are on channel 1. The two access points using channel 1 are on either side of the access

point using channel 11 and sufficiently apart so that they do not interfere with each other when they transmit frames. Assuming no other APs are in the vicinity, is CCI still a possibility in this network and why?

Options:

A- Yes, because the client devices connected to one of the channel 1 APs will transmit frames that reach the other channel 1 AP as well as clients connected to the other channel 1 AP.
B- No, because the APs are far enough apart that no CCI will occur.
C- No, because CCI only occurs in the 5 GHz frequency band.
D- Yes, because channel 11 loops around and causes CCI with channel 1.

Answer:

A

Explanation:

CCI is still a possibility in this network because the client devices connected to one of the channel 1 APs will transmit frames that reach the other channel 1 AP as well as clients connected to the other channel 1 AP. CCI stands for co-channel interference, which is a type of interference that occurs when two or more devices transmit on the same channel within range of each other. CCI reduces performance and capacity because it causes contention and collisions on the wireless medium, which leads to retransmissions and delays. CCI can be mitigated by increasing physical separation between devices using the same channel or by reducing transmit power levels to limit coverage area. In this scenario, three access points are used within a facility. One access point is on channel 11 and the other two are on channel 1. The two access points using channel 1 are on either side of the access point using channel 11 and sufficiently apart so that they do not interfere with each other when they transmit frames. However, this does not prevent CCI from occurring between their client devices that are connected on channel 1. For example, if a client device connected to one of the channel 1 APs sends a frame to another device on the wired network or on another wireless network (such as an Internet server or a VoIP phone), that frame will be heard by both channel 1 APs as well as any other client devices connected to either of them on channel 1. This will cause CCI because these devices will have to wait for the channel to be clear before they can transmit their own frames. The answer that CCI only occurs in the 5 GHz frequency band is incorrect; CCI can occur in any frequency band where devices use the same channel. The answer that channel 11 loops around and causes CCI with channel 1 is also incorrect; channel 11 does not loop around and it operates in a different frequency band than channel 1.Reference:CWNA-109 Study Guide, Chapter 5: Radio Frequency Signal and Antenna Concepts, page 147

Question 5

Question Type: MultipleChoice

When considering data rates available in HT and VHT PHY devices, in addition to the modulation, coding, channel width, and spatial streams, what impacts the data rate according to the MCS tables?

Options:

A- Frequency band in use
B- client drivers
C- guard interval
D- Antenna Height

Answer:

C

Explanation:

The guard interval is a short period of time inserted between the symbols of an OFDM signal to prevent inter-symbol interference and improve the robustness of the transmission1. The guard interval can have different values depending on the 802.11 standard and the configuration of the device.For example, 802.11n supports two guard intervals: 800 ns (normal) and 400 ns (short)2.802.11ac supports the same guard intervals as 802.11n, plus an optional 200 ns guard interval for 80 MHz and 160 MHz channels3.802.11ax supports three guard intervals: 800 ns, 1600 ns, and 3200 ns4.

The guard interval affects the data rate because it determines the duration of each symbol. A shorter guard interval means more symbols can be transmitted in a given time, resulting in a higher data rate. However, a shorter guard interval also means less protection against inter-symbol interference, which may degrade the signal quality and increase the error rate. Therefore, there is a trade-off between data rate and reliability when choosing the guard interval.

The MCS tables for HT and VHT PHY devices show the data rates for different combinations of modulation, coding, channel width, spatial streams, and guard intervals.For example, for a VHT device using MCS 9 with QAM-256 modulation, 5/6 coding rate, 80 MHz channel width, and one spatial stream, the data rate is 433.3 Mbps with a normal guard interval (800 ns) and 486.7 Mbps with a short guard interval (400 ns)2. Therefore, the guard interval impacts the data rate according to the MCS tables.

Question 6

Question Type: MultipleChoice

You have implemented an 802.11ax WLAN for a customer. All APs are four stream HE APs. The customer states that it is essential that most of the clients can use the OFDMA modulation scheme. What do you tell the customer?

Options:

A- The clients that must support OFDMA must also be upgraded to 802.11ax
B- OFDMA is an optional feature of 802.11ax and most APs don't even support it
C- All 5 GHz PHYs use OFDM modulation, so you will achieve OFDMA everywhere in 5 GHz
D- If the devices support 802.11ac, they can be updated to support OFDMA through driver upgrades

Answer:

A

Explanation:

OFDMA is a new modulation scheme introduced in 802.11ax that allows multiple users to share the same channel by dividing it into smaller subchannels called resource units (RUs). This improves the efficiency and capacity of the WLAN by reducing contention and overhead. However, to use OFDMA, both the AP and the client must support 802.11ax and negotiate the parameters of the subchannel allocation.Therefore, the customer needs to upgrade the clients that require OFDMA to 802.11ax devices12.

