**7. How does the 4-way handshake ensure mutual authentication between the client and the access point?**

* Both the client and the access point already share the Pairwise Master Key (PMK).
* During the 4-way handshake, they exchange random numbers called nonces (ANonce from AP, SNonce from client).
* They use the PMK + nonces + their MAC addresses to generate a new key called the Pairwise Transient Key (PTK).
* Each side calculates the PTK separately - the PTKs must match if both sides have the correct PMK.
* The access point sends a message encrypted with the new key, and the client must correctly respond to it.
* If both sides verify the messages correctly, it proves they both know the PMK without actually sharing it.
* This ensures **mutual authentication** and sets up a secure encrypted connection.