Register No:	99220040772
Name:	V Vishwaradhya
Class/Section:	9312/S24
Ex.No:	**15**
Date of Submission	dd.mm.yyyy
Name of the Experiment	**Firewall Configuration**
Google Drive link of the packet tracer file (give view permission):	https://drive.google.com/drive/folders/1bMlU-KbUtB3OwtHSbBf6EbDQIdGUGgGr?usp=sharing

Objective(s):

To design and implement Firewall server configuration using packet tracer

Introduction:

A firewall is a security system designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. Its primary function is to create a barrier between a trusted internal network and untrusted external networks, such as the internet, to protect against unauthorized access, cyberattacks, and data breaches.

The main requirements of configuring the firewall on a web server in computer networking and how to allow access to a certain site and deny the ping of that site. This assignment requires using special software called Cisco Packet Tracer where students can download for free from the Cisco Academy site (Netacad.com) and install it on their computers. Students should use the newest version of the software to do this assignment. This process should be done in the following steps:

1. Assign IP address to the Server.

2. Activate the DHCP service on the server.

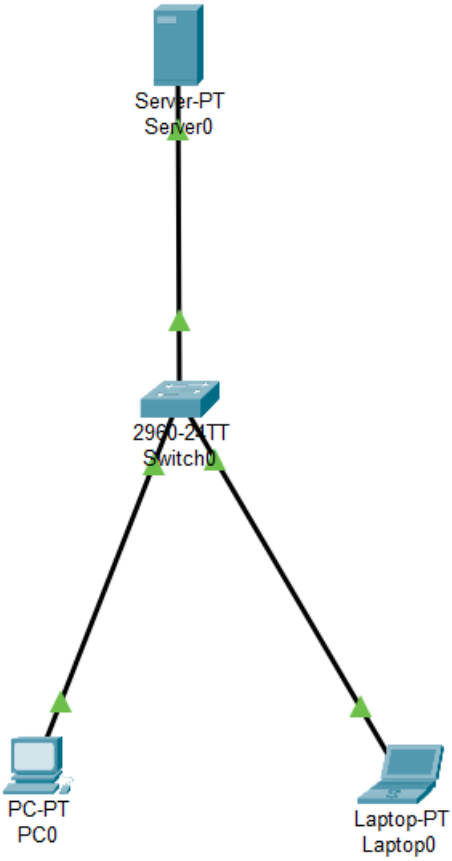
3. Activate the HTTP services on the server.

4. Configure the firewall within the server by Denying the ICMP and Allow the IP.

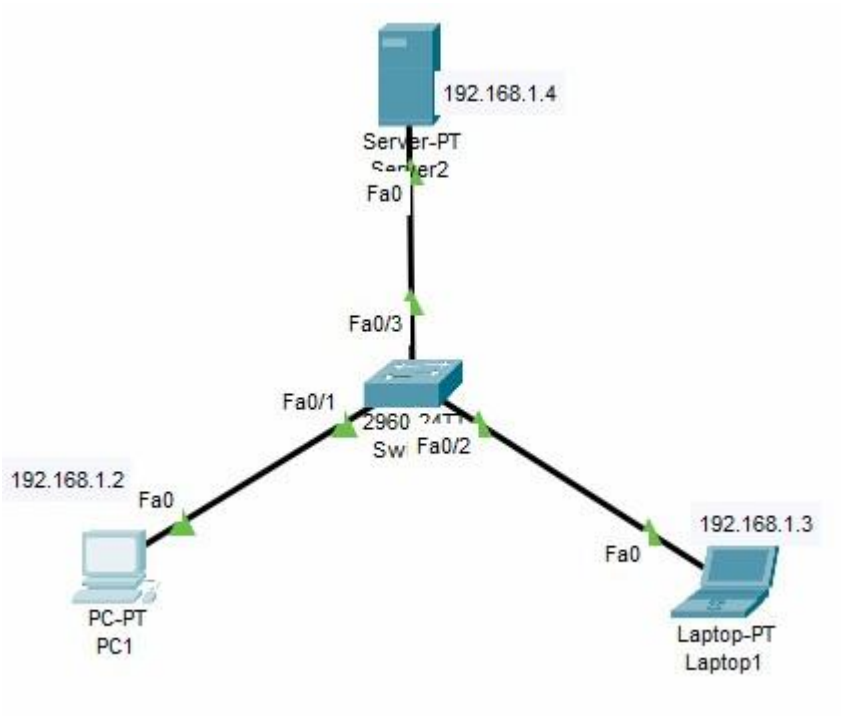
5. Reconfigure the server by allowing the ICMP and IP on the server.

6. Ping the server and access the URL for each computer. Students should successfully access URL but should receive a "Request time out" when pinging that site.

