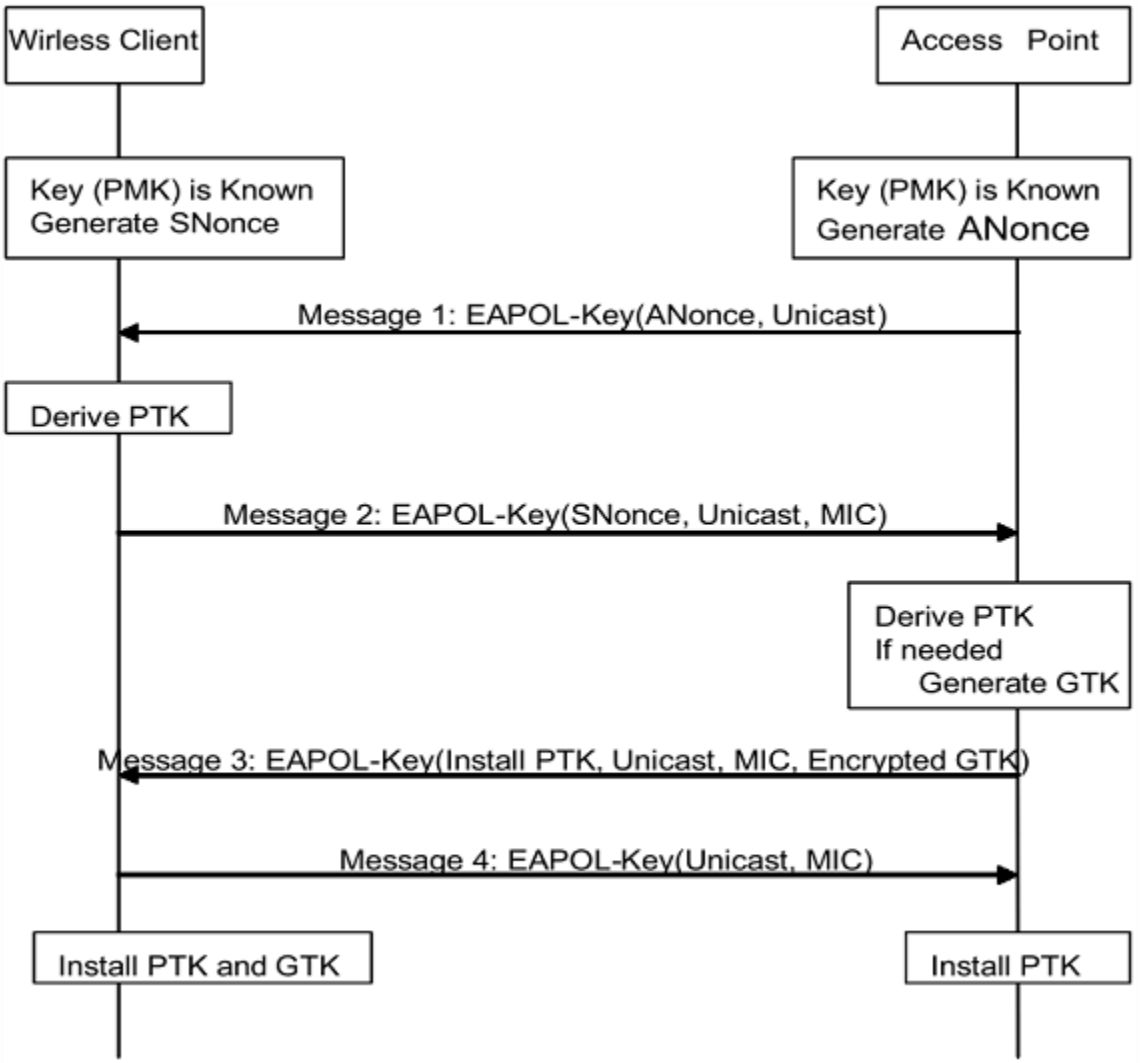
WPA2 Personal:

WPA2-Personal uses a shared password (Pre-Shared Key) for authentication between the client and access point, suitable for home or small networks.



The 4-way handshake:

Both the client and the AP derive the **Pairwise Master Key (PMK)** independently using the **Pre-Shared Key (PSK)** (-> network password) and SSID (-> network name). During the 4-Way Handshake, the AP generates an **Authenticator Number used once (ANonce)**, and the client generates an **Supplicant Number used once (SNonce)**.

