### Q6) EAPOL 4-Way Handshake

The **4-Way Handshake** is a critical process in Wi-Fi security (WPA/WPA2/WPA3) that establishes secure encryption keys between a client (Supplicant) and an AP (Authenticator). Below is a detailed breakdown of each step and the keys generated.

**1. Purpose of the 4-Way Handshake**

* **Mutual Authentication**: Confirms both the AP and client know the **Pairwise Master Key (PMK)**.
* **Key Derivation**: Generates fresh session keys for encrypting data.
* **Prevents Replay Attacks**: Uses nonces (random numbers) to ensure uniqueness.

**2. Pre-Requisites**

* **PMK (Pairwise Master Key)**: Generated from:
  + **WPA2-Personal**: Derived from the **Pre-Shared Key (PSK)** (Wi-Fi password).
  + **WPA2-Enterprise**: Generated during 802.1X/EAP authentication.
* **ANonce/SNonce**: Random numbers from the AP (Authenticator) and client (Supplicant).

**3. The 4-Way Handshake Steps**

**Step 1: AP → Client (Message 1)**

* **AP sends**:
  + **ANonce** (AP’s random number).
  + No encryption (sent in clear text).
* **Client action**:
  + Uses **ANonce + PMK + SNonce** to compute:
    - **PTK (Pairwise Transient Key)** = PBKDF2(PMK, ANonce + SNonce + MAC addresses)
  + Splits PTK into subkeys:
    - **KCK (Key Confirmation Key)**: Validates Message 2 integrity.
    - **KEK (Key Encryption Key)**: Encrypts GTK (Group Temporal Key) in Message 3.
    - **TK (Temporal Key)**: Encrypts unicast data frames.

**Step 2: Client → AP (Message 2)**

* **Client sends**:
  + **SNonce** (Client’s random number).
  + **MIC (Message Integrity Code)**: Hash of the message using **KCK** to prove knowledge of PMK.
* **AP action**:
  + Computes its own **PTK** using PMK + ANonce + SNonce.
  + Verifies the **MIC** to authenticate the client.

**Step 3: AP → Client (Message 3)**

* **AP sends**:
  + **GTK (Group Temporal Key)**: Encrypted with **KEK** (for multicast/broadcast traffic).
  + **MIC**: Integrity check using KCK.
  + **Install PTK instruction**: Signals the client to start encryption.
* **Client action**:
  + Decrypts **GTK** using KEK.
  + Stores **GTK** for multicast decryption.

**Step 4: Client → AP (Message 4)**

* **Client sends**:
  + **ACK + MIC**: Confirms PTK/GTK installation.
* **AP action**:
  + Enables encryption for the client’s traffic.

**4. Keys Derived from the Handshake**

|  |  |  |
| --- | --- | --- |
| Key | Purpose | Lifetime |
| PMK | Root key derived from PSK or 802.1X. Never transmitted. | Persistent (until password change). |
| PTK | Session key for unicast traffic. Split into KCK, KEK, and TK. | Valid until session ends. |
| KCK | Validates MIC in Messages 2/3/4. | Short-term (handshake only). |
| KEK | Encrypts GTK in Message 3. | Short-term (handshake only). |
| TK | Encrypts unicast data (e.g., AES-CCMP in WPA2). | Session duration. |
| GTK | Encrypts broadcast/multicast traffic (shared across all clients). | Rotated periodically by AP. |

**5. Why Each Step Matters**

1. **Message 1**: Initiates the handshake; provides ANonce for PTK derivation.
2. **Message 2**: Client proves PMK knowledge via MIC; provides SNonce.
3. **Message 3**: Securely delivers GTK; activates encryption.
4. **Message 4**: Final confirmation; secures the link.

**6. Security Implications**

* **PTK Freshness**: Nonces (ANonce/SNonce) ensure keys are unique per session.
* **MIC Protection**: Prevents forgery (e.g., attackers can’t fake Message 2 without PMK).
* **GTK Rotation**: AP changes GTK periodically to prevent eavesdropping on multicast.

**7. Example Workflow (WPA2-Personal)**

1. Client connects to "HomeWiFi" (PSK = "password123").
2. **PMK** = PBKDF2("password123", SSID, 4096 iterations).
3. 4-Way Handshake generates **PTK** and **GTK**.
4. All data is encrypted with **TK**; broadcasts use **GTK**.

|  |  |  |  |
| --- | --- | --- | --- |
| Step | Sender → Receiver | Key Action | Security Goal |
| 1 | AP → Client | Sends ANonce → PTK derivation. | Initiate secure session. |
| 2 | Client → AP | Sends SNonce + MIC (KCK). | Prove PMK knowledge. |
| 3 | AP → Client | Sends encrypted GTK (KEK) + MIC. | Secure multicast traffic. |
| 4 | Client → AP | ACK + MIC. | Confirm encryption activation. |

* The 4-Way Handshake ensures **mutual authentication** and **dynamic key generation**.
* **PTK** protects unicast traffic; **GTK** protects multicast.
* Without this handshake, Wi-Fi encryption (WPA2/WPA3) would be vulnerable to replay attacks.