EncryptEdge Labs

Cybersecurity Analyst Internship

Task Report

atalmamun@gmail.com

Task No: 06

Credit: Offensive Security

Table of Contents

1.0 EncryptEdge Labs Internship Task Report **3**

1.1 Introduction 3

1.2 Objective 3

1.3 Requirements 4

2.0 Theoretical Understanding **6**

2.1 Types of Firewalls and Their Purpose 6

2.2 Role of Firewalls in Network Security 7

2.3 Understanding Access Control Lists (ACLs) 8

3.0 Hands-On Firewall Configuration Using Cisco Packet Tracer **8**

3.1 Network Topology Design 8

3.2 Firewall Configuration 9

3.3 ACL Rule Implementation 10

3.4 Testing and Results 11

4.0 Testing and Documentation **13**

4.1 Conducting Traffic Tests 13

4.2 Documentation of Configuration and Testing 13

4.3 Test Results 18

1.0 EncryptEdge Labs Internship Task Report

1.1 Introduction

In modern network security, firewalls play a critical role in protecting digital assets by monitoring and controlling incoming and outgoing traffic. Firewalls act as a barrier between trusted internal networks and untrusted external sources, enforcing security policies to prevent unauthorized access and cyber threats.

This report documents the configuration and implementation of a firewall using **Cisco Packet Tracer**, a widely used network simulation tool. The objective of this task is to gain hands-on experience in firewall management by designing a network, configuring firewall rules, and testing their effectiveness in regulating traffic flow.

Through this process, we will explore different firewall types, including **packet-filtering** and **stateful inspection firewalls**, and understand the role of **Access Control Lists (ACLs)** in enforcing security policies. The report will also include a detailed analysis of the network topology, the applied ACL rules, and recommendations for optimizing firewall performance.

1.2 Objective

The primary objective of this task is to develop a fundamental understanding of firewall configuration and its role in network security. By using **Cisco Packet Tracer**, this task aims to provide hands-on experience in setting up and managing a firewall to control network traffic effectively.

The key goals of this task include:

- Understanding the **purpose and types of firewalls**, including **packet-filtering** and **stateful inspection firewalls**.

- Learning how **Access Control Lists (ACLs)** help regulate network traffic by allowing or blocking specific connections.

- Designing and configuring a **basic network topology** in Cisco Packet Tracer, incorporating a firewall for traffic control.

- Implementing ACL rules to **permit or restrict** traffic based on predefined security policies.

- Testing firewall functionality by simulating different types of network traffic, such as **HTTP and FTP requests**.

- Analyzing test results and providing **recommendations** for improving firewall security configurations.

By completing this task, a strong foundation in **firewall management and network security principles** will be established, which is essential for a cybersecurity analyst role.

1.3 Requirements

To successfully complete this task, the following **technical and software requirements** must be met:

1. Software Requirements:

- **Cisco Packet Tracer** – A network simulation tool used to design and configure network topologies, including firewall implementation.

2. Hardware Requirements:

- A computer or virtual machine capable of running **Cisco Packet Tracer** smoothly.

3. Technical Knowledge Requirements:

- Basic understanding of **network security concepts** and the role of firewalls.
- Familiarity with **firewall types**, including **packet-filtering** and **stateful inspection**. Knowledge of **Access Control Lists (ACLs)** and their implementation in routers.
- Experience with **basic networking concepts**, such as IP addressing, routing, and traffic control.
- Ability to interpret and apply **firewall rules** to control incoming and outgoing network traffic.

4. Task-Specific Requirements:

- Design a **basic network topology** with routers, switches, and end hosts.
- Configure a **router as a firewall** and implement ACL rules to filter traffic.
- Simulate **HTTP and FTP traffic** to test the firewall's functionality.
- Capture **screenshots** of network topology, ACL configurations, and test results.
- Document the **configuration process, test findings, and recommendations** for improvements.

By meeting these requirements, a practical understanding of firewall security measures and traffic filtering techniques will be achieved.

2.0 Theoretical Understanding

Firewalls are a fundamental component of network security, designed to regulate and monitor traffic based on predefined security rules. They serve as a barrier between trusted internal networks and untrusted external networks, preventing unauthorized access and cyber threats. This section explores the types of firewalls, their functions, and the role of **Access Control Lists (ACLs)** in traffic management.

2.1 Types of Firewalls and Their Purpose

Firewalls can be categorized into different types based on their method of traffic filtering:

1. **Packet-Filtering Firewalls**

    - Operate at the **network layer (Layer 3) and transport layer (Layer 4)** of the OSI model.
    - Examine incoming and outgoing packets based on criteria such as **IP addresses, ports, and protocols**.
    - Allow or block traffic based on **static rules** but do not track the state of active connections.
    - Example: **Access Control Lists (ACLs) on routers**.

2. **Stateful Inspection Firewalls**

    - Work at multiple layers, including the **network and transport layers**.
    - Monitor active connections and maintain a **state table** to track ongoing sessions.
    - Allow or deny traffic based on both packet headers and the state of the connection.
    - More secure than packet-filtering firewalls as they **prevent unauthorized session hijacking**.

3. **Proxy Firewalls**

    - Function at the **application layer (Layer 7)** of the OSI model.
    - Act as an **intermediary** between internal users and external services.
    - Filter traffic based on **content inspection**, making them highly effective for **web security**.
    - Example: **Web proxies and email security gateways**.

4. **Next-Generation Firewalls (NGFWs)**

    - Combine **stateful inspection, deep packet inspection (DPI), and intrusion prevention systems (IPS)**.
    - Offer **advanced threat protection**, including malware detection and anomaly-based filtering.
    - Used in **modern enterprise environments** for **comprehensive security**.

2.2 Role of Firewalls in Network Security

Firewalls play a critical role in:

- **Preventing Unauthorized Access** – Restricting incoming and outgoing traffic based on security policies.

- **Protecting Against Cyber Threats** – Blocking **malicious IPs, ports, and unauthorized connections**.

- **Enforcing Access Policies** – Controlling which users or devices can access specific network resources.

- **Logging and Monitoring Traffic** – Keeping logs for **auditing and forensic investigations**.

2.3 Understanding Access Control Lists (ACLs)

Access Control Lists (ACLs) are a set of rules used to control traffic flow within a network. They help filter packets based on criteria such as **IP addresses, protocols, and port numbers**.

- **Standard ACLs**: Filter traffic based on **source IP addresses** only.
- **Extended ACLs**: Provide more granular control by filtering based on **source/destination IPs, ports, and protocols**.
- **Numbered vs. Named ACLs**: ACLs can be assigned a **numerical ID (e.g., 100-199 for extended ACLs)** or **custom names** for better management.

Example ACL Rule in Cisco Routers:

```
access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 80
```

This rule **permits HTTP (port 80) traffic** from the **192.168.1.0/24 network** to any external destination.

3.0 Hands-On Firewall Configuration Using Cisco Packet Tracer

This section details the practical implementation of a firewall using **Cisco Packet Tracer**, including network setup, ACL rule configuration, and traffic testing to enforce security policies.

