8.3.4 Wireless Authentication and Access Methods Facts

Wireless networks encrypt communications using a security protocol, typically WPA2 or WPA3. However, to securely authenticate users and distribute authentication keys, other methods need to be used.

This lesson covers the following topics:

- Access methods
- Authentication protocols

Access Methods

Choose an access method for a wireless network based on the use of the network. The following table describes access methods:

Access Method	Description
Pre-shared key (PSK)	A pre-shared key is a passphrase that is used to access the wireless network. This is probably the most commonly used access method.
Wi-Fi Protected Setup (WPS)	Wi-Fi Protected Setup works only on a network that uses a PSK and WPA2. WPS allows a device to securely connect to a wireless network without typing in the PSK. To do this, you: - Push a button on the access point that causes the access point to search for devices in range. - Push the WPS button on the device to automatically join it to the access point. If there is no button, enter the eight-digit pin that is unique to the access point. Some devices and access points can also use Near Field Communication (NFC) during the WPS process to connect to each other.
Open Network	An open network has no authentication at all and allows anyone to connect to the network. This access method should be used only in public places that want to offer free wireless access.
Captive Portal	Many open networks implement a captive portal. Captive portals force a user to view and interact with them before accessing a network. A hotel network is a good example captive portal use. When using a captive portal: - The user connects to the wireless network but is redirected to a captive portal page before internet access is granted. - The user might be prompted to agree to the terms and conditions of using the network or even asked to pay a fee before being granted access.

Authentication Protocols

Enterprise level networks need a higher level of security. Many enterprise networks use the 802.1x protocol to authenticate users to the wireless network. 802.1x is a standard for local area networks created by The Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA). This standard is often labeled IEEE 802.1x.

Once a user is authenticated to a wired network, the port the user is connected to is activated. If the user activation fails, the port remains off. The 802.1x protocol can be implemented in a wireless network by enabling a virtual port when the user is authenticated. There are three components in a 802.1x setup:

- The *supplicant* is the wireless client.
- The *authentication server* contains a centralized database for user authentication.
- The *authenticator* is a device responsible for handling the communications between the supplicant and authentication server.

802.1x implementations on wireless networks often use Remote Authentication Dial-In Service (RADIUS). RADIUS was developed in 1991. It was originally used to authenticate users to the remote network over a dial-up network. RADIUS is known as a triple-A protocol. This means it provides authentication, authorization, and accounting.

When using 802.1x authentication for wireless networks with RADIUS, be aware that:

- A RADIUS server is required to centralize user account and authentication information. A centralized database for user authentication is required to allow wireless clients to roam between cells and authenticate using the same account information.
- PKI is required for issuing certificates. At a minimum, the RADIUS server must have a server certificate. To support mutual authentication, each client must also have a certificate.
- The wireless access point is a RADIUS client.
- The wireless access point forwards the wireless device's credentials to the RADIUS server for authentication.
- A RADIUS federation is multiple RADIUS servers that communicate with each other after establishing a trust relationship. These servers may be on different networks and could span multiple organizations.

To ensure the authentication information being sent is secure, the Extensible Authentication Protocol (EAP) is used. EAP is a framework in which other protocols work. The following table explains EAP and the protocols:

Protocol	Description
Extensible Authentication Protocol (EAP)	EAP is a set of interface standards that allows various authentication methods to be used: - EAP supports multiple authentication methods (smart cards, biometrics, and digital certificates). - Using EAP, the client and server negotiate the characteristics of authentication.
Protected Extensible Authentication Protocol (PEAP)	PEAP provides authentication in an SSL/TLS tunnel with a single certificate on the server. PEAP: - Creates a secure communication channel for transmitting certificate or login credentials.

	▪ Enables mutual authentication by requiring the server to prove its identity with the client. ▪ Was a collaborative effort between Cisco, Microsoft, and RSA.
EAP Flexible Authentication via Secure Tunneling (EAP-FAST)	EAP-FAST uses a Protected Access Credential (PAC) to authenticate users. EAP-FAST: ▪ Establishes a TLS tunnel in which client authentication credentials are transmitted. ▪ Is susceptible to attackers who intercept the Protected Access Credential (PAC) and use it to compromise user credentials. This vulnerability is mitigated by manual PAC provisioning or by using server certificates. ▪ Was created by Cisco.
EAP Transport Layer Security (EAP-TLS)	EAP-TLS uses Transport Layer Security (TLS) and is considered to be one of the most secure EAP standards available. EAP-TLS: ▪ Is widely supported by almost all manufacturers of wireless LAN hardware and software. ▪ Requires signed client-side and server-side certificate authority (CA) PKI certificates. ▪ Is labor-intensive and expensive to implement.
EAP Tunneled Transport Layer Security (EAP-TTLS)	EAP-TTLS also uses a CA signed certificate. EAP-TTLS: ▪ Is an updated version of EAP-TLS. ▪ Requires only one CA signed certificate on the server, simplifying the implementation process.