**6. Explain each steps involved in EAPOL 4-way handshake and the purpose of each keys derived from the process**

The **EAPOL 4-way handshake** is a crucial process in WPA (Wi-Fi Protected Access) and WPA2 for establishing secure communication between a wireless client (station) and an access point (AP). It ensures that both devices can derive the same keys for encryption, providing a secure connection.

**Steps in the EAPOL 4-Way Handshake:**

1. **Message 1: AP → Client (Anonymized Key Frame)**
   * The AP generates a nonce (ANonce) and sends it to the client in the first message. This nonce ensures that each handshake is unique and prevents replay attacks. It signals that the AP is ready to start the handshake process.
2. **Message 2: Client → AP (Auth Key Frame)**
   * The client generates its own nonce (SNonce) and sends it to the AP. The client also indicates that it’s ready to proceed with the handshake.
3. **Message 3: AP → Client (Group Key Frame)**
   * The AP uses both the ANonce and SNonce, along with the PMK (Pairwise Master Key) and MAC addresses of both devices, to compute the **pairwise transient key** (PTK). The AP also sends the **group temporal key** (GTK) to the client for encrypting multicast and broadcast traffic.
4. **Message 4: Client → AP (Confirmation Key Frame)**
   * The client sends a confirmation back to the AP to finalize the handshake. This confirms that both devices have successfully derived the same keys and that secure communication can begin.

**KEYS:**

**Pairwise Master Key (PMK)**:

* The PMK is the foundation of the key exchange, typically derived from a pre-shared key (PSK) or from an EAP process. It’s the starting point for generating other keys in the handshake.

**Pairwise Transient Key (PTK)**:

* The PTK is derived from the PMK, ANonce, SNonce, and the MAC addresses of the client and AP. It’s used for encrypting unicast (client-to-AP or AP-to-client) traffic, ensuring secure communication between the two devices.

**Group Temporal Key (GTK)**:

* The GTK is used to encrypt multicast and broadcast traffic sent by the AP to all connected clients. It’s shared with all clients but only needs to be sent once during the handshake.