National College of Ireland

Configuration Manual

MSc Research Project
Masters in Cybersecurity

Shouvik Roychowdhury
Student ID: x23179015

School of Computing
National College of Ireland

Supervisor: Raza Ul. Mustafa

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Shouvik Roychowdhury
Student ID:	X23179015
Programme:	Masters in cybersecurity **Year:** 2024
Module:	Practicum part 2
Lecturer:	Supervisor
Submission Due Date:	12-12-2024
Project Title:	Configuration Manual
Word Count:	715 **Page Count:** 10

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:

Date: 12-12-2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	

Date:	
Penalty Applied (if applicable):	

Configuration Manual

Shouvik Roychowdhury
Student ID: x23179015

1 Introduction

This configuration manual provides detailed instructions of the setup Microsoft Threat model and Cisco Packet Tracer and the security features simulated implemented in it.

2 System configuration

Hardware of the system.

- Processor i5 10th gen
- Operating system: Windows 11 Pro
- Storage: 1 TB SSD
- Ram: 16GB DDR4

Versions of the software used:

- Cisco Packet Tracer: 7.3.0
- Microsoft Threat Modelling Tool: v2016
- Note that the Microsoft Tool is a single threaded application and might lag on some systems.

3 Setup and configure development environment

This section provides instructions to download and setup both tools with proper templates as is required with the Microsoft threat modelling tool:

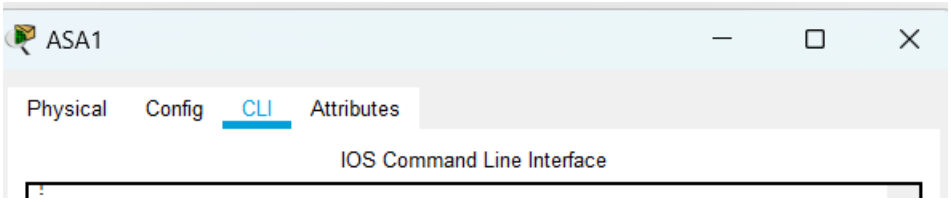
- Download the correct version of Cisco Packet Tracer from the website: https://learningnetwork.cisco.com/s/question/0D53i00000Kt599CAB/download-packet-tracer

- Download the Microsoft Threat Modelling Tool from here: https://www.microsoft.com/en-in/download/details.aspx?id=49168

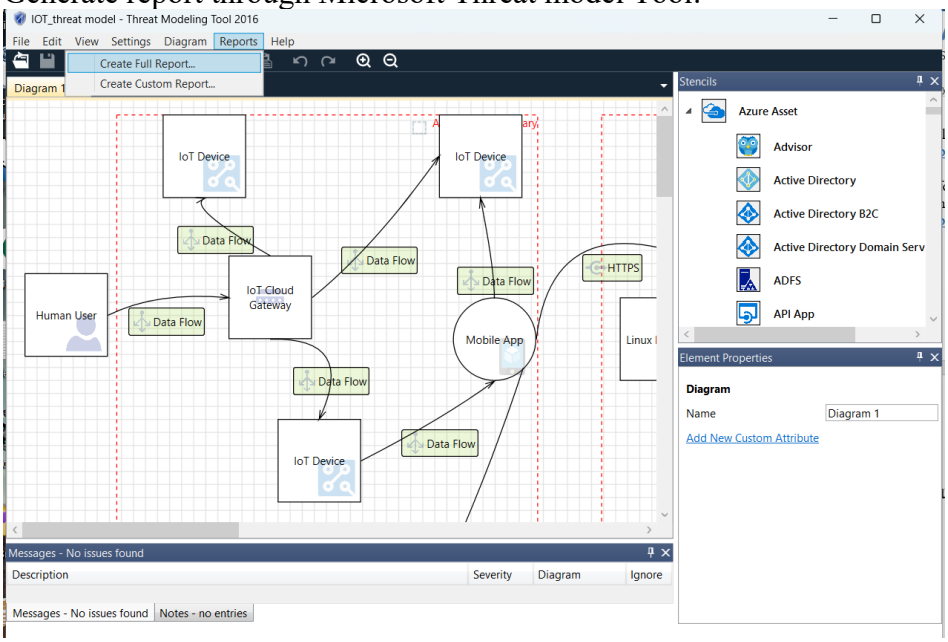
- Download the correct stencils from the GitHub page for the Microsoft tool (Note that I will be attaching the files in the model link) this will provide the necessary components to build the network model: https://github.com/AzureArchitecture/threat-model-templates

