CWNA-109 Q&As

Certified Wireless Network Administrator

Pass CWNP CWNA-109 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/cwna-109.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CWNP Official Exam Center

QUESTION 1

Which directional antenna types are commonly used by indoor Wi-Fi devices in a MIMO multiple spatial stream implementation?

A. Dipole and yagi

B. Grid and sector

C. Patch and panel

D. Dish and grid

Correct Answer: C

Patch and panel antennas are directional antenna types that are commonly used by indoor Wi-Fi devices in a MIMO multiple spatial stream implementation. These antennas have a flat rectangular shape and can be mounted on walls or ceilings to provide coverage in a specific direction. They have a moderate gain and a relatively wide beamwidth, making them suitable for multipath environments where signals can reflect off different surfaces and create multiple spatial streams. Patch and panel antennas can also support polarization diversity, which means they can transmit and receive both horizontally and vertically polarized waves, increasing the MIMO performance. References: 1, Chapter 2, page 72; 2, Section 2.4

QUESTION 2

What is required when operating 802.11ax APS in the 6 GHz band using passphrase- based authentication?

A. VHT PHY

B. HT PHY

C. SAE

D. CCMP

Correct Answer: C

SAE (Simultaneous Authentication of Equals) is required when operating 802.11ax APs in the 6 GHz band using passphrase-based authentication. SAE is a secure and robust authentication method that is defined in the IEEE 802.11s amendment and is also known as WPA3-Personal or WPA3-SAE. SAE is based on a cryptographic technique called Dragonfly Key Exchange, which allows two parties to establish a shared secret key using a passphrase, without revealing the passphrase or the key to an eavesdropper or an attacker. SAE also provides forward secrecy, which means that if the passphrase or the key is compromised in the future, it does not affect the security of past communications. SAE is required when operating 802.11ax APs in the 6 GHz band using passphrase-based authentication because of the new regulations and standards that apply to this band. The 6 GHz band is a new frequency band that was opened for unlicensed use by the FCC and other regulatory bodies in 2020. The 6 GHz band offers more spectrum and less interference than the existing 2.4 GHz and 5 GHz bands, which can enable higher performance and efficiency for Wi-Fi devices. However, the 6 GHz band also has some restrictions and requirements that are different from the other bands, such as: The 6 GHz band is divided into two sub-bands: U-NII-5 (5925-6425 MHz) and U- NII-7 (6525-6875 MHz). The U-NII-5 sub-band is subject to DFS (Dynamic Frequency Selection) rules, which require Wi-Fi devices to monitor and avoid using channels that are occupied by radar systems or other primary users. The U- NII-7 sub-band is not subject to DFS rules, but it has a lower maximum transmit power limit than the U-NII-5 sub-band. The Wi-Fi devices that operate in the 6 GHz band are called 6E devices, which stands for Extended

Spectrum. 6E devices must support 802.11ax technology, which is also known as Wi-Fi 6 or High Efficiency (HE). 802.11ax is a new standard that improves the performance and efficiency of Wi-Fi networks by using features such as OFDMA (Orthogonal Frequency Division Multiple Access), MU- MIMO (Multi-User Multiple Input Multiple Output), BSS Coloring, TWT (Target Wake Time), and HE PHY and MAC enhancements. The 6E devices that operate in the 6 GHz band must also support WPA3 security, which is a new security protocol that replaces WPA2 and provides stronger encryption and authentication for Wi-Fi networks. WPA3 has two modes: WPA3Personal and WPA3-Enterprise. WPA3-Personal uses SAE as its authentication method, which requires a passphrase to establish a secure connection between two devices. WPA3-Enterprise uses EAP (Extensible Authentication Protocol) as its authentication method, which requires a certificate or a credential to authenticate with a server. Therefore, SAE is required when operating 802.11ax APs in the 6 GHz band using passphrase-based authentication because it is part of WPA3-Personal security, which is mandatory for 6E devices in this band. References: , Chapter 3, page 120; , Section 3.2 9of30

QUESTION 3

An IEEE 802.11 amendment is in the daft state. What impact does this draft amendment have on the 802.11 standard?

