DATA COMMUNICATION AND COMPUTER NETWORKING

Project Report: Design and of a Simulated Networking using Cisco Packet Tracer

Names	Muneeb Ahmad
Registration Numbers	FA21-BEE-145
Class	BEE-6B
Instructor's Name	Dr. Ali Mustafa

Lab Assessment

Pre-Lab	**In-Lab**	**Post Lab**			**Total**
		Data Presentation	**Data Analysis**	**Writing Style**	

Title:

Design and Testing of a Simulated Network using Cisco Packet Tracer

1. Introduction

This report presents the design and testing of a small simulated network using Cisco Packet Tracer. The network consists of four personal computers (PCs), two switches, one router, and a simulated firewall configuration. The goal of this simulation is to understand basic network design principles and to implement a simple security mechanism through firewall rules.

2. Objectives

1. To design a basic LAN setup using Cisco Packet Tracer.
2. To connect multiple PCs using switches and routers.
3. To test communication using **ping** and **message transfer** between PCs.
4. To apply basic firewall rules to **allow or block traffic**.

3. Network Components Used

Component	Quantity
PCs	4
Switches	2
Router	1
Copper	As needed
Packet Tracer Firewall	1

4. Network Design

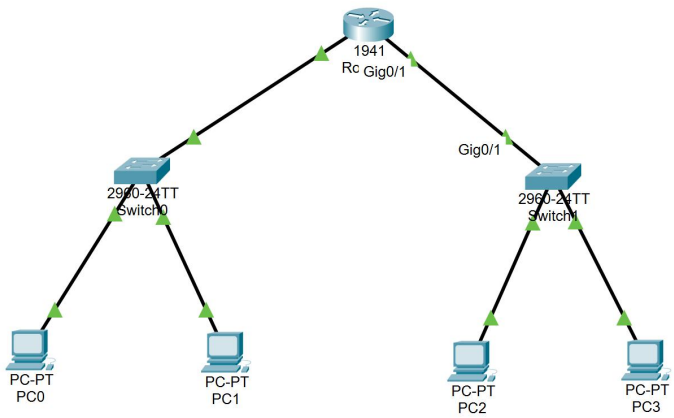


Figure 1: Network using Cisco Packet Tracer

1. **PC0 and PC1** are connected to **Switch0**.
2. **PC2 and PC3** are connected to **Switch1**.
3. Both switches are connected to **Router0** using straight-through cables.

The router is configured with two interfaces to handle traffic between both switches.

Static IPs were assigned to each PC.

Firewall rules (Access Control Lists - ACLs) were applied on the router to:

Allow certain traffic (e.g., only PC0 can access PC2)

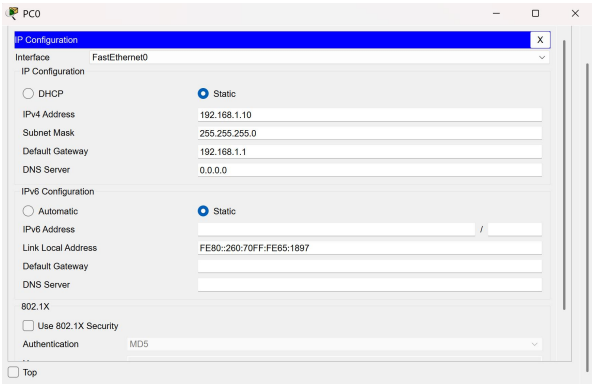
Deny other traffic (e.g., block PC1 from accessing PC0)

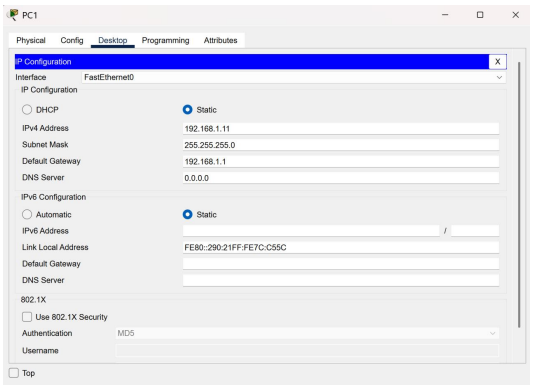
5. IP Addressing Scheme

Router:

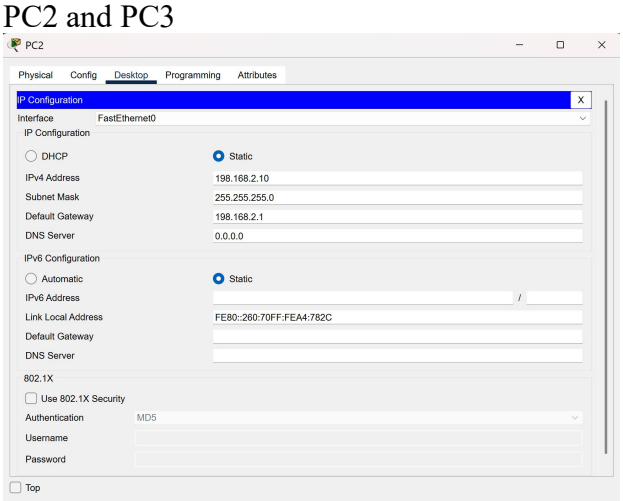
```
        --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface g0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#interface g0/1
Router(config-if)#ip address 198.168.2.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

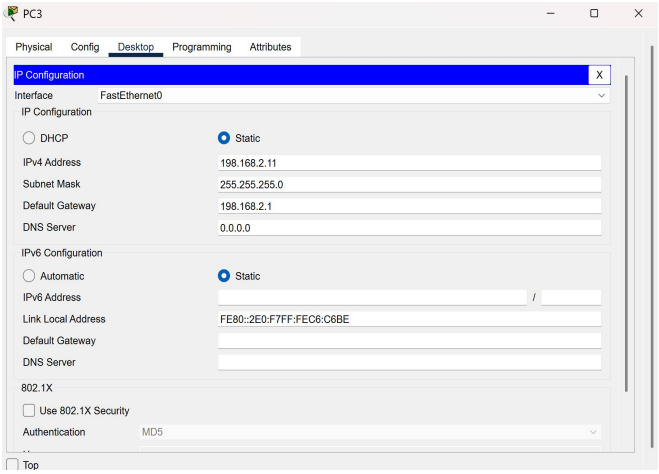
PC0 and PC1





PC2 and PC3





Device	IP Address	Subnet Mask
PCO	192.168.1.10	255.255.255.0
PC1	192.168.1.11	255.255.255.0
PC2	198.168.2.10	255.255.255.0
PC3	198.168.2.11	255.255.255.0
Router0(g0/0)	192.168.1.1	255.255.255.0
Router0(g0/1)	198.168.2.1	255.255.255.0

6. Firewall Configuration

1. To **Allow PC2 to access PC0.**
2. To **Block PC1 from Accessing PC0**.

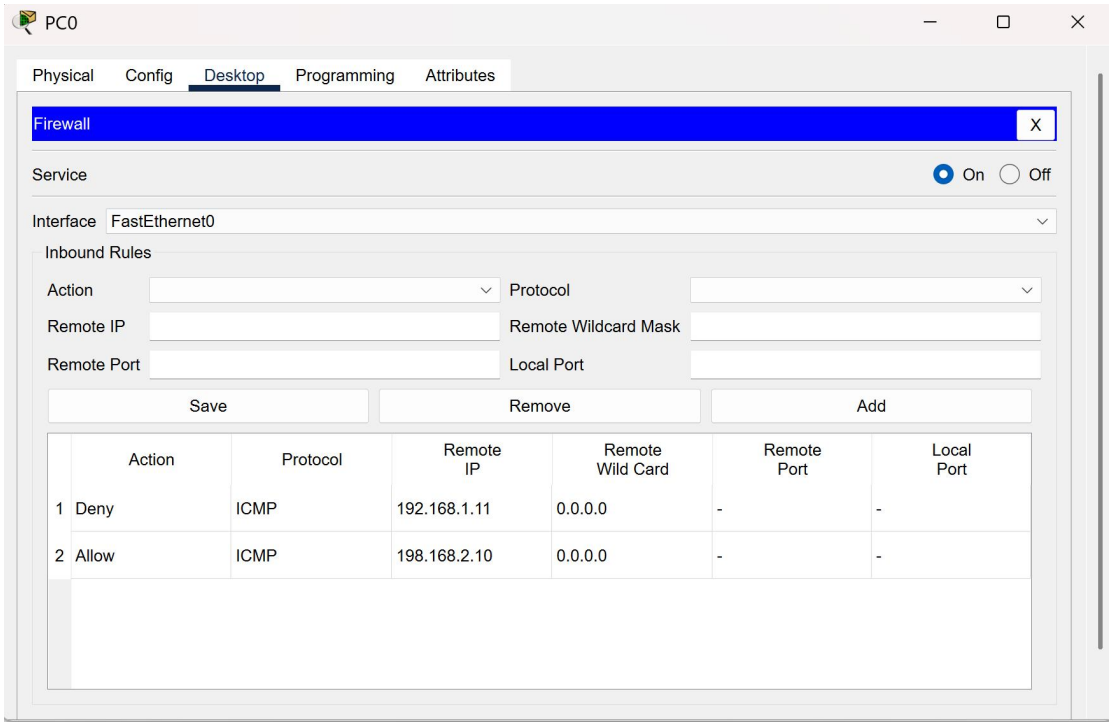
