Green University of Bangladesh

Department of Computer Science and Engineering (CSE)
Semester: (Fall, Year: 2022), B.Sc. in CSE (Day)

Smart University Network System

Course Title: Computer Networking Lab
Course Code: CSE312
Section: 201D7

Students Details

Name	ID
Joy Munshi	201002143

Submission Date: 07-01-2023
Course Teacher's Name: Mr. Palash Roy

[For teachers use only: [Don't write anything inside this box]

Lab Project Status

Marks:	**Signature:**
Comments:	**Date:**

Contents

Chapter 1

Introduction

The University Smart Network System is designed to present a secure and reliable network system for an educational institution. It consists of a network system built using Cisco Packet Tracer, which is a powerful network simulator. This system will provide students, faculty, and staff with secure access to the university's servers and resources. It will also provide a secure and reliable communication system for the university's members, staff, and students.

The system will use telnet, remote SSH, firewall, and smart devices to provide secure access and reliable communication. Telnet will be used to access the university's servers, while remote SSH will allow users to securely connect to the university's network from any location. The firewall will protect the university's network from malicious attacks, while the smart devices will allow the university to monitor the network for any suspicious activities.

The system will also be equipped with a variety of security measures, such as strong passwords, encryption, and two-factor authentication. All of these measures will ensure that the university's network is secure and reliable. Additionally, the system will be able to handle large amounts of data and will be able to scale as the university's network grows.

Finally, the system will be able to easily integrate with other systems, such as learning management systems, student information systems, and student record systems. This will allow for seamless integration with the university's other systems and will ensure that the university's resources are secure and reliable.

The University Smart Network System will provide the university with a secure and reliable communication system that can easily scale and integrate with other systems. It will provide secure access and reliable communication for faculty, staff, and students. It will also provide a secure and reliable network system that can easily handle large amounts of data. Finally, it will be able to easily integrate with other systems, such as learning management systems, student information systems, and student record systems.

1.1 Overview

1. **Telnet:** Telnet is a protocol used for remote access to a computer. It allows users to log into a remote device, such as a router or switch, and execute

commands or transfer files. Telnet is commonly used in networking to allow remote access to a network device, such as a router or switch, to configure, monitor, or diagnose network devices.

2. **Remote SSH:** SSH (Secure Shell) is a secure remote access protocol that allows users to access a computer or device remotely over a network. SSH provides an encrypted connection and is used for secure file transfer and remote system administration.

3. **Firewall:** A firewall is a security device used to protect a network from unauthorized access. Firewalls can be hardware or software, and are used to filter traffic, allowing only specific types of traffic to pass through. Firewalls can be used to protect against malicious attacks, as well as to control access to resources, such as websites and applications.

4. **Smart Devices:** Smart devices are network-connected devices that are used to monitor and control physical devices, such as lights, locks, and security systems. Smart devices can be used to automate tasks, such as turning on lights when movement is detected, or locking a door when a user leaves a certain area

1.2 Motivation

The university smart network system is designed to facilitate secure and efficient communication and data transfer between students, faculty, staff, and other university personnel. The system uses telnet, remote ssh, firewalls, and smart devices in order to provide a secure environment for the users.

Telnet provides a text-based, command-line interface that allows users to remotely connect to a network. Telnet is used to communicate between student and faculty computers, as well as other smart devices such as tablets, smartphones, and other devices.

Remote SSH is used to securely access a network from a remote host. SSH provides secure communication and data transfer between multiple hosts, and is used to provide secure access to the university's network from remote locations.

Firewalls are used to protect the university's network from malicious attacks and other threats. Firewalls are configured to block unauthorized access to the network, and can also be used to monitor and control the flow of traffic over the network.

Smart devices are used to provide an easy way for users to interact with the network. Smart devices can be used to access the university's network from any location, and can be configured to provide secure access to the network.

Cisco Packet Tracer is a network simulation tool used to design, configure, and troubleshoot networks. Cisco Packet Tracer can be used to configure the university's network, as well as simulate and troubleshoot the network.

The motivation for this project is to build a university smart network system using Telnet, remote SSH, Firewall and smart devices. This system is designed to provide a secure, reliable and efficient network infrastructure that is scalable and can easily be managed and maintained. The system will provide secure remote access to university resources, and allow for the integration of smart devices into the university network. The system will also provide a secure and reliable connection to the internet, allowing students, faculty, and staff to access and use online resources. This project is expected to have a positive impact on student learning and performance, as well as increased efficiency in staff operations. I was actually inspired for this project when I read this article [1].

1.3 Problem Definition

1.3.1 Problem Statement

The problem we are trying to address with our university smart network system is the need to securely and efficiently connect all of the various devices on the university's network, including computers, smart devices, servers, and other networking equipment. To do this, we will be using a variety of technologies, including Telnet, Remote SSH, firewalls, DHCP, VLANs, and smart devices.
One of the key challenges we face is ensuring that all of these devices can communicate with each other in a secure and reliable manner. To address this, we will be implementing robust security measures, such as firewalls, to prevent unauthorized access to the network. Additionally, we will be using Telnet and Remote SSH to allow for remote access to the network and to enable administrators to remotely manage and troubleshoot any issues that may arise.
Another challenge is ensuring that the network can handle the high volume of traffic that is expected to be generated by the large number of devices that will be connected to it. To address this, we will be using DHCP to dynamically assign IP addresses to devices as they join the network, and we will be using VLANs to segment the network and help manage traffic.
Finally, we will be using smart devices, such as switches and routers, to help manage and optimize the performance of the network. By using Cisco Packet Tracer to simulate and test different network configurations, we can ensure that our university smart network system is able to meet the needs of the university and its students, faculty, and staff.

1.4 Design Goals/Objectives

The goals or objectives of our university smart network system project are:

- To securely and reliably connect all of the various devices on the university's network, including computers, smart devices, servers, and other networking equipment.

- To implement robust security measures, such as firewalls, to prevent unauthorized access to the network and protect against potential threats.

- To use Telnet and Remote SSH to allow for remote access to the network and enable administrators to remotely manage and troubleshoot any issues that may arise.

- To use DHCP to dynamically assign IP addresses to devices as they join the network, and to use VLANs to segment the network and help manage traffic.
- To use smart devices, such as switches and routers, to help manage and optimize the performance of the network.
- To use Cisco Packet Tracer to simulate and test different network configurations and ensure that they can handle the expected levels of traffic.
- To create a robust, secure, and efficient university smart network system that meets the needs of the university and its students, faculty, and staff.

1.5 Application

Our university smart network system project aims to create a secure and efficient network for a university that can connect all of the various devices used by students, faculty, and staff. This system will use a variety of technologies, including Telnet, Remote SSH, firewalls, DHCP, VLANs, and smart devices, to achieve its goals.

One key application of this project in the real world is the use of Telnet and Remote SSH to allow for remote access to the network. This is useful for administrators who need to remotely manage and troubleshoot the network, as well as for users who need to access resources on the network from off-campus locations.

Another important application is the use of firewalls to secure the network against potential threats. A firewall is a security system that controls incoming and outgoing network traffic based on predetermined security rules. By configuring the firewall to block or allow certain types of traffic, it is possible to protect the network from viruses, malware, and unauthorized access.

DHCP is another key technology that will be used in our university smart network system. DHCP allows for the automatic assignment of IP addresses to devices as they join the network, which can greatly simplify the process of setting up and configuring new devices.

VLANs are also an important part of our university smart network system. VLANs allow for the creation of virtual LANs within a single physical network, which can be useful for segmenting the network and managing traffic. For example, a university might use VLANs to create separate networks for faculty, staff, and students, or to create a separate network for a specific department or research group.

