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.pass4itsure.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 factor does not influence the distance at which an RF signal can be effectively received?

A. Receiving station\\'s radio sensitivity

B. Receiving station\\'s output power

C. Transmitting station\\'s output power

D. Free Space Path Loss

Correct Answer: B

In wireless communication, several factors influence the effective reception of RF signals, including the receiving station\\'s radio sensitivity, the transmitting station\\'s output power, and free space path loss. However, the receiving station\\'s

output power does not influence the distance at which an RF signal can be effectively received. The key factors that impact signal reception distance are:

Receiving Station\\'s Radio Sensitivity: This refers to the lowest signal strength at which the receiver can process a signal with an acceptableerror rate. Higher sensitivity allows for better reception at greater distances. Transmitting Station\\'s

Output Power: This is the power with which a transmitter sends out a signal. Higher output power can extend the range of transmission, making it easier for distant receivers to detect the signal. Free Space Path Loss (FSPL): FSPL

represents the attenuation of radio energy as it travels through free space. It increases with distance and frequency, reducing the signal strength as the distance from the transmitter increases. The output power of the receiving station is

related to how strong a signal it sends out, not how well it can receive or process incoming signals. Therefore, it does not affect the reception distance of incoming RF signals.

References:

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

RF fundamentals and RF design considerations in wireless communication systems.

QUESTION 2

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 3

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 4

You are the network administrator for ABC Company. Your manager has recently attended a wireless security seminar. The seminar speaker taught that a wireless network could be hidden from potential intruders if you disabled the broadcasting of the SSID in Beacons and configured the access points not to respond to Probe Request frames that have a null SSID field.

Your manager suggests implementing these security practices. What response should you give to this suggestion?

A. Any 802.11 protocol analyzer can see the SSID in clear text in frames other than Beacons frames. This negates any security benefit of trying to hide the SSID in Beacons and Probe Response frames.

B. To improve security by hiding the SSID, the AP and client stations must both be configured to remove the SSID from association request and response frames. Most WLAN products support this.

C. Any tenants in the same building using advanced penetration testing tools will be able to obtain the SSID by exploiting WPA EAPOL-Key exchanges. This poses an additional risk of exposing the WPA key.

D. This security practice prevents manufacturers\\' client utilities from detecting the SSID. As a result, the SSID cannot be obtained by attackers, except through social engineering, guessing, or use of a WIPS.

Correct Answer: A

The response that you should give to your manager\\'s suggestion of implementing the security practices of disabling the broadcasting of the SSID in Beacons and configuring the access points not to respond to Probe Request frames that have a null SSID field is that any 802.11 protocol analyzer can see the SSID in clear text in frames other than Beacons frames. This negates any security benefit of trying to hide the SSID in Beacons and Probe Response frames. The SSID (Service Set Identifier) is a human-readable name that identifies a WLAN and allows users to connect to it. The SSID is transmitted in clear text in several types of 802.11 frames, such as Beacon frames, Probe Request frames, Probe Response frames, Association Request frames, Association Response frames, Reassociation Request frames, and Reassociation Response frames. Some people may think that hiding the SSID can improve the security of the WLAN by making it invisible to potential intruders. However, this is not true, as hiding the SSID only removes it from Beacon frames and Probe Response frames that have a null SSID field. The SSID is still present in other types of frames that can be easily captured and analyzed by any 802.11 protocol analyzer or wireless scanner tool. Therefore, hiding the SSID does not provide any real security benefit and may even cause some compatibility and performance issues for legitimate users. References: 1, Chapter 4, page 133; 2, Section 4.1

QUESTION 5

Your consulting firm has recently been hired to complete a site survey for a company desiring an indoor coverage WI-AN. Your engineers use predictive design software for the task, but the company insists on a pre-design site visit.

What task should be performed as part of the pre-design visit to prepare for a predictive design?

A. Install at least one AP on each side of the exterior walls to test for co-channel interference through these walls

B. Collect information about the company\\'s security requirements and the current configuration of their RADIUS and user database servers

C. Test several antenna types connected to the intended APS for use in the eventual deployment

D. Evaluate the building materials at the facility and confirm that the floor plan documents are consistent with the actual building

Correct Answer: D

A pre-design site visit in preparation for a predictive wireless LAN design is essential for gathering physical and environmental data about the site. The key tasks to be performed during such a visit include:

Evaluating Building Materials: Different materials (concrete, glass, wood, etc.) have varying effects on RF signal propagation. Understanding the materials present helps in accurately predicting how signals will behave within the environment.

Floor Plan Verification: Ensuring that the floor plan documents are an accurate representation of the actual building layout is crucial. Discrepancies between the floor plans and the physical layout can lead to inaccuracies in the predictive

design.

The other options, while potentially valuable in other contexts, are not directly related to preparing for a predictive design:

Installing APs(option A) for testing co-channel interference is more aligned with an active site survey rather than a pre-design visit for a predictive design. Collecting information about security requirements(option B) is important but is not

directly related to the physical aspects of the site that would impact a predictive design.

Testing antenna types(option C) would typically be part of an active site survey or the actual deployment phase, not a pre-design visit for predictive modeling. Therefore, option D is the correct answer, focusing on evaluating physical aspects

crucial for accurate predictive modeling.

References:

CWNA Certified Wireless Network Administrator Official Study Guide:

ExamCWNA-109, by David D. Coleman and David A. Westcott. Best practices for conducting pre-design site visits in wireless network planning.

Latest CWNA-109 Dumps CWNA-109 PDF Dumps CWNA-109 Practice Test