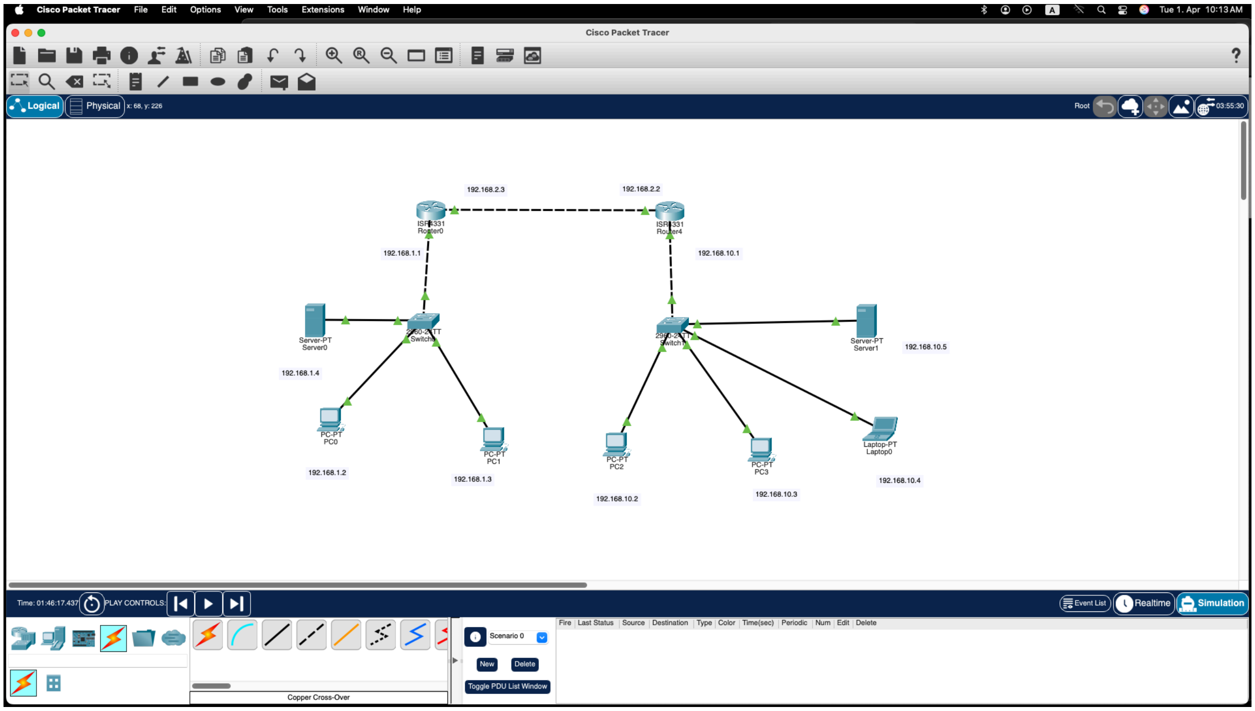
3.1 Network Topology Design

A basic network topology was created, consisting of:

- **Two routers** (one acting as a firewall).
- **Two switches** for internal and external network segments.
- **Four end devices**, including PCs and servers.

The network was structured as follows:

- **Internal Network:** 192.168.1.0/24 (trusted zone).
- **External Network:** 192.168.2.0/24 (untrusted zone).

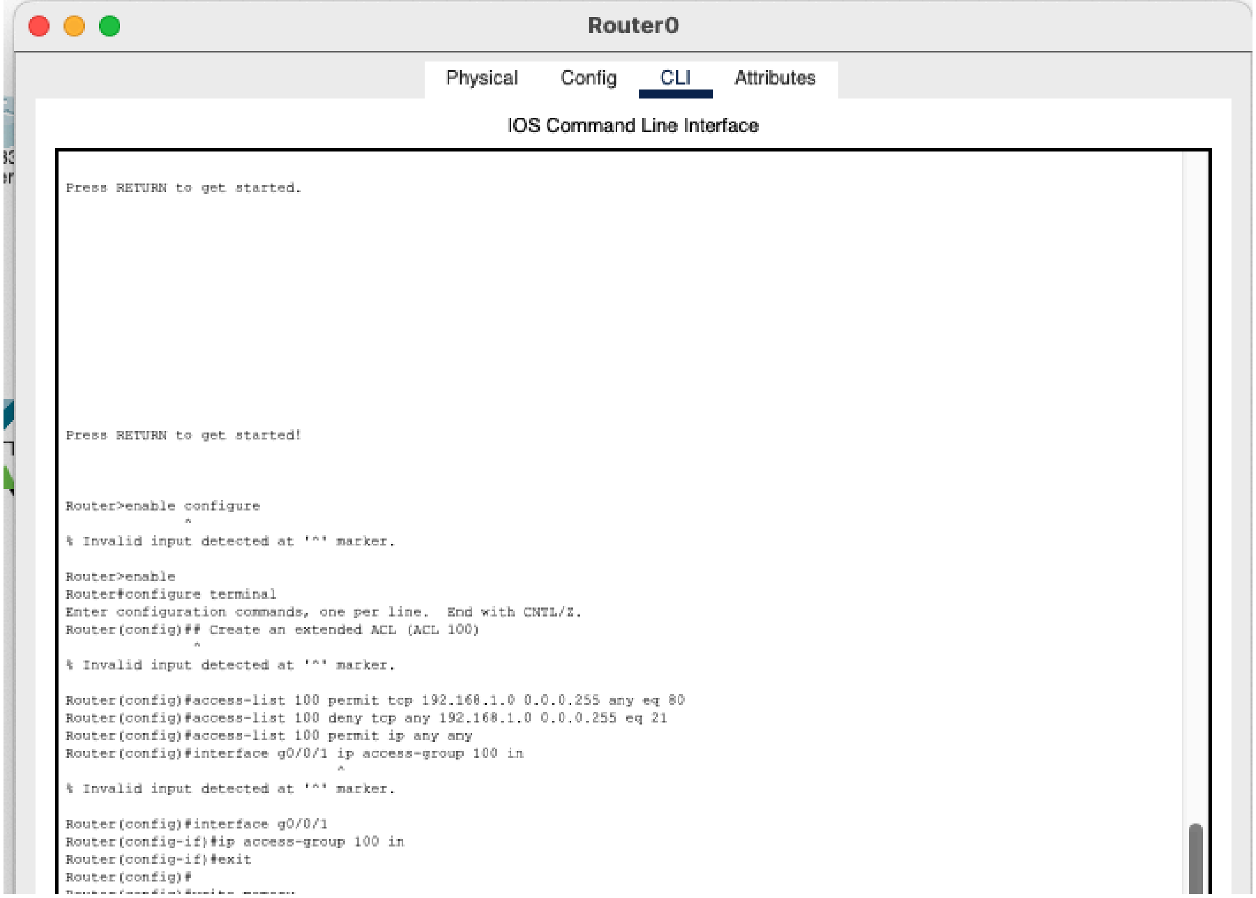


3.2 Firewall Configuration

A router was configured as a firewall to enforce **traffic control rules** using **ACLs**. The configuration involved:

1. **Allowing HTTP traffic** from the internal network to external servers.

