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.geekcert.com/cwna-109.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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 2

What security solution is deprecated in the 802.11 standard and should never be used in any modern WLAN deployment?

A. Shared Key Authentication

B. Open System Authentication

C. CCMP

D. AES

Correct Answer: A

Shared Key Authentication is a security solution that was defined in the original 802.11 standard as an alternative to Open System Authentication, which does not provide any security at all. Shared Key Authentication uses WEP (Wired Equivalent Privacy) to encrypt and authenticate data frames between the client station and the AP. However, WEP has been proven to be extremely vulnerable to various attacks that can easily crack the encryption key and compromise the network security. Therefore, Shared Key Authentication is deprecated in the 802.11 standard and should never be used in any modern WLAN deployment . References: [CWNA-109 Study Guide], Chapter 10: Wireless LAN Security, page 401; [CWNA-109Study Guide], Chapter 10: Wireless LAN Security, page 391; [Wikipedia], Wired Equivalent Privacy.

QUESTION 3

Which IEEE 802.11 physical layer (PHY) specification includes support for operation in the 2.4 GHz, 5 GHz, and 6 GHz bands?

A. VHT (802.11ac).

B. HT(802.11n)

C. HR/DSSS (802.11b)

D. HE (802.11ax)

Correct Answer: D

The IEEE 802.11ax standard, also known as High-Efficiency Wireless (HEW) or simply HE, includes support for operation across multiple frequency bands: 2.4 GHz, 5 GHz, and, with the appropriate regulatory approvals, the 6 GHz band.

This makes option D the correct answer. Here\\'s how it compares to the other options:

HE (802.11ax): Introduced as an enhancement over previous standards, 802.11ax is designed to improve efficiency, especially in dense environments. It supports operation in the 2.4 GHz, 5 GHz, and 6 GHz bands (the latter pending

regulatory approval in various regions), making it highly versatile and future-proof. VHT (802.11ac): Very High Throughput, or 802.11ac, operates exclusively in the 5 GHz band. It introduced significant speed improvements over its

predecessor (802.11n) but does not support the 2.4 GHz or 6 GHz bands. HT (802.11n): High Throughput, or 802.11n, supports operation in both the 2.4 GHz and 5 GHz bands. However, it does not include support for the 6 GHz band. HR/

DSSS (802.11b): High-Rate Direct Sequence Spread Spectrum, or 802.11b, operates only in the 2.4 GHz band. It was one of the early Wi-Fi standards and does not support 5 GHz or 6 GHz bands.

Given these distinctions, only 802.11ax (option D) supports operation across all three mentioned bands, aligning with the requirements stated in the question.

References:

IEEE 802.11ax-2021: High-Efficiency Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

Understanding the 802.11ax (Wi-Fi 6) standard and its implications for modern wireless networking.

QUESTION 4

What statement about 802.11 WLAN performance is true?

A. In modem networks, both centralized and distributed data forwarding work well for most standard office deployments

B. In most WLANs, no special skill or tuning is required to get peak performance

C. WLANs perform better as more wireless clients connect with each AP

D. To get the best performance out of an AP, you should disable data rates of 72 Mbps and lower

Correct Answer: A

The statement that in modern networks, both centralized and distributed data forwarding work well for most standard office deployments is true about WLAN performance. Data forwarding refers to how wireless frames are transmitted from wireless clients to wired networks or vice versa through wireless access points (APs). Centralized data forwarding means that all wireless frames are sent to a central controller or gateway before being forwarded to their destinations. Distributed data forwarding means that wireless frames are forwarded directly by the APs to their destinations without going through a central controller or gateway. Both methods have their advantages and disadvantages, depending on the network size, topology, traffic pattern, security, and management requirements. However, in modern networks, both methods can achieve high performance and scalability for most standard office deployments, as they can leverage advanced features such as fast roaming, load balancing, quality of service, and encryption. The other statements about WLAN performance are false. In most WLANs, special skill or tuning is required to get peak performance, such as selecting the appropriate channel, power, data rate, and antenna settings. WLANs perform worse as more wireless clients connect with each AP, as they cause more contention and interference on the wireless medium. To get the best performance out of an AP, you should not disable data rates of 72 Mbps and lower, as they are needed for backward compatibility and range extension. References: CWNA-109 Study Guide, Chapter 9: Wireless LAN Architecture, page 2811

QUESTION 5

You are performing a post-implementation validation survey. What basic tool can be used to easily locate areas of high co-channel interference?

A. Throughput tester

B. Laptop-based spectrum analyzer

C. Access point spectrum analyzer

D. Wi-Fi scanner

Correct Answer: D

A Wi-Fi scanner is a basic tool that can be used to easily locate areas of high co-channel interference. A Wi-Fi scanner is a software application that can run on a laptop, tablet, smartphone, or other device that has a Wi-Fi adapter. A Wi-Fi scanner can scan the wireless environment and display information about the detected access points and client stations, such as their SSID, BSSID, channel, signal strength, security, and data rate. A Wi-Fi scanner can also show the channel utilization and overlap of different access points, which can indicate the level of co-channel interference. Co-channel interference is a type of interference that occurs when multiple access points use the same or adjacent channels within the same coverage area. Co-channel interference can reduce the throughput and performance of the WLAN, as the access points and client stations have to contend for the channel access and avoid collisions. To identify

areas of high co-channel interference, a Wi-Fi scanner can be used to measure the signal strength and channel utilization of different access points and compare them with a threshold or a baseline. Alternatively, a Wi-Fi scanner can also use a color-coded heat map to visualize the co-channel interference level in different locations. References: 1, Chapter 7, page 279; 2, Section 4.3