**Q9)Problem Solved by 802.1X in a Network**  
IEEE 802.1X addresses the **problem of unauthorized access** to a network. In an open network, anyone who physically connects a device (via Ethernet or Wi-Fi) can potentially access network resources, which is a major security risk. 802.1X solves this by introducing a **secure authentication mechanism** before allowing any device to communicate with the network.

**How 802.1X Works to Solve the Problem**

* **Port-Based Network Access Control:** 802.1X controls access at the point of connection (port). When a device (called the "supplicant") connects, the network device (called the "authenticator," like a switch or access point) blocks all traffic except authentication traffic.
* **Authentication Process:** The authenticator forwards authentication requests to a centralized server (like a RADIUS server) known as the "authentication server." Only after successful verification are normal network privileges granted.
* **Preventing Rogue Access:** Without proper credentials (like username/password, certificates, or smartcards), a device is not allowed onto the network. Even if someone plugs into a port or connects to Wi-Fi, they stay isolated until authenticated.
* **Supports Secure Methods:** It works with protocols like EAP (Extensible Authentication Protocol), allowing strong, flexible authentication (like certificates, multi-factor authentication).

**Benefits**

* **Strong Security:** Devices must prove their identity before accessing the network.
* **Prevents Unauthorized Users:** No access is given until authentication succeeds.
* **Dynamic Policies:** Based on user/device identity, different levels of access can be granted.
* **Works on Wired and Wireless Networks:** Commonly used in enterprise Wi-Fi, but also for Ethernet LAN security