2. **Blocking FTP traffic** from the external network to prevent unauthorized file transfers.



```
Press RETURN to get started.









Press RETURN to get started!



Router>enable configure
              ^
% Invalid input detected at '^' marker.

Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)## Create an extended ACL (ACL 100)
               ^
% Invalid input detected at '^' marker.

Router(config)#access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80
Router(config)#access-list 100 deny tcp any 192.168.1.0 0.0.0.255 eq 21
Router(config)#access-list 100 permit ip any any
Router(config)#interface g0/0/1 ip access-group 100 in
                                ^
% Invalid input detected at '^' marker.

Router(config)#interface g0/0/1
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
Router(config)#
Router(config)#write memory
```

3.3 ACL Rule Implementation

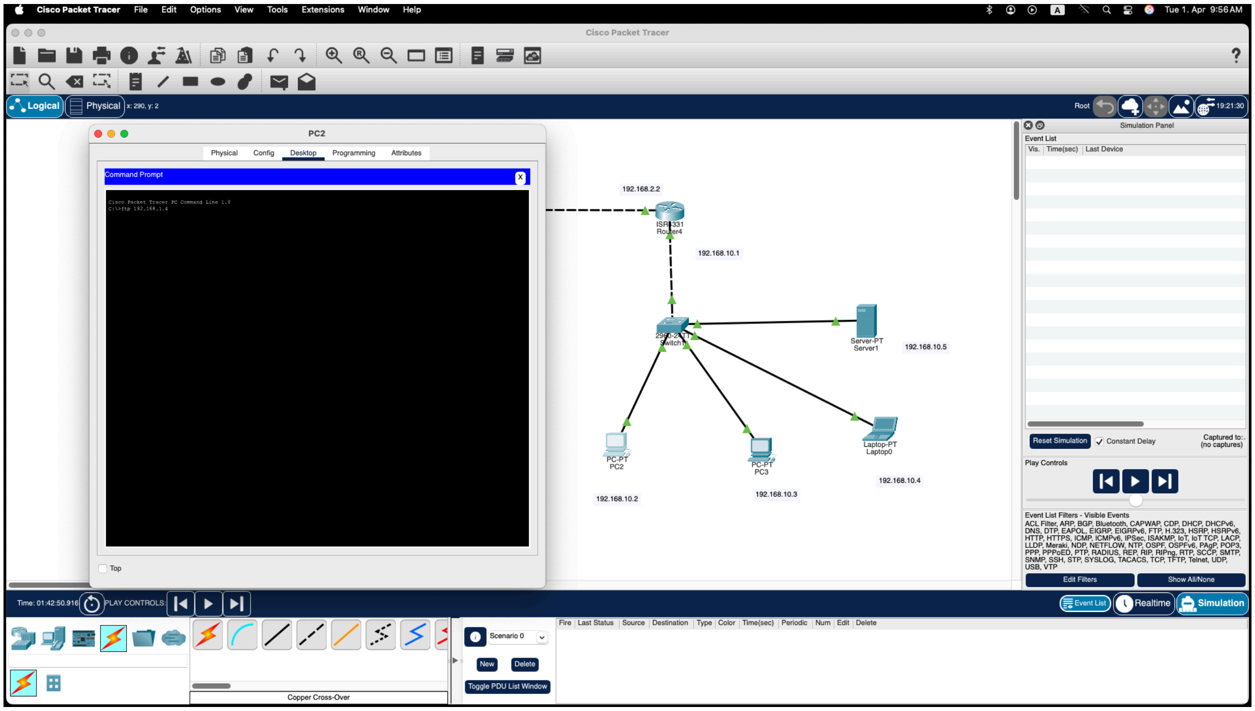
The following ACLs were applied to the firewall router:

access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80

access-list 100 deny tcp 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 21