4 Generating report and setting up security features

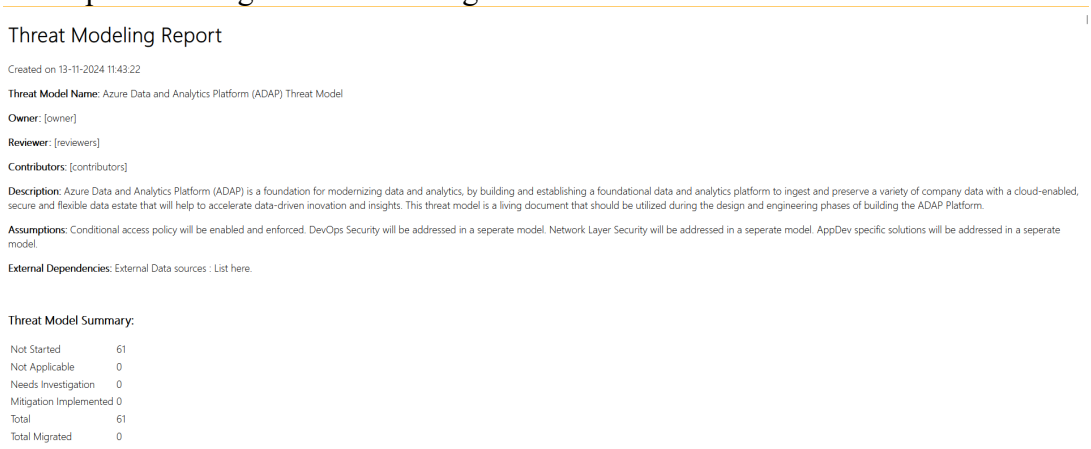
- Note: before starting I want to show how to get into cisco packet tracer's command line, which is common for all simulated devices. Double click on the device and select CLI.



- Generate report through Microsoft Threat model Tool:



- The report is now generated showing threats of the enitre model:



Threat Modeling Report

Created on 13-11-2024 11:43:22

Threat Model Name: Azure Data and Analytics Platform (ADAP) Threat Model

Owner: [owner]

Reviewer: [reviewers]

Contributors: [contributors]

Description: Azure Data and Analytics Platform (ADAP) is a foundation for modernizing data and analytics, by building and establishing a foundational data and analytics platform to ingest and preserve a variety of company data with a cloud-enabled, secure and flexible data estate that will help to accelerate data-driven inovation and insights. This threat model is a living document that should be utilized during the design and engineering phases of building the ADAP Platform.