1. **Device Requirements:**
   1.PC
   2.SWITCH
   3.LAPTOP
   4.SERVER
2. **Network Diagram for your experiment (draw the diagram either hand drawing/ms paint or any other drawing tools)**



3. **Network Diagram (Packet tracer diagram before configuration):**



4. **Configuration details:**

Device Name	Interface Name	IP Address	Subnet mask	Default Gateway
PC0	FA0/1	192.168.1.2	255.255.255.0	192.168.1.1
LAPTOP	FA0/2	192.168.1.3	255.255.255.0	192.168.1.1
SWITCH	FA0/3			
SERVER		192.168.1.4	255.255.255.0	192.168.1.1

5. **Describe step by step configuration steps properly (you may copy the commands used in the configuration tab and paste it.)**

$cofigure ip of server and pc

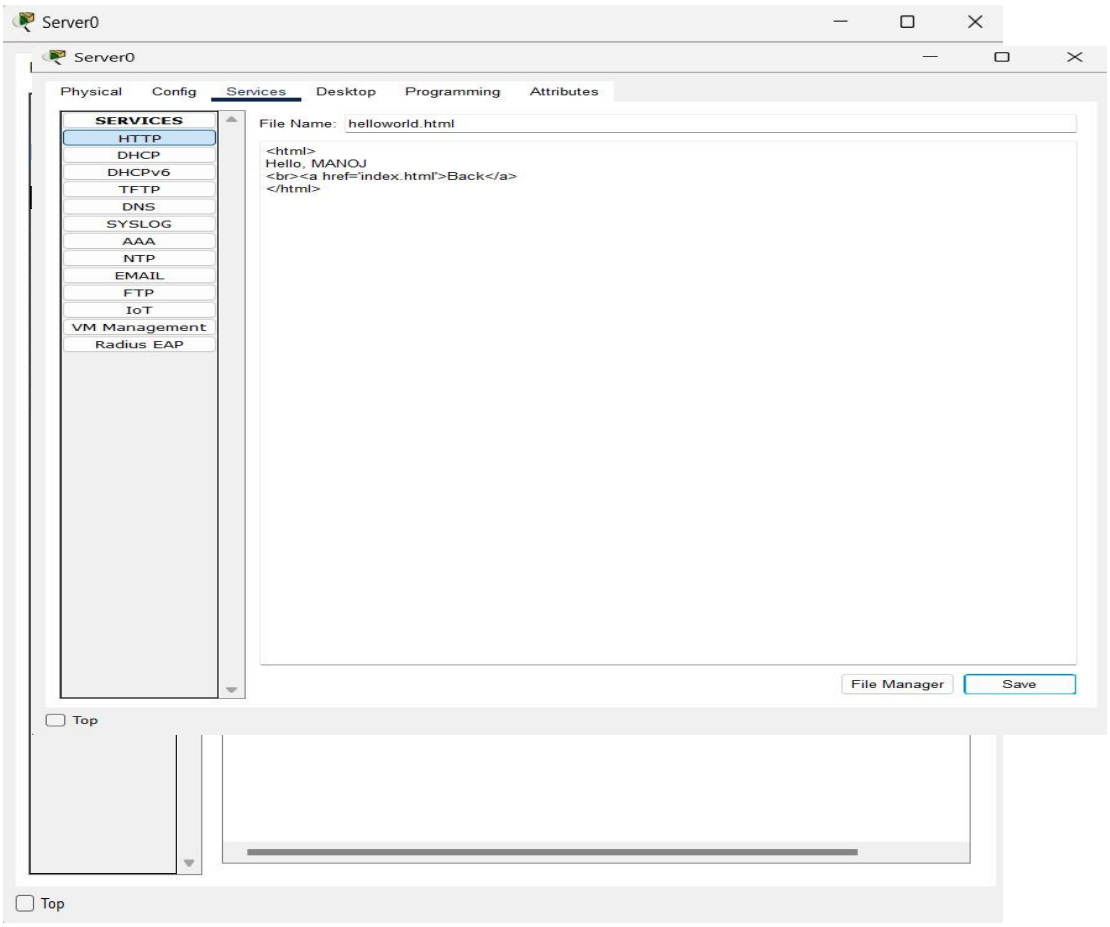
$turn on services of http and dhcp in services tab