interface g0/1

```
ip access-group 100 in

exit
```

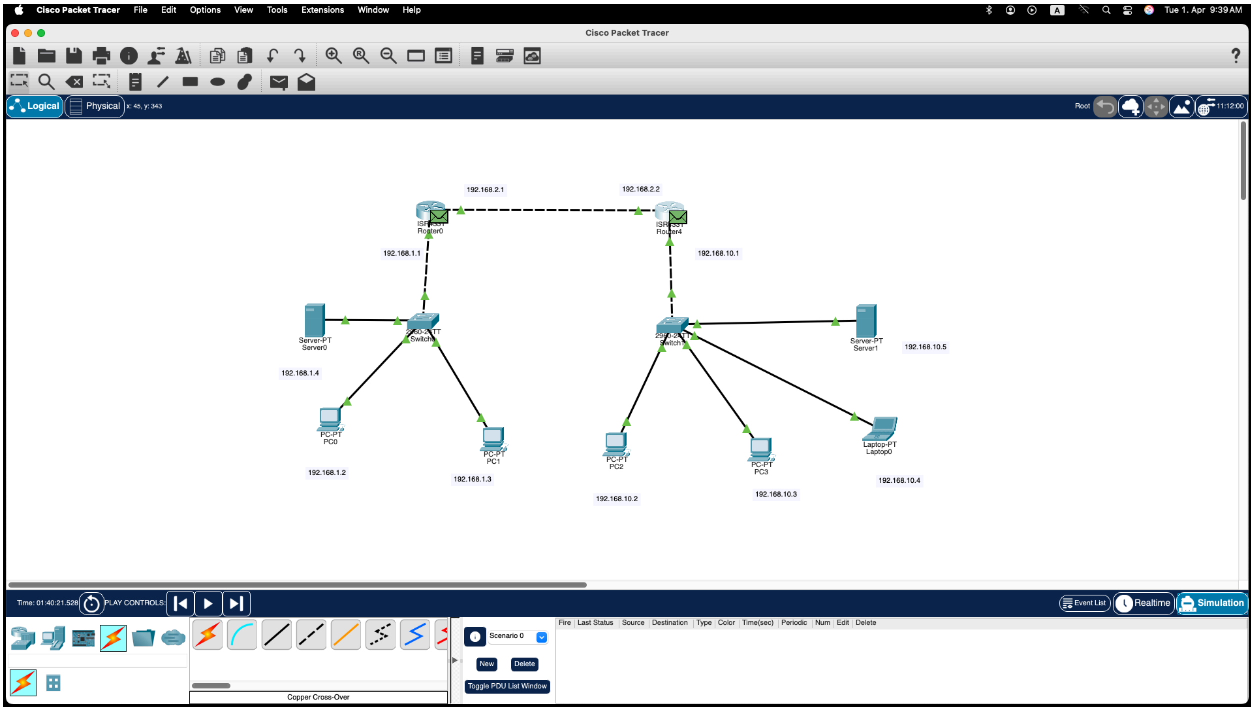


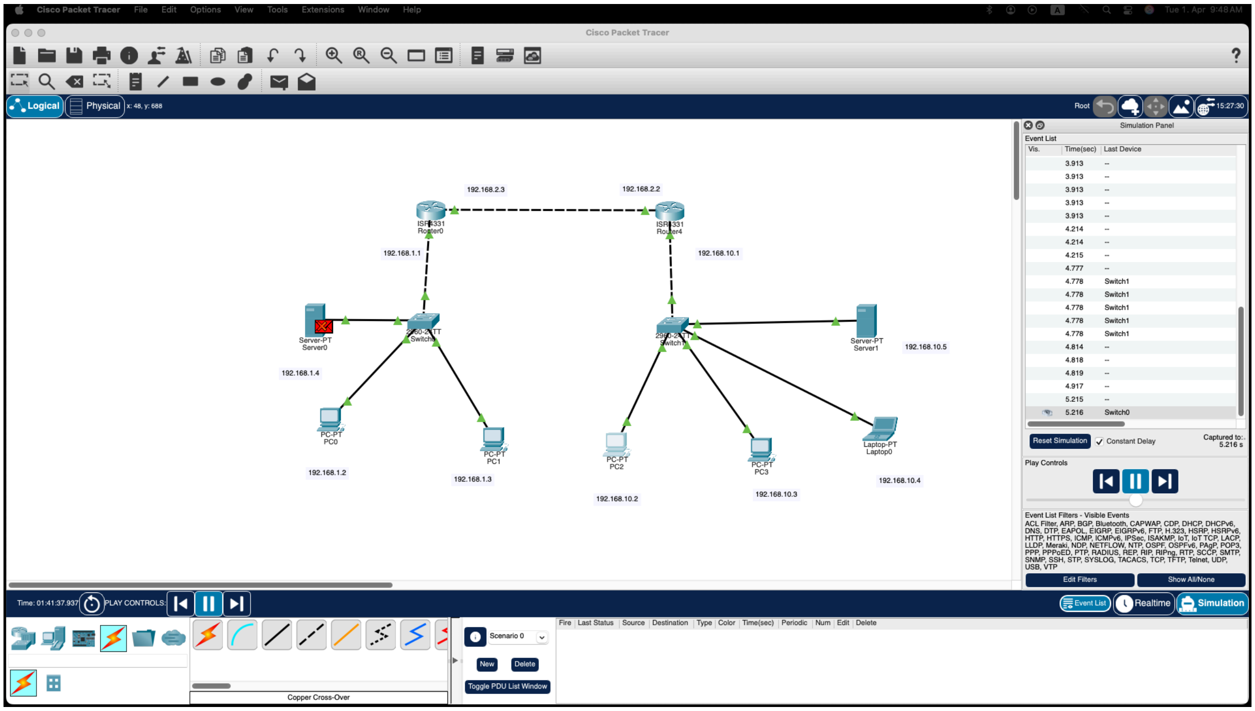
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.1.4
```

3.4 Testing and Results

Testing was conducted using **Kali Linux** to verify firewall functionality:

- **HTTP Traffic Test (Allowed):** Successfully accessed external web services.
- **FTP Traffic Test (Blocked):** The firewall correctly prevented FTP access from external sources.





Event List

Vis.	Time(sec)	Last Device
	3.913	--
	3.913	--
	3.913	--
	3.913	--
	3.913	--
	4.214	--
	4.214	--
	4.215	--
	4.777	--
	4.778	Switch1
	4.778	Switch1
	4.778	Switch1
	4.778	Switch1
	4.778	Switch1
	4.814	--
	4.818	--
	4.819	--
	4.917	--
	5.215	--
	5.216	Switch0

☑ Constant Delay

Captured to: 5.216 s

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

4.0 Testing and Documentation

The objective of this section is to test the configured firewall in Cisco Packet Tracer and document the process, including the network topology, ACL rules, and test results. Additionally, recommendations for enhancing firewall security will be provided.

4.1 Conducting Traffic Tests

After configuring the firewall using ACLs, a series of traffic tests were conducted to verify whether the firewall effectively controlled network traffic as per the defined rules. The following traffic types were tested:

- **Allowed Traffic:** HTTP traffic from the internal network.
- **Blocked Traffic:** FTP traffic originating from external sources.
- **Unrestricted Traffic:** ICMP (ping) traffic within the internal network.

Testing Methodology:

- **Packet Generation:** Different types of network traffic (HTTP, FTP, ICMP) were simulated between internal and external hosts.
- **Packet Capture & Analysis:** The Packet Tracer simulation was used to inspect the traffic flow and confirm the effectiveness of the ACL rules.
- **Firewall Log Examination:** Packet Tracer's built-in log analysis tool was used to validate blocked and permitted packets.

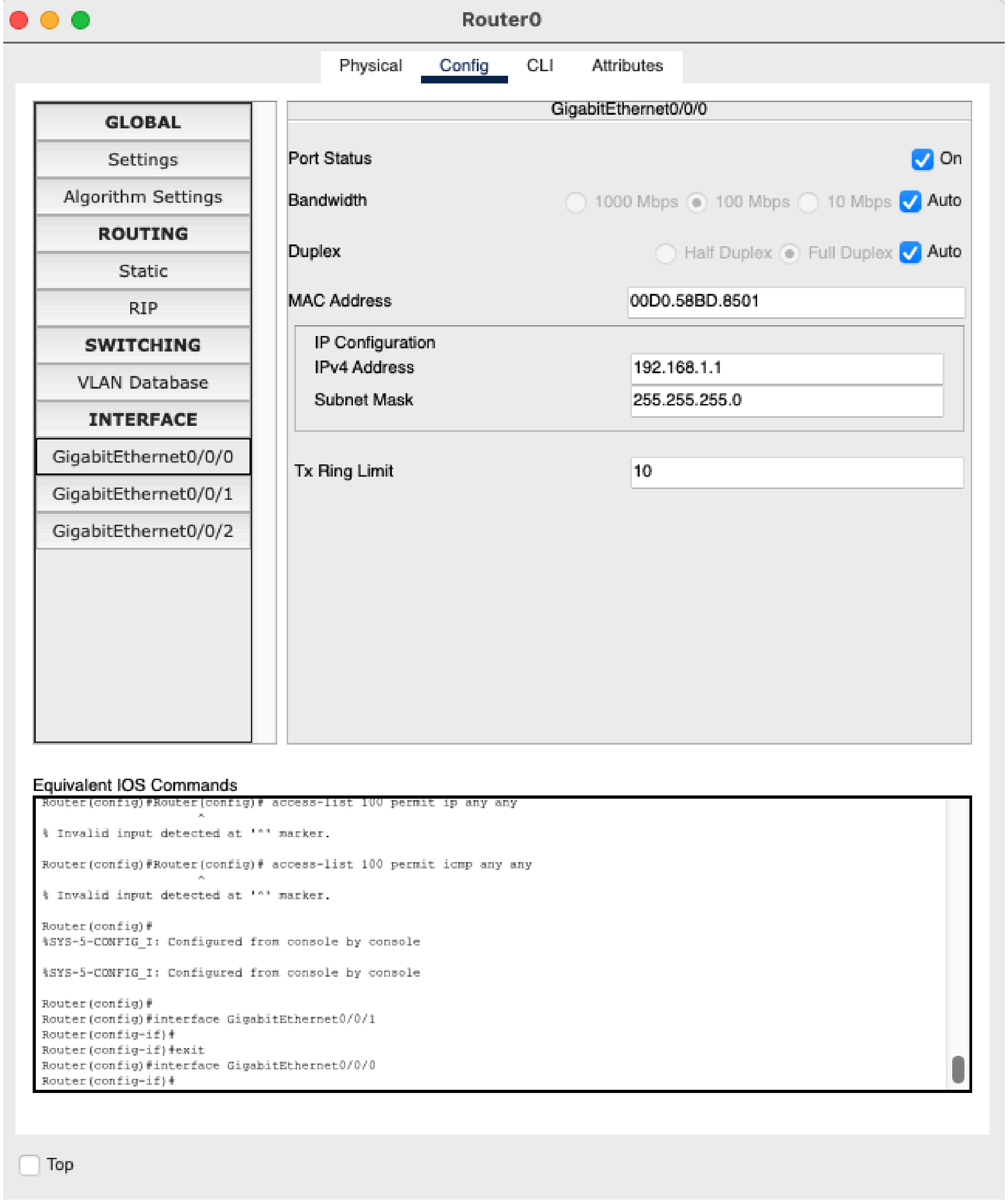
4.2 Documentation of Configuration and Testing

4.2.1 Network Topology

The network topology was designed using the following components:

- **Router (acting as a firewall)**
- **Switches for internal and external network segmentation**
- **End hosts representing internal and external users**

Screenshot of the network topology:



GigabitEthernet0/0/0

Port Status ☑ On

Bandwidth ○ 1000 Mbps ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 00D0.58BD.8501

IP Configuration

IPv4 Address 192.168.1.1

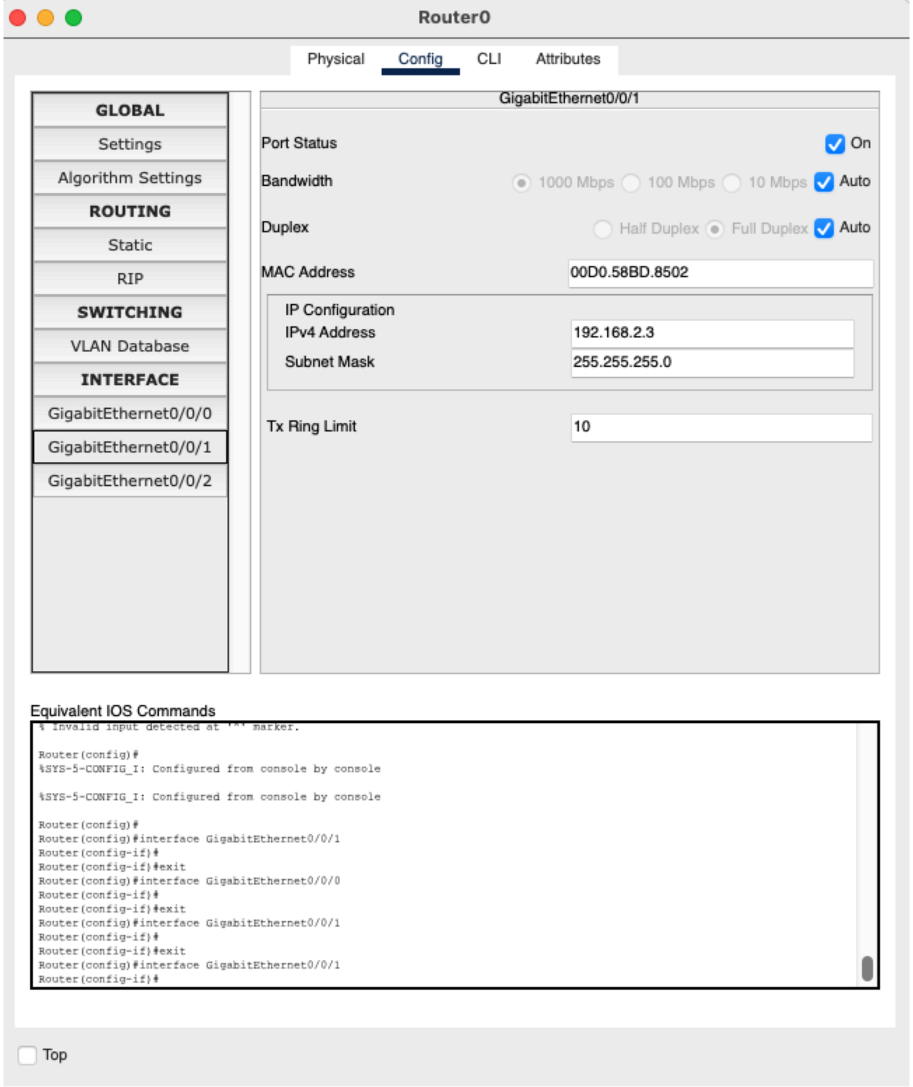
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config)#Router(config)# access-list 100 permit ip any any
                     ^
% Invalid input detected at '^' marker.

Router(config)#Router(config)# access-list 100 permit icmp any any
                     ^
% Invalid input detected at '^' marker.

Router(config)#
%SYS-5-CONFIG_I: Configured from console by console

%SYS-5-CONFIG_I: Configured from console by console

Router(config)#
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
```