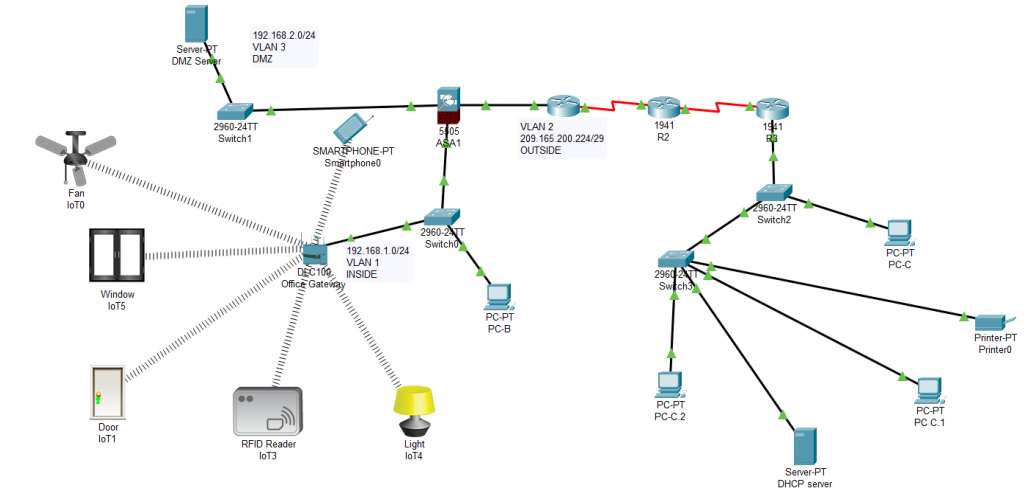
Assumptions: Conditional access policy will be enabled and enforced. DevOps Security will be addressed in a seperate model. Network Layer Security will be addressed in a seperate model. AppDev specific solutions will be addressed in a seperate model.

External Dependencies: External Data sources : List here.

Threat Model Summary:

Not Started	61
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	61
Total Migrated	0

- Implementing the network structure in cisco packet tracer: Note this file will be attached in moodle link .



- Implementing Security Features starting with firewall: the password on the firewall is: **roy123** and then do a show run to check all firewall rules:

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 209.165.200.226 255.255.255.248
!
!
route outside 0.0.0.0 0.0.0.0 209.165.200.255 1
!
```

- Setting up access control lists:

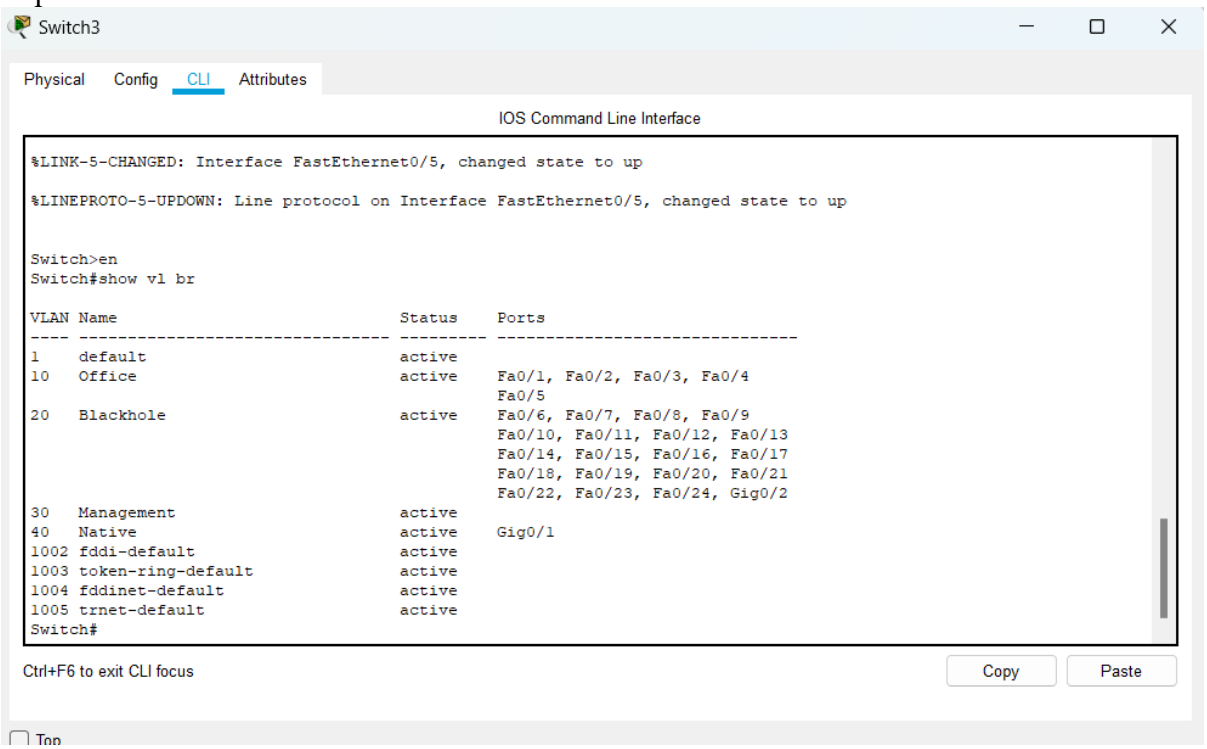
```
!
!