A. Devices will be released based on the draft amendment and the draft amendment features are part of the standard.

B. No impact: Until an amendment is ratified, it does not become part of the standard.

C. No impact: Draft amendments do not become part of the standard until a working group is formed.

D. The standard is changed to reflect the new capabilities as soon as an amendment enters the draft stage.

Correct Answer: B

An IEEE 802.11 amendment is a proposed change or addition to the existing 802.11 standard, which defines the specifications and protocols for wireless LANs. An amendment goes through several stages of development, such as draft, sponsor ballot, and final approval, before it is ratified by the IEEE Standards Association and becomes part of the standard. Until then, it has no official impact on the standard, although some vendors may release products based on draft amendments to gain a competitive edge or to influence the final outcome of the amendment . References: [CWNA-109 Study Guide], Chapter 1: Overview of Wireless Standards, Organizations, and Fundamentals, page 25; [CWNA-109Study Guide], Chapter 1: Overview of Wireless Standards, Organizations, and Fundamentals, page 23; [IEEE website], IEEE-SA Standards Development Process.

QUESTION 4

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?

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

Correct Answer: A

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. References: 1:CWNA-109Official Study Guide, page 144 2: OFDMA

QUESTION 5

What statement describes the authorization component of a AAA implementation?

A. Verifying that a user is who he says he is.

B. Implementing a WIPS as a full-time monitoring solution to enforce policies.

C. Granting access to specific network services or resources according to a user profile.

D. Validating client device credentials against a database.

Correct Answer: C

Granting access to specific network services or resources according to a user profile describes the authorization component of a AAA implementation. AAA stands for Authentication, Authorization, and Accounting, which are three functions that are used to control and monitor access to network resources and services. Authentication is the process of verifying that a user is who he says he is, by using credentials such as username, password, certificate, token, or biometric data. Authorization is the process of granting access to specific network services or resources according to a user profile, which defines the user\\'s role, privileges, and permissions. Accounting is the process of recording and reporting the usage of network services or resources by a user, such as the duration, volume, type, and location of the access. AAA can be implemented by using different protocols andservers, such as RADIUS, TACACS+, LDAP, Kerberos, or Active Directory. References: 1, Chapter 11, page 449; 2, Section 7.1

QUESTION 6

A client STA must choose the best AP for connectivity. As part of the evaluation, it must verify compatible data rates. What can the client STA use to verify that an AP supports the same data rates that it supports?

A. Beacon frames transmitted by the AP

B. Data frames sent between the AP and current clients STAs

C. Authentication frames transmitted by the other client STAs

D. Probe request frames transmitted by other client STAs

Correct Answer: A

The client STA can use Beacon frames transmitted by the AP to verify that an AP supports the same data rates that it supports. Beacon frames are management frames that are periodically broadcasted by the APs to announce their presence, capabilities, and parameters. Oneof the information elements contained in the Beacon frames is the Supported Rates or Extended Supported Rates, which lists the data rates that the AP can use for communication. The client STA can compare its own data rates with those advertised by the AP to determine if they are compatible. Data frames, authentication frames, and probe request frames do not contain information about data rates. References:

[CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 133; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 123.

QUESTION 7

An 802.11 WLAN transmitter that emits a 50 mW signal is connected to a cable with 3 dB of loss. The cable is connected to an antenna with 16 dBi of gain. What is the power level at the Intentional Radiator?

