# CWSP-205$^{Q\&As}$

## Certified Wireless Security Professional

## Pass CWNP CWSP-205 Exam with 100% Guarantee

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

**https://www.pass2lead.com/cwsp-205.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**

Given: You support a coffee shop and have recently installed a free 802.11ac wireless hot-spot for the benefit of your customers. You want to minimize legal risk in the event that the hot-spot is used for illegal Internet activity.

What option specifies the best approach to minimize legal risk at this public hot-spot while maintaining an open venue for customer Internet access?

A. Configure WPA2-Enterprise security on the access point

B. Block TCP port 25 and 80 outbound on the Internet router

C. Require client STAs to have updated firewall and antivirus software

D. Allow only trusted patrons to use the WLAN

E. Use a WIPS to monitor all traffic and deauthenticate malicious stations

F. Implement a captive portal with an acceptable use disclaimer

Correct Answer: F

**QUESTION 2**

Given: Your network includes a controller-based WLAN architecture with centralized data forwarding. The AP builds an encrypted tunnel to the WLAN controller. The WLAN controller is uplinked to the network via a trunked 1 Gbps Ethernet port supporting all necessary VLANs for management, control, and client traffic.

What processes can be used to force an authenticated WLAN client\\'s data traffic into a specific VLAN as it exits the WLAN controller interface onto the wired uplink? (Choose 3)

A. On the Ethernet switch that connects to the AP, configure the switch port as an access port (not trunking) in the VLAN of supported clients.

B. During 802.1X authentication, RADIUS sends a return list attribute to the WLAN controller assigning the user and all traffic to a specific VLAN.

C. In the WLAN controller\\'s local user database, create a static username-to-VLAN mapping on the WLAN controller to direct data traffic from a specific user to a designated VLAN.

D. Configure the WLAN controller with static SSID-to-VLAN mappings; the user will be assigned to a VLAN according to the SSID being used.

Correct Answer: BCD

**QUESTION 3**

What security benefits are provided by endpoint security solution software? (Choose 3)

A. Can prevent connections to networks with security settings that do not conform to company policy

B. Can collect statistics about a user\\'s network use and monitor network threats while they are connected

C. Can restrict client connections to networks with specific SSIDs and encryption types

D. Can be used to monitor for and prevent network attacks by nearby rogue clients or APs

Correct Answer: ABC

**QUESTION 4**

Given: The ABC Corporation currently utilizes an enterprise Public Key Infrastructure (PKI) to allow employees to securely access network resources with smart cards. The new wireless network will use WPA2-Enterprise as its primary authentication solution. You have been asked to recommend a Wi-Fi Alliance-tested EAP method.

What solutions will require the least change in how users are currently authenticated and still integrate with their existing PKI?

A. EAP-FAST

B. EAP-TLS

C. PEAPv0/EAP-MSCHAPv2

D. LEAP

E. PEAPv0/EAP-TLS

F. EAP-TTLS/MSCHAPv2

Correct Answer: B

**QUESTION 5**

Wireless Intrusion Prevention Systems (WIPS) provide what network security services? (Choose 2)

A. Configuration distribution for autonomous APs

B. Wireless vulnerability assessment

C. Application-layer traffic inspection

D. Analysis and reporting of AP CPU utilization

E. Policy enforcement and compliance management

Correct Answer: BE

**QUESTION 6**

What wireless authentication technologies may build a TLS tunnel between the supplicant and the authentication server before passing client authentication credentials to the authentication server? (Choose 3)

![Pass2Lead logo](https://Pass2Lead.com)
A. EAP-MD5

B. EAP-TLS

C. LEAP

D. PEAPv0/MSCHAPv2

E. EAP-TTLS

Correct Answer: BDE

**QUESTION 7**

ABC Company has deployed a Single Channel Architecture (SCA) solution to help overcome some of the common problems with client roaming. In such a network, all APs are configured with the same channel and BSSID. PEAPv0/EAP-MSCHAPv2 is the only supported authentication mechanism.

As the Voice over Wi-Fi (STA-1) client moves throughout this network, what events are occurring?

A. STA-1 initiates open authentication and 802.11 association with each AP prior to roaming.

B. The WLAN controller is querying the RADIUS server for authentication before the association of STA-1 is moved from one AP to the next.

C. STA-1 controls when and where to roam by using signal and performance metrics in accordance with the chipset drivers and 802.11k.

D. The WLAN controller controls the AP to which STA-1 is associated and transparently moves this association in accordance with the physical location of STA-1.

Correct Answer: D

**QUESTION 8**

What statements are true about 802.11-2012 Protected Management Frames? (Choose 2)

A. 802.11w frame protection protects against some Layer 2 denial-of-service (DoS) attacks, but it cannot prevent all types of Layer 2 DoS attacks.

B. When frame protection is in use, the PHY preamble and header as well as the MAC header are encrypted with 256- or 512-bit AES.

C. Authentication, association, and acknowledgment frames are protected if management frame protection is enabled, but deauthentication and disassociation frames are not.

