5.12.3 Wireless Authentication Facts

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.

When using 802.1x authentication for wireless networks:

- 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.
- A 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.

802.1x authentication uses either certificates or user names and passwords for authentication. Each is supported through extensible protocols such as the following:

Protocol	Description
Extensible Authentication Protocol (EAP)	Extensible Authentication Protocol (EAP) is a set of interface standards that allows you to use various authentication methods. - EAP supports multiple authentication methods (for example, smart cards, biometrics, and digital certificates). - WPA and WPA2 can use five different EAP methods to authenticate to a wireless network. - Using EAP, the client and server negotiate the characteristics of authentication. - There are several EAP implementations that you need to be familiar with: - EAP-TLS uses Transport Layer Security (TLS) and is considered one of the most secure EAP standards available. A compromised password is not enough to break into EAP-TLS-enabled systems because the attacker must also have the client's private key. - EAP-MD5 offers minimal security and is susceptible to dictionary attacks and man-in-the-middle attacks. - EAP-FAST is a replacement for LEAP that uses a Protected Access Credential (PAC) to establish a TLS tunnel in which client authentication credentials are transmitted. While more secure than EAP-MD5 and LEAP, EAP-FAST can still be compromised if the attacker can intercept the PAC.
Light-weight Extensible Authentication Protocol (LEAP)	Light-weight Extensible Authentication Protocol (LEAP) is a Cisco-proprietary technology. LEAP: - Requires a Cisco RADIUS server and Cisco software on the client's side. - Requires the minimum of a digital certificate on the server side and passwords and Cisco drivers on the client side. LEAP does not use PKI. - Can be upgraded to have digital certificates on both sides. - Transmits some of the information in cleartext. - Is based on the MS CHAP protocol. LEAP is considered to be the weakest 802.1x protocol. It does not use SSL/TLS to encapsulate authentication data. LEAP is also susceptible to dictionary attacks. LEAP's major weakness is that it uses MS-CHAPv1 in an unencrypted form for authentication. MS-CHAPv1 is vulnerable to offline dictionary attacks against dictionary-based passwords. In a dictionary attack, an attacker would sniff both the challenge and the response during LEAP authentication and then run through all the words in a dictionary in an attempt to obtain the response that matches the challenge. If successful, the attacker has then guessed the password and can pose as the client. The main countermeasure to dictionary attacks is to use a strong password policy.
Protected Extensible Authentication Protocol (PEAP)	Protected Extensible Authentication Protocol (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 Flexible Authentication via Secure Tunneling (EAP-FAST) is a replacement for LEAP that uses a Protected Access Credential (PAC).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.

EAP Transport Layer Security (EAP-TLS)	EAP Transport Layer Security (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 client-side and server-side Certificate Authority (CA) signed certificates. ▪ Is labor-intensive and expensive to implement.
EAP Tunneled Transport Layer Security (EAP-TTLS)	EAP Tunneled Transport Layer Security (EAP-TTLS) also uses a CA signed certificate. ▪ Only one CA signed certificate is required on the server, simplifying the implementation process.