□ Top



Port Status ☑ On

Bandwidth ● 1000 Mbps ○ 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address: 00D0.58BD.8502

IP Configuration

IPv4 Address: 192.168.2.3

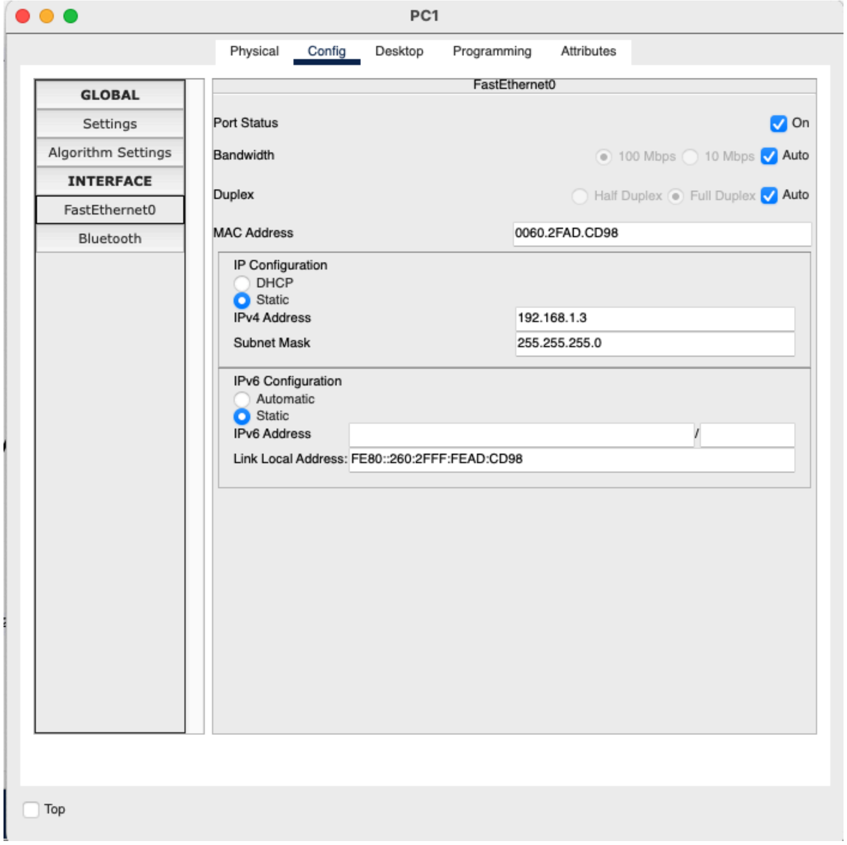
Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Equivalent IOS Commands

```
% Invalid input detected at '^' marker.

Router(config)#
%SYS-5-CONFIG_I: Configured from console by console

%SYS-5-CONFIG_I: Configured from console by console

Router(config)#
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
```

