Department of Computer Science Technology
Cyber Security Program
CET262 - Network Operation and Management
Spring 2025

Project Report

A project of Project 9: IoTSecLab – Securing Smart Devices in Campus Network

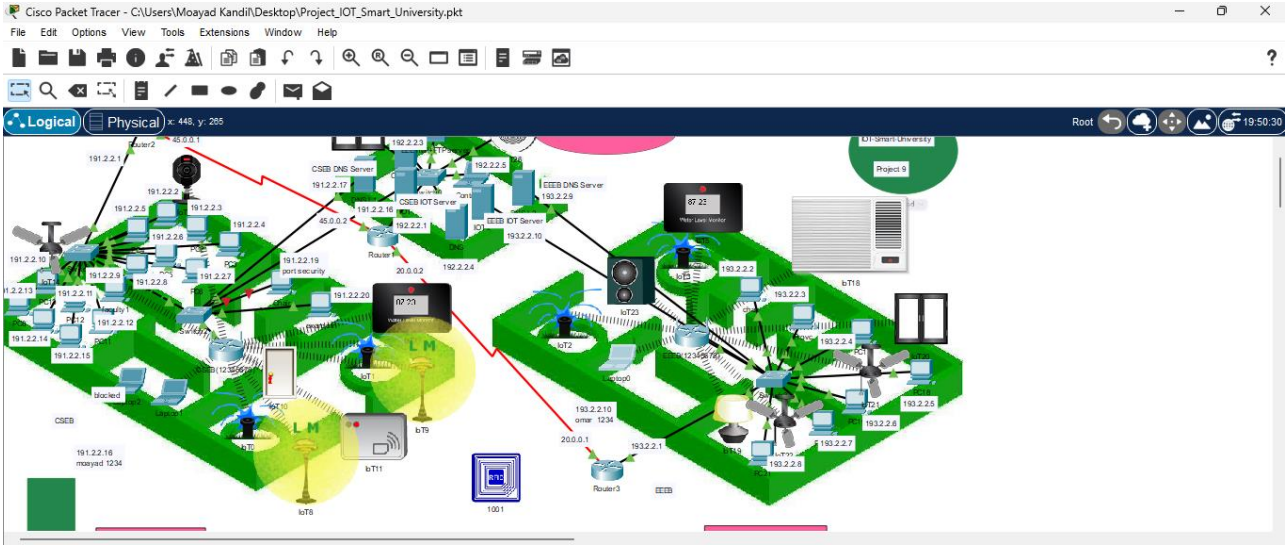
Submitted by	Submitted to
Moayad Ayman 230105619 Bavly Wagyh 230103983 Omar Ahmed 230105097 Galal Ahmed 230103349 Noreen Kamal 230104820	Dr. Hesham Sakr Eng. Suleiman Haitham Eng. Merna Ayman

ELSEWEDY UNIVERSITY OF TECHNOLOGY
- POLYTECHNIC OF EGYPT -

Content

1. Introduction
2. Motivation
3. Objectives
4. Description and Screen shots
5. Limitations
6. Conclusion and future plan

Introduction



"Smart University Network Design Using Cisco Packet Tracer" is a simulation project which demonstrate the smart way to manage a university. In this project we designed a network between two campus and a server station. For simplicity there are only two floor of two department lactated in different place. Assume one is city campus and another is the main campus. There are two lab and two class room. All the PC of CSE department are connected to a single network. There also IOT servers and DNS servers into each campus. All PC of main campus also connected

to its network. To maintain connection with server and also to other campus we connected the inner network to an outer world router. Each router then connected to each other like the internet. Server station have both mail and ftp server which provide services to both campus through the internet. Each campus have also a wireless router where all the IOT devices are connected. We can connect any end devices to this wireless network also.

To make a university smart we focused on IOT devices. As we said every campus have its own IOT server, so this IOT devices can control from the campus as well as from internet because the IOT servers are also connected to the internet. There are lawn sprinkler to water the garden automatically. In the door there is a RFID (Radio Frequency Identification) reader which can read valid RFID and send command to open the door. A camera was installed which can access a classified user like exam controller to visit the exam hall virtually from his office. There also fan, window, air conditioner, light and smoke detector and all of them can control by any PC or Mobile phone. That was a short overview of the project, we will see how the network configured in upcoming section.

