Name: Aswath S

College: Vellore Institute of Technology, Vellore

Reg.No: 21BEC2188

Wi-Fi Training Program 2025

Module 6

Question 8:

What will happen if we put a wrong passphrase during a 4Way handshake?

Solution:

If you enter a **wrong passphrase** during the **4-way handshake**, the authentication will **fail**.

1. **Passphrase is used to derive the PMK**:
   The passphrase you enter is used by both the **client** (your device) and the **Access Point (AP)** to generate the **Pairwise Master Key (PMK)**.
2. **PMK mismatch**:
   If the passphrase is wrong, the **PMK generated** by the client will not match the **PMK** generated by the AP because they both use different passphrases.
3. **4-way handshake failure**:
   As the handshake proceeds, both the AP and client will attempt to **compute the same PTK** (Pairwise Transient Key) using the PMK. Since the PMK is different, the resulting PTKs won't match.
4. **Message Integrity Code (MIC) failure**:
   During the handshake, both the client and the AP send a **MIC** (Message Integrity Code) to confirm the authenticity of the keys. If the PTK is wrong (due to the incorrect PMK), the **MICs won't match**.
5. **Authentication failure**:
   Because the MICs don't match, the **4-way handshake fails**. The client will not be able to **authenticate** with the AP and will not be able to join the network.
6. **No encryption keys established**:
   Since the handshake fails, no **encryption keys** are established, and the communication between the client and AP remains unprotected. The connection attempt is aborted.