Finally, smart devices, such as switches and routers, will be used to help manage and optimize the performance of the network. These devices are equipped with advanced software and hardware that allows them to intelligently route and manage network traffic, helping to ensure that the network is running smoothly and efficiently.

Overall, our university smart network system project has the potential to greatly improve the connectivity and security of a university's network, enabling students, faculty, and staff to more effectively access the resources they need to succeed [1].

Chapter 2

Design/Development/Implementation of the Project

2.1 Introduction

First, we will begin by conducting a needs assessment to determine the specific requirements of the university's network. This will involve gathering information about the types of devices that will be connected to the network, the expected levels of traffic, and any specific security or other requirements.

Next, we will design the overall architecture of the network, taking into account the needs identified in the needs assessment and the capabilities of the various technologies that will be used. This will involve determining the specific configurations and settings for technologies such as Telnet, Remote SSH, firewalls, DHCP, VLANs, and smart devices.

Once the design of the network has been finalized, we will begin the development phase, which involves implementing and testing the various components of the network. This may involve installing and configuring servers, switches, and other networking equipment, as well as setting up Telnet and Remote SSH connections and configuring the firewall and other security measures.

Finally, once all of the components of the network have been developed and tested, we will move on to the implementation phase, which involves deploying the network in a live environment and ensuring that it is functioning as intended. This will involve performing final tests, making any necessary adjustments, and providing training and support to users as needed.

Overall, the design, development, and implementation of our university smart network system project will involve a collaborative effort between a team of network administrators and other IT professionals, and will require careful planning and execution to ensure that the final product meets the needs of the university and its users.

2.2 Project Details

Our university smart network system project aims to create a secure and efficient network for a university that can connect all of the various devices used by students, faculty, and staff. This system will use a variety of technologies, including Telnet, Remote SSH, firewalls, DHCP, VLANs, and smart devices, to achieve its goals.

2.2.1 Key Components

1. **SSH and Telnet** One key component of the project is the use of Telnet and Remote SSH to allow for remote access to the network. Telnet is a networking protocol that allows for the remote control of devices over a network, while Remote SSH is a more secure version of Telnet that uses encryption to protect data as it is transmitted. By using Telnet and Remote SSH, administrators will be able to remotely manage and troubleshoot the network, as well as provide users with the ability to access resources on the network from off-campus locations.

2. **Firewall** Another important component of the project is the use of firewalls to secure the network against potential threats. A firewall is a security system that controls incoming and outgoing network traffic based on predetermined security rules. By configuring the firewall to block or allow certain types of traffic, it is possible to protect the network from viruses, malware, and unauthorized access.

3. **DHCP** DHCP is another key technology that will be used in our university smart network system. DHCP allows for the automatic assignment of IP addresses to devices as they join the network, which can greatly simplify the process of setting up and configuring new devices. By using DHCP, network administrators will be able to quickly and easily add new devices to the network without having to manually assign IP addresses.

4. **VLAN** VLANs are also an important part of our university smart network system. VLANs allow for the creation of virtual LANs within a single physical network, which can be useful for segmenting the network and managing traffic. For example, a university might use VLANs to create separate networks for faculty, staff, and students, or to create a separate network for a specific department or research group. By using VLANs, network administrators will be able to more easily manage and control the flow of traffic on the network.

Finally, smart devices, such as switches and routers, will be used to help manage and optimize the performance of the network. These devices are equipped with advanced software and hardware that allows them to intelligently route and manage network traffic, helping to ensure that the network is running smoothly and efficiently. By using smart devices, network administrators will be able to more easily monitor and troubleshoot the network, as well as make adjustments

to improve its performance.
Overall, our university smart network system project will involve the careful planning and implementation of a range of technologies to create a secure and efficient network that meets the needs of the university and its users.

2.3 Implementation

2.3.1 Planning

The workflow

The work flow for our university smart network system project would typically involve the following steps:

1. Conduct a needs assessment to determine the specific requirements of the university's network, including the types of devices that will be connected, the expected levels of traffic, and any specific security or other requirements.
2. Design the overall architecture of the network, taking into account the needs identified in the needs assessment and the capabilities of the various technologies that will be used. This will involve determining the specific configurations and settings for technologies such as Telnet, Remote SSH, firewalls, DHCP, VLANs, and smart devices.
3. Begin the development phase, which involves implementing and testing the various components of the network. This may involve installing and configuring servers, switches, and other networking equipment, as well as setting up Telnet and Remote SSH connections and configuring the firewall and other security measures.

2.3.2 Componets Required

Tools and libraries

The tools and libraries that would be used in our university smart network system project would depend on the specific technologies and devices being used. Some of the tools and libraries that might be used in this type of project include:

- Switch: A switch is a networking device that connects devices on a network and forwards data between them. Switches can be used to segment the network into smaller subnetworks, helping to improve performance and manage traffic.
- Cisco 2811 router: A Cisco 2811 router is a networking device that connects devices on a network and forwards data between them. It can be used to connect devices to the internet, as well as to create and manage virtual LANs (VLANs).

- PC: A personal computer (PC) is a general-purpose computer that can be used for a variety of tasks, including word processing, internet browsing, and running specialized software.

- Laptop: A laptop is a portable computer that can be easily carried and used in a variety of locations.

- Servers: A server is a computer or device that provides services to other computers or devices on a network. Servers can be used to store and manage data, run applications, and provide access to resources such as printers and scanners.

- Fan: A fan is a mechanical device that is used to circulate air and keep a room or device cool.

- Light: A light is a device that produces light and is used to illuminate an area or provide visibility.

- Door: A door is a movable structure that is used to open and close an entrance to a building or room.

- Window: A window is an opening in a wall or roof that allows light and air to enter a building or room.

2.4 Implementation Details

Ip Configuration

Place all of the components according to the design of the network. This may involve installing servers, switches, routers, and other networking equipment in the appropriate locations. Building C is our Control room.Here I have use class 3 IP for lab end devices and class 1 Ip for cloud and line connections.