Motivation

Now a days every University have a network to communicate internally and externally. But there are few where there is a smart system. Where the work can be done more efficiently and also in smart way. For example, to take attendance of students a teacher needs at least 20 minutes. If the student number is large then we know how much it takes. But what if we install an IOT device to each class room. This IOT will able to read students ID card or face or any kind of unique identity data and upload the data to a server where a database will maintain the data. Like form 10:00 am to 11:30 am is the networking class then the IOT device will send the data to server and the server will count the attendance for this class. It will save lots of time for a large number of student. From this concept we thought how to make a network like this. We didn't implement this concept in this project but this was a great motivation. Not attendance is the only case. Smart devices are changing our life. To communicate between them networks must be developed. Maybe in near future IOT devices and other

network component will be more affordable to users. Then we will able to implement this types of networks anywhere we want.

Objectives:

To design a network where PC, server, IOT devices can work together. One campus can communicate to another internally and externally via internet. Using IOT device's data university will managed in smart way. Add some service like mail, ftp etc.

Descriptions

First come to the background. The background image designed on Auto Cad software and imported here. Then added all the devices step by step based on necessity. Different types of devices connected using copper straight-through wire and same types using copper cross-over wire. Pc was added to the network first and assigned a unique IPv4 address to each. All network's netid also identical. PC and servers IP configuration is like fig1.

IP address is unique and Gateway is the router IP address where the network is connected to another network. Router used to connect all campus and server stations.

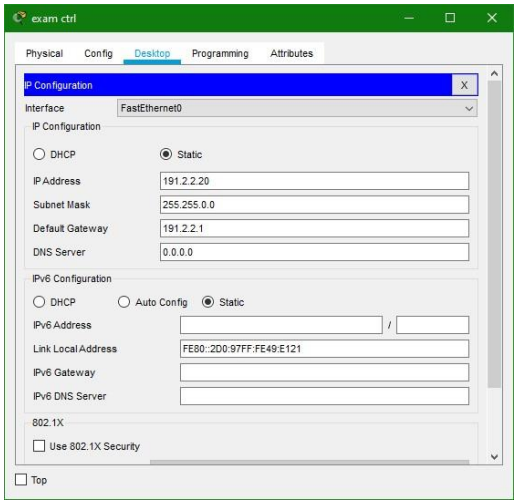


Fig1: PC or server IP configuration

There are another types of component, Warless router (WRT300N) which make a subnetwork. It's same like an end device to the connected switch, have a unique ip address and same gateway like other devices. Inside the subnetwork of this router we used DHCP protocol which maintain all the devices connected to it. The wireless router have three interface internet, LAN and wireless so does three configuration like fig 2 and fig3. IP address is unique and Gateway is the router IP address where the network is connected to another network. Same like a PC. To connect the router to a switch use internet port .

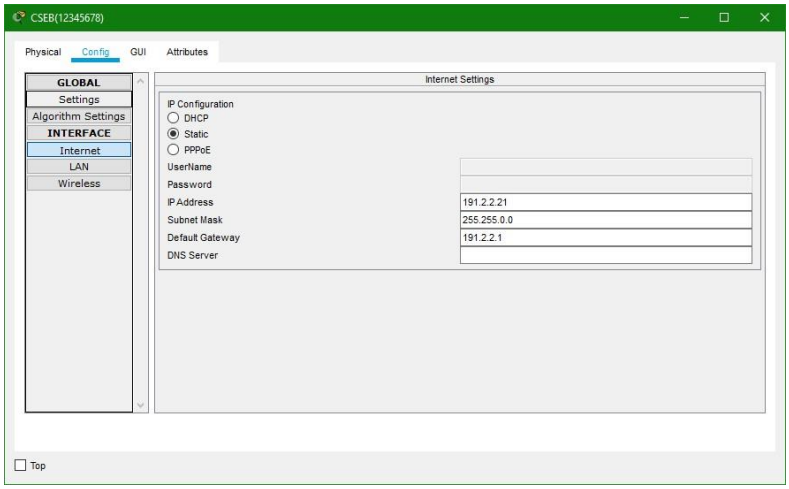
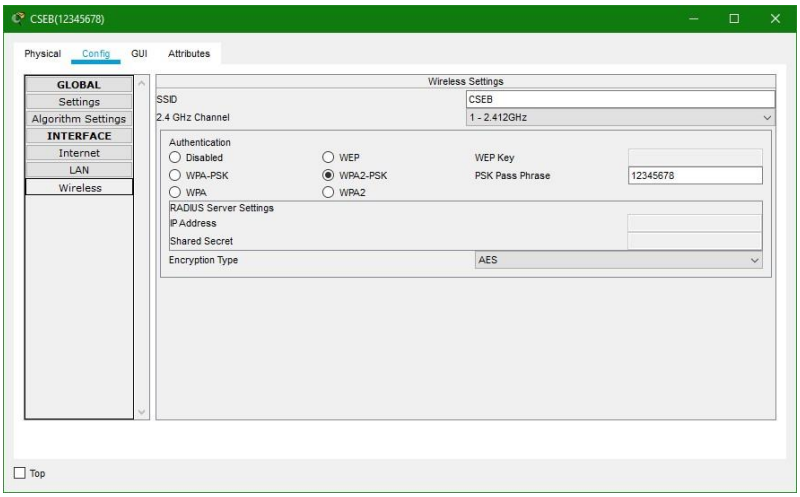


