Chapters 20 – 21: Wireless Security and Connectivity Exam (Answers)

itexamanswers.net/chapters-20-21-wireless-security-and-connectivity-exam-answers.html

December 19, 2020

CCNPv8 ENCOR (Version 8.0) – Wireless Security and Connectivity Exam

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. Which term describes the role of a Cisco switch in the 802.1X port-based access control?

- authentication server
- **authenticator**
- supplicant
- agent

Explanation: 802.1X port-based authentication defines specific roles for the devices in the network:
Client (Supplicant) – The device that requests access to LAN and switch services
Switch (Authenticator) – Controls physical access to the network based on the authentication status of the client
Authentication server – Performs the actual authentication of the client

2. What method of wireless authentication is dependent on a RADIUS authentication server?

- **WPA2 Enterprise**
- WPA Personal
- WEP
- WPA2 Personal

Explanation: WPA2 Enterprise relies on an external RADIUS server to authenticate clients when they attempt to connect. WEP and WPA/WPA2 Personal both use a pre-shared key that the clients must know in order to authenticate.

3. Which wireless encryption method is the most secure?

- **WPA2 with AES**
- WEP
- WPA2 with TKIP
- WPA

Explanation: IEEE 802.11i and WPA2 both use the Advanced Encryption Standard (AES) for encryption. AES is currently considered the strongest encryption protocol. WPA2 does not use TKIP (Temporal Key Integrity Protocol). It is WPA that uses TKIP. Although WPA provides stronger encryption than WEP, it is is not as strong as WPA2 (AES).

4. A network administrator is configuring a RADIUS server connection on a Cisco 3500 series WLC. The configuration requires a shared secret password. What is the purpose for the shared secret password?

- It is used to authenticate and encrypt user data on the WLAN.
- It allows users to authenticate and access the WLAN.
- It is used by the RADIUS server to authenticate WLAN users.
- **It is used to encrypt the messages between the WLC and the RADIUS server.**

Explanation: The RADIUS protocol uses security features to protect communications between the RADIUS server and clients. A shared secret is the password used between the WLC and the RADIUS server. It is not for end users.

5. Which WLAN security protocol avoids attacks by strengthening the key exchange between clients and APs using a method known as Simultaneous Authentication of Equals?

- WEP
- **WPA3-Personal**
- WPA-Personal
- WPA2-Personal

Explanation: With WPA-Personal and WPA2-Personal modes, a malicious user can eavesdrop and capture the four-way handshake between a client and an AP. WPA3-Personal avoids such attacks by strengthening the key exchange between clients and APs through a method knows as SAE (Simultaneous Authentication of Equals).

6. Which configuration is supported as the authentication server for implementation of 802.1X on Cisco devices?

- TACACS+ security system with EAP extensions
- **RADIUS security system with EAP extensions**

- RADIUS security system with 3DES extensions
- TACACS+ security system

Explanation: The RADIUS security system with EAP extensions is the only supported authentication server to be used in 802.1X port-based authentication.

7. A network administrator of a small advertising company is configuring WLAN security on a Cisco WLC. The administrator decides to use the WPA2 PSK authentication method. On which OSI layer does WPA2 PSK provide security?

- Layer 1
- **Layer 2**
- Layer 3
- Layer 7

Explanation: Protocols such as WPA2 (PSK and Enterprise) and 802.1x are used to provide Layer 2 WLAN security by requiring successful authentication before access to the WLAN is allowed.