The other options are not correct because they do not reflect the reality of OFDMA.Option B is incorrect because OFDMA is a mandatory feature of 802.11ax for both downlink and uplink transmissions, and all 802.11ax APs must support it1. Option C is incorrect because OFDM and OFDMA are different modulation schemes, and OFDM does not allow multiple users to share the same channel.Option D is incorrect because 802.11ac devices cannot support OFDMA through driver upgrades, as they lack the hardware and firmware capabilities to do so2.

Question 7

Question Type: MultipleChoice

A dual-band 802.11ac AP must be powered by PoE. As a class 4 device, what power level should be received at the AP?

Options:

A- 30 W
B- 12.95 W
C- 25.5 W
D- 15.4 W

Answer:

C

Explanation:

PoE has different standards that define different power levels for PSEs and PDs. The original standard, IEEE 802.3af, defines two classes of PSEs: Class 3 (15.4 W) and Class 4 (30 W). The newer standard, IEEE 802.3at, also known as PoE+, defines four classes of PSEs: Class 0 (15.4 W), Class 1 (4 W), Class 2 (7 W), and Class 3 (12.95 W). The power level received at the PD is always lower than the power level provided by the PSE, due to cable resistance and power dissipation. The IEEE standards specify the minimum power level that must be received at the PD for each class of PSE.For a Class 4 PSE, the minimum power level received at the PD is 25.5 W910.Reference:CWNA-109 Study Guide, Chapter 7: Power over Ethernet (PoE), page 295;CWNA-109 Study Guide, Chapter 7: Power over Ethernet (PoE), page 289.

Question 8

Question Type: MultipleChoice

Lynne runs a small hotel, and as a value added service for his customers he has implemented a Wi-Fi hot-spot. Lynne has read news articles about how hackers wait at hot-spots trying to take advantage of unsuspecting users. He wants to avoid this problem at his hotel.

What is an efficient and practical step that Lynne can take to decrease the likelihood of active attacks on his customers' wireless computers?

Options:

A- Enable station-to-station traffic blocking by the access points in the hotel.
B- Implement Network Access Control (NAC) and require antivirus and firewall software along with OS patches.
C- Implement an SSL VPN in the WLAN controller that initiates after HTTPS login.
D- Require EAP-FAST authentication and provide customers with a username/password on their receipt.

Answer:

A

Explanation:

In a public Wi-Fi hotspot, like the one Lynne runs in his hotel, ensuring customer security against active attacks is crucial. Active attacks involve unauthorized access, eavesdropping, or manipulation of the network traffic. To mitigate such threats, an effective and practical step is:

Station-to-Station Traffic Blocking: Also known as client isolation, this feature prevents direct communication between devices connected to the Wi-Fi network. By enabling this on the access points, Lynne can significantly decrease the likelihood of active attacks like man-in-the-middle (MITM) attacks, where an attacker intercepts and possibly alters the communication between two parties.

The other options, while beneficial for network security, might not be as straightforward or practical for Lynne's situation:

Network Access Control (NAC) requires a more complex infrastructure and management, which might not be ideal for a small hotel setup.

Implementing an SSL VPN adds an extra layer of security but might complicate the login process for users, potentially affecting the user experience.

Requiring EAP-FAST authentication provides secure authentication but may not be feasible for transient customers who expect quick and easy network access.

Therefore, enabling station-to-station traffic blocking is a practical and efficient measure that Lynne can implement to enhance customer security on the Wi-Fi network.

CWNA Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109, by David D. Coleman and David A. Westcott.

Best practices for securing a wireless network in a public hotspot environment.

Question 9

Question Type: MultipleChoice

In a long-distance RF link, what statement about Fade Margin is true?

Options:

A- A Fade Margin is unnecessary on a long-distance RF link if more than 80% of the first Fresnel zone is clear of obstructions.
B- The Fade Margin is a measurement of signal loss through free space and is a function of frequency and distance.
C- Fade Margin is an additional pad of signal strength designed into the RF system to compensate for unpredictable signal fading.
D- The Fade Margin of a long-distance radio link should be equivalent to the receiver's low noise filter gain.

