EX.NO:06

Date:

Secure WLAN Setup using 802.1X Authentication with RADIUS

Aim:

To configure a secure Wireless LAN (WLAN) using **802.1X authentication** with a **RADIUS server**, ensuring only authenticated users can connect to the wireless network.

Theory:

- **802.1X** is a port-based access control protocol that provides authentication before allowing devices onto the network.
- **RADIUS (Remote Authentication Dial-In User Service)** is used to centralize authentication, authorization, and accounting.
- Process Flow:
    1. The **client (Laptop, Smartphone, Tablet)** requests access through the Access Point (AP).
    2. The **AP (Authenticator)** forwards credentials to the **RADIUS server**.
    3. The **RADIUS server (Authentication Server)** verifies credentials from its database.
    4. If valid, the client is granted access to the WLAN; otherwise, denied.

This ensures only authorized users can connect, providing better **security** compared to WPA2-PSK.

Required Equipment:

1. Cisco Switch (2960)
2. Wireless Access Points
3. End Devices – Laptop, Smartphone, Tablet
4. Server (Configured as RADIUS server)
5. Copper Straight-through cables
6. Cisco Packet Tracer software

Procedure:

Step 1: Build the Topology

- Connect **Access Points → Switch → RADIUS Server**.
- Connect **Laptop, Smartphone, Tablet** wirelessly to APs.
- Configure the **Server0** as RADIUS server.

Step 2: Configure the RADIUS Server (Server0)

1. Go to **Services → AAA**
    - Enable AAA.
    - Configure a RADIUS username and password.
    - Example:
        - Username: student
        - Password: cisco123
2. Enable RADIUS Authentication service.

Step 3: Configure the Access Points

On each **Access Point**:

- Go to **Config → Wireless Settings**
    - SSID: SecureWiFi
    - Security: **WPA2-Enterprise** (802.1X)
    - RADIUS Server: 192.168.10.10 (Server0's IP)
    - Shared Secret: radius123

Step 4: Configure the Switch (if required for VLAN assignment)

Switch> enable

Switch# configure terminal

Switch(config)# interface fa0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

Switch(config)# interface fa0/2

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 20

Step 5: Configure Client Devices (Laptop, Smartphone, Tablet)

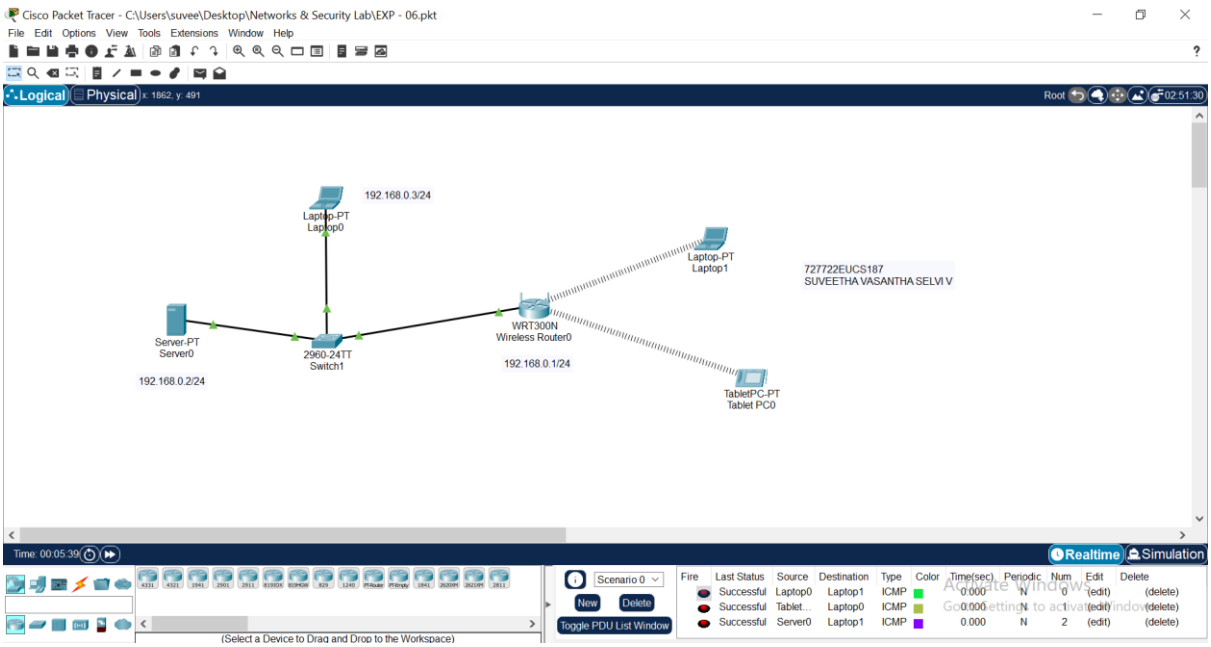
- Go to **Desktop → Wireless Settings**

- Select SSID: SecureWiFi
- Authentication: **WPA2-Enterprise**
- Enter Username: student
- Enter Password: cisco123

Testing:

1. On **Laptop, Smartphone, Tablet** → connect to SecureWiFi.
2. The AP forwards authentication request to the **RADIUS server**.
3. If username/password matches, device gets IP and network access.
4. Try accessing/pinging the server → should succeed.
5. If wrong credentials are entered → access is denied.

MODEL OUTPUT:



Result:

The WLAN was successfully secured using **802.1X authentication with RADIUS**, ensuring only authenticated clients could access the network.