Chapter 20: Quiz – Authenticating Wireless Clients (Answers) CCNPv8 ENCOR

itexamanswers.net/chapter-20-quiz-authenticating-wireless-clients-answers-ccnpv8-encor.html

January 11, 2021

1. What protocol is used to encapsulate the EAP data between the authenticator and authentication server performing 802.1X authentication?

- **RADIUS**
- TACACS+
- SSH
- MD5

Explanation: Encapsulation of EAP data between the authenticator and the authentication server is performed using RADIUS.

2. Why is WPA2 better than WPA?

- reduced processing time
- supports TKIP
- **mandatory use of AES algorithms**
- reduced keyspace

Explanation: A good way to remember wireless security standards is to consider how they evolved from WEP to WPA, then to WPA2. Each evolution increased security measures.

3. What device is considered a supplicant during the 802.1X authentication process?

- **the client that is requesting authentication**
- the switch that is controlling network access
- the authentication server that is performing
- client authentication
- the router that is serving as the default gateway

Explanation: The devices involved in the 802.1X authentication process are as follows:

- The supplicant, which is the client that is requesting network access
- The authenticator, which is the switch that the client is connecting to and that is actually controlling physical network access
- The authentication server, which performs the actual authentication

4. At a local college, students are allowed to connect to the wireless network without using a password. Which mode is the access point using?

- network
- **open**
- passive
- shared-key

Explanation: Network mode is not an authentication mode, it refers to WLAN standards for 802.11a/b/g/n/ac/ad and the ability for access points to operate in mixed mode to support different standards, but it is not an authentication mode. Open authentication is a null authentication mode because wireless connectivity is granted to any wireless device. This authentication is used where security is not a concern. Passive mode is not an authentication mode, it refers to the open advertisement of the SSID, standards, and security settings by an access point. Shared-key authentication uses a pre-shared key between the client and the access point.

5. Which combination of WLAN authentication and encryption is recommended as a best practice for home users?

- WEP and TKIP
- **WPA2 and AES**
- EAP and AES
- WPA and PSK
- WEP and RC4

Explanation: WPA2 is the Wi-Fi alliance version of 802.11i, the industry standard for authentication. Neither WEP nor WPA possess the level of authentication provided by WPA2. AES aligns with WPA2 as an encryption standard, and is stronger than TKIP or RC4. PSK refers to pre-shared passwords, an authentication method that can be used by either WPA or WPA2. EAP is intended for use with enterprise networks which use a RADIUS server.

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

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

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.

7. When using 802.1X authentication, what device controls physical access to the network, based on the authentication status of the client?

- **the switch that the client is connected to**
- the authentication server
- the supplicant
- the router that is serving as the default gateway

Explanation: The devices involved in the 802.1X authentication process are as follows:

- The supplicant, which is the client that is requesting network access
- The authenticator, which is the switch that the client is connecting and that is actually controlling physical network access
- The authentication server, which performs the actual authentication

8. What are two protocols developed by the Wi-Fi Alliance to secure wireless networks? (Choose two.)

- **WPA**
- 802.1x
- **WPA2**
- LoRaWAN
- IPsec

Explanation: Wireless communications are inherently insecuer and require encryption to protect the data being transmitted. The Wi-Fi Alliance developed WPA and WPA2 as protocols to secure wireless networks. WPA is the older of the two protocols and considered vulnerable to hacking attacks, and therefore WPA2 is recommended.

9. A network administrator of a college is configuring the WLAN user authentication process. Wireless users are required to enter username and password credentials that will be verified by a server. Which server would provide such service?

- AAA
- NAT
- SNMP
- **RADIUS**

Explanation: Remote Authentication Dial-In User Service (RADIUS) is a protocol and server software that provides user-based authentication for an organization. When a WLAN is configured to use a RADIUS server, users will enter username and password credentials that are verified by the RADIUS server before allowing to the WLAN.

10. Under which circumstance is it safe to connect to an open wireless network?

- The connection utilizes the 802.11n standard.
- The device has been updated with the latest virus protection software.
- **The connection is followed by a VPN connection to a trusted network.**
- The user does not plan on accessing the corporate network when attached to the open wireless network.

Explanation: It is never safe to connect to an open (unsecured) wireless network (especially in a public area) unless the network is being used to create a VPN connection to a remote network.

11. In a WLAN, which authentication method provides mutual two-way authentication between the clients and the AP?

- **EAP**
- Open
- PSK
- WEP

Explanation: The Extensible Authentication Protocol (EAP) for wireless networks supports multiple authentication mechanisms. The authentication methods must match between the supplicant and the authentication server.

12. Which type of authentication can prompt a user for credentials, present an acceptable use policy or display information about the enterprise before granting access to the network?

- Local EAP
- **WebAuth**
- Open Authentication
- WPA2
- EAP with Radius server support

Explanation: WebAuth requires the user to use a web browser and read information or accept policies before being granted access to the network.