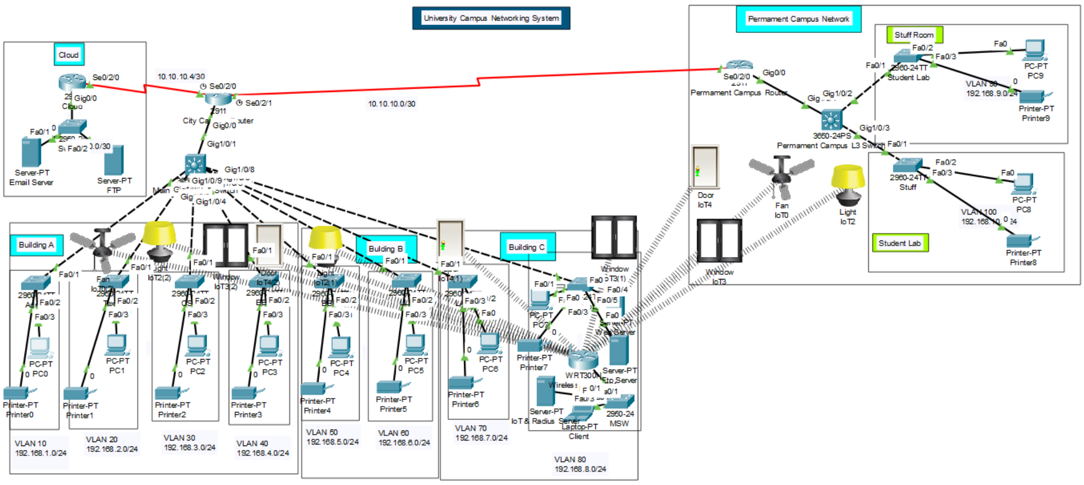
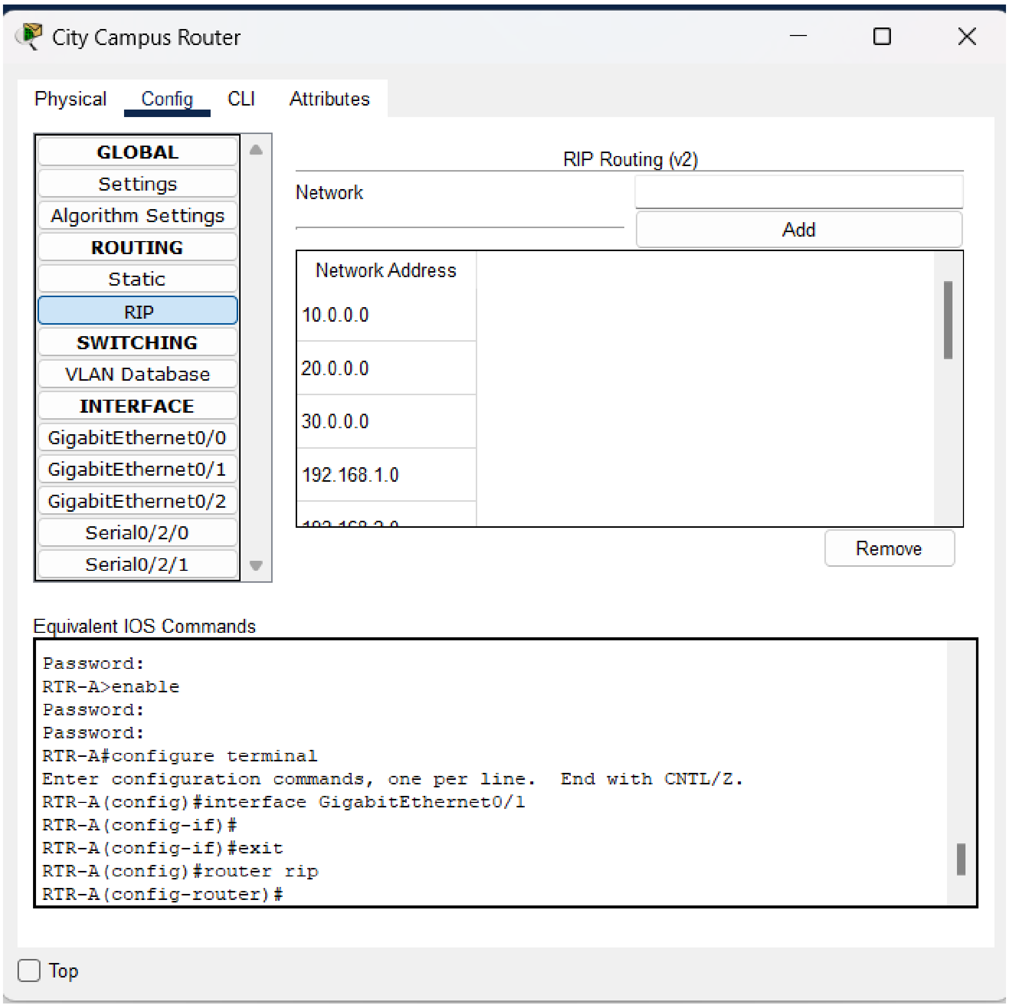


Figure 2.1: IP Configuration

Rip Configure

Generally will follow:
I have given all network ip between 3 routers (router network ip and interface ip)

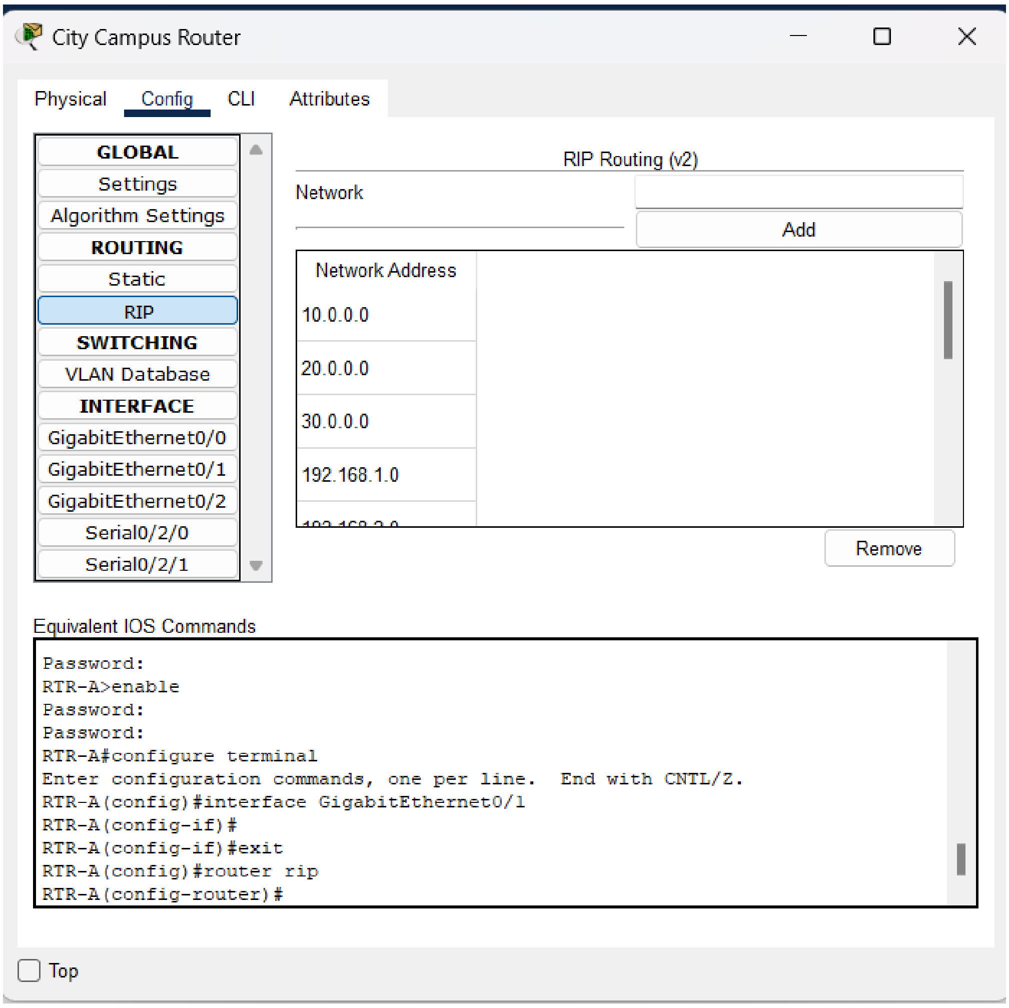


Network Address
10.0.0.0
20.0.0.0
30.0.0.0
192.168.1.0
192.168.2.0

Equivalent IOS Commands

```
Password:
RTR-A>enable
Password:
Password:
RTR-A#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RTR-A(config)#interface GigabitEthernet0/1
RTR-A(config-if)#
RTR-A(config-if)#exit
RTR-A(config)#router rip
RTR-A(config-router)#
```

Figure 2.2: RIP Configuretion



Network Address
10.0.0.0
20.0.0.0
30.0.0.0
192.168.1.0

Equivalent IOS Commands

```
Password:
RTR-A>enable
Password:
Password:
RTR-A#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RTR-A(config)#interface GigabitEthernet0/1
RTR-A(config-if)#
RTR-A(config-if)#exit
RTR-A(config)#router rip
RTR-A(config-router)#
```

Figure 2.3: RIP Configuration

Vlan Configuration

In Vlan configuration I have use 10,20,30,40,50,60,70,80,90,100 vlans. I have use dot1q encapsulation in every Vlans [2] .