8. Which WLAN security measure requires a special backend authentication server?

- **EAP**
- WPA
- WEP
- pre-shared key

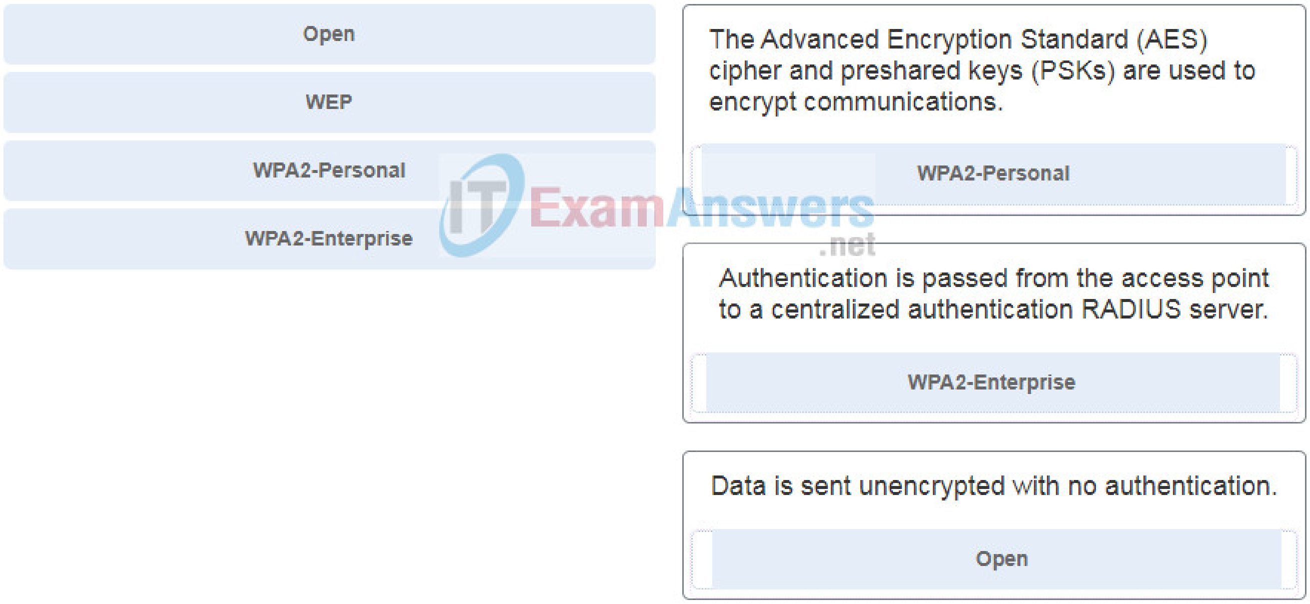
Explanation: In an WLAN (802.1x) environment with EAP, the actual client authentication is done using a back-end server like Radius even though the client is able to authenticate with the AP.

9. What advantage does WPA2 have over WPA?

- WPA2 uses a 32-bit WEP key for encryption.
- WPA2 allows the caching of key information.
- WPA2 uses static key management.
- **WPA2 uses AES instead of TKIP.**

Explanation: WPA2 uses the encryption algorithm AES (Advanced Encryption Standard) which is a stronger algorithm than WPA is, which uses TKIP (Temporal Key Integrity Protocol.) WPA was created to replace WEP (Wired Equivalent Privacy) which was easily compromised. However, the WPA TKIP had to take into account the older devices still using WEP on the network and as a result still had some of the WEP vulnerabilities. This was overcome with the creation of WPA2.

10. Match the wireless security settings to the description. (Not all options are used.)



Open

WEP

WPA2-Personal

WPA2-Enterprise

The Advanced Encryption Standard (AES) cipher and preshared keys (PSKs) are used to encrypt communications.

WPA2-Personal

Authentication is passed from the access point to a centralized authentication RADIUS server.

WPA2-Enterprise

Data is sent unencrypted with no authentication.

Open

- **WPA2-Personal** – The Advanced Encryption Standard (AES) cipher and preshared keys (PSKs) are used to encrypt communications.
- **WPA2-Enterprise** – Authentication is passed from the access point to a centralized authentication RADIUS server.
- **Open** – Data is sent unencrypted with no authentication.

11. A network administrator of a small advertising company is configuring WLAN security by using the WPA2 PSK method. Which credential do office users need in order to connect their laptops to the WLAN?

- the company username and password through Active Directory service
- a user passphrase
- **a key that matches the key on the AP**
- a username and password configured on the AP

Explanation: When a WLAN is configured with WPA2 PSK, wireless users must know the pre-shared key to associate and authenticate with the AP.

12. A network administrator is configuring a WLAN with WPA2 Enterprise on a Cisco 3500 series WLC. Client authentications will be handled by a RADIUS server. Which tab should the administrator use to add the RADIUS server information?

- **SECURITY**
- WLANs
- WIRELESS

- MANAGEMENT

Explanation: To configure the WLC with the RADIUS server information, click the SECURITY tab > RADIUS > Authentication . Click New… to add the RADIUS server information.

