

## CWSP-206<sup>Q&As</sup>

CWSP Certified Wireless Security Professional

**Pass CWNP CWSP-206 Exam with 100% Guarantee**

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

<https://www.leads4pass.com/cwsp-206.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**

Your network implements an 802.1X/EAP-based wireless security solution. A WLAN controller is installed and manages seven APs. FreeRADIUS is used for the RADIUS server and is installed on a dedicated server named SRV21. One example client is a MacBook Pro with 8 GB RAM. What device functions as the 802.1X/EAP Authenticator?

- A. WLAN Controller/AP
- B. MacBook Pro
- C. SRV21
- D. RADIUS server

Correct Answer: A

---

**QUESTION 2**

ABC Company is implementing a secure 802.11 WLAN at their headquarters (HQ) building in New York and at each of the 10 small, remote branch offices around the United States. 802.1X/EAP is ABC's preferred security solution, where possible. All access points (at the HQ building and all branch offices) connect to a single WLAN controller located at HQ. Each branch office has only a single AP and minimal IT resources. What security best practices should be followed in this deployment scenario?

- A. Remote management of the WLAN controller via Telnet, SSH, HTTP, and HTTPS should be prohibited across the WAN link.
- B. RADIUS services should be provided at branch offices so that authentication server and supplicant credentials are not sent over the Internet.
- C. An encrypted VPN should connect the WLAN controller and each remote controller-based AP, or each remote site should provide an encrypted VPN tunnel to HQ.
- D. APs at HQ and at each branch office should not broadcast the same SSID; instead each branch should have a unique ID for user accounting purposes.

Correct Answer: C

---

**QUESTION 3**

What software and hardware tools are used in the process performed to hijack a wireless station from the authorized wireless network onto an unauthorized wireless network?

- A. A low-gain patch antenna and terminal emulation software
- B. MAC spoofing software and MAC DoS software
- C. RF jamming device and a wireless radio card
- D. A wireless workgroup bridge and a protocol analyzer

Correct Answer: C

---

## QUESTION 4

A large enterprise is designing a secure, scalable, and manageable 802.11n WLAN that will support thousands of users. The enterprise will support both 802.1X/EAP-TTLS and PEAPv0/MSCHAPv2. Currently, the company is upgrading network servers as well and will replace their existing Microsoft IAS implementation with Microsoft NPS, querying Active Directory for user authentication. For this organization, as they update their WLAN infrastructure, what WLAN controller feature will likely be least valuable?

- A. SNMPv3 support
- B. 802.1Q VLAN trunking
- C. Internal RADIUS server
- D. WIPS support and integration
- E. WPA2-Enterprise authentication/encryption

Correct Answer: C

---

## QUESTION 5

ABC Company is an Internet Service Provider with thousands of customers. ABC's customers are given login credentials for network access when they become a customer. ABC uses an LDAP server as the central user credential database. ABC is extending their service to existing customers in some public access areas and would like to use their existing database for authentication. How can ABC Company use their existing user database for wireless user authentication as they implement a large-scale WPA2Enterprise WLAN security solution?

- A. Implement a RADIUS server and query user authentication requests through the LDAP server.
- B. Mirror the LDAP server to a RADIUS database within a WLAN controller and perform daily backups to synchronize the user databases.
- C. Import all users from the LDAP server into a RADIUS server with an LDAP-to-RADIUS conversion tool.
- D. Implement an X.509 compliant Certificate Authority and enable SSL queries on the LDAP server.

Correct Answer: A

[Latest CWSP-206 Dumps](#)

[CWSP-206 Exam Questions](#)

[CWSP-206 Braindumps](#)