D. Management frame protection protects disassociation and deauthentication frames.

Correct Answer: AD

**QUESTION 9**

Given: ABC Company has 20 employees and only needs one access point to cover their entire facility. Ten of ABC Company\\'s employees have laptops with radio cards capable of only WPA security. The other ten employees have laptops with radio cards capable of WPA2 security. The network administrator wishes to secure all wireless communications (broadcast and unicast) for each laptop with its strongest supported security mechanism, but does not wish to implement a RADIUS/AAA server due to complexity.

What security implementation will allow the network administrator to achieve this goal?

A. Implement an SSID with WPA2-Personal that allows both AES-CCMP and TKIP clients to connect.

B. Implement an SSID with WPA-Personal that allows both AES-CCMP and TKIP clients to connect.

C. Implement two separate SSIDs on the AP--one for WPA-Personal using TKIP and one for WPA2Personal using AES-CCMP.

D. Implement an SSID with WPA2-Personal that sends all broadcast traffic using AES-CCMP and unicast traffic using either TKIP or AES-CCMP.

Correct Answer: C

**QUESTION 10**

You are implementing an 802.11ac WLAN and a WIPS at the same time. You must choose between integrated and overlay WIPS solutions. Which of the following statements is true regarding integrated WIPS solutions?

A. Integrated WIPS always perform better from a client throughput perspective because the same radio that performs the threat scanning also services the clients.

B. Integrated WIPS use special sensors installed alongside the APs to scan for threats.

C. Many integrated WIPS solutions that detect Voice over Wi-Fi traffic will cease scanning altogether to accommodate the latency sensitive client traffic.

D. Integrated WIPS is always more expensive than overlay WIPS.

Correct Answer: C

**QUESTION 11**

Given: Many corporations configure guest VLANs on their WLAN controllers that allow visitors to have Internet access only. The guest traffic is tunneled to the DMZ to prevent some security risks.

In this deployment, what risks are still associated with implementing the guest VLAN without any advanced traffic monitoring or filtering features enabled? (Choose 2)

A. Intruders can send spam to the Internet through the guest VLAN.

B. Peer-to-peer attacks can still be conducted between guest users unless application-layer monitoring and filtering are implemented.

C. Unauthorized users can perform Internet-based network attacks through the WLAN.

D. Guest users can reconfigure AP radios servicing the guest VLAN unless unsecure network management protocols

![Pass2Lead logo](https://Pass2Lead.com)
(e.g. Telnet, HTTP) are blocked.

E. Once guest users are associated to the WLAN, they can capture 802.11 frames from the corporate VLANs.

Correct Answer: AC

## QUESTION 12

Given: You are using WEP as an encryption solution. You are using VLANs for network segregation.

Why can you not establish an RSNA?

A. RSNA connections require TKIP or CCMP.

B. RSNA connections require BIP and do not support TKIP, CCMP or WEP.

C. RSNA connections require CCMP and do not support TKIP or WEP.

D. RSNA connections do not work in conjunction with VLANs.

Correct Answer: A

## QUESTION 13

When using the 802.1X/EAP framework for authentication in 802.11 WLANs, why is the 802.1X Controlled Port still blocked after the 802.1X/EAP framework has completed successfully?

A. The 802.1X Controlled Port is always blocked, but the Uncontrolled Port opens after the EAP authentication process completes.

B. The 802.1X Controlled Port remains blocked until an IP address is requested and accepted by the Supplicant.

C. The 4-Way Handshake must be performed before the 802.1X Controlled Port changes to the unblocked state.

D. The 802.1X Controlled Port is blocked until Vender Specific Attributes (VSAs) are exchanged inside a RADIUS packet between the Authenticator and Authentication Server.

Correct Answer: C

## QUESTION 14

ABC Company uses the wireless network for highly sensitive network traffic. For that reason, they intend to protect their network in all possible ways. They are continually researching new network threats and new preventative measures. They are interested in the security benefits of 802.11w, but would like to know its limitations.

What types of wireless attacks are protected by 802.11w? (Choose 2)

A. RF DoS attacks

B. Layer 2 Disassociation attacks

C. Robust management frame replay attacks

D. Social engineering attacks

Correct Answer: BC

---

**QUESTION 15**

Given: In XYZ\'s small business, two autonomous 802.11ac APs and 12 client devices are in use with WPA2-Personal.

What statement about the WLAN security of this company is true?

A. Intruders may obtain the passphrase with an offline dictionary attack and gain network access, but will be unable to decrypt the data traffic of other users.

B. A successful attack against all unicast traffic on the network would require a weak passphrase dictionary attack and the capture of the latest 4-Way Handshake for each client.

C. An unauthorized wireless client device cannot associate, but can eavesdrop on some data because WPA2-Personal does not encrypt multicast or broadcast traffic.

D. An unauthorized WLAN user with a protocol analyzer can decode data frames of authorized users if he captures the BSSID, client MAC address, and a user\'s 4-Way Handshake.

E. Because WPA2-Personal uses Open System authentication followed by a 4-Way Handshake, hijacking attacks are easily performed.

Correct Answer: B

[CWSP-205 Study Guide](#)          [CWSP-205 Exam Questions](#)          [CWSP-205 Braindumps](#)