13. Which situation is an example of EAP deployment?

- when both the AP and client are configured with the same key or secret word for authentication by the AP
- when a wireless client sends its MAC address to the AP for authentication after being validated by the internal database of the AP
- when unauthenticated clients associate with the AP
- **when a client communicates with a RADIUS server for authenticated access to the network through the AP**

Explanation: In a 802.1x WLAN environment, WPA2 with EAP (Extensible Authentication Protocol) allows for a back-end authentication server like Radius. In this environment, even though the supplicant is authenticated by the AP, the actual authentication process is carried out by the back-end Radius server through the WLAN controller.

14. Which three statements concerning wireless network security are accurate? (Choose three.)

- **A wireless client first associates with an AP and then authenticates for network access.**
- WPA2-Personal prevents attackers from being able to use a key to unencrypt data that was already transmitted over the air.
- Every device using the WLAN must be configured with an identical pre-shared key, unless PSK with ISE is used.
- WPA versions use a three-way handshake procedure to exchange a pre-shared key between a client and an AP.
- **Open authentication uses no client or AP verification.**
- **WPA1, WPA2, and WPA3 support both PSK or 802.1x client authentication modes.**

Explanation: A wireless client first authenticates with an AP and then associates for network access. WPA versions use a four-way handshake procedure to exchange a pre-shared key between a client and an AP. WPA3-Personal prevents attackers from being able to use a key to unencrypt data that was already transmitted over the air.

15. A network administrator is configuring security for new WLANs on a Cisco WLC. Which client authentication mode should the administrator use for a large scale deployment?

- WPA2
- **802.1x**
- 802.11
- AES

Explanation: To secure wireless connections on a WLAN, you can leverage one of the three WPA versions (WPA1, WPA2, or WPA3). All three WPA versions support two client authentication modes:
Pre-Shared Key (PSK) or personal mode for smaller scale deployments
802.1x or enterprise mode for larger scale deployments

16. A network administrator is adding a new WLAN with Open Authentication on a Cisco 3500 series WLC. Which tab should the administrator use to create it?

- **General**
- QoS
- Security
- Advanced

Explanation: To create a WLAN with Open Authentication, first create a new WLAN and map it to the correct VLAN. The General tab should be accessed, the SSID string should be entered, the appropriate controller interface applied, and the status changed to Enabled.

17. A recently hired network engineer is new to the Cisco lightweight APs that the company uses. Which tool should the engineer use for managing and monitoring the wireless network?

- debug output from the lightweight AP prompt
- Layer 2 switch configuration for the switches to which the APs connect
- **WLC GUI**
- Wireshark

Explanation: The WLC GUI is used to monitor and troubleshoot wireless issues. The default screen shows the network summary information that includes connected APs and client information.

18. A network technician has received complaints from users in a particular area. Upon investigation, the technician notices a poor air quality value for the AP in that area. Which WLC GUI tab should the technician use next to determine if there are any neighbor or rogue APs interfering with the one AP?

- EVENT LOG
- TOOLS

- **RF TROUBLESHOOT**
- CLIENTS

Explanation: If a technician selects a particular AP within the WLC GUI, four tabs appear across the top: CLIENTS , RF TROUBLESHOOT , CLEAN AIR , and TOOLS . If the performance summary for a particular AP shows a poor air quality value, the RF TROUBLESHOOT tab can be used to see neighbor and rogue APs as well as the specific AP channels that could cause issues. If the AP supports both 2.4 and 5 GHz frequencies, information can be shown for each of them.

19. Users are complaining about the wireless connectivity in a particular area for a company that uses lightweight APs and wireless LAN controllers. The technician that handles the wireless networks notices that the particular AP has a poor air quality value. The technician uses the CLEAN AIR tab to further investigate and notices that there is an active interferer listed that has a duty cycle of 100%. What should the technician do next?

- Reboot the AP.
- **Track down the offending device that is using the particular frequency causing the interference.**
- Use the EVENT LOG tab to monitor clients as they attempt to join the wireless network.
- Use a different VLAN for that particular AP.