IotFirewall# access-list VLAN_ACL extended permit ip 192.168.10.0
255.255.255.0 192.168.20.0 255.255.255.0
```

Ctrl+F6 to exit CLI focus Copy Paste

- Checking switch port rules of the switches: use the command **en** to go into privilege mode and then use command **show vlan brief** to check the port security rules being

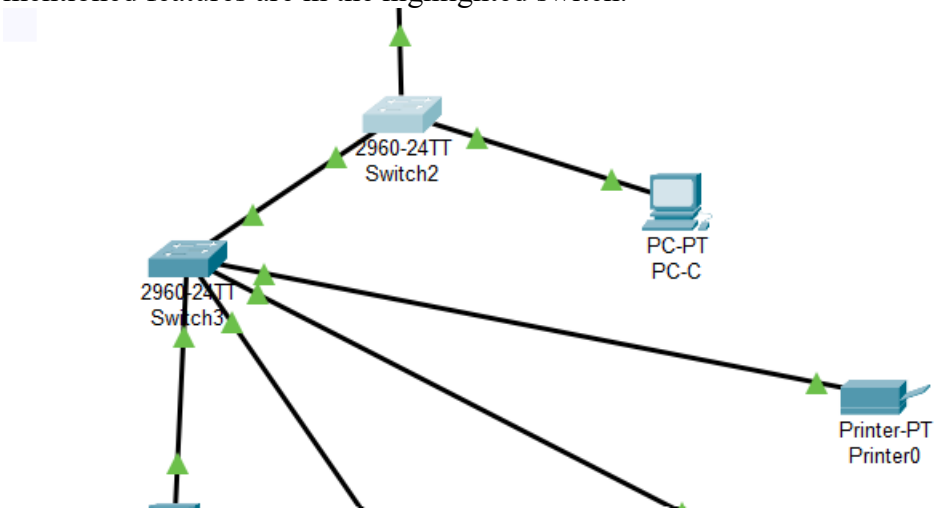
implemented.



- Checking seurity features like dhcp snooping, spanning tree mode, switchport mode access, switport negotiation and port access modes. All these can be checked by going to privilege mode on the switch by typing **en** and then doing and **show run.**