A. 25 mW

B. 250 mW

C. 500 mW

D. 1000 mW

Correct Answer: B

The power level at the Intentional Radiator (IR) is 250 mW. The IR is the point where the RF signal leaves the transmitter and enters the antenna system. To calculate the power level at the IR, we need to consider the output power level of

the transmitter, the loss of the cable, and the gain of the antenna. The formula is:

Power level at IR (dBm) = Output power level (dBm) - Cable loss (dB) + Antenna gain (dBi) We can convert the output power level of 50 mW to dBm by using the formula:

Power level (dBm) = 10 * log10(Power level (mW))

Therefore, 50 mW = 10 * log10(50) = 16.99 dBm

We can plug in the values into the formula:

Power level at IR (dBm) = 16.99 - 3 + 16 = 29.99 dBm We can convert the power level at IR from dBm to mW by using the inverse formula:

Power level (mW) = 10^(Power level (dBm) / 10)

Therefore, 29.99 dBm = 10^(29.99 / 10) = 999.96 mW However, since we need to round off the answer to the nearest integer value, we get:

Power level at IR (mW) = 1000 mW

References: [CWNP Certified Wireless Network Administrator Official Study Guide:

ExamCWNA-109], page 67; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 57.

QUESTION 8

You are troubleshooting a problem with interference from a non-802.11 device. Given that the device is not a WLAN device, you cannot use a protocol analyzer and have chosen to use a spectrum analyzer. You want to view the signal from the interfering device over time to see the activity that is generating.

What common spectrum analyzer view should you use for this analysis?

A. APs

B. Waterfall/Spectrogram

C. Real-time FFT

D. Clients

Correct Answer: B

The common spectrum analyzer view that you should use for this analysis is the Waterfall/Spectrogram view. The Waterfall/Spectrogram view shows the signal from the interfering device over time on a three-dimensional graph. The x-axis

represents frequency, the y-axis represents time, and the z-axis represents amplitude or power. The color of each pixel indicates the signal strength at a given frequency and time. The Waterfall/Spectrogram view can help you identify the

characteristics of the interference source, such as its frequency range, duty cycle, modulation type, and pattern. References: [CWNP Certified Wireless Network Administrator Official Study Guide:

ExamCWNA-109], page 524; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 494.

QUESTION 9

What can an impedance mismatch in the RF cables and connectors cause?

A. Increased range of the RF signal

B. Fewer MCS values in the MCS table

C. Increased amplitude of the RF signal

D. Excessive VSWR

Correct Answer: D

VSWR stands for Voltage Standing Wave Ratio, which is a measure of how well the impedance of the RF cable and connectors matches the impedance of the transmitter and the antenna. Impedance is the opposition to the flow of alternating current in an RF circuit, and it depends on the frequency, resistance, capacitance, and inductance of the components. A perfect impedance match would have a VSWR of 1:1, meaning that all the power is transferred from the transmitter to the antenna, and none is reflected back. However, in reality, there is always some degree of mismatch, which causes some power to be reflected back to the transmitter, creating standing waves along the cable. This reduces the efficiency and performance of the wireless system, and can also damage the transmitter. Excessive VSWR can be caused by using poor quality or damaged cables and connectors, or by using components that have different impedance ratings123. References: CWNA-109 Study Guide, Chapter 2: Radio Frequency Fundamentals, page 90; CWNA-109Study Guide, Chapter 2: Radio Frequency Fundamentals, page 86; CWNP website, CWNA Certification.

QUESTION 10

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?

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.

Correct Answer: 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 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. References: CWNA-109 Study Guide, Chapter 5: Radio Frequency Signal and Antenna Concepts, page 139

QUESTION 11

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?

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.

Correct Answer: A

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 VPNadds an extra layer of security but might complicate the login process for

users, potentially affecting the user experience. Requiring EAP-FAST authenticationprovides secure authentication but may not be feasible for transient customers who expect quick and easy network access. Therefore, enabling station-tostation traffic blocking is a practical and efficient measure that Lynne can implement to enhance customer security on the Wi-Fi network.

References:

CWNA Certified Wireless Network Administrator Official Study Guide:

ExamCWNA-109, by David D. Coleman and David A. Westcott. Best practices for securing a wireless network in a public hotspot environment.

QUESTION 12

The requirements for a WLAN you are installing state that it must support unidirectional delays of less than 150 ms and the signal strength at all receivers can be no lower than -67 dBm. What application is likely used that demands these requirements?