Fig2: wireless router internet configuration

We 're using DHCP inside this network so we can set the LAN as it is. In wireless side set a SSID by which we find the network and set an



authentication protocol and a password.

Fig3: wireless router wireless configuration

Now we will configure IOT devices. We needs an IOT server first. To configure IOT server click on it go to services→iot→ turn on the service. Now from any PC from that network go to desktop→iotMonitor→ Login. If there is no account then create one. We have three account for two campus created in the project.

Server: 191.2.2.16 Username: moayad Password: 1234.

Server: 193.2.2.10 Username: omar Password: 1234.

By using this username and password we can connect IOT devices to a server. To connect IOT with wireless network use the SSID and password of wireless router. Note that if we want to connect an IOT with wireless network IOT interface must change to wireless. To do that click on the device→Advance→I/O config. Now set NetworkAdapter : PT-IOT-NM-1W-AC. If we use the default FastEthernet interface then the configuration is same like a PC. Now the wireless and device configuration is like fig 4.

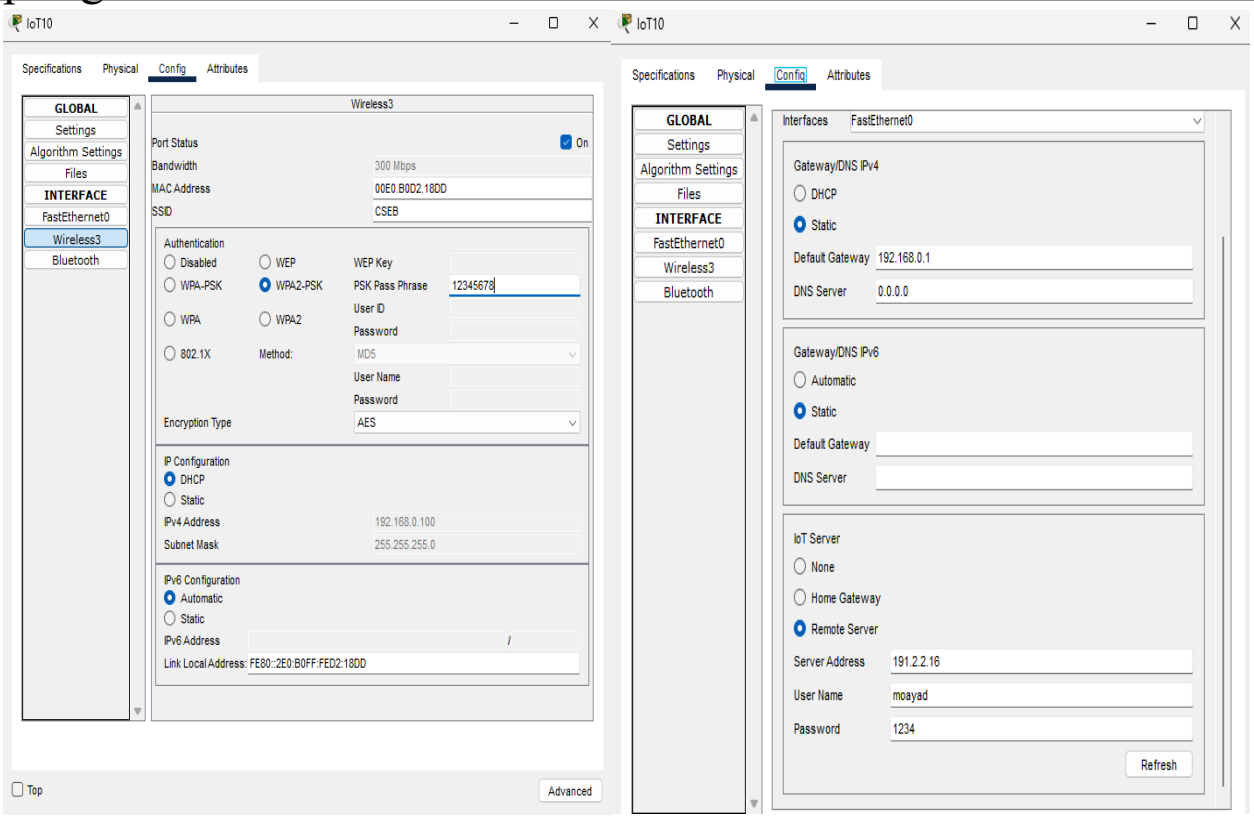


Fig4: IOT device configuration

All the IOT device's configuration are same. If the device connect to the server successfully then we can see from a PC→iotMonitor and also can setup condition to make the environment smart.

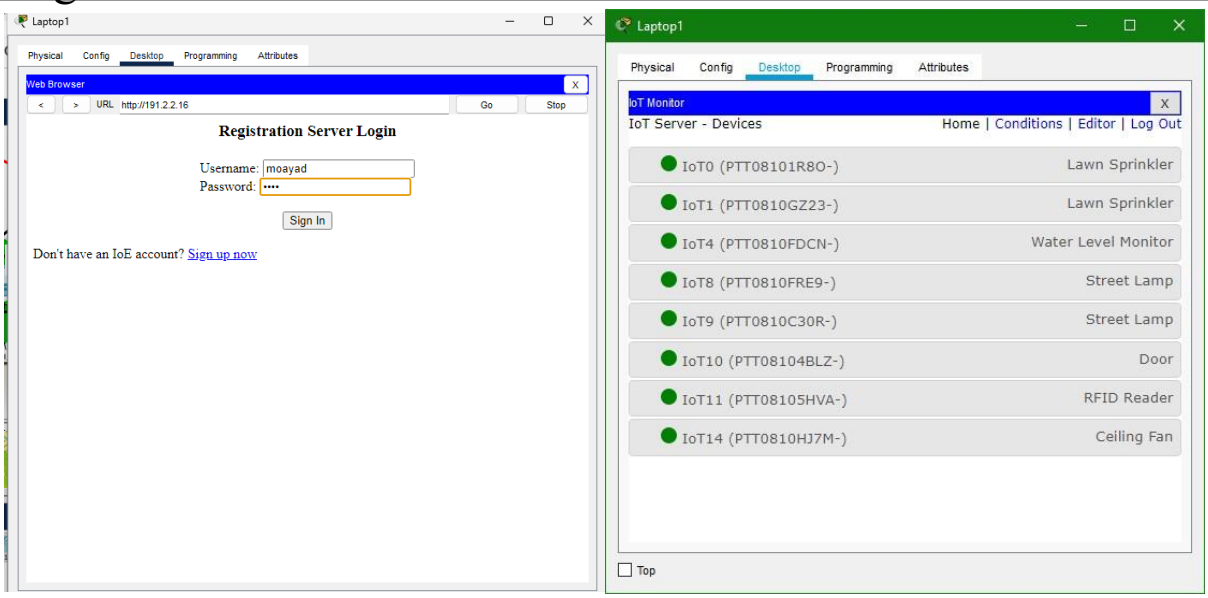


Fig5: IOT monitor from a PC

Now to connect with internet or to another campus we needs to connect to a router. We will use 3 three router so make sure that one router have enough port or add some serial port. We can easily configure these ports, just assign an IP address and use them to connect different networks. We used dynamic routing by RIP (Routing Information Protocol) protocol. The following fig 6 shows the router configurations. Make sure that the port status turned on.