Vlan Configuretion

```
#####################################
Vlan Config for all router
###################################

Router>en
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/0.10
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed state to up

Router(config-subif)#encapsulation dot1Q
% Incomplete command.
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip add
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#ex
Router(config)#int gig0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up

Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#ex
Router(config)#int gig0/0.30
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up

Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#ex
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#int gig0/0.40
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.40, changed state to up

Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.4.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#ex
Router(config)#
Router(config)#
Router(config)#
Router(config)#int gig0/0.50
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.50, changed state to up

Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip address 192.168.5.1 255.255.255.0
Router(config-subif)#ex
Router(config)#int gig0/0.60
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.60, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.60, changed state to up

Router(config-subif)#
Router(config-subif)#encapsulation dot1Q 60
Router(config-subif)#ip address 192.168.6.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#ex
Router(config)#
```

Dynamic IP Configuration

After creating VLAN for each switch we configured DHCP for City and permanent campus router. We set class 3 ip corresponding to VLANS. Here are the following CLI commands: .

Dynamic IP Configuration

```
######################
Config main campus dynamic IP
##########################

Router>en
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/0.10
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.10, changed state to up

Router(config-subif)#encapsulation dot1Q
% Incomplete command.
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip add
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#ex
Router(config)#int gig0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up

Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
Router(config-subif)#ex
Router(config)#int gig0/0.30
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up

Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
Router(config-subif)#ex
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#int gig0/0.40
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.40, changed state to up

Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.4.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#ex
Router(config)#
Router(config)#
Router(config)#
Router(config)#int gig0/0.50
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.50, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.50, changed state to up

Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip address 192.168.5.1 255.255.255.0
Router(config-subif)#ex
Router(config)#int gig0/0.60
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.60, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.60, changed state to up

Router(config-subif)#
Router(config-subif)#encapsulation dot1Q 60
Router(config-subif)#ip address 192.168.6.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#
Router(config-subif)#ex
Router(config)#
```

SSH Configure

To configure Secure Shell (SSH) in the implementation of a network, Here I have set the password minimum length to 10. The banner command is used for unwanted access. Then I set a condition that no password of 7 seconds will terminate the connection and I also set a condition that after 45 attempts it will block the user. Password will be encrypted using rsa algorithm and it will follow aaa new model. The following steps would typically be followed: .

SSH Configuration

```
RTR-A#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RTR-A(config)#interface g0/0
RTR-A(config-if)#no aaa new-model
RTR-A(config)#no ip domain-lookup
RTR-A(config)#interface g0/0
RTR-A(config-if)#ip address 192.168.12.1
% Incomplete command.
RTR-A(config-if)#ip address 192.168.12.1 255.255.255.0
RTR-A(config-if)#no sh
RTR-A(config-if)#exit
RTR-A(config)#banner mtod @ Unathorized Access Not Allowed @
                      ^
% Invalid input detected at '^' marker.

RTR-A(config)#banner m0td @ Unathorized Access Not Allowed @
                      ^
% Invalid input detected at '^' marker.

RTR-A(config)#banner motd @ Unathorized Access Not Allowed @
RTR-A(config)#security password min-length 10.
                                           ^
% Invalid input detected at '^' marker.

RTR-A(config)#security password min-length 10
RTR-A(config)#line console 0
RTR-A(config-line)#exec-timeout 7 0
RTR-A(config-line)#password joymunshi12345
RTR-A(config-line)#login
RTR-A(config-line)#line vty 0 4
RTR-A(config-line)#exec-timeout 7 0
RTR-A(config-line)#password joymunshi12345
RTR-A(config-line)#login
RTR-A(config-line)#transport input ssh
RTR-A(config-line)#ip domain-name gigts.org
RTR-A(config)#crypto key generate rsa
% You already have RSA keys defined named RTR-A.ggts.org .
% Do you really want to replace them? [yes/no]: 1024
% Please answer 'yes' or 'no'.
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: RTR-A.gigts.org
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

RTR-A(config)#username joy secret joymunshi12345
*Mar 1 0:28:33.336: %SSH-5-ENABLED: SSH 1.99 has been enabled
RTR-A(config)#aaa new-model
RTR-A(config)#enable secret joymunshi12345
RTR-A(config)#service password-encryption
RTR-A(config)#login block-for 45 attemts 3 within 100
                                      ^
% Invalid input detected at '^' marker.

RTR-A(config)#login block-for 45 attempts 3 within 100
RTR-A(config)#
RTR-A#
%SYS-5-CONFIG_I: Configured from console by console
```

Telnet Configuration

I configured each switch telnet according to vlan. Here I have set the password minimum length to 10. The banner command is used for unwanted access. Then

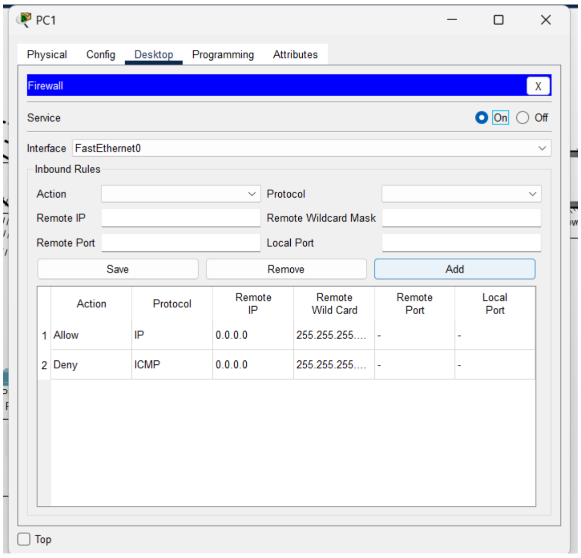
I set a condition that no password in 7 seconds will terminate the connection and I also set a condition that after 45 attempts it will block the user. Password will be encrypted using rsa algorithm and it will follow aaa new model. The following steps would typically be followed: .

Telnet Configuretion

```
Switch>en
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname RTR
RTR(config)#hostname SW1
SW1(config)#interface vlan 10
SW1(config-if)#ip address 192.168.1.10 255.255.255.0
SW1(config-if)#no sh
SW1(config-if)#exit
SW1(config)#banner motd @ Unauthorized Access Not Allowed @
SW1(config)#secrurity password min-length 10
SW1(config)#line console 0
SW1(config-line)#exec-timeout 7 0
SW1(config-line)#password joymunshi12345
SW1(config-line)#login
SW1(config-line)#
SW1#
%SYS-5-CONFIG_I: Configured from console by console
```

Firewall Configuretion

I blocked all ICMP on the firewall. But I have approved the IP.