A. VoIP

B. E-Mail

C. FTP

D. RTLS

Correct Answer: A

VoIP (Voice over Internet Protocol) is an application that is likely used that demands the requirements of unidirectional delays of less than 150 ms and the signal strength at all receivers can be no lower than -67 dBm. VoIP is an application that allows users to make and receive voice calls over a network, such as the Internet or a WLAN. VoIP is a real-time and interactive application that requires high quality of service (QoS) to ensure good user experience and satisfaction. One of the QoS metrics for VoIP is delay, which is the time it takes for a voice packet to travel from the sender to the receiver. Delay can affect the quality and intelligibility of the voice conversation, as well as the synchronization and naturalness of the dialogue. The ITU-T G.114 recommendation suggests that the maximum acceptable one-way delay for VoIP should be less than 150 ms, as anything higher than that can cause noticeable degradation and annoyance to

the users. Another QoS metric for VoIP is signal strength, which is the measure of how strong the RF signal is at the receiver. Signal strength can affect the reliability and performance of the wireless connection, as well as the data rate and throughput of the VoIP traffic. The CWNA Official Study Guide recommends that the minimum signal strength for VoIP should be -67 dBm, as anything lower than that can cause packet loss, retries, jitter, and other issues that can impair the voice quality. References: 1, Chapter 10, page 398; 2, Section 6.1

QUESTION 13

What frame type is used to reserve the wireless medium for the transmission of high data rate frames that may not be understood by all clients connected to the BSS?

A. RTS

B. ACK C. Beacon

D. PS-Poll

Correct Answer: A

The frame type that is used to reserve the wireless medium for the transmission of high data rate frames that may not be understood by all clients connected to the BSS is RTS. RTS stands for Request to Send and is a control frame that is sent by a station to request access to the medium for a specified duration. The RTS frame contains the source and destination MAC addresses, as well as a Network Allocation Vector (NAV) value that indicates how long the medium will be occupied. The destination station responds with a Clear to Send (CTS) frame that echoes the NAV value and grants permission to the source station. All other stations in the BSS hear either the RTS or CTS frame and update their NAV timers accordingly, deferring their transmissions until the medium is free. The RTS/CTS mechanism can be used to prevent hidden node problems, reduce collisions, and protect high data rate frames that use features such as 802.11n or 802.11ac that may not be compatible with legacy stations. ACK, Beacon, and PS-Poll are not used to reserve the medium for high data rate frames. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 112; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 102.

QUESTION 14

You are tasked with performing a throughput test on the WLAN. The manager asks that you use open source tools to reduce costs. What open source tool is designed to perform a throughput test?

A. iPerf

B. PuTTy

C. IxChariot

D. Python

Correct Answer: A

iPerf is an open source tool that is designed to perform a throughput test on the WLAN. iPerf is a cross-platform command-line tool that can measure the bandwidth and quality of network links by generating TCP or UDP traffic between two endpoints.iPerf can run as either a server or a client mode, depending on whether it receives or sends traffic. iPerf can also report various metrics of network performance, such as throughput, jitter, packet loss, delay, and TCP window size. To perform a throughput test on the WLAN using iPerf, one device needs to run iPerf in server mode and another device needs to run iPerf in client mode. The devices need to be connected to the same WLAN network

and have their IP addresses configured properly. The device running iPerf in client mode needs to specify the IP address of the device running iPerf in server mode as well as other parameters such as protocol, port number, duration, interval, bandwidth limit, packet size, etc. The device running iPerf in server mode will listen for incoming connections from the client device and send back acknowledgments or responses depending on the protocol used. The device running iPerf in client mode will send traffic to the server device according to the specified parameters and measure the network performance. The device running iPerf in client mode will display the results of the throughput test at the end of the test or at regular intervals during the test. The results can show the average, minimum, maximum, and instantaneous throughput of the network link, as well as other metrics such as jitter, packet loss, delay, and TCP window size. References: 1, Chapter 7, page 287; 2, Section 4.3

QUESTION 15

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

A. CCC

B. Non-Wi-Fi interference

C. CCI

D. ACI

Correct Answer: C

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.