Q5. Brief about the client association process

Scanning: Find available APs.

Authentication: Exchange auth request/response frames.

Association: Send association request; AP sends response.

Key exchange (if WPA/WPA2): EAPOL 4-way handshake.

Client joins network: It can now send/receive data.

Q6. Explain each steps involved in EAPOL 4-way handshake and the purpose of each keys derived from the process

1. Message 1: AP sends Authenticator Nonce to client.
2. Message 2: Client generates SNonce and sends it with MIC (message integrity code) to AP.
3. Message 3: AP derives PTK, sends GTK (Group Temporal Key) encrypted with PTK.
4. Message 4: Client confirms install of keys.

Keys Derived:

- PMK (Pairwise Master Key): From passphrase/802.1X.
- PTK (Pairwise Transient Key): For unicast data between client and AP.
- GTK (Group Temporal Key): For broadcast/multicast data.
- KCK/KMK: Derived from PTK for message integrity.