Service ● On ○ Off

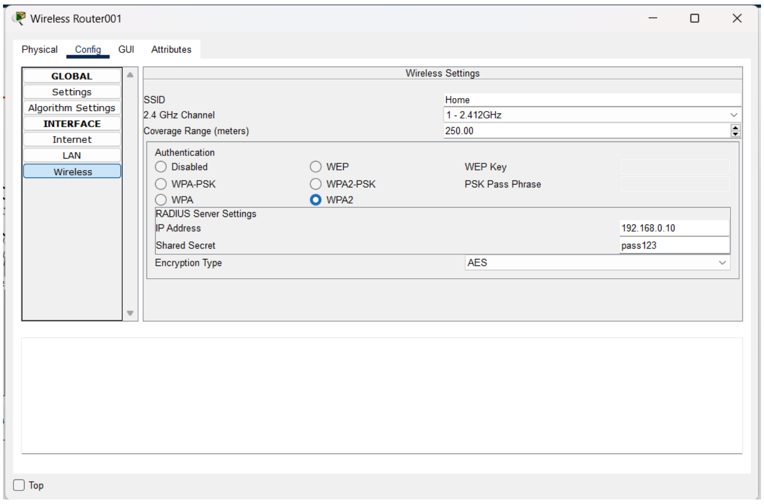
Interface FastEthernet0

	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1	Allow	IP	0.0.0.0	255.255.255....	-	-
2	Deny	ICMP	0.0.0.0	255.255.255....	-	-

Figure 2.4: Firewall Configuretion

Iot Device Configuretions

First we will configure the wireless router then we will configure all IoT devices



Wireless Settings

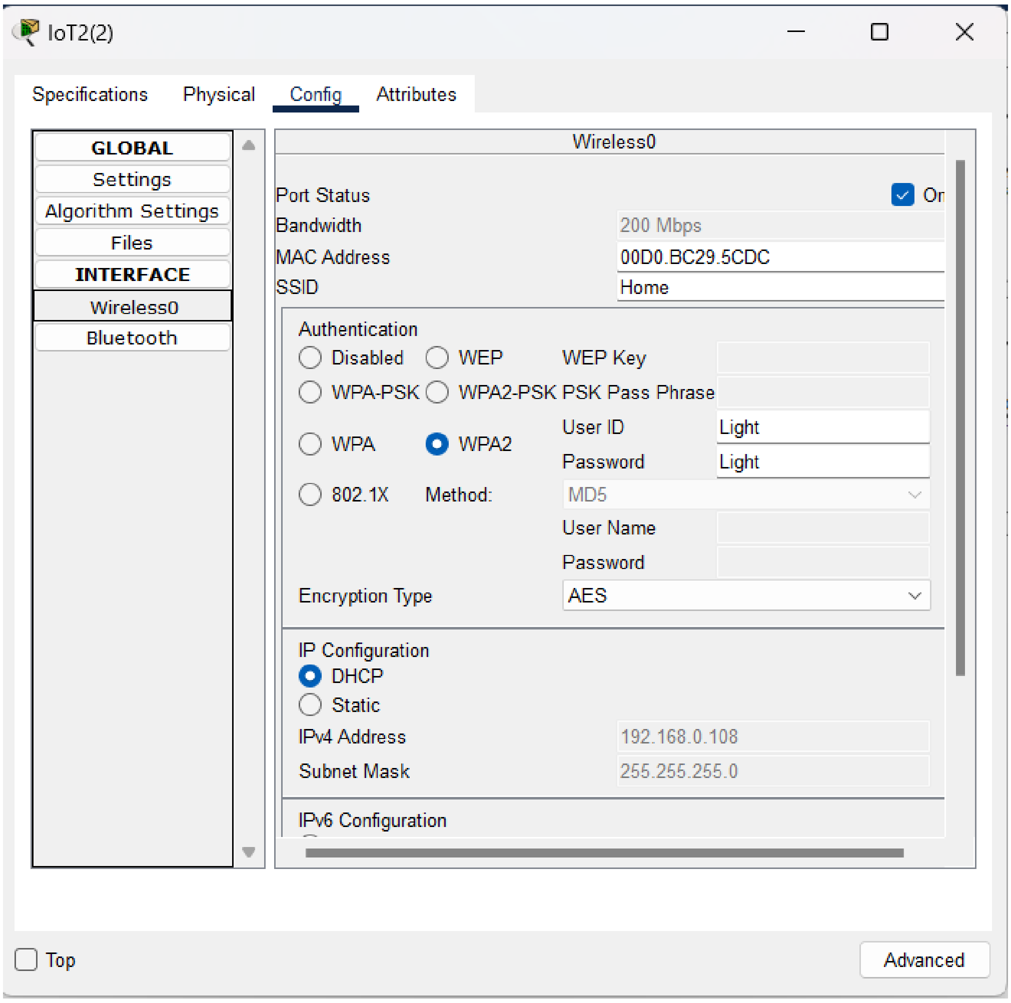
SSID: Home
2.4 GHz Channel: 1 - 2.412GHz
Coverage Range (meters): 250.00

Authentication
○ Disabled ○ WEP WEP Key
○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase
○ WPA ● WPA2

RADIUS Server Settings
IP Address: 192.168.0.10
Shared Secret: pass123

Encryption Type: AES

Figure 2.5: Wireless router Configuretion



Wireless0

Port Status ☑ On
Bandwidth: 200 Mbps
MAC Address: 00D0.BC29.5CDC
SSID: Home

Authentication
○ Disabled ○ WEP WEP Key
○ WPA-PSK ○ WPA2-PSK PSK Pass Phrase
○ WPA ● WPA2 User ID: Light
Password: Light
○ 802.1X Method: MD5
User Name
Password
Encryption Type: AES

IP Configuration
● DHCP
○ Static
IPv4 Address: 192.168.0.108
Subnet Mask: 255.255.255.0

IPv6 Configuration

Figure 2.6: Iot Device Configuretion

Chapter 3

Performance Evaluation

3.1 Simulation Environment/ Simulation Procedure

To test SSH and Telnet and Iot devices using ICMP. We need to disable the firewall then open our central PC.

3.1.1 SSH Test

First open Pc7 then goto desktop->CMD.Then type "telnet 192.168.8.80".then it will goto switch 7 configuration mode.we have to enter the password joy1234 then we can enter the switch.If we want to go switch configure mode it will ask for password again.If 2 times failed it. [?]

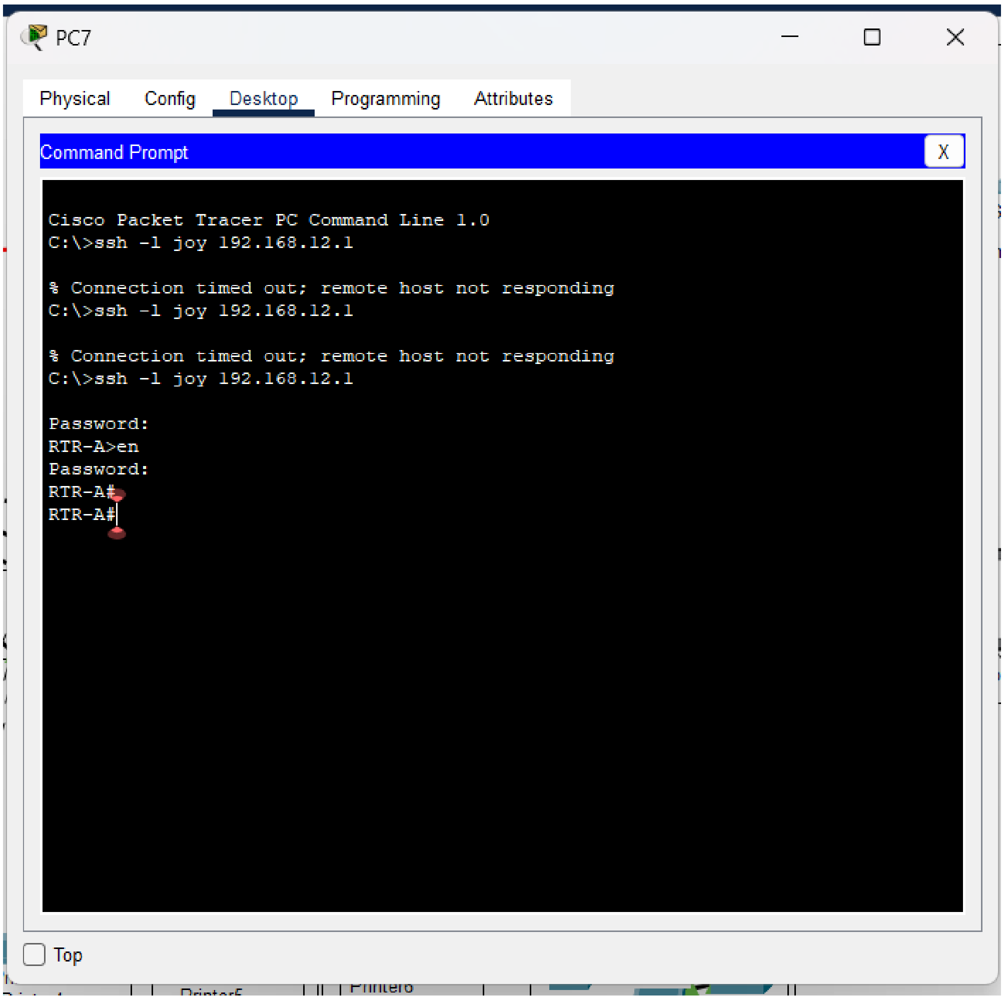
3.1.2 Telnet Test

To test telnet we need to open CLI of PC7. If we want to access the first switch in the city campus that is VLAN 10. We need to enter telnet 192.168.1.10. Then it will open the switch and if we give N command it will. Ask for a password again to enable switch terminal. [3]

