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 best describes WPA2 in relation to 802.11 wireless networks?

A. WPA2 is the standard that defines security for WLANs.

B. WPA2 is a certification created by the Wi-Fi Alliance that validates devices correctly implement CCMP/ AES.

C. WPA2 is the second version of WPA and it enhances security through the use of TKIP instead of WEP.

D. WPA2 is specified in the 802.11 standard as implementing CCMP/AES.

Correct Answer: B

WPA2 (Wi-Fi Protected Access 2) is a security certification program developed by the Wi-Fi Alliance to secure wireless computer networks. It is important to understand the following: WPA2 and the 802.11 Standard: While WPA2 is based on elements of the 802.11i amendment to the 802.11 standard, it is not itself a standard but rather a certification to ensure devices comply with certain security criteria, including the correct implementation of CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) and AES (Advanced Encryption Standard). CCMP/AES Implementation: WPA2 enhances the security of wireless networks by using CCMP for encryption, which is based on AES, a robust encryption algorithm. This represents a significant security improvement over WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) that used TKIP (Temporal Key

Integrity Protocol).

WPA vs. WPA2: WPA was the interim security enhancement over WEP, utilizing TKIP for encryption. WPA2, however, moved to the more secure AES-based encryption method. Contrary to option C, WPA2 does not enhance security by

using TKIP; it uses CCMP/AES.

Therefore, option B correctly describes WPA2 as a certification program ensuring devices properly implement the more secure CCMP/AES encryption methods.

References:

Wi-Fi Alliance website for WPA2 certification details. IEEE 802.11i-2004: Amendment for Enhanced Security.

QUESTION 2

When a STA has authenticated to an AP (AP-1), but still maintains a connection with another AP (AP-2), what is the state of the STA on AP-1?

A. Transitional

B. Unauthenticated and Unassociated

C. Authenticated and Unassociated

D. Authenticated and Associated

Correct Answer: C

Authenticated and Unassociated. According to one of the web search results1, a STA can be authenticated to multiple

APs, but it can only be associated to one AP at a time. Association is the process of establishing a logical link between the STA and the AP, which allows the STA to send and receive data frames through the AP2. Therefore, when a STA has authenticated to an AP-1, but still maintains a connection with another AP-2, it means that the STA is authenticated to both APs, but only associated to AP-2. The state of the STA on AP-1 is authenticated and unassociated, which means that the STA can switch to AP-1 without repeating the authentication process, but it cannot send or receive data frames through AP-1 until it becomes associated.

QUESTION 3

What is the most effective method for testing roaming in relation to 802.11 VoIP handsets?

A. Use a spectrum analyzer to monitor RF activity during a VoIP call.

B. Use a protocol analyzer to capture the traffic generated when a laptop roams.

C. Place a call with the handset and move around the facility to test quality during roaming.

D. Use the built-in roaming monitor built into all VoIP handsets.

Correct Answer: C

The most effective method for testing roaming in relation to 802.11 VoIP handsets is to place a call with the handset and move around the facility to test quality duringroaming. This method allows you to evaluate the actual performance and user experience of VoIP calls over wireless networks, as well as identify any potential issues such as signal strength, interference, latency, jitter, packet loss, or handoff delays. A spectrum analyzer can only show you the RF activity during a VoIP call, but not how it affects the voice quality or roaming behavior. A protocol analyzer can capture the traffic generated when a laptop roams, but it cannot simulate the characteristics of a VoIP handset such as battery life, antenna design, codec support, or QoS features. A built-in roaming monitor is not a common feature in all VoIP handsets, and it may not provide accurate or comprehensive information about the roaming process. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 487; [Voice over Wireless LAN 4.1 Design Guide], page 6-19.

QUESTION 4

When a client station sends a broadcast probe request frame with a wildcard SSID, how do APs respond?

A. Each AP responds in turn after preparing a probe response and winning contention.

B. For each probe request frame, only one AP may reply with a probe response.

C. Each AP checks with the DHCP server to see if it can respond and then acts accordingly.

D. After waiting a SIFS, all APs reply at the same time with a probe response.

Correct Answer: A

In the 802.11 wireless networking protocols, when a client station sends a broadcast probe request frame with a wildcard SSID (Service Set Identifier), it is essentially asking for any nearby access points (APs) to identify themselves. The way

APs respond to such a probe request is governed by standard 802.11 behavior, which includes:

Probe Request Handling: Upon receiving a broadcast probe request, each AP that can serve the client prepares a probe

response. The response includes information about the AP, such as its SSID, supported data rates, and other

capabilities.

Contention-Based Mechanism: Wireless networks use a contention-based mechanism (CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance) for medium access. Each AP must wait for a clear channel and win the contention

process before it can send its probe response.

Independent Responses: Each AP operates independently in responding to the probe request. There is no coordination between APs to decide which one responds first or at all, leading to multiple APs sending probe responses, each after

winning the contention for the medium.

Option A accurately reflects this process, indicating that each AP prepares and sends a probe response in turn, contingent upon winning the medium contention. The other options suggest mechanisms (such as coordination with a DHCP

server or simultaneous responses after a Short Interframe Space (SIFS)) that do not align with standard 802.11 procedures for handling broadcast probe requests.

References:

IEEE 802.11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

CWNA Certified Wireless Network Administrator Official Study Guide: Exam PW0- 105, by David D. Coleman and David A. Westcott.

QUESTION 5

You recently purchased four laptops containing dual-band 802.11ac adapters. The laptops can connect to your 2.4 GHz network, but they cannot connect to the 5 GHz network. The laptops do not show the 5 GHz SSIds, which are different than the 2.4 GHz SSIDs. Existing devices can connect to the 5 GHz SSIDs with no difficulty. What is the likely problem?

A. Interference from non-Wi-Fi sources

B. Faulty drivers

C. DoS attack

D. Interference from other WLANs

Correct Answer: B

The likely problem that causes this scenario is faulty drivers. Drivers are software components that enable the communication between the operating system and the hardware devices, such as the wireless adapters. Faulty drivers can cause various issues with the wireless connectivity, such as not detecting or connecting to certain networks, dropping connections, or reducing performance. Faulty drivers can be caused by corrupted files, outdated versions, incompatible settings, or hardware defects. To fix faulty drivers, you can try to update, reinstall, or roll back the drivers, or contact the manufacturer for support. Interference from non-Wi-Fi sources, DoS attack, or interference from other WLANs are not likely to cause this scenario, as they would affect all devices in the same area, not just the new laptops. References: [CWNP Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 562; [CWNA: Certified Wireless Network Administrator Official Study Guide: ExamCWNA-109], page 532.

CWNA-109 VCE Dumps CWNA-109 Practice Test CWNA-109 Braindumps