UNIVERSITY OF DERBY

COLLEGE OF SCIENCE AND ENGINEERING
MATHS AND COMPUTER SCIENCE

Lab 8: Internet of Things (IoT) Networks using Packet Tracer

Lab Task

Each scenario (provided in course resources for this lab) helps you understand IoT device interaction, networking, and security. The setup involves configuring connectivity (wired/wireless), automation, and access control. Your task is to run and analyse these IoT networks and then document your observations through a structured report.

Scenario 1

Description

This scenario simulates a smart home environment where IoT devices (light, sprinklers, doors) are connected to a Home Gateway. The user/owner can control these devices via a smartphone.

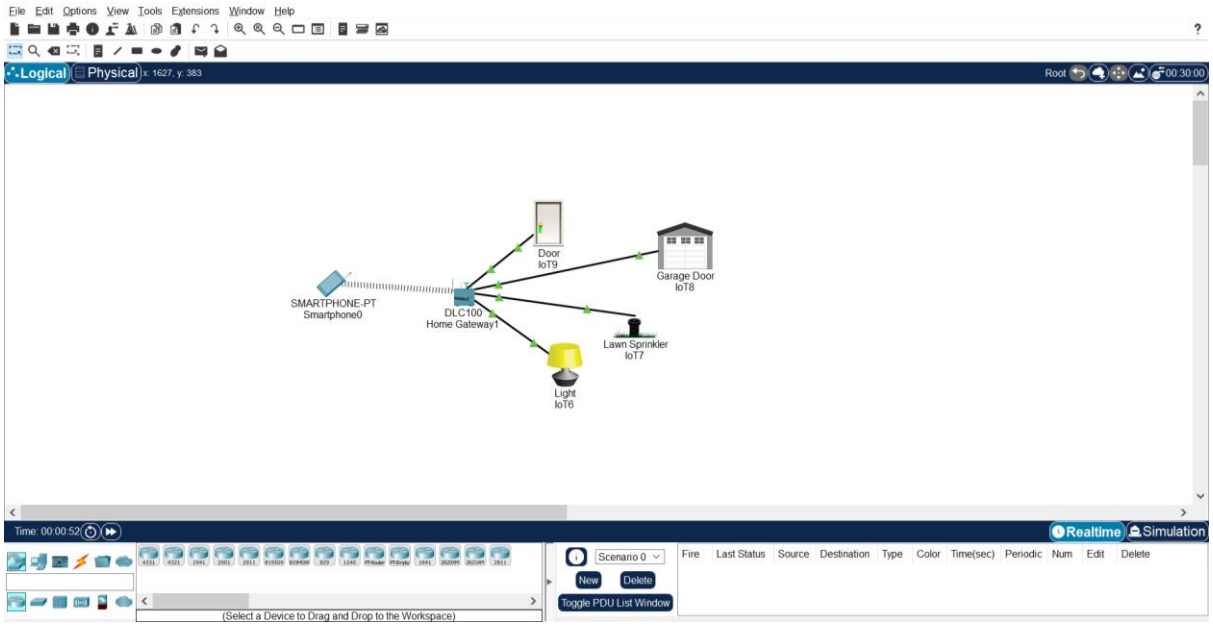

Figure 1: Scenario 1

Setting Up the Devices

1. **Home Gateway Setup**
    - **Ensure the Home Gateway is powered on and connected to the network.**
    - **Check that the Wi-Fi SSID is set and IoT devices are connected.**
2. **Adding IoT Devices**

- **Go to the Physical Devices workspace and select IoT devices (e.g., lights, fans).**
- **Connect them wirelessly to the Home Gateway.**
- **Assign IP addresses (either DHCP or manually).**

3. **Configuring Device Control**
   - **Use a PC or tablet to access the Home Gateway's web interface.**
   - **Test turning IoT devices on and off.**
   - **Create automation rules.**

Scenario 1 Exercises: Controlling Devices with a Home Gateway

1. **Basic Device Control**

- Open **Cisco Packet Tracer** and load the scenario.
- Click on the **Home Gateway** and open its **web interface** in a PC's browser.
- Turn devices **on and off** (e.g., lights, fans, alarm).
- Observe the device status change in **real-time and via simulation**.

2. **Automation Rules**

- Set an **automation rule** (e.g., if garage door is open turn off sprinkler).
- Check if the automation executes correctly.
- Modify the rule and test how it affects device behaviour.