3.2 Results Analysis/Testing

3.2.1 SSH

See we can access the router from PC7.

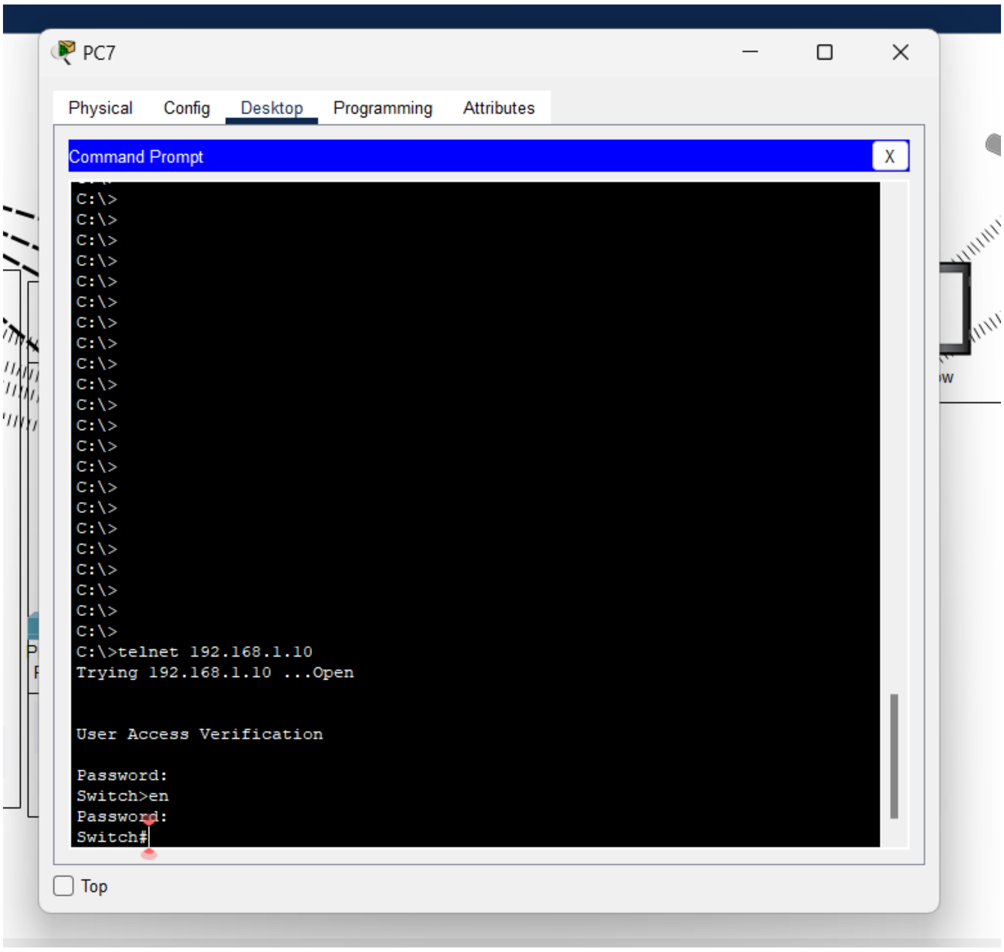


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l joy 192.168.12.1

% Connection timed out; remote host not responding
C:\>ssh -l joy 192.168.12.1

% Connection timed out; remote host not responding
C:\>ssh -l joy 192.168.12.1

Password:
RTR-A>en
Password:
RTR-A#
RTR-A#
```

Figure 3.1: Output Of SSH Configuration

3.2.2 Telnet Test

See we can access switches admin panel using PC7

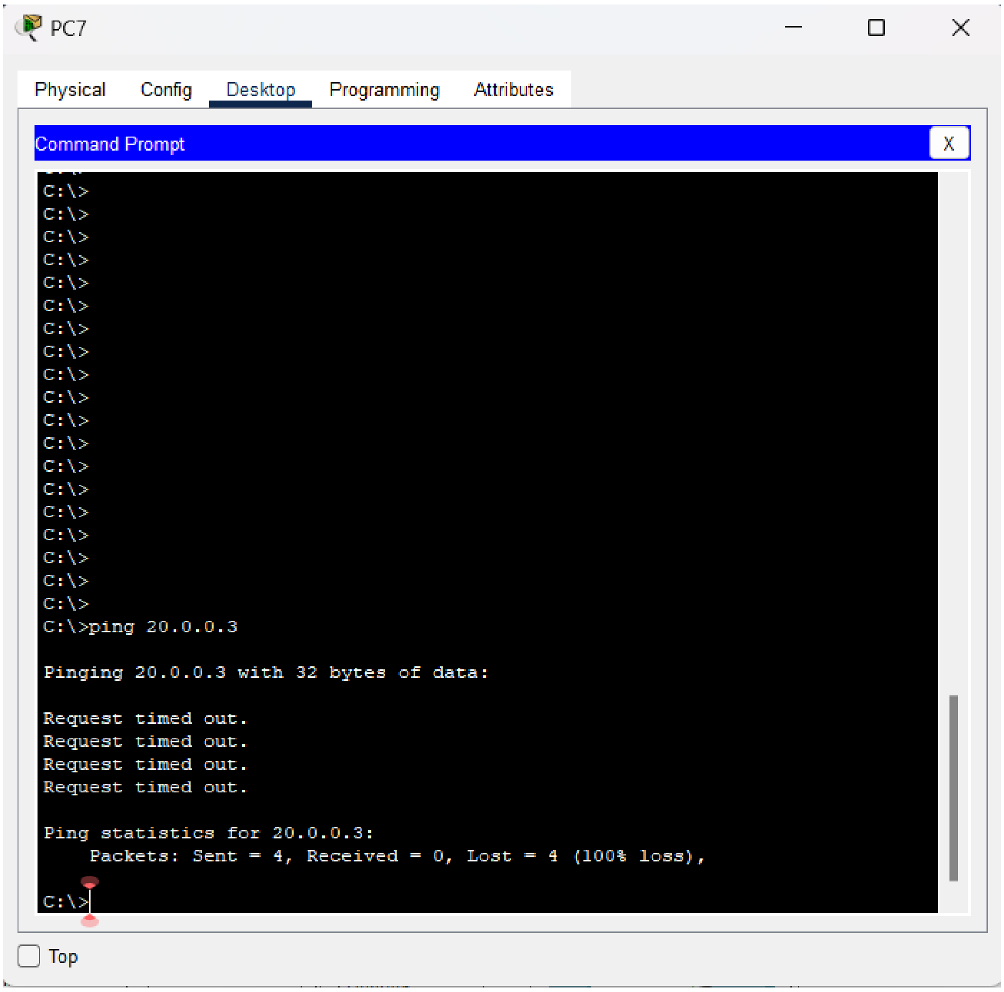


