Name: Aswath S

College: Vellore Institute of Technology, Vellore

Reg.No: 21BEC2188

Wi-Fi Training Program 2025

Module 6

Question 6:

What is the role of the Pairwise Master Key (PMK) in the 4-way handshake?

Solution:

The Pairwise Master Key (PMK) plays a central role in the 4-way handshake of Wi-Fi security (like in WPA2 and WPA3).
Its role is:

- The PMK is a secret key shared between the client (like your phone or laptop) and the Access Point (Wi-Fi router) before the handshake begins.
- During the 4-way handshake, the PMK is used to derive another key called the Pairwise Transient Key (PTK).
- The PTK is then used to encrypt and protect the actual data communication between the device and the router.
- The handshake ensures that both sides prove they know the PMK without actually sending the PMK over the air — keeping it safe from attackers.
- It also establishes fresh session keys every time a new connection is made, improving security.