```
!
!
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/4
 switchport access vlan 10
 --More--
```

- **Checking ARP and snooping protection in the second switch:** the previously mentioned features are in the highlighted switch.

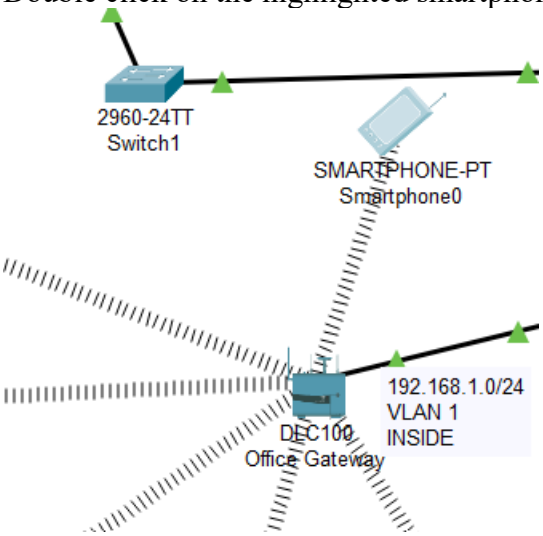


Again to check features do a **show run** giving us the following.

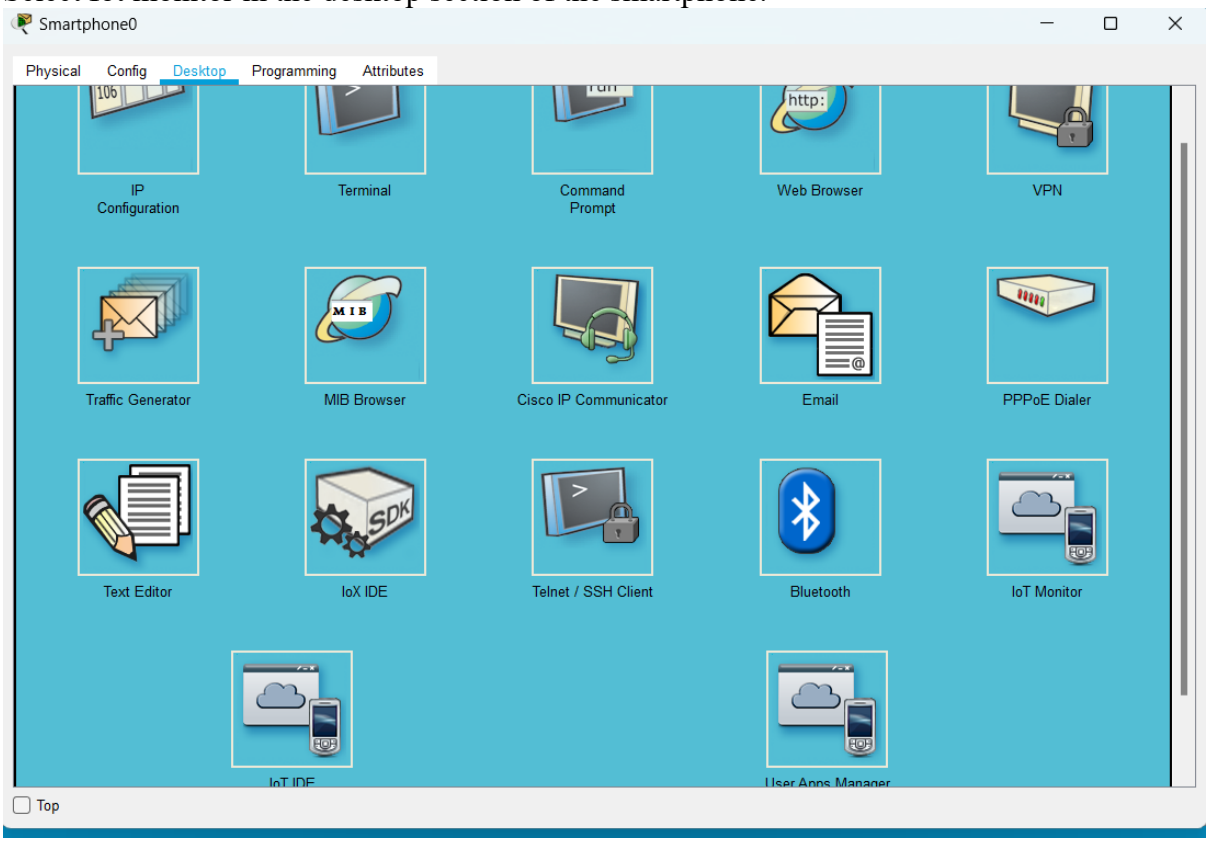
```
hostname Switch
!
!
!
!
ip arp inspection vlan 1,10,20,30,40
ip arp inspection validate src-mac dst-mac ip
