Name: Aswath S

College: Vellore Institute of Technology, Vellore

Reg.No: 21BEC2188

Wi-Fi Training Program 2025

Module 6

Question 7:

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

Solution:

The **4-way handshake** ensures **mutual authentication** between the **client** (like a laptop or phone) and the **Access Point (AP)** (Wi-Fi router) through **key confirmation** without revealing the secret (PMK) directly.

Here's how it works step-by-step:

1. **AP sends a random number (ANonce) ➔** The Access Point sends a random value (called ANonce) to the client.
2. **Client generates its own random number (SNonce) ➔** The client creates its own random value (called SNonce).
3. **Both sides compute the PTK ➔** Using the PMK, the ANonce, the SNonce, and their MAC addresses, both the client and the AP independently compute the **Pairwise Transient Key (PTK)**.
4. **Client sends SNonce and a Message Integrity Code (MIC) ➔** The client sends the SNonce along with a MIC (Message Integrity Code) to prove it calculated the PTK correctly.
5. **AP verifies the MIC ➔** The AP checks the MIC to confirm that the client knows the correct PMK.
6. **AP sends its own MIC ➔** The AP then sends a MIC back to the client, which the client checks.
7. **Both confirm each other ➔** If both MICs are correct, both the client and AP know each other are legitimate — mutual authentication is complete.