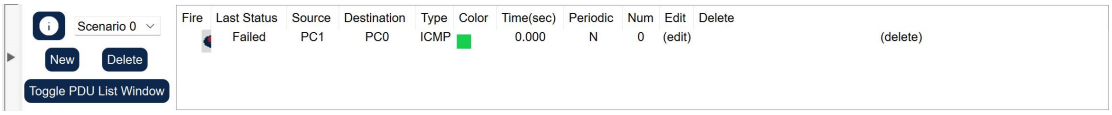


Figure 2: Firewall at PC0

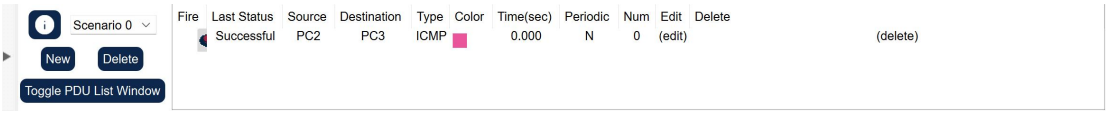
7. Testing and Results

Ping tests were conducted between all PCs:

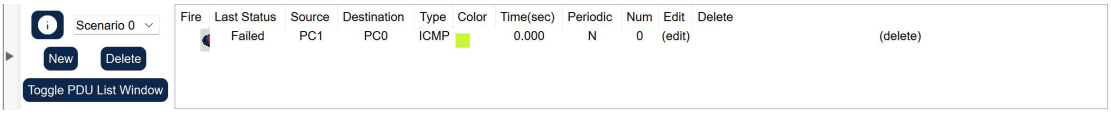
PC0 ↔ PC1: Successful



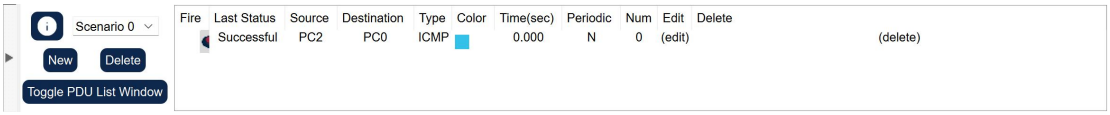
PC2 ↔ PC3: Successful



PC1 → PC0: Blocked (as expected due to firewall rule)



PC0 → PC2: Allowed



8. Conclusion

The network was successfully designed and simulated in Cisco Packet Tracer. Connectivity between PCs through switches and routers was achieved, and basic firewall rules were effectively implemented using ACLs. This simulation enhanced understanding of network design, router configuration, and basic network security.