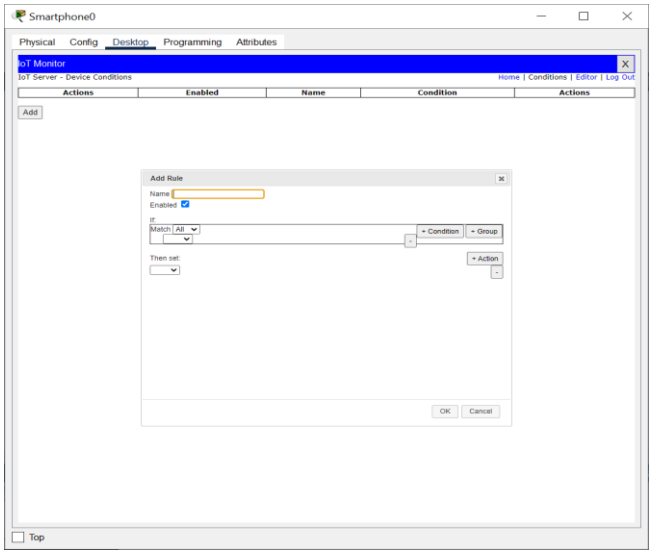

Figure 2: Setting Rules/ conditions

Optional exercises:

3. **Connecting New Devices**

- Add a **new IoT device** (e.g., a smart thermostat) from the device list.
- Connect it to the **Home Gateway** using Wi-Fi.
- Access the Home Gateway's interface to check if the new device appears.

4. **Network Testing**

- Disconnect and reconnect a device to see if it automatically **reconnects**.
- Change **Wi-Fi security settings** (e.g., set WPA2 password) and try reconnecting.
- Disable Wi-Fi and check if wired devices still function.

Expected Observations

- How long does it take for devices respond to commands?
- Do devices automatically reconnect after a disconnect?
- How do automation rules work in practice?

Scenario 2

Description

This scenario involves a smart home network with both wired and wireless connections. The switch and access point (AP) provide connectivity, while the server manages IoT functions.

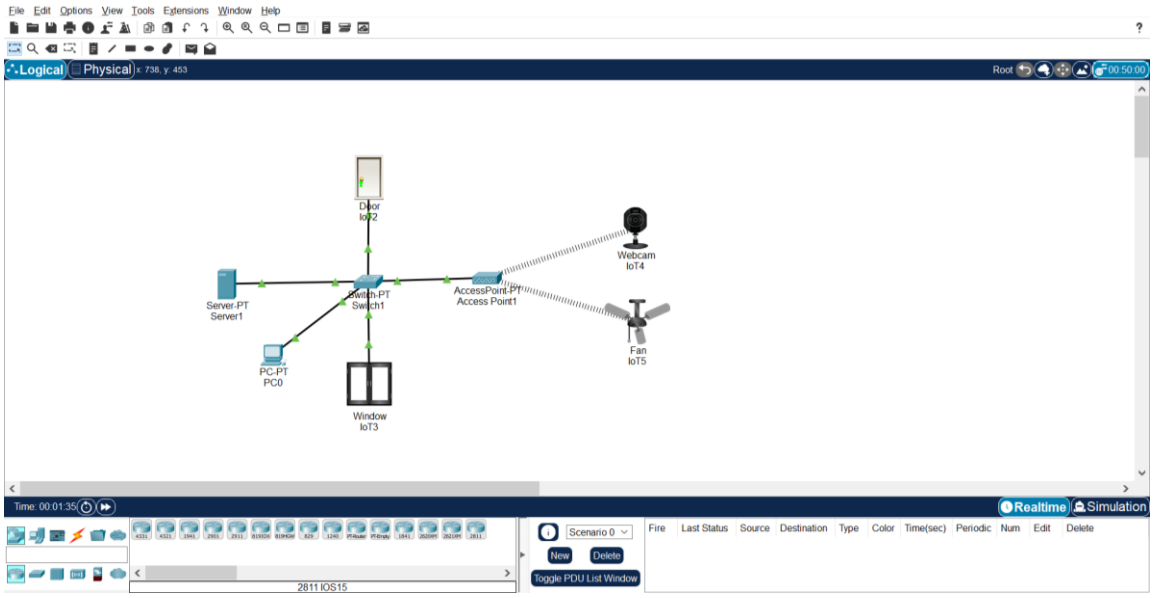

Figure 3: Scenario 2

Setting Up the Devices

1. Switch and Access Point Setup
    - Ensure the switch connects to all devices via Ethernet.
    - Configure the Access Point (AP) with an SSID and password.
    - Connect wireless IoT devices to the AP.
2. Server Configuration
    - Determine the server's role (e.g., DHCP, web, or IoT controller).
    - If DHCP is enabled, ensure devices receive IP addresses dynamically.
    - If it has a web service, open a PC's browser and check its status.
3. Testing the Network
    - Use Command Prompt (ping device_IP) to verify connectivity.
    - Try accessing the server's web interface to check IoT device status.
    - Modify network security settings

Scenario 2 Exercises

1. Network Connectivity

- Identify key devices: **Switch, Access Point (AP), Server**.
- Open the PC's **Command Prompt** (Desktop > Command Prompt).
- Run ping to test connectivity to different devices (e.g., ping 192.168.1.1).
- Add rules or conditions and analyse the behaviour using simulation.