!
ip dhcp snooping vlan 1,10,20,30,40
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
 --More--
```

5 Testing the simulation

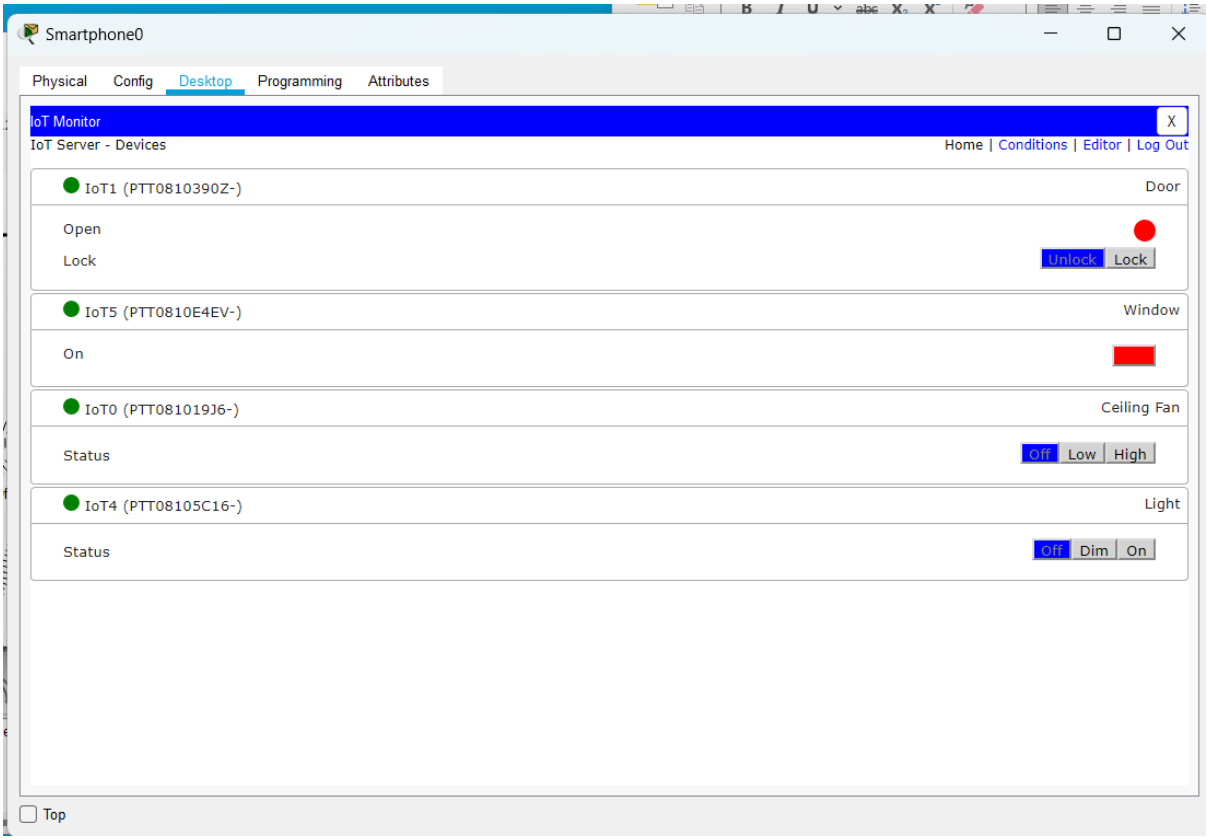
- Double click on the highlighted smartphone which is connected to the IoT gateway:



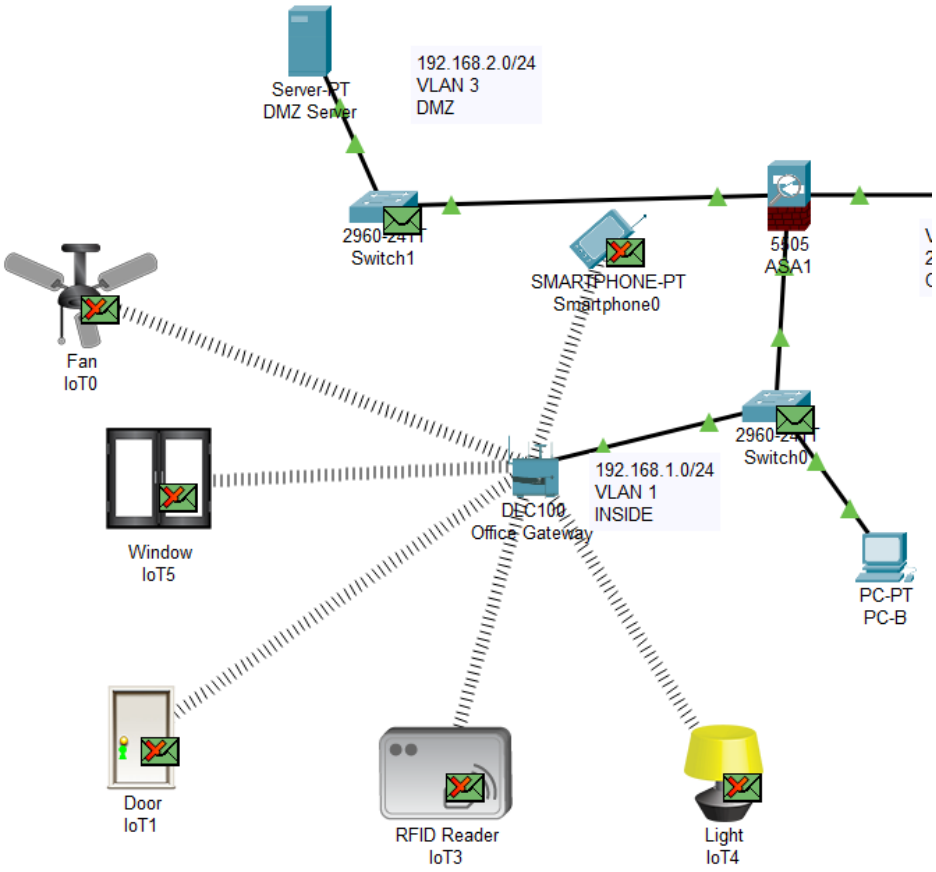
- Select Iot monitor in the desktop section of the smartphone.



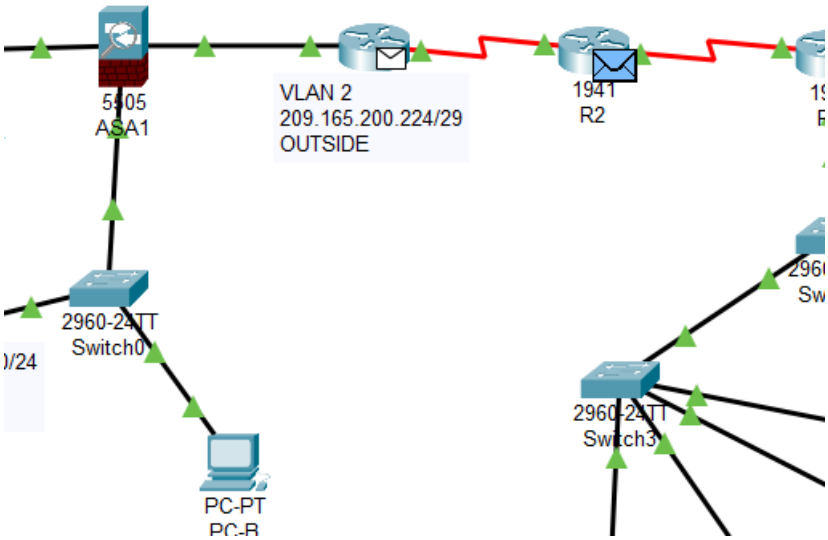
- In the IoT monitor all devices can be interacted with:



- Checking firewall rules by going to simulation mode: The traffic from firewall can go inside the network.



- The traffic from outside cannot comeback in:



References

1. Cisco Networking Academy, n.d. *Cisco Packet Tracer*. [online] Available at: https://www.netacad.com/cisco-packet-tracer [Accessed 10 December 2024].

2. Microsoft, n.d. *Threat modeling*. [online] Available at: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling?oneroute=true [Accessed 10 December 2024].