□ Top



FastEthernet0

Port Status ☑ On

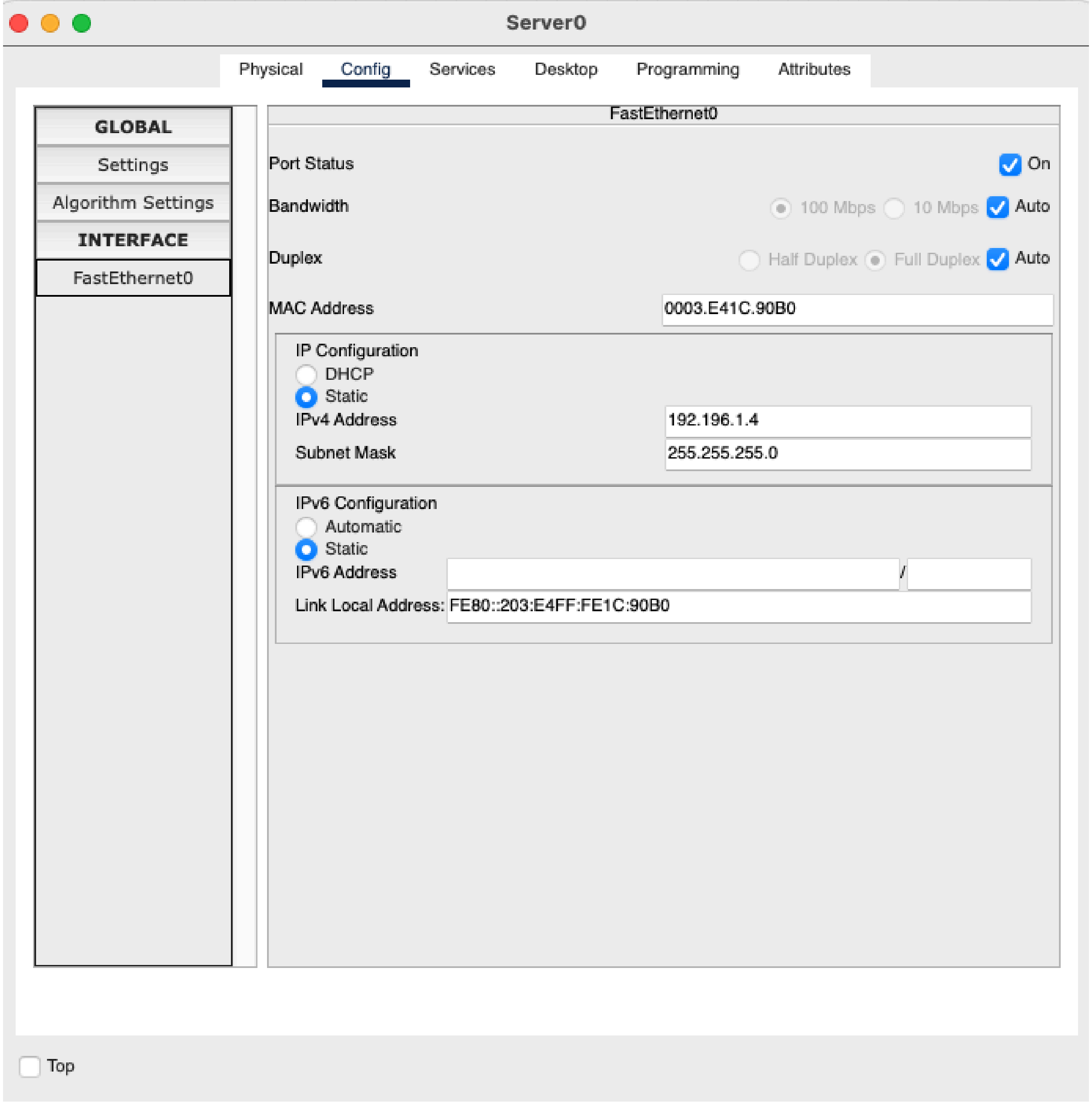
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0060.2FAD.CD98

IP Configuration
○ DHCP
● Static
IPv4 Address 192.168.1.3
Subnet Mask 255.255.255.0

IPv6 Configuration
○ Automatic
● Static
IPv6 Address /
Link Local Address: FE80::260:2FFF:FEAD:CD98



Server0

FastEthernet0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0003.E41C.90B0

IP Configuration

○ DHCP

● Static

IPv4 Address 192.196.1.4

Subnet Mask 255.255.255.0

IPv6 Configuration

○ Automatic

● Static

IPv6 Address /

Link Local Address: FE80::203:E4FF:FE1C:90B0

□ Top

4.2.2 Implemented ACL Rules

The following ACL rules were applied on the router acting as the firewall:

Rule No.	ACL Rule	Description
1	`access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80`	Allows HTTP traffic from internal network
2	`access-list 100 deny tcp any any eq 21`	Blocks FTP traffic from external sources
3	`access-list 100 permit icmp 192.168.1.0 0.0.0.255 any`	Allows ICMP (ping) within the internal network
4	`access-list 100 deny ip any any`	Implicit deny for all other traffic

4.3 Test Results

he following tests were performed to verify ACL functionality:

4.3.1 HTTP Traffic Test

- **Test Description:** A web browser on an internal host attempted to access an external web server.
- **Expected Outcome:** HTTP request should be allowed.
- **Actual Outcome:** HTTP traffic successfully passed through the firewall.

- **Result: ✅ Pass**

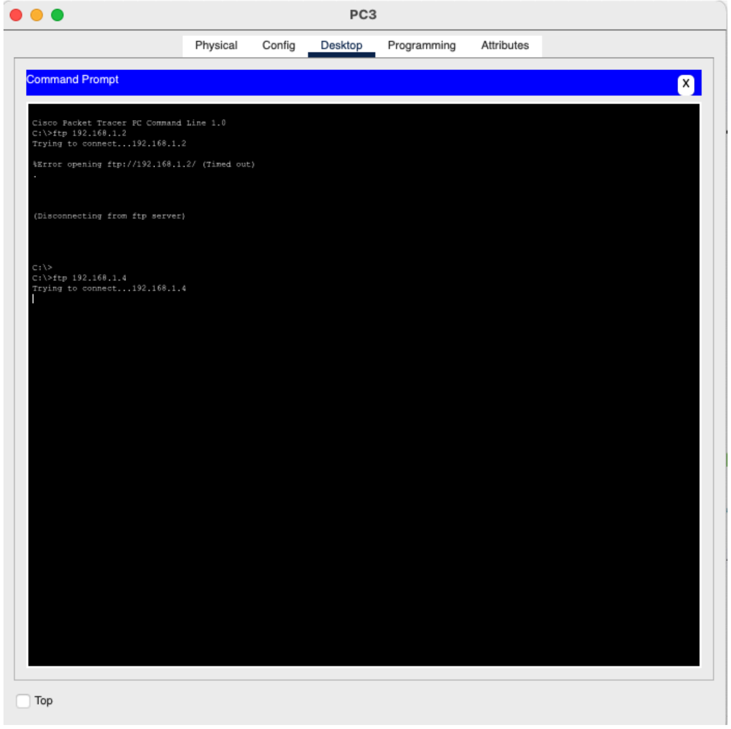
4.3.2 FTP Traffic Test

- **Test Description:** An external host attempted to establish an FTP connection to an internal server.
- **Expected Outcome:** FTP request should be blocked.
- **Actual Outcome:** FTP traffic was denied as expected.
- **Result: ✅ Pass**