2. Wireless Network Setup

- Change the **Wi-Fi SSID name** in the **AP settings**.
- Reconnect a wireless device to the new network name.
- Enable **WPA2 security** and try connecting with a password.

3. Device Communication through the Server

- Check if the **server provides DHCP** by ensuring devices get an **IP address**?
- If there's a web server, try accessing it using a **browser on PC0 (See Fig. 3)**.
- Disable the server and observe if IoT devices stop responding.

Figure 4:Login using browser on PC0

4. Security and Network Failures

- Try **disconnecting** the switch and check what happens to device connectivity.

Expected Observations

- The impact of changing Wi-Fi security settings.
- How the IoT system behaves when the server is offline.

Scenario 3

Description

This scenario models a **smart parking system** with **RFID-based vehicle entry**. The Parking space is monitored using a motion sensor.

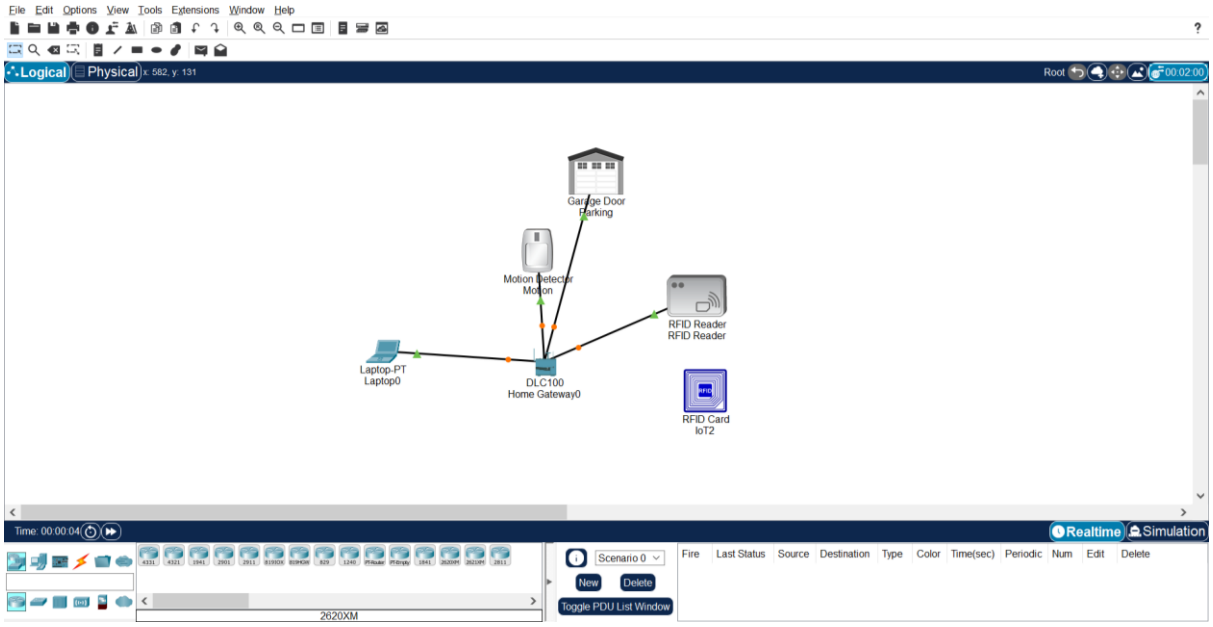

Figure 5: Scenario 3 (smart parking system)

Setting Up the Devices:

1. **RFID System Setup**
    - Ensure the **RFID reader** is connected to the **control system**.

- Assign **RFID tags** to vehicles and test entry.

2. **Testing**
    - Simulate a **vehicle with an authorized RFID tag** entering.
    - Check if the **barrier opens** and the system updates available spaces.
    - Test an **unauthorized vehicle** and observe if access is denied.

Scenario 3 exercises: Smart Parking System

1. Basic Parking Operations

- Move the **RFID tag within proximity of the reader**.
- Check if the **barrier gate opens**.
- Simulate a car moving past the motion detector (hold alt key and move the mouse) and observe changes.

2. Security Settings

- Set an access rule: only allow certain **RFID tags** to enter.
- Try to enter with an unauthorized car and check the system's response.

Expected Observations

- How the parking system monitors vehicles.
- Whether unauthorized cars are correctly blocked.

Report

Write a structured report of not more than 100 words for each subsection as given below.

1. Introduction

- Briefly describe each scenario and its objectives.

2. Network and Device Setup

- Overview of devices used (routers, switches, IoT).
- Configuration steps (IP addresses, automation rules, security).

3. Experimental Interactions

- List of modifications and tests performed.

4. Observations and Analysis

- Network behaviour (traffic, latency, failures).
- Security and reliability considerations.
- Performance under different conditions.

5. Conclusion

- Summary of key findings.
- Recommendations for improvements.