Explanation: When an AP is an issue, one of the best places to start is the WLC GUI. A particular AP can be selected, and the performance summary shows an overall view of the resources being used, clients, and the status of a particular AP. On the CLEAN AIR tab, the duty cycle shows the percentage of time the offending device is transmitting. A duty cycle value of 100% means the offending device can affect the channel all the time. The technician should track down the offending device or select a different RF channel for the AP.

20. A company uses lightweight APs. Which criterion must be in place before an AP can successfully accept clients for a particular WLAN?

- The AP must be physically connected to the WLC.
- The AP must have wireless connectivity with a distribution layer switch.
- **The AP must have connectivity to an access layer switch.**
- The AP must have wireless connectivity with an AAA server.

Explanation: In order to be shown in the list of active APs in the wireless LAN controller (WLC) GUI, an AP must be connected to an access layer switch and have connectivity with the WLC.

21. In addition to signal-to-noise ratio, what is used by a Cisco wireless LAN controller to determine which AP will respond to a client request to associate?

- security protocol
- LAP
- client MAC
- WEP version
- **RSSI**

Explanation: RSSI stands for Received Signal Strength Indicator. It is an estimated measure of power level that a RF client device is receiving from an access point or router. The greater the RSSI value, the stronger the signal.

22. What are two common issues that could cause a specific user to have problems when trying to connect to the wireless network within a company that uses lightweight APs? (Choose two.)

- interference from cellular carriers
- AP to WLC connectivity
- **distance from the AP**
- **authentication**
- interference from FM radio stations

Explanation: When a single client is having wireless issues in the corporate environment, check the distance from the client to the AP, client authentication, and that the client has IP addressing information.

23. What is the function provided by CAPWAP protocol in a corporate wireless network?

- CAPWAP provides connectivity between an access point using IPv6 addressing and a wireless client using IPv4 addressing.
- CAPWAP provides the encryption of wireless user traffic between an access point and a wireless client.
- **CAPWAP provides the encapsulation and forwarding of wireless user traffic between an access point and a wireless LAN controller.**
- CAPWAP creates a tunnel on Transmission Control Protocol (TCP) ports in order to allow a WLC to configure an autonomous access point.

Explanation: CAPWAP is an IEEE standard protocol that enables a WLC to manage multiple APs and WLANs. CAPWAP is also responsible for the encapsulation and forwarding of WLAN client traffic between an AP and a WLC.

24. Several users from the same area cannot connect to the wireless network. The company uses lightweight APs and WLCs. What is one of the first things that the technician should check?

- client authentication
- authentication server issues
- sources of RF interference
- **the AP**

Explanation: When users from the same area report an issue, check the AP to see that it is working or is misconfigured.

25. A network engineer is working with a user to troubleshoot connectivity of a laptop to a lightweight AP. The user has rebooted the laptop, and the network engineer is checking the connection status of the client from the WLC GUI. The client connection status dot is showing black on the DHCP step, just as it did before the reboot. What can the network engineer learn from this output?

- The DHCP server is down.
- The laptop has successfully received IP addressing information or has been statically configured.
- **The WLC controller has not received client IP addressing information from the DHCP server.**
- The switch to which the AP connects needs an IP helper address configured.
- The client is configured for a static IP address.

Explanation: The client connection status on the WLC GUI shows a dot for particular steps used by a client when joining a wireless network. The dot can be black if a step is unsuccessful and green if the step is successful. The DHCP step shows whether the WLC has learned the client IP address from a DHCP server.

26. A network administrator is configuring a WLC to provide WLAN access to users in an office building. When testing the newly created WLAN, the administrator does not see the SSID from a wireless device. What is a possible cause?

- The APs have not been configured for the new WLAN.
- **The new WLAN needs to be enabled.**
- The RADIUS server is not operational.
- The WLAN security setting is incorrect.

Explanation: After a new WLAN is created and configured on a WLC, it should be enabled before it can be accessed by users.

27. A network technician is checking the status of a live AP on the WLC. On the Access Point View screen, the technician notices that the AP is using channel 11 and the channel utilization is 35%. However, the technician notices that there is no wireless client associated with the AP. What is a possible explanation for the channel utilization?

- The CAPWAP tunnel between the AP and the WLC is down.
- **Nearby APs and clients are also using channel 11.**
- The AP is operating in FlexConnect mode.
- The radio has malfunctioned and is preventing clients from association to the AP.

