Name: Aswath S

College: Vellore Institute of Technology, Vellore

Reg.No: 21BEC2188

Wi-Fi Training Program 2025

Module 6

Question 10:

How does 802.1X enhance security over wireless networks

Solution:

802.1X enhances security over wireless networks by providing a robust **authentication framework** that ensures only **authorized devices and users** can access the network, preventing unauthorized access and securing communications. Here's how it works:

1. Strong Authentication

- **802.1X uses centralized authentication** via a **RADIUS (Remote Authentication Dial-In User Service)** server. The **client device (supplicant)** must provide valid credentials (such as a username and password, a certificate, or a smart card) to the **authentication server** before gaining access to the network.
- This ensures that only **trusted users or devices** can connect to the wireless network.

2. Protection Against Unauthorized Access

- In traditional **open wireless networks** (like those found in coffee shops), anyone within range can connect. **802.1X prevents this** by requiring a **successful authentication** process before allowing network access.
- If a device cannot **authenticate properly**, it is **denied access** to the network.

3. Encryption of Credentials

- During the **authentication process**, **802.1X employs EAP (Extensible Authentication Protocol)** methods that can use **strong encryption** (like **EAP-TLS** with certificates) to **protect sensitive information** like usernames, passwords, and other credentials.
- This ensures that attackers cannot easily intercept or **sniff** credentials while they are being transmitted over the air.

4. Mutual Authentication

- **802.1X supports mutual authentication**, meaning that **both the client (supplicant) and the access point (authenticator)** authenticate each other. This prevents **man-in-the-**

middle (MITM) attacks where an attacker might try to impersonate the access point to capture authentication information.

- The access point ensures it is communicating with a legitimate device, and the device ensures it's connecting to a legitimate network.

5. Dynamic Key Exchange

- Once authentication is successful, **802.1X facilitates the exchange of unique encryption keys** (such as **Pairwise Transient Key (PTK)**) between the client and the access point.
- These encryption keys are used to **secure the communication** between the client and AP, ensuring data integrity and confidentiality during transmission.
- The **dynamic nature** of the key exchange prevents attackers from using static keys to decrypt network traffic.

6. Role-Based Access Control

- With 802.1X, administrators can implement **role-based access control (RBAC)**. After authentication, different users or devices can be assigned **different levels of access** based on roles.
- For example, employees might have full access to corporate resources, while guests might only have access to the internet.

7. Protection Against Eavesdropping

- In **unencrypted wireless networks**, attackers can easily **eavesdrop** on unprotected traffic. By requiring **authentication before any data is exchanged**, **802.1X** ensures that communication between devices is only possible after a secure, encrypted tunnel is established.

8. Prevention of Rogue Devices

- **802.1X helps prevent rogue devices** (unauthorized access points or devices) from joining the network. Only devices that authenticate with the RADIUS server are allowed to connect.
- This prevents **rogue APs** (evil twin attacks) from tricking legitimate devices into connecting to them.