WPA2-Enterprise is **a more secure version of WPA2 Wi-Fi that utilizes IEEE 802.1X for authentication, typically with a RADIUS server**. Unlike WPA2-PSK (Personal), which uses a pre-shared key, WPA2-Enterprise uses individual user credentials, making it suitable for larger organizations needing centralized access control.

**Key Features and Benefits:**

- **Enhanced Security:** WPA2-Enterprise offers stronger security compared to WPA2-PSK by employing individual user authentication and secure encryption protocols.
- **Centralized Management:** It allows for centralized management of user accounts and access permissions through a RADIUS server.
- **Scalability:** WPA2-Enterprise can handle a large number of users and devices, making it suitable for large organizations.
- **Network Access Control:** It supports Network Access Protection (NAP) and can enforce policies on device compliance before allowing access to the network.
- **Multiple Authentication Methods:** It supports various EAP methods, including PEAP (Protected Extensible Authentication Protocol) with MSCHAPv2, for a more secure authentication process.

**How it Works:**

1. A device attempts to connect to the WPA2-Enterprise network.
2. The device sends authentication information, such as a username and password, to the Access Point.
3. The Access Point forwards the authentication request to the RADIUS server.
4. The RADIUS server verifies the user's credentials against its database or Active Directory.
5. If the credentials are valid, the RADIUS server provides the Access Point with authorization to allow the device to connect.
6. The Access Point and the device establish a secure, encrypted connection using WPA2 encryption.