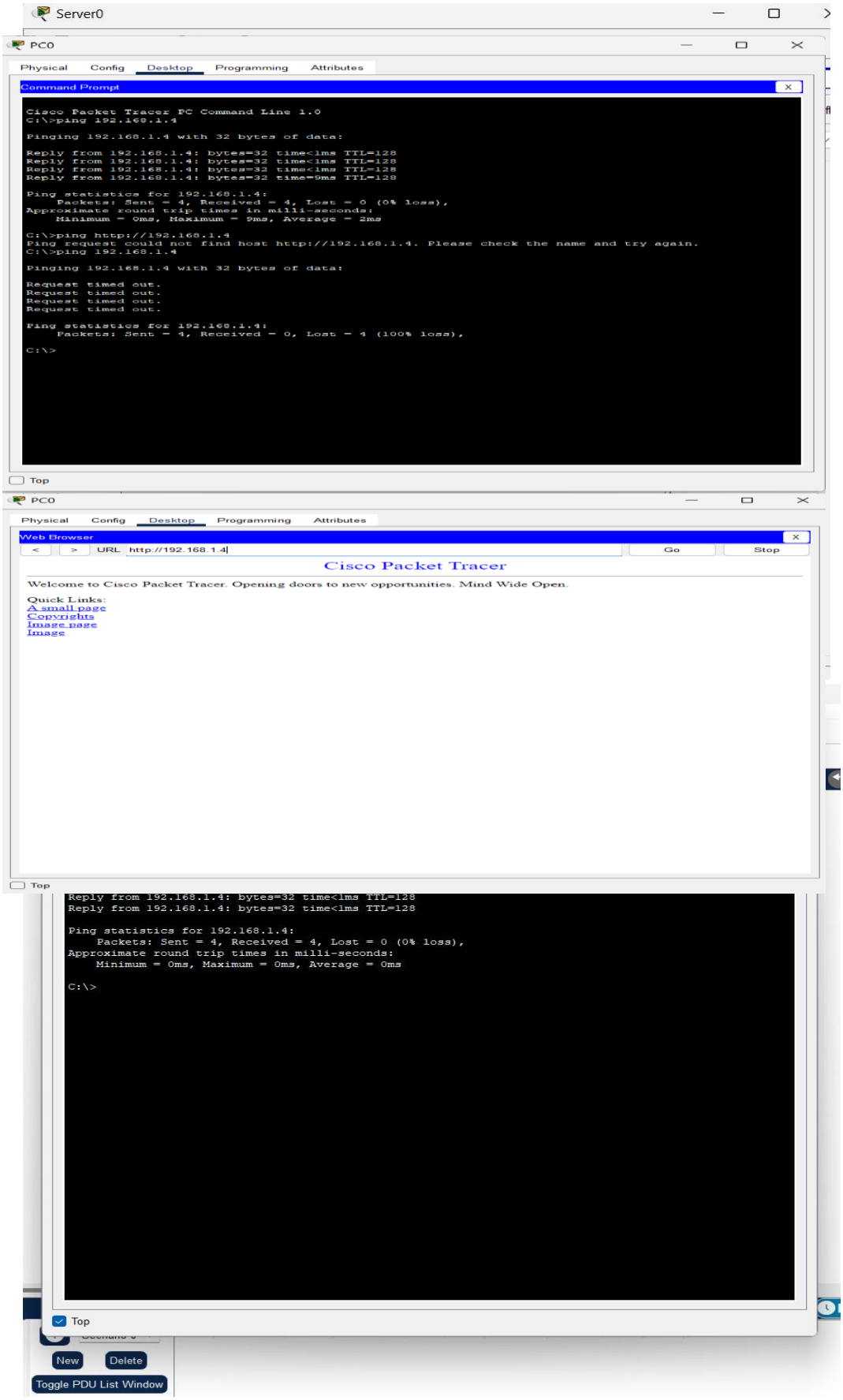
$configure the ip http for web browser

$Goto IP firewall in desktop tab allow ip and deny icmp

$now ping with pc and open the webpage of the ip ,pinging should be denyed and webpage should be open

6. **Output Diagram (Minimum 3 screenshot):**




Server0
PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.4
Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=9ms TTL=128
Ping statistics for 192.168.1.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 9ms, Average = 2ms
C:\>ping http://192.168.1.4
Ping request could not find host http://192.168.1.4. Please check the name and try again.
C:\>ping 192.168.1.4
Pinging 192.168.1.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.4:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top
PC0
Physical
Config
Desktop
Programming
Attributes
Web Browser
URL
http://192.168.1.4
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image
Top
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top
New
Delete
Toggle PDU List Window

W

Rubrics for Experiment Assessment:

Rubrics	Good	Normal	Poor	Marks
Creation of Topology (4)	Created the topology, Identify the proper devices and making the connections **(4)**	Created the topology, Identify the proper devices, making the connections But missing some features **(3)**	Created wrong topology, Failed to Identify the proper devices and making connections **(1)**	
Verify the connectivity (4)	Verified the connectivity in all the levels **(4)**	Verified the connectivity at some levels (only some nodes) **(2)**	Verified the connectivity is not done. **(1)**	
Timely Completion (2)	Completed the lab before the allotted time **(2)**	Completed the lab after the deadline **(1)**	Did not submitted before grading **(0)**	
			Total	

CONCLUSION (provide conclusion about this experiment):

In this experiment, we configured a network with a Server at 192.168.1.4 to host HTTP services, accessible from a PC (192.168.1.2) and Laptop (192.168.1.3) within a simple LAN. By assigning static IPs and enabling HTTP, we ensured successful web page access, but the Server's lack of a native firewall prevented blocking ICMP, resulting in successful pings instead of the desired "Request timed out." Implementing a Router with ACLs to deny ICMP while allowing HTTP successfully met all objectives, demonstrating the importance of proper traffic filtering for network control.