### Q7) How the 4-Way Handshake Ensures Mutual Authentication

The **4-way handshake** is a fundamental process in **WPA2** and **WPA3** that:

1. **Authenticates** both the client and access point (AP).
2. **Derives fresh encryption keys** (PTK, GTK) for secure communication.
3. **Prevents replay attacks** by using dynamic nonces.

**1. Prerequisites**

* Both the **client** and **AP** already possess the **Pairwise Master Key (PMK)** (derived from the Wi-Fi password or 802.1X authentication).
* The PMK is **never transmitted**—it’s used to generate session-specific keys.

**2. The 4-Way Handshake Process**

**Message 1 (AP → Client)**

* AP sends an **ANonce** (AP-generated random number).
* **Purpose:**
* Allows the client to compute the **Pairwise Transient Key (PTK)** using:
* The AP hasn’t proven its identity yet—this is just the first step.

**Message 2 (Client → AP)**

* Client generates its own **SNonce** (client random number) and computes the **PTK**.
* Sends **SNonce + MIC (Message Integrity Code)** to the AP.
* The **MIC** is a cryptographic hash (using the PTK) to prove the client knows the PMK.
* **Authentication Achieved:**
* The AP verifies the MIC. If valid, the **client is authenticated** (only someone with the PMK could generate the correct MIC).

**Message 3 (AP → Client)**

* AP sends the **Group Temporal Key (GTK)** for multicast traffic, encrypted with the PTK.
* Includes a **MIC** (to prove AP knows the PMK).
* **Authentication Achieved:**
* The client verifies the AP’s MIC. If valid, the **AP is authenticated** (only the real AP could derive the PTK and generate the correct MIC).

**Message 4 (Client → AP)**

* Client sends a confirmation to the AP, signaling that keys are installed.
* **Finalizes Mutual Authentication:**
* Both parties have now proven they possess the PMK.
* Session keys (PTK/GTK) are activated for encrypted communication.