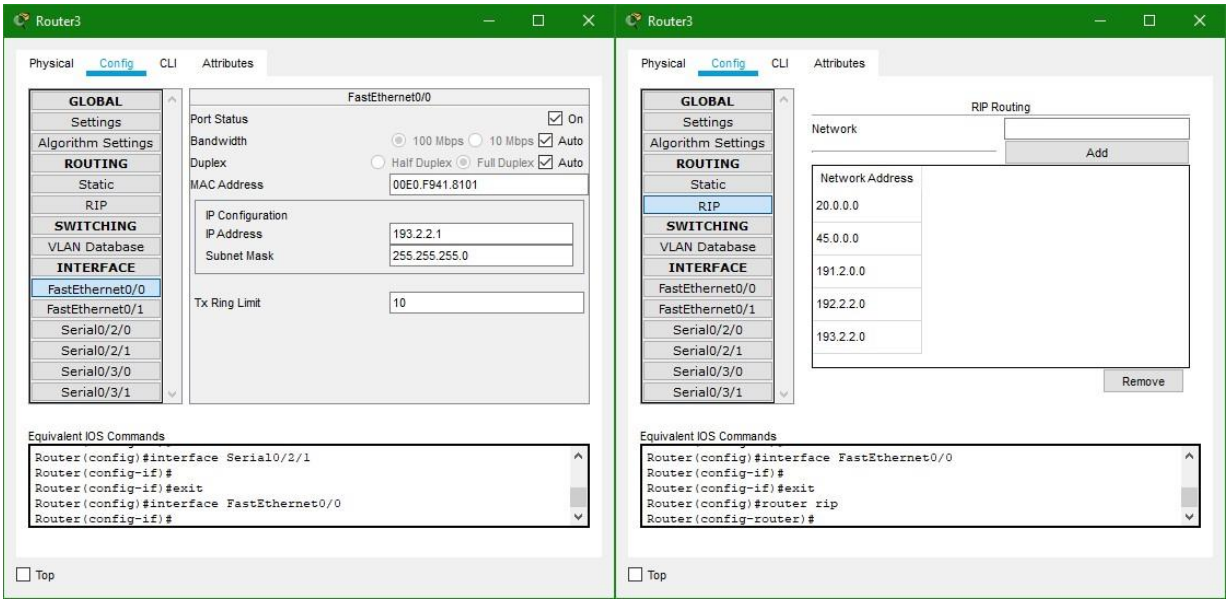


Fig6: Router configuration

DNS server configuration are simple. Turn on the service and add records to it. That's it. To configure mail server go to email again turn on the SMTP and Pop3 service set a domain name for mail and add some users. In case of FTP server go to FTP turn on the service create some user with access permission limits.

That was an overall description about how all the devices are configured and connected through a network.

Access Control List

Device: Router3
ACL Type: Standard Access Control List
ACL Number: 10
Interface Applied: FastEthernet 0/1 (Inbound direction)

Configuration Summary:

A standard access list (access-list 10) is configured to control access to the router interface based on the source IP address.

Permitted IP Addresses:

The following individual IP addresses are explicitly permitted:

CopyEdit

192.168.0.102 – 192.168.0.119

These entries allow only hosts with these specific IP addresses to access the router interface.

Denied IP Address:

One specific host is explicitly **denied**:

193.2.2.2

This is done using:

access-list 10 deny 193.2.2.2

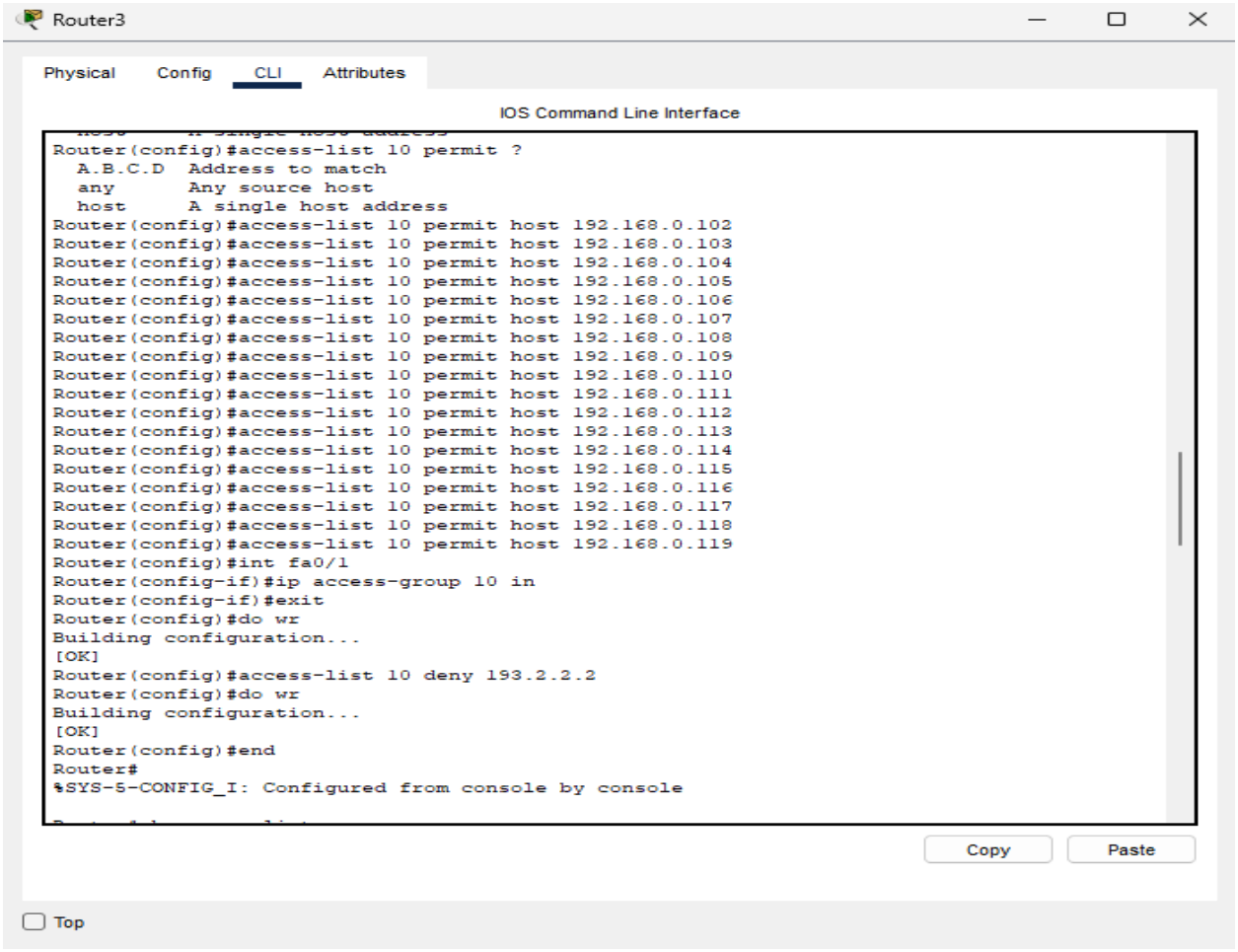
Note: Any IP address **not explicitly permitted** is implicitly denied by default, due to the implicit deny any rule at the end of all ACLs.

Interface Association:

The ACL is applied **inbound** on interface FastEthernet 0/1:

ip access-group 10 in

This means traffic **coming into** the router through this interface will be filtered according to the rules defined in ACL 10.



Security

Port Security Configuration

Device: Cisco Switch (Switch2)
Interface Configured: FastEthernet 0/4 (fa0/4)

Configuration Summary:

The following security configurations have been applied to interface fa0/4:

1. **Switchport Mode:**
    - Set to access mode (switchport mode access).
    - Assigned to access VLAN (switchport access).
2. **Port Security Enabled:**
    - Port security activated with switchport port-security.
3. **MAC Address Restriction:**
    - A specific MAC address 0040.0B45.E0CB is statically assigned using:

switchport port-security mac-address 0040.0B45.E0CB

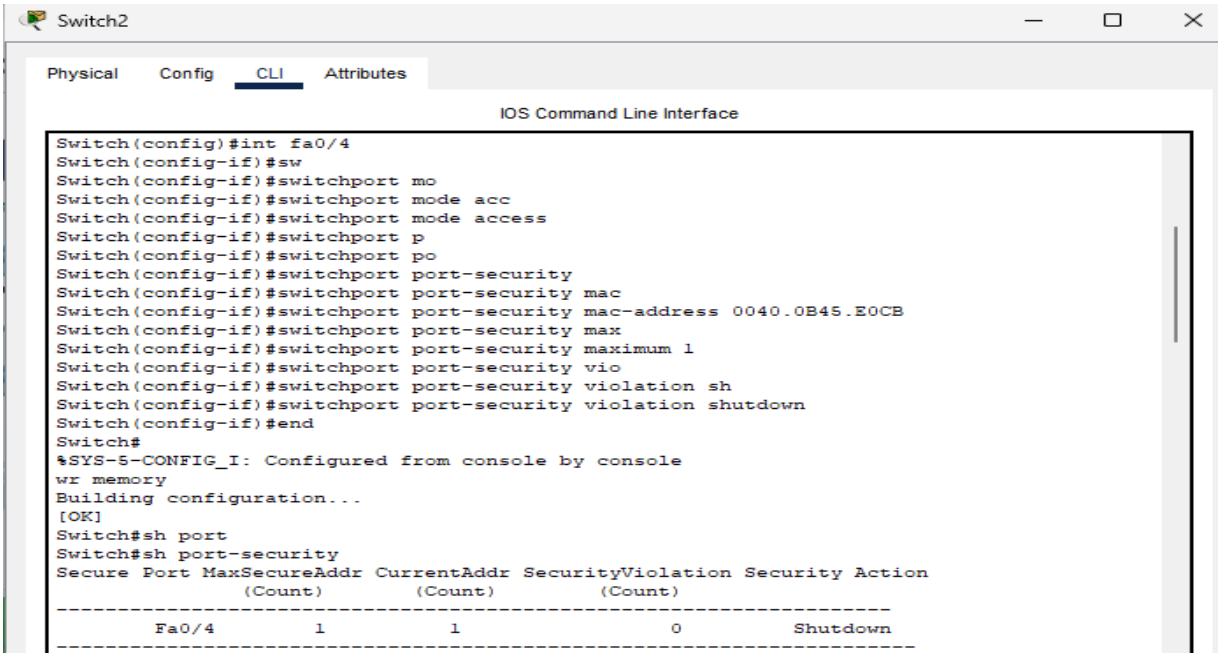
4. **Maximum MAC Addresses Allowed:**
    - Only one MAC address is allowed (maximum 1).

5. **Violation Mode:**
    - If a security violation occurs, the port will **shut down** (violation shutdown).

Verification Output (show port-security):

- **Port:** Fa0/4
- **MaxSecureAddr:** 1
- **CurrentAddr:** 1
- **SecurityViolation:** 0
- **Security Action:** Shutdown

This indicates that the port is currently secure, with one valid MAC address learned and no violations detected.



MAC Address Filtering :

Device: Wireless Router (CSEB(12345678))
Wireless Port: 2.4 GHz
Filtering Mode: MAC Address Filtering Enabled

Access Control Mode:
The option “Prevent PCs listed below from accessing the wireless network” is selected.

This means the MAC addresses listed in the filter list will be blocked from accessing the wireless network.

MAC Address Filter List:
Only one active MAC address is listed and being blocked:

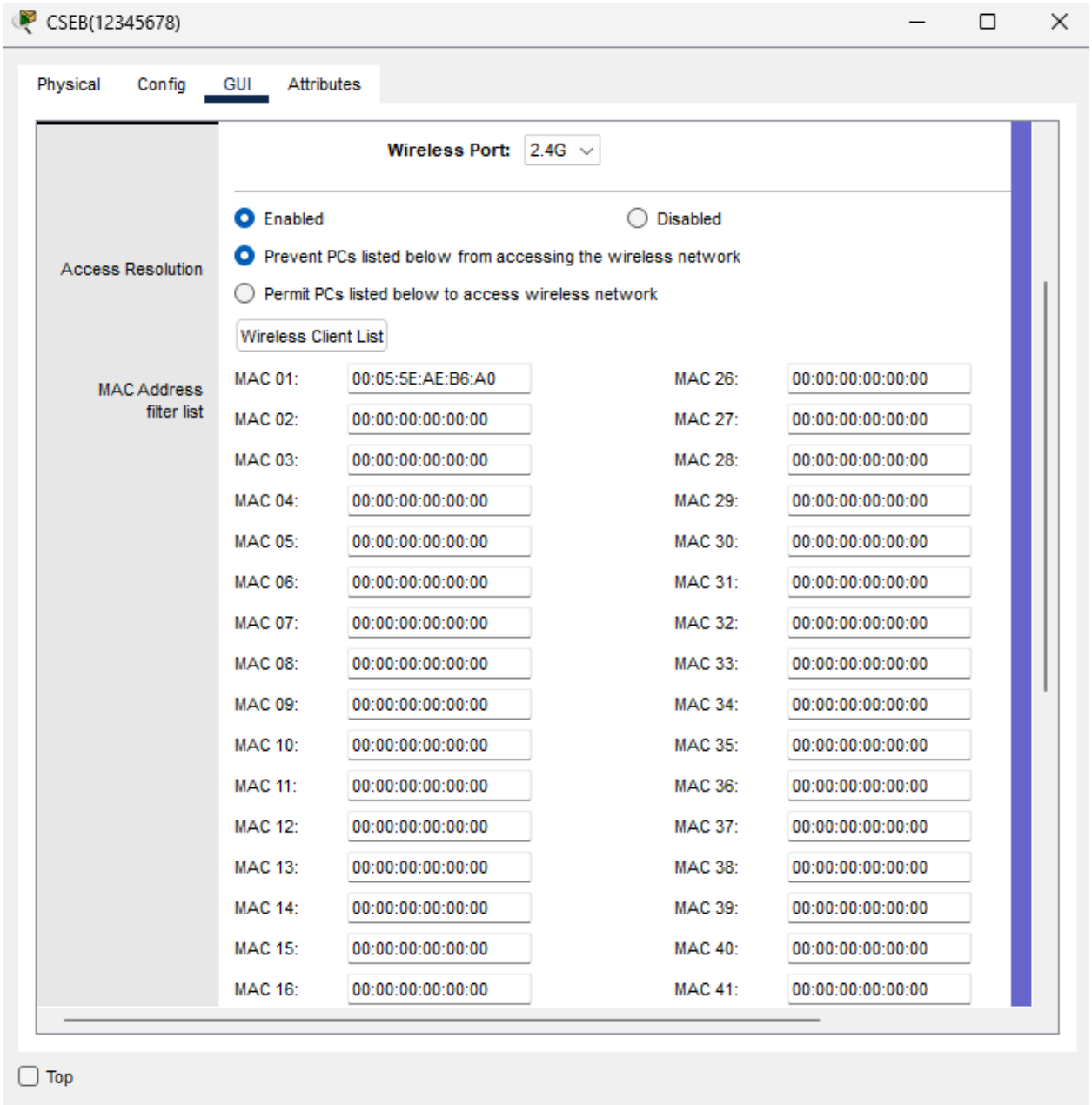
MAC 01: 00:05:5E:AE:B6:A0

All other fields contain 00:00:00:00:00:00, which are placeholders and do not affect access.

Security Implication:
This setup allows all devices to connect to the wireless network except the device with the MAC address 00:05:5E:AE:B6:A0.

MAC filtering adds a basic layer of security by limiting device access based on physical addresses. However, it can be bypassed

by MAC spoofing and should be used in conjunction with stronger security measures (like WPA2/WPA3 encryption)



Limitations

The project doesn't demonstrate all possible smart services. There are many more way to make a university smarter. There could be teacher's rooms, meeting rooms, smart car garage which automatically check in or check out cars by its number plate. Instant communication could be establish via IP phone. And many more. The security of IOT server and devices must be a serious concern. We are just presenting some basic concepts in this project.

Conclusion & Future Plan

The project shows only some basic IOT devices that is not enough to make a university smart. But from the project we can imagine how it could be done. The designed worked properly on cisco packet tracer simulator. Sometimes the simulator may generate errors but it will fix in a few seconds.

In future we needs more research to find out what we needs. If we can identify our needs we will able to develop the project much more. We can add more IOT devices more internet services etc. to make a fully smart university.

END