Enhancing Wifi Security in an IoT network

Name: Girish Dyal
Student ID: 2012046
BSc Computer Science level 3
Supervisor: Dr. Avinash Mungur

PROBLEM DEFINITION

- As the number of IoT devices continues to grow, the attack surface for hackers also increase
- Lack of proper security mechanism in IoT device has made them easy targets for hackers
- The limited resources of IoT devices makes it challenging to implement strong security measures
- In a local network, IoT devices and traditional computers are connected to the same central access point. This makes the IoT devices exposed to anyone that may have access to the local network, subsequently increasing their security risks
- There are authentication or encryption solutions that are implemented but this does not really solve the issue

Aims and Objectives

Aims:

- Construct a smart home IoT system where IoT devices are in a star topology
- Protect communication of IoT devices by isolating them from the main network
- Ensuring the power requirements of devices are preserved
- Only IoT devices can wirelessly connect to the IoT gateway
- Ensure that only authorize device can manage the IoT devices

Objectives:

- To enhance the Wi-Fi security of IoT devices by segmenting the local network
- Create separate network for each group
- Set up a password-protected gateway with WPA2 protocols
- Configure switch to create VLANs & router to create logical interfaces for VLANs
- Configure password parameters on both switch and router

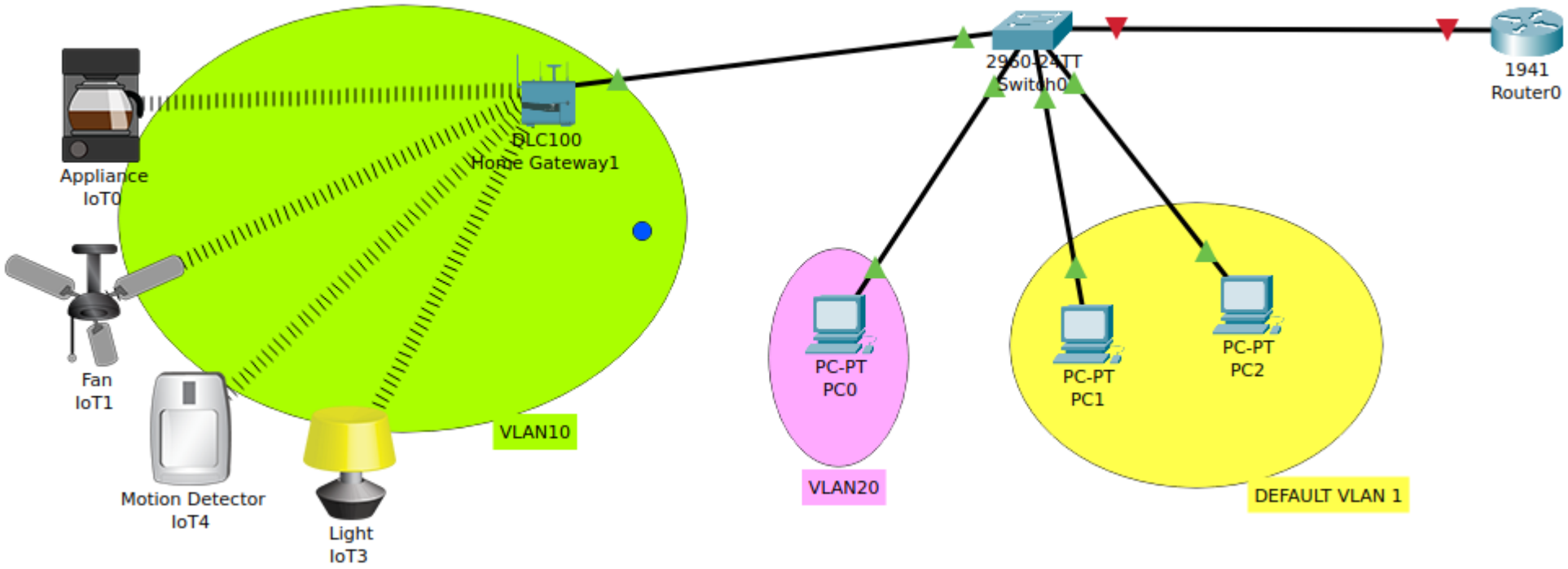
Project Scope

- Reduce attack surface
- Better access control to resources and data
- Easier for network administrators to monitor network traffic

Proposed Solution

- Isolating all the IoT devices from the main network
- Creating separate virtual networks by using VLANs on switch
- Design an IoT topology that segments the network based on device types
- Allow only authorized users to monitor IoT devices

Design



Tool used

Project progress