Explanation: The channel utilization indicates how much of the available airtime is being consumed. If the wireless network is not well deployed, other APs and clients may use the same channel 11 somewhere nearby. If those devices are busy transmitting on channel 11 and this AP is within range to receive their signals, the AP will note that the channel is in use.

28. A network technician is checking the status of a live AP on the WLC. On the Access Point View screen, the technician notices that the AP is using channel 11 and the noise level is -30 dBm. Which conclusion can be drawn with the information?

- The radio is malfunctioning.
- Too many wireless clients are connected to the AP.
- **There are some non-802.11 devices around that interfere with the WLAN signal.**
- Wireless clients are transmitting a large amount of media data through the AP.

Explanation: On the Access Point View screen, a technician can check the operating status of connected APs. One important indicator is the noise level on a channel. Noise is usually considered to be the energy received from non-802.11 sources. Ideally, the noise level should be as low as possible, usually around –90 or –100 dBm, so that 802.11 signals can be received intelligibly and accurately.

29. Users report that accesses to the wireless network inside a meeting room are not successful even after repeated attempts. A network technician verifies that the meeting room space is served by a lightweight AP and the radio is working. What is a likely cause of the problem?

- The AP is operating in FlexConnect mode.
- **The AP has lost connectivity to the WLC.**
- The radio signal is too weak.
- Too many users are trying to connect to the AP.
- Successfully operating a lightweight AP and providing a working BSS require the following:

- The AP must have connectivity to the access layer switch.
- The AP must have connectivity to the WLC, unless it is operating in FlexConnect mode.

Explanation: The facts that no wireless clients can associate with the LAP and that the radio is working suggest that the AP has lost the connection to the WLC.

30. A network administrator opens the Client View screen on the WLC to review the performance data of a wireless client. The administrator notices that the client has a connection score value of 78%. What can the administrator conclude from this information?

- The client has a received signal strength of 78% at the AP.
- The client is using its wireless connection only 78% of the time.
- **The client is currently using a data rate that is 78% of its maximum capability.**
- The client is currently in the bottom 78% of all wireless clients in data usage.

Explanation: The connection score shown in the Client View window is determined by dividing the current data rate of the client by the lower maximum supported date rate. It is a measure of how much of its maximum capability it is using. If the client had a maximum rate of 100 Mbps, then a connection score of 78% would mean the client is currently using 78 Mbps.

31. A network administrator receives a complaint from a laptop user of slow web accesses through the wireless network. The administrator reviews the information in the Client View screen of the WLC and finds that the connection speed of the client is 30 Mbps and it has a connection score of 21%. What is likely the problem?

- Other APs on the network are over utilizing the channel.
- The AP has a defective radio.
- There are too many wireless users on the network.
- **The client is too far from the AP.**

Explanation: The connection score shown in the Client View window is determined by dividing the current data rate of the client by the lower maximum supported date rate of either the client or the AP. A connection score of 21% results from the client current data rate of 30 Mbps divided by the maximum data rate which would be 144 Mbps (30 / 144 = .21). This indicates that the client is too far away from the associated AP.

32. A network administrator of a college is configuring WLAN security with WPA2 Enterprise authentication. Which server is required when deploying this type of authentication?

- AAA
- DHCP
- **RADIUS**
- SNMP

Explanation: WAP2 Enterprise provides stronger secure user authentication than WPA2 PSK does. Instead of using a pre-shared key for all users to access a WLAN, WPA2 Enterprise requires that users enter their own username and password credentials to be authenticated before they can access the WLAN. The RADIUS server is required for deploying WPA2 Enterprise authentication.

33. Which two hybrid modes can cause compatibility issues when configured on a WLAN controller? (Choose two.)

- **WPA with AES**
- WPA3 with CCMK
- WPA2 with CCMK
- WPA2 with AES
- **WPA2 with TKIP**

Explanation: The WLAN will only be as secure as the weakest security suite you configure on it. Ideally, you should use WPA2 or WPA3 with AES/CCMP and try to avoid any other hybrid mode. Hybrid modes such as WPA with AES and WPA2 with TKIP can cause compatibility issues.