EAPOL 4-way Handshake

The 4-way handshake is a mutual authentication and key derivation process that occurs after the client has completed the **scanning, authentication, and association** phases with the AP. Its primary goals are:

1. **Mutual Authentication**: Verify that both the station and AP possess the correct **Pairwise Master Key (PMK)**, ensuring they are authorized to communicate.
2. **Key Derivation**: Generate session-specific encryption keys to secure unicast and multicast/broadcast traffic.
3. **Key Installation**: Distribute and install these keys to enable encrypted data communication.

The handshake uses **EAPOL-Key frames** encapsulated in 802.11 Data frames, exchanged over the wireless link. It derives two main types of keys:

- **Pairwise Transient Key (PTK)**: For unicast (point-to-point) traffic between the station and AP.
- **Group Temporal Key (GTK)**: For multicast and broadcast traffic within the BSS.

The PMK, which serves as the foundation for key derivation, is typically derived from:

- A **Pre-Shared Key (PSK)** in WPA2-Personal or WPA3-Personal (e.g., the Wi-Fi password).
- An **802.1X/EAP exchange** in WPA2-Enterprise or WPA3-Enterprise, involving an authentication server (e.g., RADIUS).

Detailed Steps of the EAPOL 4-way Handshake

The 4-way handshake consists of four message exchanges (Messages 1–4) between the AP (authenticator) and the station (supplicant). Each step has a specific purpose in authenticating the parties, deriving keys, and ensuring secure key installation.

Step 1: Message 1 (AP to Station)

- **Description**: The AP initiates the handshake by sending the first **EAPOL-Key frame** to the station.
- **Content**:
    - **ANonce**: A random number (nonce) generated by the AP.
    - **Key Information**: Indicates the handshake's purpose (e.g., pairwise key derivation).
    - **Key MIC (Message Integrity Code)**: Set to zero in Message 1, as no MIC is computed yet.

- **Purpose**:
    - Provide the station with the AP's nonce (ANonce), which is used in key derivation.
    - Signal the start of the handshake, prompting the station to generate its own nonce and compute the PTK.
- **Station's Action**:
    - Receives the ANonce.
    - Generates its own nonce (**SNonce**).
    - Computes the **Pairwise Transient Key (PTK)** using:
        - **PMK** (already known from PSK or 802.1X).
        - **ANonce** (from the AP).
        - **SNonce** (generated by the station).
        - **MAC addresses** of the AP and station.
        - **SSID** of the network.
    - The PTK is derived using a **Pseudo-Random Function (PRF)**, typically HMAC-SHA1 in WPA2 or HMAC-SHA256 in WPA3
    - The PTK is split into subkeys (described later).

Outcome: The station has computed the PTK and is ready to respond.

Step 2: Message 2 (Station to AP)

- **Description**: The station sends an **EAPOL-Key frame** back to the AP, confirming receipt of Message 1 and providing its nonce.
- **Content**:
    - **SNonce**: The station's random number (nonce).
    - **Key Information**: Confirms pairwise key derivation.
    - **Key MIC**: A Message Integrity Code computed over the EAPOL-Key frame using the **KCK (Key Confirmation Key)**, a subkey derived from the PTK.
    - **RSN Information Element**: Details the station's security capabilities (e.g., WPA2, WPA3, cipher suites).
- **Purpose**:
    - Deliver the SNonce to the AP, enabling it to compute the PTK.
    - Prove the station's possession of the PMK by including a valid MIC, computed using the KCK.
    - Confirm the station's security parameters for compatibility.
- **AP's Action**:
    - Receives the SNonce and RSN IE.
    - Computes the PTK using the same inputs as the station (PMK, ANonce, SNonce, MAC addresses, SSID).
    - Verifies the MIC using the KCK derived from the PTK.
    - If the MIC is valid, the AP confirms the station's authenticity (i.e., it knows the PMK).

Outcome: The AP has computed the PTK and verified the station's authenticity. Both parties now share the same PTK.