Answer:

C

Explanation:

Fade Margin is an additional pad of signal strength designed into the RF system to compensate for unpredictable signal fading. It is the difference between the receiver's sensitivity and the actual received signal level. A higher Fade Margin indicates a more robust link that can withstand interference, attenuation, or other factors that may reduce the signal strength. A lower Fade Margin means that the link is more susceptible to failure or performance degradation.Fade Margin is usually expressed in decibels (dB) and can be calculated by subtracting the receiver sensitivity from the received signal level.Reference:1, Chapter 2, page 51;2, Section 2.1

Question 10

Question Type: MultipleChoice

You are attempting to locate the cause of a performance problem in two WLAN cells in a mostly overlapping coverage are

a. You note that one AP is on channel 1 and the other is on channel 2. When you document your findings, what term do you use to describe the problem in this configuration?

Options:

A- CCC
B- Non-Wi-Fi interference
C- CCI
D- ACI

Answer:

C

Explanation:

The term used to describe the problem in this configuration is Co-Channel Interference (CCI)1.CCI occurs when multiple access points are on the same or overlapping channels, causing interference and degradation in network performance1.In this case, one AP is on channel 1 and the other is on channel 2, which are overlapping channels, leading to CCI1.

Question 11

Question Type: MultipleChoice

What is appended to the end of each 802.11 data frame after the payload?

Options:

A- Preamble
B- MAC header
C- PHY header
D- FCS

Answer:

D

Explanation:

The FCS (Frame Check Sequence) is appended to the end of each 802.11 data frame after the payload. The FCS is a 4-byte field that contains a CRC-32 (Cyclic Redundancy Check) value that is calculated based on the contents of the MAC header and the payload of the frame. The FCS is used by the receiver to verify the integrity of the frame and to detect any errors or corruption that may have occurred during transmission. If the FCS does not match with the expected value, the frame is discarded by the receiver.Reference:, Chapter 4, page 139; , Section 4.2

Question 12

Question Type: MultipleChoice

What statement about 802.11 WLAN bridges is true?

Options:

A- WLAN bridges only work in the 2.4 GHz frequency band and they support only SISO communications
B- WLAN bridges must use a channel with acceptable SNR at both transceivers to maintain the desired data rate bi-directionally
C- WLAN bridges may support MIMO communications, but only if used in the 5 GHz frequency band
D- WLAN bridges must be implemented such that no interference occurs on the channel anywhere between the two endpoints used to establish the bridge

Answer:

B

Explanation:

WLAN bridges must use a channel with acceptable SNR at both transceivers to maintain the desired data rate bi-directionally. A WLAN bridge is a device that connects two or more networks using the 802.11 protocol. A WLAN bridge must have a clear and strong signal between the two endpoints to ensure reliable and fast data transmission. The signal-to-noise ratio (SNR) is a measure of the quality of the signal, which depends on the distance, interference, obstacles, and antenna gain between the transceivers. A higher SNR means a better signal quality and a higher data rate. A lower SNR means a worse signal quality and a lower data rate.Therefore, a WLAN bridge must use a channel with acceptable SNR at both transceivers to maintain the desired data rate bi-directionally1.

Question 13

Question Type: MultipleChoice

802. 11ax (HE) introduces Resource Units that can be used to allow communications with multiple devices at the same time, on the same channel, in the same BSS. What feature of 802.1 lax provides this functionality?

Options:

A- 6 GHz support
B- TWT
C- Wi-Fi-LTE
D- OFDMA

Answer:

D

Explanation:

The feature of 802.11ax (HE) that provides this functionality isOFDM

A . OFDMA stands for Orthogonal Frequency Division Multiple Access and is a technology that allows multiple devices to communicate simultaneously on the same channel in the same BSS. OFDMA works by dividing a channel into smaller subchannels called Resource Units (RUs), which are composed of groups of subcarriers or tones. Each RU can be assigned to a different device based on its bandwidth requirement and signal quality. This way, OFDMA can increase the efficiency and capacity of the channel by reducing overhead, contention, and latency. OFDMA can also support both uplink and downlink multi-user transmissions using trigger frames and buffer status reports. 6 GHz support, TWT, and Wi-Fi-LTE are not features of 802.11ax that provide this functionality.Reference:[CWNP Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 226; [CWNA: Certified Wireless Network Administrator Official Study Guide: Exam CWNA-109], page 216.

To Get Premium Files for CWNA-109 Visit

https://www.p2pexams.com/products/cwna-109

For More Free Questions Visit

https://www.p2pexams.com/cwnp/pdf/cwna-109

