Q10) IEEE 802.1X enhances security over wireless networks by **requiring devices to authenticate** before they are allowed to access the network, thus preventing unauthorized users from connecting. It uses protocols like **EAP (Extensible Authentication Protocol)** for secure credential exchange and works with a **RADIUS server** to verify identities. After successful authentication, **dynamic encryption keys** are generated, making the wireless communication **private and secure** against eavesdropping and attacks.

**Detailed Explanation:**

**1. Authentication Before Access:**  
Before a wireless device (like a laptop or phone) can join the network, it must prove its identity through 802.1X. This stops attackers from simply connecting to the Wi-Fi.

**2. Dynamic Encryption Keys:**  
Once authentication succeeds, the system generates **unique session keys** for each device. These keys are used to encrypt data traffic, ensuring confidentiality even if someone tries to listen in.

**3. Strong Credential Verification:**  
Instead of simple passwords (like in WPA-PSK), 802.1X supports complex credentials like certificates, smartcards, or username/password combinations verified against secure servers.

**4. Defense Against Rogue Devices and Attacks:**  
802.1X ensures that rogue devices (fake access points, unauthorized users) cannot easily connect, protecting the network from common wireless attacks like **Man-in-the-Middle (MITM)** or **Evil Twin attacks**.