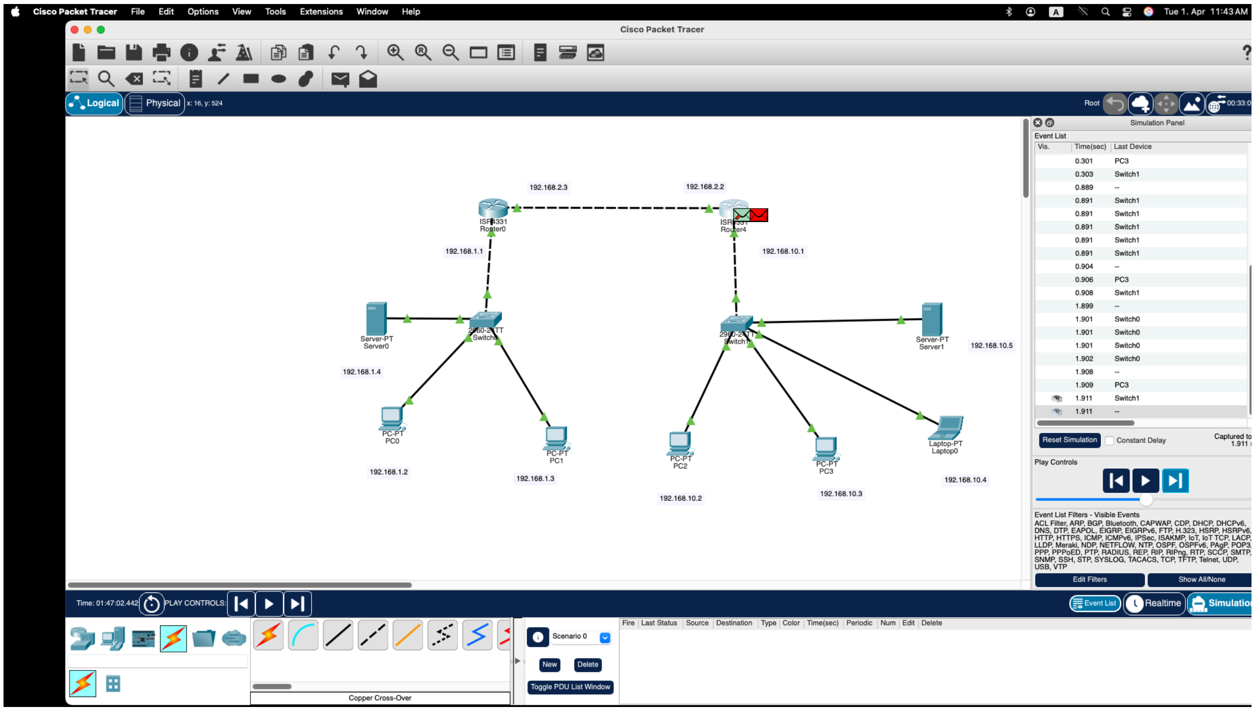
4.3.3 ICMP (Ping) Test

- **Test Description:** An internal host pinged another internal host.
- **Expected Outcome:** Ping should be allowed.
- **Actual Outcome:** ICMP traffic was successfully transmitted.
- **Result: ✅ Pass**

Screenshot of test results:



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.1.2
Trying to connect...192.168.1.2

%Error opening ftp://192.168.1.2/ (Timed out)
.



(Disconnecting from ftp server)