```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>telnet 192.168.1.10
Trying 192.168.1.10 ...Open


User Access Verification

Password:
Switch>en
Password:
Switch#
```

Figure 3.2: A graphical result of your project

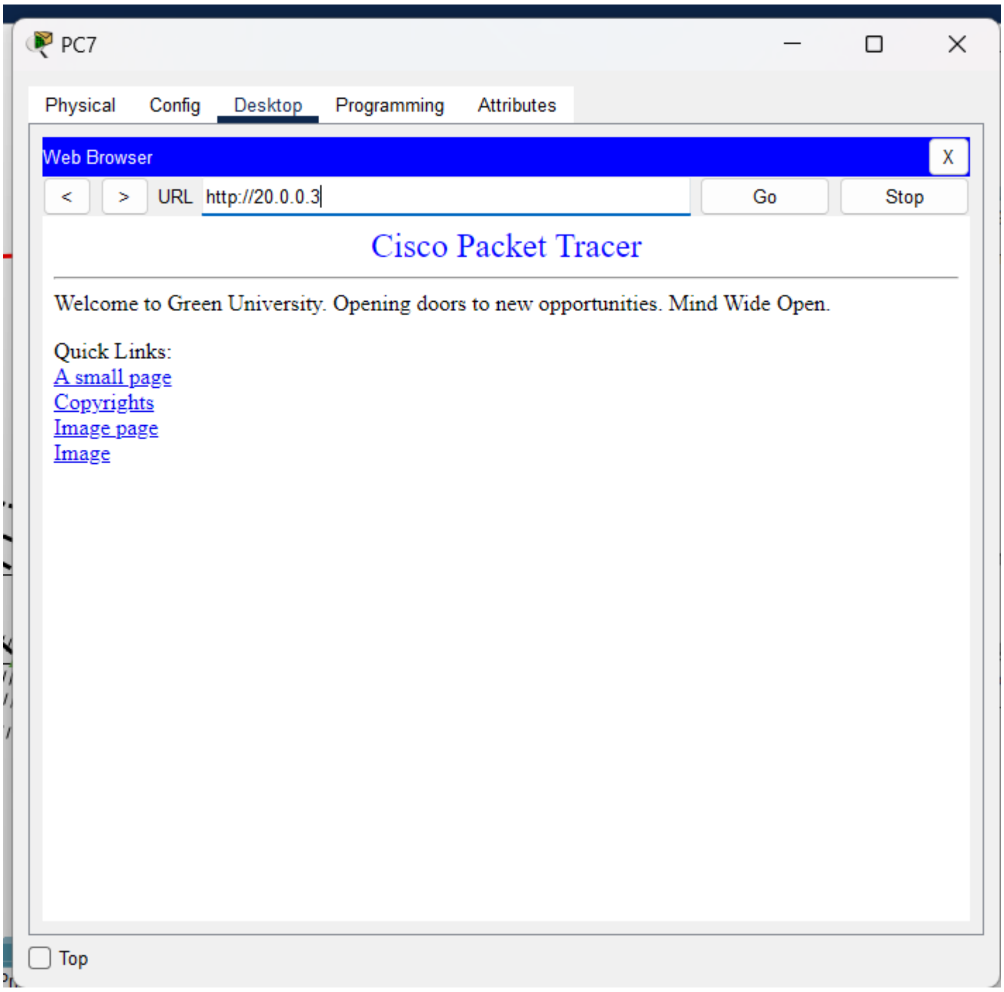
Firewall Test

As I said before the firewall only allows IP. This will block ICMP. Let's look at the figure3.4.If we try to connect webserver through ip,it will deny



```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 20.0.0.3

Pinging 20.0.0.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 20.0.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 3.3: Firewall ping



http://20.0.0.3

Cisco Packet Tracer

Welcome to Green University. Opening doors to new opportunities. Mind Wide Open.

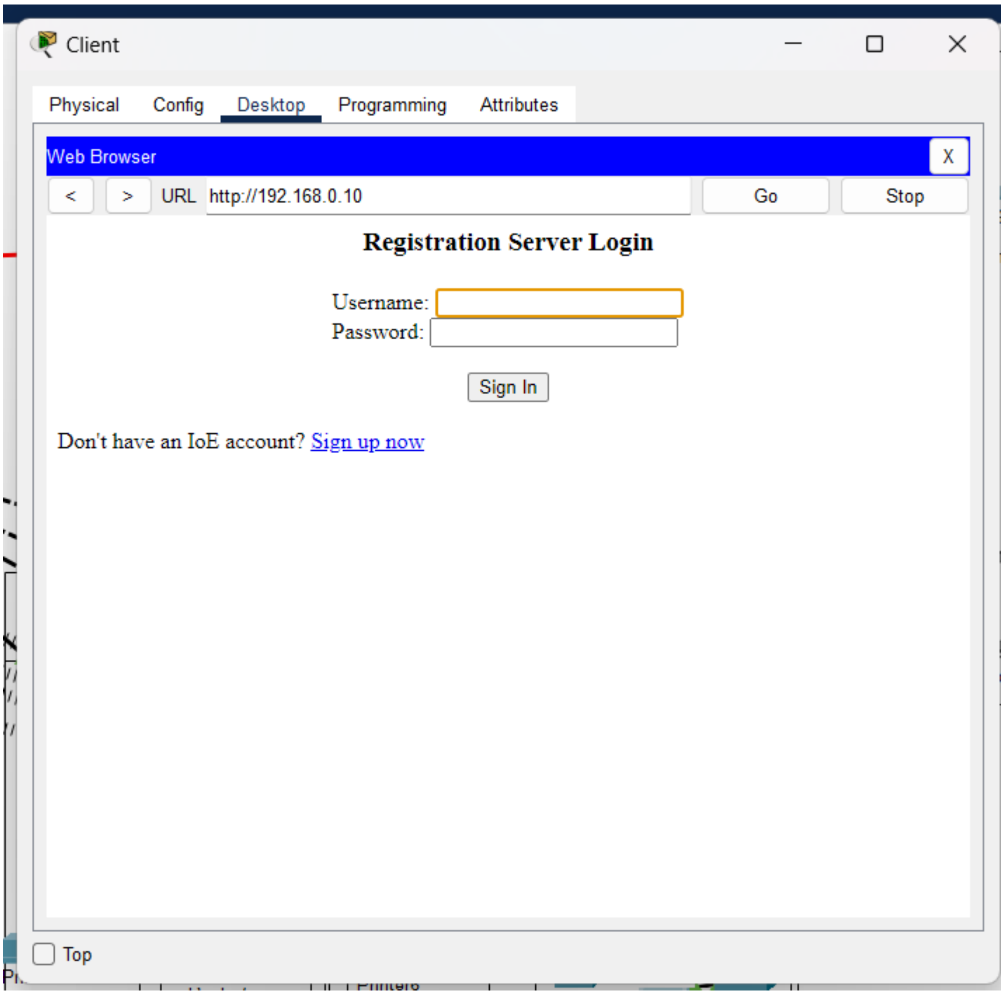
Quick Links:
A small page
Copyrights
Image page
Image

Figure 3.4: Firewall IP

If we try to connect throuh IP.It will successfully connect to website.

