802.1X Enhances Wireless Network Security

1. **Strong User/Device Authentication**:
    - **Problem Addressed**: Earlier protocols like WEP and WPA-PSK relied on shared keys, which were easily compromised (e.g., via brute-force attacks) and didn't verify individual users or devices.
    - **How 802.1X Helps**:
        - Uses the **Extensible Authentication Protocol (EAP)** to authenticate each user or device with unique credentials (e.g., username/password, digital certificates).
        - Supports secure EAP methods like **EAP-TLS** (certificate-based), **PEAP** (password-based with TLS tunnel), or **EAP-TTLS**, ensuring strong identity verification.
        - Authentication is handled by a central **RADIUS server**, preventing unauthorized devices from connecting, even if they know a shared passphrase.
2. **Mutual Authentication to Prevent Rogue APs**:
    - **Problem Addressed**: Wireless networks are vulnerable to rogue Access Points (APs) or man-in-the-middle attacks, where attackers impersonate legitimate APs to steal credentials or data.
    - **How 802.1X Helps**:
        - EAP methods like EAP-TLS require **mutual authentication**, where the client verifies the AP's identity (e.g., via a server certificate) and the AP verifies the client's identity.
        - This ensures clients connect only to legitimate APs, mitigating risks of evil twin or spoofing attacks.
3. **Dynamic Key Management**:
    - **Problem Addressed**: Static keys in WEP and WPA-PSK are vulnerable to cracking over time and don't change per session, increasing the risk of data interception.
    - **How 802.1X Helps**:
        - After successful authentication, 802.1X generates a unique **Pairwise Master Key (PMK)** for each client session, delivered securely via the RADIUS server.
        - The PMK is used in the **4-way handshake** to derive session-specific keys (**Pairwise Transient Key, PTK** for unicast and **Group Temporal Key, GTK** for multicast/broadcast).
        - Dynamic keys ensure that each session uses fresh encryption keys, reducing the impact of a compromised key and enhancing data confidentiality.
4. **Centralized Authentication and Policy Enforcement**:
    - **Problem Addressed**: Managing access for many users/devices in large wireless networks using shared keys is insecure and unscalable, with no way to enforce user-specific policies.
    - **How 802.1X Helps**:
        - Integrates with a RADIUS server to centralize authentication, allowing administrators to manage credentials, revoke access, and apply policies (e.g.,

        VLAN assignment, bandwidth limits, or access restrictions) based on user/device identity.
        - Supports integration with enterprise directories (e.g., Active Directory, LDAP), enabling seamless user management and role-based access control.

5. **Protection Against Brute-Force Attacks**:
    - **Problem Addressed**: WPA-PSK is susceptible to offline brute-force attacks if the 4-way handshake is captured, especially with weak passphrases.
    - **How 802.1X Helps**:
        - In 802.1X (WPA Enterprise), there's no shared passphrase; authentication relies on EAP methods, which are not vulnerable to offline attacks.
        - EAP-TLS uses certificates, which are nearly impossible to brute-force, and password-based methods like PEAP protect credentials within a TLS tunnel, requiring an attacker to compromise the RADIUS server or intercept the TLS session.

Work Flow
Components:

- **Supplicant**: The client device (e.g., laptop, smartphone) seeking access.
- **Authenticator**: The Wi-Fi AP, which controls network access.
- **Authentication Server**: A RADIUS server that verifies credentials.

Process:

1. The client associates with the AP but is blocked from full network access.
2. The client sends EAP credentials to the AP, which forwards them to the RADIUS server.
3. The RADIUS server authenticates the client (e.g., via EAP-TLS or PEAP) and, if successful, sends a PMK to the AP and client.
4. The 4-way handshake uses the PMK to derive PTK and GTK, establishing a secure, encrypted connection.