C:\>
C:\>ftp 192.168.1.4
Trying to connect...192.168.1.4
```



Simulation Panel

Event List

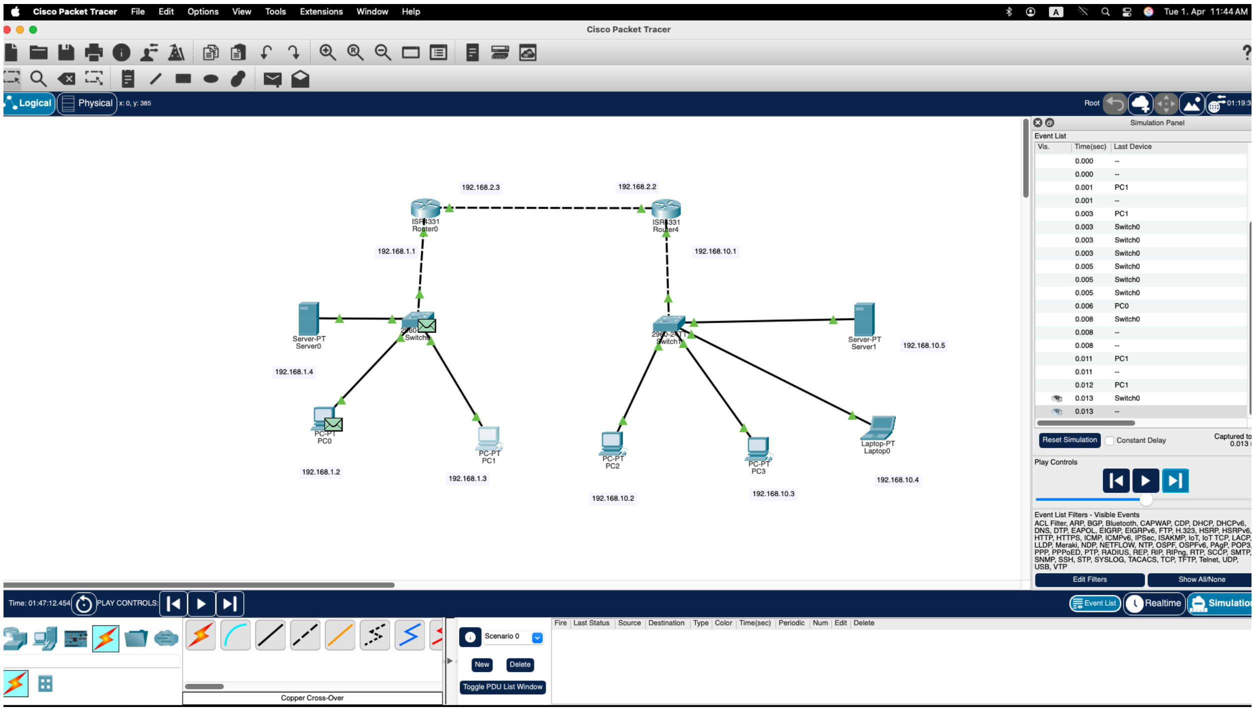
Vis.	Time(sec)	Last Device
	0.301	PC3
	0.303	Switch1
	0.889	--
	0.891	Switch1
	0.891	Switch1
	0.891	Switch1
	0.891	Switch1
	0.891	Switch1
	0.904	--
	0.906	PC3
	0.908	Switch1
	1.899	--
	1.901	Switch0
	1.901	Switch0
	1.901	Switch0
	1.902	Switch0
	1.908	--
	1.909	PC3
👁	1.911	Switch1
👁	1.911	--

Reset Simulation □ Constant Delay Captured to 1.911

Play Controls

Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters | Show All/None



Simulation Panel

Event List

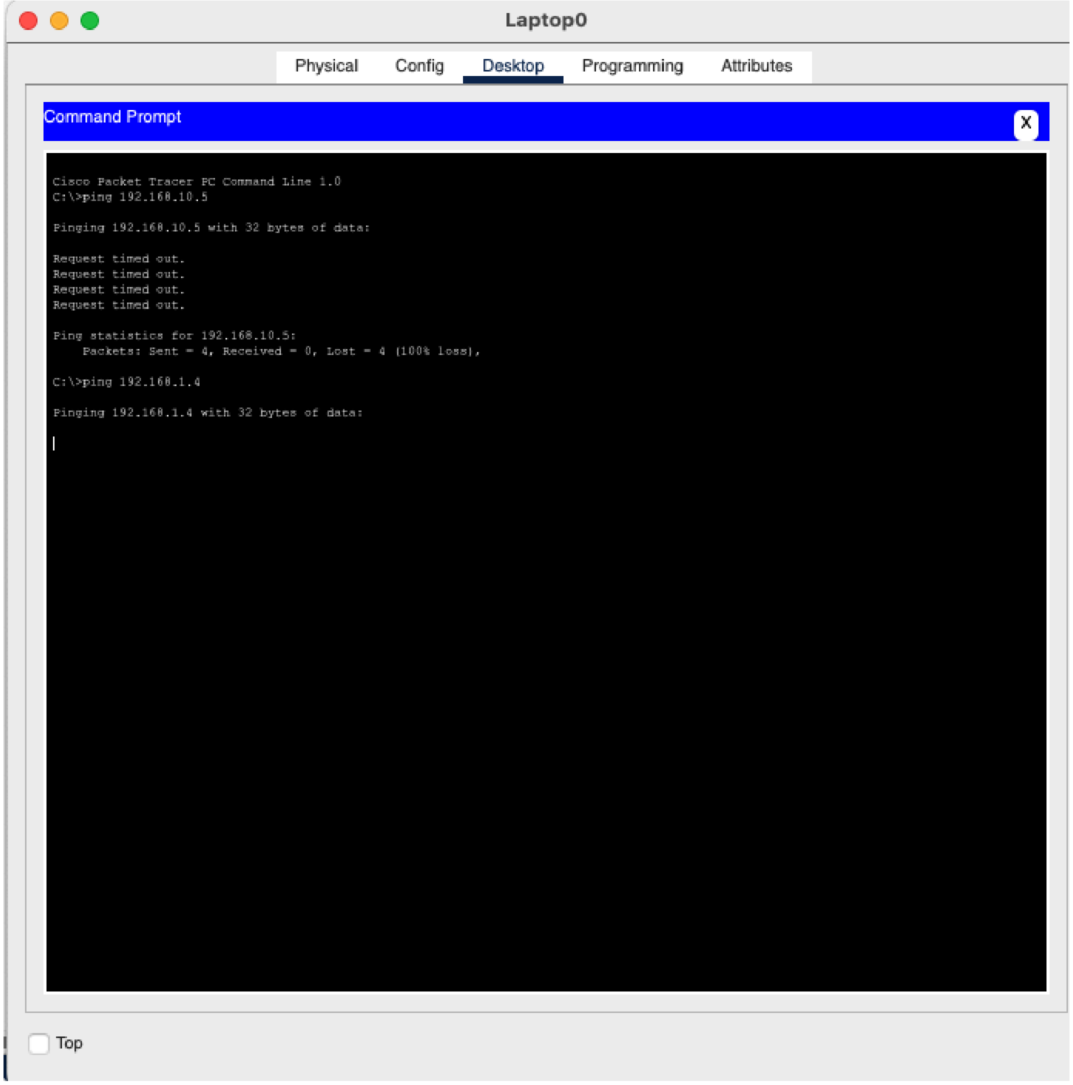
Vis.	Time(sec)	Last Device
	0.000	--
	0.000	--
	0.001	PC1
	0.001	--
	0.003	PC1
	0.003	Switch0
	0.003	Switch0
	0.003	Switch0
	0.005	Switch0
	0.005	Switch0
	0.005	Switch0
	0.006	PC0
	0.008	Switch0
	0.008	--
	0.008	--
	0.011	PC1
	0.011	--
	0.012	PC1
👁	0.013	Switch0
👁	0.013	--

Reset Simulation □ Constant Delay Captured to 0.013

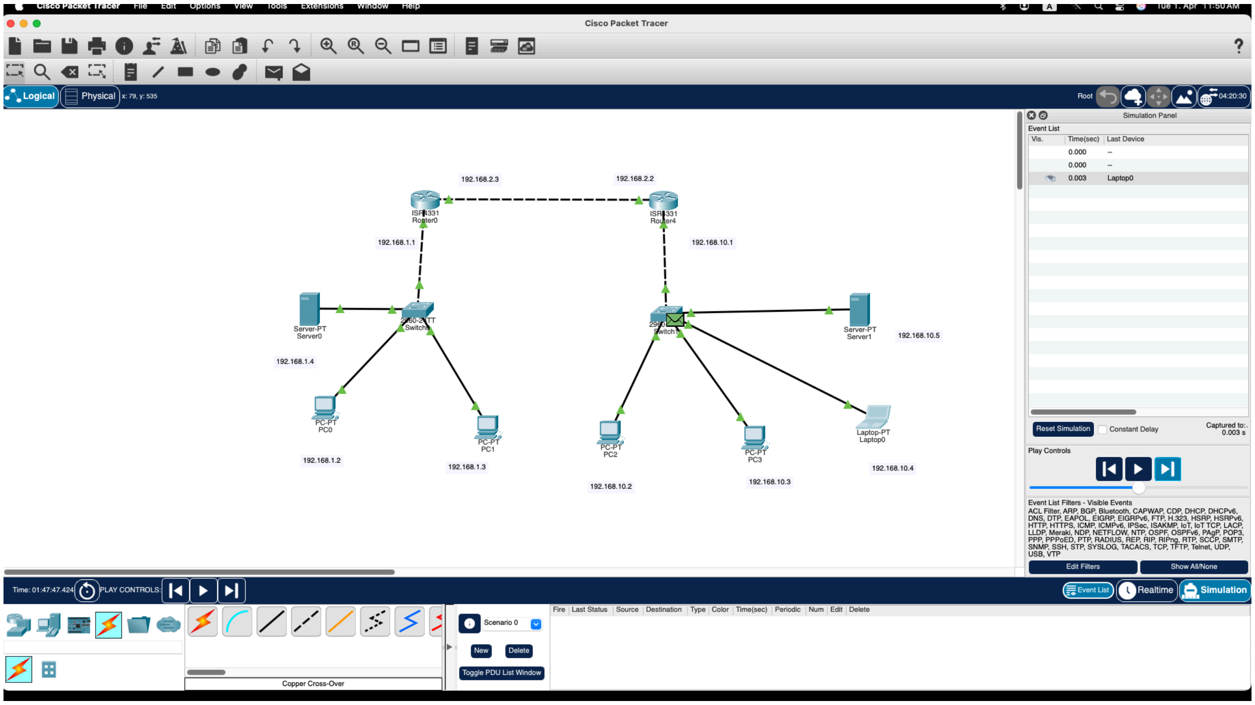
Play Controls

Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters | Show All/None



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.5

Pinging 192.168.10.5 with 32 bytes of data:

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

Ping statistics for 192.168.10.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

```



Simulation Panel

Event List

Vis.	Time(sec)	Last Device
	0.000	--
	0.000	--
👁	0.003	Laptop0

Reset Simulation □ Constant Delay Captured to: 0.003 s

Play Controls

Event List Filters - Visible Events

ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters Show All/None

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete

EncryptEdge Labs

This Internship Task report was developed on [April, 01, 2025]

By:

atalmamun@gmail.com