3.2.3 Iot Devices Test

Here we can control all door,light,fan from one laptop of building C.First we have to login. Then we can control all IoT devices



http://192.168.0.10

Registration Server Login

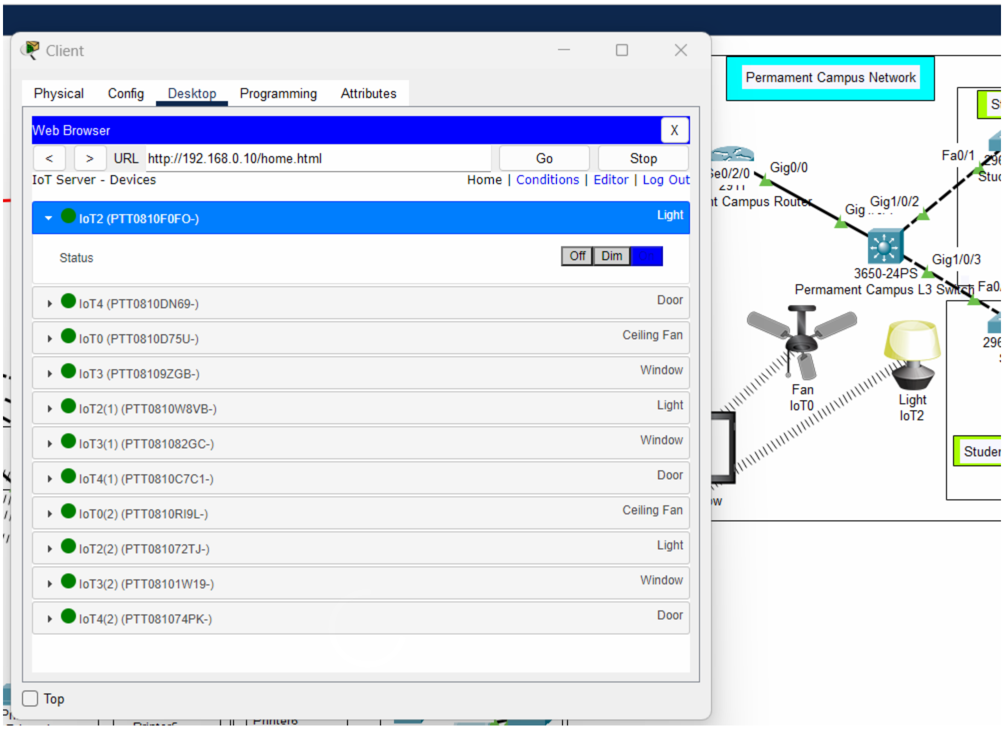
Username:

Password:

Sign In

Don't have an IoE account? Sign up now

Figure 3.5: Router Login


Client

Physical | Config | Desktop | Programming | Attributes

Web Browser

URL http://192.168.0.10/home.html

IoT Server - Devices

Home | Conditions | Editor | Log Out

```
▾ ● IoT2 (PTT0810F0FO-)          Light
    Status                       Off  Dim  On
▸ ● IoT4 (PTT0810DN69-)          Door
▸ ● IoT0 (PTT0810D75U-)          Ceiling Fan
▸ ● IoT3 (PTT08109ZGB-)          Window
▸ ● IoT2(1) (PTT0810W8VB-)       Light
▸ ● IoT3(1) (PTT081082GC-)       Window
▸ ● IoT4(1) (PTT0810C7C1-)       Door
▸ ● IoT0(2) (PTT0810RI9L-)       Ceiling Fan
▸ ● IoT2(2) (PTT081072TJ-)       Light
▸ ● IoT3(2) (PTT08101W19-)       Window
▸ ● IoT4(2) (PTT081074PK-)       Door
```

□ Top

Figure 3.6: Iot Devices

3.3 Results Overall Discussion

So first we configured SSH remote login for admin named joy.which is working perfectly Then we want telnet remote login for admin which is working perfectly We have added firewall to our website which is fully working. But we can not access Permament campus router from city campus router.Same problem telnet also.The project may be constrained by limited budget, personnel, or other resources, which could impact its ability to achieve its goals.

Chapter 4

Conclusion

4.1 Discussion

In this chapter, we discussed the design, development, and implementation of a university smart network system using a variety of technologies such as Telnet, Remote SSH, firewalls, DHCP, VLANs, and smart devices. We described the work flow of the project, including the steps involved in conducting a needs assessment, designing the network architecture, developing and testing the various components, and implementing the network in a live environment. We also discussed the tools and libraries that might be used in such a project, as well as the steps involved in configuring RIP and SSH. Finally, we listed some of the potential problems that could be encountered during the project and the importance of careful planning and troubleshooting to address these issues. Overall, the university smart network system project is a complex undertaking that requires a thorough understanding of networking technologies and a systematic approach to design, development, and implementation.

4.2 Limitations

There are a number of limitations that could potentially impact the success of a university smart network system project. Some of the key limitations to consider include:

1. Budget constraints: One of the major limitations of any IT project is the budget available for its development and implementation. A university smart network system is likely to involve the procurement of a variety of hardware and software components, which can be costly. Ensuring that there is sufficient budget to cover these costs and any unforeseen expenses that may arise is crucial to the success of the project.

2. Personnel constraints: Another key limitation is the availability of personnel with the necessary expertise to design, develop, and implement the network. Ensuring that the team working on the project has the necessary skills and experience is essential to its success.

3. Compatibility issues: As mentioned earlier, the university smart network system is likely to be comprised of a variety of different devices and operating systems, which could lead to compatibility issues when trying to connect them all together. Ensuring that all of the components of the network are compatible and able to work together seamlessly is essential to its success.

4. Security risks: Another important consideration is the potential for security breaches on the network. Ensuring that the network is properly secured and protected against threats such as viruses, malware, and unauthorized access is crucial to its success.

To address these and other limitations, it will be important to carefully plan and manage the project, as well as to have robust systems in place for monitoring and troubleshooting any issues that may arise. It will also be important to conduct ongoing critical analysis of the project to identify and address any limitations or problems as they arise.

4.3 Scope of Future Work

There are many potential directions that a university smart network system project could take in the future. Some possible areas for further work and extension of the project could include:

1. Network expansion: As the university grows and the number of devices on the network increases, it may be necessary to expand the network to accommodate these additional devices. This could involve adding more servers, switches, and other networking equipment to the network, as well as upgrading the capacity of existing components.

2. Network optimization: Another potential area of focus could be optimizing the performance of the network to ensure that it is running smoothly and efficiently. This could involve identifying and addressing bottlenecks or other issues that may be impacting the network's performance, as well as making adjustments to the configuration of the network to improve its efficiency.

3. Network security: Ensuring the security of the network will likely be an ongoing concern, and there may be a need to continually update and improve the network's security measures to keep up with evolving threats. This could involve implementing new technologies or protocols, as well as conducting regular security audits to identify and address potential vulnerabilities.

4. Integration with other systems: Another potential area of focus could be integrating the university smart network system with other systems and technologies, such as learning management systems, student information systems, or other systems used by the university.

5. User support: Finally, there may be a need to provide ongoing support and training to users of the network to ensure that they are able to effectively

use the network and its resources. This could involve providing documentation, user guides, and other resources, as well as offering in-person or online training sessions.

Overall, the future work of a university smart network system project will depend on the specific needs and goals of the university, as well as the evolving landscape of IT technologies and trends.

References

[1] Ankur Utsav, Amit Abhishek, Annu Kumari, and Himanshu Raj Daksh. Smart irrigation system using cisco packet tracer. In *2022 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*, pages 297–301. IEEE, 2022.

[2] N Hari Prasad, B Karunakar Reddy, B Amarnath, and M Puthanial. Intervlan routing and various configurations on vlan in a network using cisco packet tracer. *International Journal for Innovative Research in Science and Technology*, 2(11):749–758, 2016.

[3] Sotiris Ioannidis, Angelos D Keromytis, Steve M Bellovin, and Jonathan M Smith. Implementing a distributed firewall. In *Proceedings of the 7th ACM conference on Computer and communications security*, pages 190–199, 2000.