Step 3: Message 3 (AP to Station)

- **Description**: The AP sends a third **EAPOL-Key frame** to the station, delivering the **Group Temporal Key (GTK)** and confirming the handshake's progress.
- **Content**:
    - **ANonce**: Repeated for consistency (optional in some implementations).
    - **Key Information**: Indicates GTK installation and pairwise key confirmation.
    - **Key MIC**: A MIC computed over the frame using the KCK.
    - **GTK**: The Group Temporal Key, encrypted with the **KEK (Key Encryption Key)**, a subkey of the PTK, to protect it during transmission.
    - **RSN Information Element**: Confirms the AP's security parameters (e.g., group cipher suite).
- **Purpose**:
    - Deliver the GTK to the station for encrypting multicast and broadcast traffic.
    - Confirm the AP's possession of the PMK by including a valid MIC.
    - Instruct the station to install the PTK and GTK for data encryption.
- **Station's Action**:
    - Verifies the MIC using the KCK to ensure the AP's authenticity.
    - Decrypts the GTK using the KEK.
    - Installs the PTK and GTK in its wireless interface for encrypting/decrypting data frames.
    - Prepares to acknowledge the handshake's completion.

Outcome: The station has received and installed the GTK, and both parties have confirmed mutual possession of the PMK.

Step 4: Message 4 (Station to AP)

- **Description**: The station sends the final **EAPOL-Key frame** to the AP, acknowledging successful receipt of the GTK and PTK installation.
- **Content**:
    - **Key Information**: Confirms key installation.
    - **Key MIC**: A MIC computed over the frame using the KCK.
- **Purpose**:
    - Confirm to the AP that the station has installed the PTK and GTK and is ready for secure communication.
    - Provide final assurance of the station's authenticity via the MIC.
- **AP's Action**:

    - Verifies the MIC to ensure the station's integrity.
    - Installs the PTK and GTK in its wireless interface (if not already done).
    - Enables encrypted data communication with the station.

Outcome: The handshake is complete, and both the station and AP have installed the necessary keys for secure communication. Data frames can now be encrypted and transmitted.

Keys Derived from the 4-way Handshake

The 4-way handshake derives two primary keys: the **Pairwise Transient Key (PTK)** and the **Group Temporal Key (GTK)**. These keys are used to secure data communication and are derived or distributed as follows:

1. Pairwise Transient Key (PTK)

- **Derivation**:
    - Computed by both the station and AP in Steps 1 and 2 using the PMK, ANonce, SNonce, MAC addresses, and SSID.
    - Generated using a Pseudo-Random Function (PRF), typically HMAC-SHA1 (WPA2) or HMAC-SHA256 (WPA3).
    - Size: 384 bits (WPA2 with CCMP) or 512 bits (WPA3), split into subkeys.
- **Subkeys**:
    - **Key Confirmation Key (KCK)** (128 bits):
        - **Purpose**: Used to compute the MIC in EAPOL-Key frames (Messages 2–4) to verify message integrity and authenticate the parties.
        - **Role**: Ensures the station and AP share the same PMK and protects against tampering during the handshake.
    - **Key Encryption Key (KEK)** (128 bits):
        - **Purpose**: Encrypts the GTK during transmission in Message 3 to ensure confidentiality.
        - **Role**: Protects the GTK from eavesdropping, ensuring only the intended station can decrypt it.
    - **Temporal Key (TK)** (128 bits for CCMP, 256 bits for TKIP):
        - **Purpose**: Encrypts and decrypts unicast data frames between the station and AP.
        - **Role**: Secures point-to-point communication, ensuring confidentiality and integrity of user data.
- **Purpose**:
    - The PTK provides session-specific keys for unicast traffic, ensuring each station-AP pair has unique encryption keys.
    - Enhances security by deriving fresh keys for each session, reducing the risk of key compromise.

- **Lifetime**: The PTK is valid for the duration of the association or until a new handshake is triggered (e.g., due to rekeying or reassociation).

2. Group Temporal Key (GTK)

- **Derivation**:
    - Generated by the AP (not derived from the PTK) and distributed to the station in Message 3.
    - Based on a **Group Master Key (GMK)** and a group nonce (GNonce), typically using a PRF.
    - Size: 128 bits (CCMP) or 256 bits (TKIP).
- **Purpose**:
    - Encrypts and decrypts multicast and broadcast frames within the BSS, ensuring all associated stations can receive group traffic (e.g., ARP requests, multicast video).
    - Ensures group traffic is secure from unauthorized devices.
- **Lifetime**:
    - The GTK is periodically rekeyed by the AP (e.g., every few hours or after a station disassociates) to maintain security.
    - The AP distributes a new GTK to all stations using a **Group Key Handshake** (a 2-message EAPOL exchange).