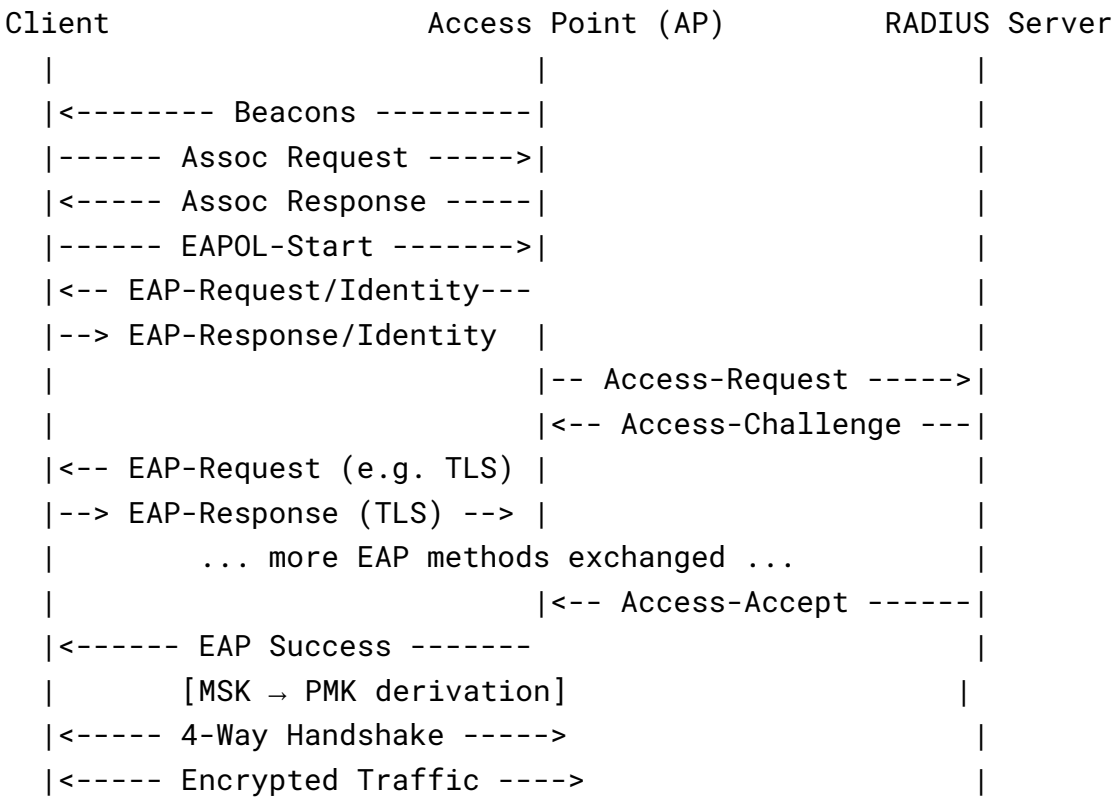
1. In **Message 1,** the AP sends the ANonce to the client.
2. The client receives the ANonce. With the help of PMK, ANonce, SNonce, and the MAC Addresses of both, the client derives the

Pairwise Transient Key (PTK).
The client sends the SNonce, and a **Message Integrity Code (MIC)**, which protects the message, and lets the AP know that the client is in possession of the **PTK**.

3. The AP now, with the help of the same values (PMK, ANonce, SNonce, MAC addresses), calculates the **PTK** for itself.
   The AP also generates a **Group Temporal Key (GTK)**, which is used to encrypt **broadcast and multicast traffic**.
   The **GTK** is encrypted using the **PTK** and then sent to the client, protected by the **MIC**, in **Message 3**.
4. The client installs the **PTK** and the **GTK**, and finally in **Message 4**, sends a **MIC** to confirm successful installation of the keys, and signals that the client is now ready to begin encrypted communication.

WPA2 Enterprise:

WPA2-Enterprise uses 802.1X and a RADIUS server to authenticate users individually with credentials, ideal for large or corporate networks.



Steps:

1. The usual management frame exchange takes place (Beacon → Probe → Authentication → Association Request/Response).
2. The authentication starts when the client sends an **EAPOL-Start** to the Access Point (AP).
3. The AP sends an **EAP-Request/Identity** to the client, asking for the user's identity.
4. The client replies with an **EAP-Response/Identity**, providing the username.
5. The AP encapsulates this in a **RADIUS Access-Request** and forwards it to the **RADIUS server**.
6. The RADIUS server checks the user credentials and, if more info is needed, sends an **Access-Challenge** (e.g., to begin an EAP-TLS session).
7. Multiple **EAP method exchanges** follow (e.g., TLS handshake or PEAP tunnel with inner authentication).
8. Once authentication is successful, the RADIUS server sends an **Access-Accept**, along with the **MSK**.
9. The AP sends an **EAPOL-Success** to the client, completing the EAP authentication.
10. The AP and client derive the **PMK** from the **MSK** and begin the **4-way handshake** to derive encryption keys (PTK, GTK).

Wireshark:

1. With the help of Beacon frames we can see and understand which Wifi security is being used (WPA personal/enterprise).
   a. Under ‘IEEE 802.11 Wireless Management’ -> ‘Tagged Parameters’ -> ‘Tag: RSN Information’ -> ‘Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK’ -> under this, we have various type numbers which tell us which wifi security is being used.
   b. For example: PSK (2) -> WPA2 Personal
      802.1X -> WPA2 Enterprise
      SAE (8) -> WPA3 Personal
      802.1X -> WPA3 Enterprise

2. With the help of Beacon frames we can even know which 802.11 standard is being used:

Wi-Fi Standard	Max speed	Frequency
Wi-Fi 4 (802.11n)	600 Mbps	2.4 GHz & 5 GHz
Wi-Fi 5 (802.11ac)	6.9 Gbps	Only 5 GHz
Wi-Fi 6 (802.11ax)	9.6 Gbps	2.4 GHz, 5 GHz & 6 GHz (Wi-Fi 6E)
Wi-Fi 7 (802.11be) - Future	46 Gbps (Theoretical)	2.4 GHz, 5 GHz, and 6 GHz

   a. 'IEEE 802.11 Wireless Management' -> 'Tagged Parameters' -> 'Tag: HT Capabilities (**802.11n** D1.10)'
      HT Capabilities → **802.11n**
      VHT Capabilities → **802.11ac**
      HE Capabilities → **802.11ax**
   b. 'Radiotap Header v0, Length 24' -> 'Channel frequency: 5180 [**5 GHz 36**]' -> will tell the frequency which will help us know the standard.
      2.4 GHz → Could be **b/g/n**
      5 GHz → Could be **a/n/ac/ax**
      6 GHz → Likely **802.11ax (Wi-Fi 6E)**
   c. '802.11 radio information' -> 'PHY type: **802.11a** (OFDM) (5)'

Wifi scanning commands in console
Hidden ssid
Why probe response is not mandatory
Why my device keeps listening to beacon frames even after connecting