### Q8) What Happens If a Wrong Passphrase Is Used During the 4-Way Handshake?

If a client enters an **incorrect passphrase** during the 4-way handshake in WPA2 or WPA3-Personal, the authentication process will **fail**.

**1. Key Derivation Fails**

* The **Pairwise Master Key (PMK)** is derived from:
* The passphrase.
* The SSID (network name).
* A hashing algorithm (PBKDF2-SHA1 for WPA2, SAE for WPA3).
* **If the passphrase is wrong**, the PMK will **not match** the one stored on the access point (AP).

**2. Handshake Failure During Message 2**

* **Message 1 (AP → Client):**
* The AP sends an **ANonce** (random number).
* The client (with the wrong passphrase) computes an **incorrect PTK** (Pairwise Transient Key).
* **Message 2 (Client → AP):**
* The client sends its **SNonce** and a **MIC (Message Integrity Code)**.
* Since the PTK is wrong, the **MIC will be invalid**.
* The AP detects the invalid MIC and **rejects the handshake**.

**3. Observable Consequences**

* **Connection Timeout:**
* The client won’t receive **Message 3** (GTK) from the AP.
* After retries (typically 3–4 attempts), the client disconnects.
* **Error Messages:**
  + The client OS may display:
    - *"Incorrect password"* (Windows/macOS).
    - *"Authentication failed"* (Linux/Android).
  + The AP logs may show **failed authentication attempts**.

**4. Security Implications**

* **No Data Exposure:**
  + The PMK and PTK are **never transmitted**, so an attacker can’t deduce the passphrase from the failed handshake.
* **Brute-Force Protection:**
* WPA2/WPA3 rate-limits handshake attempts, slowing down password-guessing attacks.
* WPA3’s **SAE (Dragonfly)** makes offline brute-forcing nearly impossible.

**5. Differences Between WPA2 and WPA3**

|  |  |  |
| --- | --- | --- |
| **Scenario** | **WPA2 (PSK)** | **WPA3 (SAE)** |
| **Wrong Passphrase** | Handshake fails (invalid MIC). | Handshake fails (SAE hash mismatch). |
| **Brute-Force Risk** | Vulnerable to offline dictionary attacks. | Resistant to offline attacks. |
| **Error Feedback** | Generic "password incorrect" message. | Same, but harder to exploit. |